E-commerce - Legal issues

Rohas Nagpal
Asian School of Cyber Laws

Life will knock us down.
But we can choose whether or not to get back up.

Published in 2019 by Asian School of Cyber Laws.

No investigation has been made of common-law trademark rights in any word. Words that are known to have current trademark registrations are shown with an initial capital and are also identified as trademarks.

The inclusion or exclusion of any word, or its capitalization, in this book is not, however, an expression of the publisher's opinion as to whether or not it is subject to proprietary rights, nor is it to be regarded as affecting the validity of any trademark.

This book is provided "as is" and Asian School of Cyber Laws makes no representations or warranties, express or implied either in respect of this book or the software, websites and other information referred to in this book.

By way of example, but not limitation, Asian School of Cyber Laws makes no representations or warranties of merchantability or fitness for any particular purpose or that the use of licensed software, database or documentation will not infringe any third party patents, copyrights, trademarks or other rights.

Printed in India

The chosen case scenarios are for instructional purposes only and any association to an actual case and litigation is purely coincidental. Names and locations presented in the case scenarios are fictitious and are not intended to reflect actual people or places.

Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement, recommendation, or favoring by Asian School of Cyber Laws, and the information and statements shall not be used for the purposes of advertising.

Contents

ONE

1. Introduction

According to its preamble, the Information Technology Act, 2000 is an "…Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information…."

Statement of objects and reasons of the Information Technology Act, 2000 are:

New communication systems and digital technology have made dramatic changes in the way we live. A revolution is occurring in the way people transact business. Business and consumer are increasingly using computers to create, transmit and store information in the electronic from instead of traditional paper documents. Information stored form has many advantages.

It is cheaper, easier to store and retrieve and speedier to communicate. Although people are aware of these advantages, they are reluctant to conduct business or conclude any transaction in the electronic form due to lack of appropriate legal framework.

The two principal hurdles which stand in the way of facilitating electronic commerce and electronic governance are the requirement as to writing and signature for legal recognition. At present many legal provisions assume the

existence of paper based records and document and records which should bear signatures.
The law of evidence is traditionally based upon paper-based records and oral testimony. Since electronic commerce eliminates the need for paper-based transactions, hence to facilitate e-commerce the need for legal changes have become an urgent necessity. International trade through the medium of e-commerce is growing rapidly in the past few years and many countries have switched over from traditional paper based commerce to e-commerce.

The United Nations Commission on International Trade Law (UNCITRAL) adopted the model laws on electronic commerce in 1996. The General Assembly of United Nations by its Resolution no. 51/162 dated 30th January, 1997 recommended that all states should give favourable considerations to the said model law when they enact or revise their laws. The model law provides for equal treatment of users of electronic communication and paper based communication.

Pursuant to a recent declaration by member countries, the World Trade Organization is likely to form a work programme to handle its work in this area including the possible creation of multilateral trade deals through the medium of electronic commerce. There is a need for bringing in suitable amendments in the existing laws in our country to facilitate e-commerce. It is, therefore, proposed to provide for legal recognition of electronic records and digital signature.

This will enable the conclusion of contracts and the creation of rights and obligations through the electronic medium. It is also proposed for a regulatory regime to supervise the certifying authorities issuing digital signature certificates.

To prevent the possible misuse arising out of transactions and other dealings concluded over the electronic medium, it is also proposed to create civil liabilities for contravention of the provisions of the proposed legislation. With a view to facilitate electronic governance, it is proposed to provide for the use and acceptance of electronic records and digital signatures in the government office and its agencies.

This will make the citizens interaction with the government offices hassle free. The proposal was also circulated to the state governments. They have supported the proposed legislation and have also expressed urgency for such legislation.

Statement of objects and reasons of the Information Technology (Amendment) Act, 2008 are:

1. The Information Technology Act was enacted in the year 2000 with a view to give a fillip to the growth of electronic commerce, to facilitate e-governance, to prevent computer based crimes and ensure security practices and procedures in the context of widest possible use of information technology worldwide.

2. With proliferation of information technology enabling services such as e-governance, e-commerce and e-transactions, protection of personal data and information and implementation of security practices and procedures in relation to these applications of electronic communications have assumed greater importance and they require harmonization with the provision of the Information Technology Act. Further, protection of critical information infrastructure is pivotal to national security, economy, public health and safety, so it has become necessary to declare such infrastructure as protected system as to restrict its access.

3. A rapid increase in the use of computer and internet has given rise to new forms of crimes like publishing sexually explicit material in electronic form, video voyeurism and breach of confidentially and leakage of data by intermediary, e-commerce frauds like personation commonly known as phishing, identity theft and offensive messages through communication services. So, penal provisions are required to be included in the Information Technology Act, the Indian Penal Code, the Indian Evidence Act and the Code of Criminal Procedure to prevent such crimes.

4. UNCITRAL in the year 2001 adopted the model law on electronic signatures. The General Assembly of the United Nations by its Resolution no. 56/80, dated 12th December, 2001, recommended that all states accord favourable consideration to the said model law on electronic signature since the digital signature are linked to a specific technology under the existing provisions of the Information Technology Act, it has become necessary to provide for alternate technology of electronic signature for bringing harmonization with model law.

5. The service providers may be authorized by the central government or the state government to set up, maintain and upgrade the computerised facilities and also collect, retain and appropriate service charges for providing such services at such as may be specified by the Central Government or the State Government.

TWO

2. Digital Signatures - technical issues

The Information Technology Act, 2000 (IT Act) prescribes digital signatures as a means of authentication of electronic records. In short, a digital signature has the same function as that of a handwritten signature.

However, