



Cyber Laws For CxO

Be Aware... Be Empowered

February 2010

Editor

Naavi

www.naavi.org

Publisher

Ujvala Consultants Pvt
Ltd

www.ujvala.com

Digital Signatures were defined in ITA 2000 as a system of authentication of electronic documents based on asymmetric cryptography and hashing.

The Act also placed an elaborate infrastructure for issue of digital certificates including creation of an authority called the Controller of Certifying Authorities in India and a system of licensing of Certifying Authorities.

However, adoption of Digital Signature in the Indian community is still at a very nascent stage and this issue examines the causes and remedies.

Theme

Digital Signatures

In This Issue

Editorial: GOI needs to invest more in Outreach programs

Knowledge+: Digital Signature as an IS Tool

News Snippets: Disclosure of Data Breach Incidents and others

Interviews: Dr N. Vijayaditya, CCA, Ravi Jagannathan, CEO, E Mudhra

Questions and Answers

Archived Issues will be available at
<http://www.cyberlaws4cxo.com>

Editor's Note



Digital Signatures were introduced in India through the Information Technology Act 2000 (ITA 2000) as the only method of authentication of electronic document which was legally recognized as equivalent to written signatures.

ITA 2008 has also introduced the concept of Electronic Signatures which could be any technology other than the PKI based system adopted as Digital Signature in ITA 2000.

Despite the advantages inherent in the system of digital signatures, its adoption has not been to the expected level. After the introduction of the mandatory use of digital signatures in MCA returns, there are more than 10 lakh digital certificate holders in India but they mostly restrict the use of the digital signature only for their MCA or Income Tax purposes.

Even the corporate sector which should have embraced the digital signatures for non repudiable electronic communication and digital contracts have not made use of digital signatures.

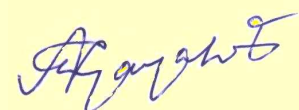
As a result, we have companies sending employment letters through undigitally signed e-mails, paving the way for employment related frauds. Non usage of digital signatures in Banking has paved the way for Phishing frauds and exposed the Indian Banking system to avoidable risks. Frauds in online broking and insurance are also attributable to some extent on non usage of digital signatures.

The US \$ 4 million fraud by an employee of WIPRO who withdrew money from WIPRO Bank accounts by stealing password of an authorized person should be an eye opener to Companies for immediate adoption of digital signatures in all important communication with Bankers, vendors and employees, present and prospective.

The delay in adoption of digital signatures as a preferred way of secure communication on the net is largely due to the lack of proper education at all levels. To ensure better adoption of digital signatures, Government of India needs to invest heavily into out reach programs either directly or through other agencies. Simultaneously, IT companies need to introduce applications that are compatible for use with digital signatures so that more and more users see value in acquiring digital signature capability.

Wider adoption of digital signatures for authentication of electronic documents is expected to reduce the incidence of frauds and Cyber Crime.

Let's hope 2010 will be an year in which Digital Signatures make a substantial progress in the country.



February 21, 2010

Interview of the Month.-1

Dr N Vijayaditya is the Controller of Certifying Authority - Information Technology Ministry of Communications and Information Technology Government of India.

Formerly, the Director General of National Informatics Centre, he was responsible for supervising implementation of several e-Governance projects at the Centre and States.

Dr Vijayaditya holds a Master's Degree in Computer Science from Indian Statistical Institute, Kolkata and a Ph.D in Information Systems from University of North Carolina, USA.

He has done research in the areas of Pattern Recognition, Graph Theory, Information Systems and Networks. He has guided students in Ph.D and Master's programs.

Dr Vijayaditya has been a recipient of many awards such as "2001 VASVIK Award" in recognition of his contribution in the area of Information & Communication Technology from Vividhlaxi Audyogik Samshodhan Vikas Kendra, Mumbai and Skoch Challenger-2005 Award for "ICT Man of the Year".

He has also received Bhoovikas Samman for Lifetime Excellence from Bhoovigyan Vikas Foundation, New Delhi. Received Special Achievements in GIS Awards "Making a Difference in People's Lives" at the ESRI User Conference at Sandiego, USA.



Dr N Vijayaditya

How important is the introduction of the concept of "Electronic Signatures" in ITA 2008? Is Indian IT industry ready to utilize the opportunities created?

The concept of electronic signatures has been introduced in the IT (Amendment) Act, 2008, so that new technologies can be brought under the ambit of the Act.

The IT Act, 2000 was technology-specific in favour of Public Key Cryptography based Digital Signatures. As of now, this technology is still the only one that meets the requirements for authentication & non-repudiation as laid down under the IT Act. Digital Signature is one type of electronic signature and is being used in a variety of applications.

Digital Signatures have been around in India for the last 8 years. Has the adoption rate in the community been upto your expectations? Are there any plans to promote the use of digital signatures by the common man?

The growth of use of Digital Signatures elsewhere in the world also has been mainly because of e-governance applications. The MCA-21 e-filing project of the Ministry of Corporate Affairs has been one of the major users contributing to the growth of use of Digital Signatures in the country. Digital Signatures are also being used in e-Procurement by various Government Departments, Import-Export clearances in DGFT, Income Tax Returns filing, Banking, etc. Several other applications are in the pipeline.

Office of CCA has been engaged in promoting the use of Digital Signatures. Awareness programmes have been conducted in this regard. Office of CCA is also engaged in promoting the use of Digital Signatures in several applications including Income Tax and Banking.

Interview of the Month. 1



**N Vijayaditya,
CCA of India**

Despite Digital Signatures being the only form of authentication of electronic documents in ITA 2000, no Bank in India seems to have introduced Digital Signatures for authentication of banking transactions in the last 9 years. Can we expect some developments in this direction during 2010?

At present, individual bank officers are using digital signatures to initiate electronic transactions in National Electronic Funds Transfer (NEFT) and Real Time Gross Settlement (RTGS).

At the receiving branch/office the signature is verified. Demat statements issued by banks are also being digitally signed in a number of cases. We expect increasing use of digital signatures in several retail and banking applications.

What precautions need to be taken by digital certificate holders to prevent instances of frauds involving digital signatures?

The holder of the Digital Signature Certificate should secure the private key being used for creating Digital Signatures. It has to be ensured that the private key is generated on a secure device conforming to FIPS 140-1/2 recommendations so that the key cannot be extracted from the device.

Additionally the holder has to protect use of the private key through a PIN and also ensure that possession of the device containing the private key is not given to any other person for any reason whatsoever.

Are there any new initiatives which CCA has been planning to introduce digital signatures in Mobile Transactions?

Office of CCA has been exploring the possibility of integrating Digital Signature capabilities in mobile phones keeping the requirements of the IT Act in view.

This includes for example, the need for the Digital Signature creating private key to be generated within the mobile phone and thereafter to remain in the custody of the subscriber at all times. Some technology options are also being examined in this regard.



Mr. Ravi Jagannathan has been the Managing Director & CEO of 3i Infotech Consumer Services Ltd. (Subsidiary of 3i Infotech) since its inception in June 2008.

Prior to his current assignment, Mr. Jagannathan has held several senior-level positions in 3i Infotech, including being the head of the Enterprise Solution Group in the US and being in charge of the Technology Services Group in US and UK, in his capacity as the Senior Vice President of 3i Infotech Inc.

Mr. Jagannathan has globe trotted quite extensively and has participated in many Indian and international panel discussions and seminars. He has a global experience of over 20 years in the fields of Management, Finance, Project Management, Technology Consulting and Business Development.

Mr. Jagannathan has also managed the Oracle Technology Practice of UBICS, Inc., US, prior to joining 3i Infotech. Further, in his capacity as a Chartered Accountant and management consultant, he has directed teams of professionals to provide a variety of Business, Management and Technology consulting for many MNC clients including ICICI, Citibank N.A, State Bank of India, HUDCO, Indian Bank, New Century Machinery Ltd., and Procter & Gamble Ltd.

Mr. Jagannathan holds a Bachelor's Degree in Commerce and is a Fellow Member of the Institute of Chartered Accountants of India.

How do you foresee the growth of digital signature usage by the industry in India?

Today few areas in Government (like Income Tax, MCA 21, IRCTC & eProcurement) use DSC – I see a lot of new applications be it land records management, Other Tax payments etc. use DSC in the near future.

Banking is another area which is expected to adopt DSC immediately especially considering the non-repudiable related benefits.

We are launching new applications like MyLoan, MyInsurance and MyMoney where one could transact using digital signature eliminating the need for physical application forms. Mobile commerce is another area wherein digital signature can play a pivotal role.

What is the potential for digital signatures being used to secure the emerging mobile banking scenario in India?

The potential is quite high. I believe a safe and secure way to enable mobile banking is to deploy PKI based solutions (digital signature).

Ministry of IT and also the RBI heavily recommend financial institutions to adopt PKI technology. In my opinion many people are still not fully aware of the vulnerabilities using non-pki based mobile banking solutions and also about availability of PKI based solutions.

Interview of the Month-2



Ravi
Jagannathan

What in your opinion is the reason for the slow adoption of Digital Signature usage in India? What could be the remedies?

There are several factors contributing to slow adoption. I will pick price and lack of applications.

One of the key objectives of 3i CSL is to deliver enough applications for consumer usage while making it more affordable.

In countries which have high penetration of Digital signatures, I see the financial institutions providing the PKI platform for its customers, Indian banking industry along with Government sector can drive quicker adoption.

ITA 2008 provided for new technologies for authentication of electronic documents. Are there any industry initiatives in introducing cost effective alternatives to PKI based digital signature systems?

Considering the provisions made in ITA 2008 – we have recently launched SecMsg, a PKI based secure SMS platform. There are couple of alternatives we have explored for voice based authentication and sim based solutions which has potential.

I am still advocating PKI based authentication as it has all the requisite approvals and provisions in ITA backed by a robust technology.

How does the Indian systems for authentication of electronic documents in the form of the digital signatures and the proposed electronic signatures compare with the developments in other countries?

Lot of countries in Europe, Americas as well as several countries in far-east has very high adoption of Digital signature based authentication. As stated the underlying technology is the same but the applications and usage areas created in the aforesaid countries far outnumber the application/usage in India. Countries like Sweden, Taiwan, Hong Kong have majority of their population using digital signatures for conducting banking transactions or stock trading. India being one of the fastest growing economies will soon adopt a similar route which will provide better banking and e-governance environment.

Disclosure of Data Breach Incidents

“The biggest surprise to computer-security experts isn’t that Google Inc was targeted by attackers from China. It’s that the Internet giant chose to disclose the incident.. There’s a culture of secrecy around any bad news..” so said a security expert in Wall Street Journal last week.

India is no different. We all know that “Phishing” is a daily crime reported in all major Banks. However, neither the individual Banks nor the RBI has taken efforts to apprise the Internet Banking public of the extent of the Phishing Risk on the Indian public.

However, this attitude appears to be headed for a change .. not voluntarily.. but by mandatory provisions in law.

Under the HITECH Act applicable to US Health information processors, “Data Breach Notification” provisions became effective from September 23, 2009. Under this provision, any Business Associate becoming aware of data breach must inform the Covered Entity. The Covered Entity needs to inform individual victims and HHS. In certain cases they also need to put up a notice on their website and also give advertisements in local news papers. HHS also needs to put up the information on the website and also report to US Congress once an year.

This will therefore be the norm in future. Will India follow suit?

The draft rules under Section 70B of ITA 2008 distributed for public response contained a requirement for periodical reporting of Security Breach Incidents from the private sector corporate sector. For the time being, the industry appears to have stalled this move.

May be ...in due course when the rule is finally notified, there may be a surprise in store for the corporates. Data Breach/Cyber Crime Notification may become mandatory.

Who Loses?

An employee of Infosys was recently arrested in Delhi for having made a hoax mobile call to the airport to delay a flight which he feared he would miss.

The employee was arrested on terrorist charges and would be tried and punished appropriately in due course. He would lose his job for the present and also for the best part of the future in the organized sector.

However, we should not lose sight that the Company also lost an employee on whom an investment had already been made in training and development. Though employee attrition is part of any Company’s woes, losing employees because of their tendency to take the law lightly, is perhaps avoidable through a well executed HR plan.

Some companies may feel, “I am anyway losing 15% of my employees every year to other reasons. What if there is one more?”. Unfortunately Cyber Crime related attrition is not that simple. The outgoing employee may actually create a huge damage to the company before he leaves. Hence, An employee saved is more than an employee recruited.

Perhaps HR departments need to do research on “Identification of Cyber Offence tendencies” in employees, training them to strengthen the internal defenses of “Cyber Ethics ” and in high risk cases, subjecting the chosen employees through a “Counselling and rehabilitative programme”

Bank Reimburses Lost Amount with Interest to a Phishing Victim

Phishing victims of Banks are often confronted by the Banks that the loss has to be borne by the victim customer since the fraud was facilitated by his negligence. Despite the German Courts holding Banks liable for Phishing and Danish Banking Regulator specifying that Banks are responsible for any hacking into their systems, Indian Banks were often hiding behind the “Account Opening Form and Instructions contained there in” to avoid Phishing liabilities.

Though one of the Adjudication applications is kept pending in Chennai beyond reasonable time presumably because of the hesitation of the adjudicator to come to a decision, it was interesting to note that the Banking Ombudsman in Chennai recently ordered a Bank in Bangalore to repay the Phished amount along with interest to the complaining customer. The Bank also obliged without demur.

This has once for all sealed the position in India that “Phishing Liability is on the Bank”. This was not only evident in general Banking law but was specifically confirmed in Section 66A of the ITA 2008.

Media Disinformation on Prevalent Laws

Common man who does not have access to appropriate knowledge resources rely on the daily news paper for his education on what are the prevailing laws that affect him. So when Times of India carried a front page article on February 11th in all its editions stating that according to the amendments made to ITA 2000 with effect from October 27, 2009, "Government cannot ban porn websites", the news was received in trust as an important point of education on the new ITA 2008.

Unfortunately, others were quick to disagree and point out that the report was not based on a proper assessment of the provisions and the Government in deed had the powers to ban porn websites. Naavi also pointed out that the TOI itself was even guilty enough to be accused of violations of ITA 2008. See www.naavi.org for more details. The motivation for the controversial article is unknown.

Will UID increase Identity Theft Incidents?

Fraud experts estimate that about 0.17% of the population in Europe fell victim to ID thefts in 2009 while in US, there were 3.39% of the population who fell victim to ID thefts. Even considering that Internet penetration in USA is around 90% while in Europe it is around 52% the increased incidence of ID thefts in USA is alarming.

According to one study, the reason for this is that in US any business can subscribe to the credit bureau and use the credit scoring instantly to assess some one else's risk of default. In Europe the bureaus only allow negative information to be shared and the data base is otherwise is not easily accessible to any one.

Also in US, credit cards with magnetic strips are still prominent use while Europe is moving to "Chip and Pin" technology with the use of Smart Cards.

More than these reasons, experts feel that the key problem lies in the fact that in US, the Social Security Numbers are used as a "Universal Identifier". On the other hand the European countries use National Identity Cards which are not as universally used by all agencies as an Identifier.

These observations contain important lessons for India where we are in the process of introducing the UID (Unique Identity) for every "Resident of India" which will not only be used as an unique identifier by all credit agencies but even be created through such credit agencies. Though in India, Internet penetration is still around 7%, and hence the Identity theft concern may not be as high as in Europe or USA, it is necessary for UID Authority to consider that UID has a potential to be misused for stealing the identity of a person and used for committing financial frauds. It would therefore be necessary for UIDAI to ensure through its own security process that the system would not be amenable to abuse.

Since UIDAI would be handling "Sensitive Personal Information", it would also be obligatory for UIDAI to follow "Reasonable Security Practices" as per Section 43A of ITA 2008. Techno Legal Information Security experts would be looking forward to the actions taken by UIDAI to ensure that UID does not become an easy source of Identity Theft

Legal BPO s in India gets a Big Boost

Microsoft is reported to have assigned its US \$ 800 million legal work on Intellectual Property and Patents to India through CPA India at Noida. This should be a catalyst for a quantum growth in LPO business in India.

Digital Signature as an IS Tool

Digital Signatures have been available in India since 2002 after Safescrypt launched its services as a licensed Certifying Authority on 4th February 2002. Since then, TCS, n-Code, E-Mudhra, MTNL, NIC and IDRBT have also been licensed as CAs. Department of Commercial Taxes which had been licensed is reportedly withdrawing from the business shortly.

The use of Digital Signatures in India is currently driven mostly by the mandatory requirements for submission of annual MCA returns through submission of online forms. The full potential of the digital signature system has not been used by the Indian Corporate sector. Even the use of digital signatures in the MCA/IT has been largely in a manner that has exposed the user companies to various risks.

On February 17th, news of a major fraud in WIPRO broke out. This fraud involved an employee stealing the password of another colleague and using it to withdraw money from WIPRO's bank account and transferring the same to the accounts of the employee and his relatives. What strikes a sharp observer in this case is that the Bank was allowing withdrawals based on passwords and not on "Digital Signatures" which made it easy for the fraudster to cheat the Bank and WIPRO.

No doubt every Bank in India allows withdrawals through password authentication. But it defies logic that a major IT company like WIPRO and major Banks in India continue to ignore what is so clearly mentioned in the Indian law that "You cannot legally authenticate an Electronic Document without the use of a Digital Signature backed by a valid Digital Certificate issued by a licensed Certifying Authority".

Are our Corporate CFOs so ignorant of the law? Or do they simply don't care what is in the law? If this is the attitude of the top executives of a Company, what example are they setting to their employees for compliance of law in general and following ethics in the workplace?

On June 14, 2001, RBI issued a circular DBOD.COMP.BC.No.130/ 07.03.23/ 2000-01 providing "Internet Banking Guidelines". Under these guidelines RBI clearly indicated that according to ITA 2000, Digital Signature was the only accepted method of authentication of an electronic document. Since at that point of time the Certifying Authorities had not yet set up their services, RBI suggested that until PKI system is established, other alternate systems can be used. RBI made a categorical statement that

"From a legal perspective, security procedure adopted by banks for authenticating users needs to be recognized by law as a substitute for signature. In India, the Information Technology Act, 2000, in Section 3(2) provides for a particular technology (viz., the asymmetric crypto system and hash function) as a means of authenticating electronic record. Any other method used by banks for authentication should be recognized as a source of legal risk. (Para 7.3.1)".

This left no doubt about the intentions of the Banking regulator that as and when digital signature system becomes available, it should be used for authentication in Internet Banking systems.

...Contd

Despite this, Banks have continued to avoid use of Digital Signatures and the Chairmen and Directors of Banks are perhaps being misled by IT professionals some of whom have developed and are marketing Banking Software that is not PKI compliant.

The RBI guideline was reinforced on July 20, 2005 through another circular DBOD No . Comp.BC.14/07.03.29/2005-06 by fixing the top management in the Banks responsible for approving the Internet Banking policy. If therefore Banks have been running a “Cyber Law Non Compliant Internet Banking” system, the responsibility for the same lies squarely with the Board and the Chairman. Since the Chairman may also be responsible for SEBI Listing requirements under Clause 49 and provides the necessary Corporate Governance certificates to be published for share holder’s information, we have a dangerous scenario where the Chairmen and the Independent Directors of Banks are exposing themselves to serious charges of “Negligence” and “False Certification”.

Though Cost of incorporating Digital Signatures as a means of authentication of Internet Banking log in requests, is quite low and there are solutions available readily, Banks continue to challenge the law. It may not be long before a WIPRO like incident in a Bank will put some unfortunate Chairman in Jail and wake up the industry from the slumber they have put themselves into.

The PKI based digital signature system is not only capable of being the authentication tool approved by law and more secure than the password based authentication systems, it is also a tool that can be used for “Encryption of Transmission of Electronic Documents”. If two persons communicating through electronic messages have digital signatures, they can use each other’s public keys for encryption of the message so that the communication would have a “Person to Person Security”.

This beneficial use of digital signature for encryption however can be used only when the private key is available for decryption of a document first encrypted with the public key. Unfortunately, this benefit is being lost in the system of “Secured Digital Signature” system that we are now adopting based on hardware tokens. These tokens are equipped to generate the pair of keys at the time of certificate generation and also to pick up the hash values of the documents to be signed and carry out the private key encryption of the hash value within the token. However encrypted documents cannot be imported into the tokens or private keys be exported from the tokens for decrypting the encrypted document outside the hardware token.

This technical issue needs to be recognized by CCA to retain and encourage usage of soft token based digital signatures which are also as secure as the token based systems in terms of judicial value. Presently, the CCA has been considering the introduction of a Dual key pair systems where one pair of public and private keys is used for signing and the other for encryption. It is suggested that the private key meant for encryption is escrowed with the Certifying authority to be available for forced decryptions.

...Contd

The use of dual key pair systems is practically a difficult solution since the current technologies for issue and use of private and public keys in e-mail clients, web browsers and applications don't support the dual key pair systems and the changes to be brought into the applications are too complicated to be of practical use.

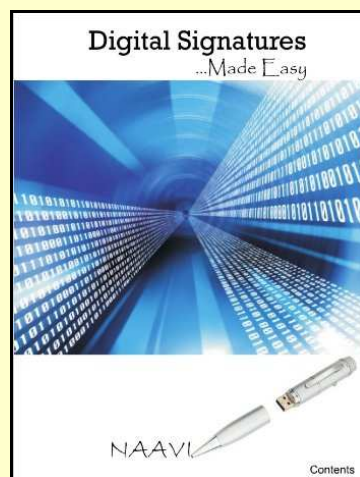
Naavi has suggested use of CEAC-Certified Digital Signature System as an alternative which perhaps can use the advantages of the current soft token based systems and still meet the consumer's requirement for judicial acceptance on par with the "Secured Digital Signatures". Once such systems are adopted by the public, the value of digital signature systems would increase and the Netizens may start using digital signatures for their day to day requirements.

Since it may be possible today to provide digital signature certificates and a suitable system for use by Banks for authenticating their clients at a very low per user fee, there is a case for RBI taking the immediate bold step to make the use of digital signatures in Internet Banking mandatory.

RBI should also ensure that "Mobile Banking" transactions are authenticated by the use of "Digital Signatures" so that there is a legal backing to the Mobile Banking transactions.

It may however be necessary for the CCA to undertake a campaign with all the Chairmen of Banks in India to explain the benefits of the use of Digital Signatures and also expose them directly to the available solutions so that Indian Banking System may go "Truly Digital".

Naavi



Free E Book available for download at Naavi.org



Details available at Naavi.org

Questions and Answers

We intend using this section of the news letter to answer the Cyber Law related queries raised by our readers. This being a special issue on Digital Signatures we are using this space to explain some of the basic concept of Digital signatures.

We appreciate if queries are raised by persons indicating their Name, Occupation and Contact details. We however don't want to restrain the readers from raising questions without revealing their identity. Such readers may therefore send the questions as "Anonymous" in which case even their e-mail ID would not be provided on the news letter.

All questions may however be sent by e-mail to naavi@in.com by e-mail with the subject line containing "Cyber Laws for CxOs".

Editor

What is a Digital Signature?

Digital signature is a method of authentication of an electronic document as per Indian Law (ITA 2000) recognized as equivalent to the written signature on a paper document. The system is defined under Section 3 of ITA 2000 and its effect is provided legal recognition under Section 5 of ITA 2000.

A derived definition of digital signature as per ITA 2000 is

"Digital Signature of a person, of a document is the hash value of the document encrypted with the private key of the person".... Naavi

ITA 2008 has also introduced the concept of "Electronic Signature" which could be any other form of authentication that may be approved by the Government under ITA 2000 which could be developed in future by using any technology other than the hash value and asymmetric encryption based Digital Signature.

How Does a Digital Signature Work?

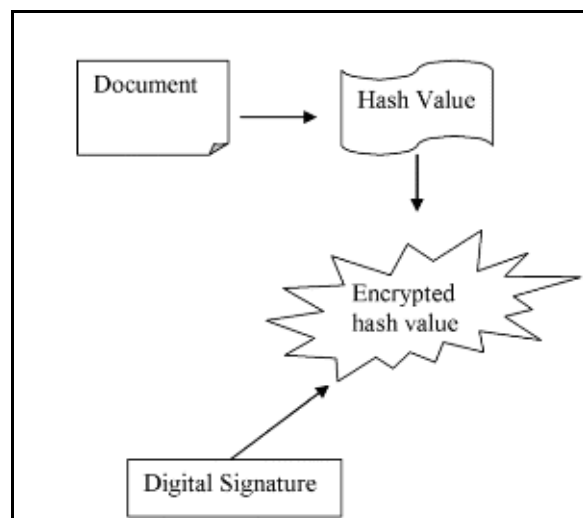
Step 1: Use the standard hash algorithm on the document to be signed to calculate the hash code.

Step 2: Use the private key to encrypt the hash code.

Encrypted Hash code is the digital signature. This can be embedded into/attached to the document.

In practice, the above steps are carried out automatically by an application which picks up the private key from where it is stored using the prescribed pass word if any.

In case the private key is stored in an external token (cryptographic key or smart card), the token has to be attached to the computer so that the application can pick up the key.



What is the Technology Behind Digital Signatures

Digital Signature uses two sub technologies namely the “Hashing” and “Asymmetric Crypto System”. “Hashing” is a process where the electronic document is taken as a numerical input into a hashing algorithm producing a hash result which is unique to the document and consistent. If the document undergoes any change, the hash value changes. Asymmetric cryptosystem is an encryption system based on a pair of keys so that encryption can be done by either of the keys but once encrypted with one of the keys of the pair, decryption is possible only with the other member of the key pair. A successful decryption with one key of a pair can therefore be accepted as evidence that the encryption was done only with the other member of the pair.

For being used in the digital signature system, one of the two keys of the pair is designated as the private key and is held confidential with the signatory and used for encryption of the hash value of a document for the purpose of signature. The other key is called the public key, is widely distributed and used for verification of the signature by a decryption process.

India presently uses SHA1 and SHA2 standard hash algorithms, RSA Encryption algorithm and issue of digital certificates under a hierarchy in which the Controller of Certifying Authorities (CCA) is the root Certifying authority of India appointed as a statutory authority. CCA licenses other agencies as “Certifying Authorities” (CA) and CAs interact with the public and enroll them as “Subscribers” to issue Digital Certificates on application.

CAs verify the identity of the applicants before digital certificates are issued, provide the technology for issuing the key pair and for maintaining the repository of certificates issued and revoked. Based on the strength of verification and other parameters, CAs issue different classes of digital certificates at different prices. Details would be made available to the public through a Certification Practice Statement available at the websites of individual CAs. The URLs of different CAs may be obtained from the CCA website <http://www.cca.gov.in>

Has there been any Cyber Crimes Committed with Digital Signatures?

There is one reported case where a digital signature of a deceased Company Director was fraudulently used by other directors causing wrongful harm to the legal heirs.

The problem could have occurred because of the prevailing insecure practice adopted by many Company Directors to leave the private key tokens with the chartered accountants, secretaries or other assistants and let them use them on their behalf.

It is necessary for Company Directors to ensure that they are not dependent on any other person to either generate their certificate in the first place or to use it subsequently.

How To use Digital Signatures in E-Mail

If you have already installed the digital certificate in your computer, then using the e-mail client application such as outlook express to send the e-mail. After composing your message if you click on the button “Digitally Sign the Message” the application will automatically complete the process only asking for the password or the token where the private key is stored in protected mode.

In case you and your addressee have earlier exchanged digitally signed e-mails the digital certificates would have also been exchanged hands and you can use the addressee’s public key to encrypt messages by clicking the required button. Ensure that you donot use encryption option if your addressee is using hardware token as he may then be unable to decrypt your message.

Questions and Answers

Who is a Certifying Authority?

Certifying Authorities are those who are licensed by the Controller of Certifying Authorities (CA) authorized to issue digital certificates to applicants as per the provisions of ITA 2000.

They issue digital certificates after due verification of the applicant's identity. Some of the CAs also provide applications for the use of Digital Signatures and provide other services to the users.

Only companies which are sound, have adequate network, maintain security systems are provided the necessary license. Foreign Certifying authorities need to obtain separate license to operate in India.

All CAs are governed under the supervision of the CCA.

List of Certifying Authorities in India and their Websites

1. Safescrypt : <http://www.safescrypt.com>
2. TCS : <http://www.tcs-ca.tcs.co.in>
3. GNFC: <http://www.ncodesolutions.com>
4. E-Mudhra: <http://www.e-Mudhra.com>
5. NIC : <https://nicca.nic.in>
6. IDRBT: <http://idrbtca.org.in>
7. MTNL: <http://www.mtnltrustline.com>

Department of Customs and Central Excise which was one of the licensed CAs ceased its operations from 8th December 2009.

Certification Practice Statement (CPS) of each of the CAs is available on the respective websites and describes the detailed terms and conditions under which Digital Certificates are issued by them.

What are the Responsibilities of a Digital Signature user?

ITA 2000 prescribes certain obligations on the subscribers and non compliance of such obligations may result in Civil and Criminal liabilities. Every subscriber is expected to ensure that the digital certificate is not used for fraudulent purpose, does not contain any false particulars about the holder (eg e-mail address, name etc) and does not involve any misrepresentation while obtaining the digital certificate. Criminal consequences can be imprisonment upto 2 years.

The subscriber has to generate the keys using the recommended security process, keep confidential custody of the private key and in the event of an accidental compromise of the private key, should inform the CA and revoke the certificate.

How To Get a Digital Certificate

Step 1: Identify a suitable CA.

Step 2 : Visit the website of the CA, download CPS and understand the different types or classes of Digital Certificates issued and obtain the price list.

Step3: Make an online application or request the company representative to call on you.

Step 4: Submit your application along with necessary documents of identity etc as may be required along with the payment of fees.

Step 5: On approval, CA will send the instructions how to pick up the Certificate. Follow the procedure and install the certificate in your system.

Precautions to be Observed While obtaining the Digital Certificate

1. Ensure correct particulars about you are furnished to the CA. Misrepresenting any information may be considered as a punishable offence.
2. Use an e-mail address for which you have POP access (ability to send an e-mail using an e-mail client application such as Outlook, Outlook express or Mozilla Thunderbird) as your e-mail ID during registration. Otherwise you may be unable to send digitally signed e-mails.
3. Allocate strong password to protect your private key whether stored as a soft token in the Computer or in the hard ware token such as the Cryptographic key or Smart Card.
4. Ensure that you alone sit before the computer and pick up the certificate. Delegation of the Certificate pick up process to any person including the agent of the CA is improper and renders the Certificate invalid.
5. If you suspect that the private key details or password to the folder containing the private key might have come to the knowledge of any other person, the certificate needs to be immediately “revoked.” Check the procedure for revocation with the CA.
6. Before installation of the Digital Certificate, it may be necessary to also download the digital certificate of the issuing CA which will be available on the CA’s website and also the digital certificate of CCA which will be available either on the CA’s website or the CCA website. (www.cca.gov.in)
7. If you are buying a “Secured Digital Certificate” with hardware token, the token may have to be first installed using the CD provided by the CA. Complete this before starting the process of picking up of the certificate.
8. During the process of picking up of the certificate carefully follow all the instructions and in particular chose to store the private key in a “Secure” manner allocating a password.
9. After the Digital Certificate is received, check if the name and e-mail address is correctly noted in the certificate. If not ask for correction immediately. Using a digital certificate with false particulars is an offence.
10. If using a hardware token, store it in a safe place under your custody. Never deposit it with any body else including your Chartered Accountant or Company Secretary or a Colleague.

How To Verify a Digital Signature

Verification of a digital signature involves,

- a) Obtaining the digital certificate of the signatory which contains his public key as well as the name and e-mail ID of the person.
- b) Calculating the hash value of the document as received
- c) Decrypting the digital signature using the public key of the signatory
- d) Matching (a) and (b)

In case of mismatch, it means that the document has changed after signature and hence the digital signature would be invalid.

In case the digital signature cannot be decrypted to yield a hash value, when the public key of a person is applied, it means that the public key is not related to the private key used for encryption. i.o.w., the digital signature does not belong to the owner of the public key.

The verification process needs a suitable application to carry out the processes (a), (b) and (c) mentioned above.

A digital signature is considered valid if the certificate was valid on the day and at the time it was signed and had not been revoked.

The date of validity of a certificate is available on the certificate itself. The revocation details are available on the revocation list normally available at the website of the CA issuing the certificate. The URL at which the revocation list can be accessed is available in the Digital Certificate.

How Does a Digital Signature Look like?

Digital Signature does not look like normal written signature. Since it is an encrypted digital file, if we try to read the digital signature in a text editor, it may look like the following:

```
IQB1AwUBMVSiA5QYCuMfgNYjAQFAKgL/ZkBfbeNEsbthba4BlrcnjqbcKgNv+a5kr45  
37y8RCd+RHm75yYh5xxA1ojELwNhbb7cltrp2V7LIOnAelws4S87UX80cLBtBcN6AACf1  
1qymC2h+Rb2j5SU+rmXWru+=QFMx
```

Applications only verify the signature and indicate whether the digital signature is valid or not.

What is an Electronic Signature?

Electronic Signature is a system suggested by ITA 2008 to supplement the PKI based digital signature system presently in vogue. As of now no such system has been identified and licensed.

Questions and Answers

Use of Digital Signatures in Companies and Banks

Companies and Banks need to use digital signatures for authenticating any electronic document if they need to be compliant with ITA 2008. For this purpose all Companies and Banks need to put in process a compliance programme which includes the following.

1. Issue digital signatures from a licensed CA to all senior employees who require to authenticate documents particularly for outside recipients.
2. Make suitable modifications in the document flow systems so that wherever authentication is required, the system asks for digital signature and provides for verification of signature at any point of time.
3. Introduce suitable changes to the document flow software to incorporate sequential signing by multiple persons at different points of time in the life cycle of a document.
4. Use encryption using the public key of the recipient whenever electronic documents are transmitted, using a soft token based digital signature system.
5. In order to enhance the evidentiary value of soft token based digital signatures use “Certified digital Signature Systems”.
6. Establish a suitable system of custody for private keys of executives ensuring that the “non repudiable” nature of digital signatures.
7. In Internet Banking, upgrade the access systems to accept digitally signed access requests instead of password based messages.

Is Banking without Digital Signature Safe?

Banking with the use of password based authentication systems instead of digital signature systems is not compliant with ITA 2000/2008 or the Internet Banking Guidelines of RBI. Legal Risk arising out of non usage of digital signatures lies with the Bank.

For a Free Trial Version of Digital Certificate

Contact: naavi@vsnl.com

For Consultancy regarding the use of Digital Signature in your business or for development of customized applications using Digital Signatures

Contact: Ujvala Consultants Pvt Ltd: ujvala@md2.vsnl.net.in

Disclosure

This is an e-news letter published by Ujvala Consultants Pvt Ltd, No 37, “Ujvala” 20th Main, B S K Stage I, Bangalore 560050. (Ph: 080 26603490).

Web: www.ujvala.com. E Mail: ujvala@md2.vsnl.net.in

The news letter is being edited by Naavi, Na.Vijayashankar, no 37/5, “Ujvala”, 20th Main, B S K Stage I, Bangalore 560050.

Web: www.naavi.org. E Mail: naavi@in.com

A copy of the news letter is also being hosted on the website <http://www.cyberlaws4cxo.com>. In future the news letter may be reproduced in any other website owned by the same management or its assignees.

The views expressed in the news letter and the hosting website would be considered as belonging to the respective authors and provided for educative purpose and are not considered as legal advice.

Any comments and complaints if any may be sent to the editor at naavi@in.com for resolution.

Contents of this news letter may be reproduced only on specific permission from the editor and with due credit.

Copyright in respect of any contributions from authors published in the news letter will be deemed to have been transferred to the publisher at the time the article is submitted for publication. In the event an author intends to publish the same article in any other publication, he shall inform the publisher of Cyber Laws For CxO the name of such other publication and also add a note “First submitted for publication with Cyber Laws For CxO” in the other publication.

Any dispute arising out of the publication shall be settled through arbitration through the virtual arbitration center <http://www.arbitration.in> as per the terms of the Indian Arbitration and Conciliation Act 1996.

For Subscription: Visit www.cyberlaws4cxo.com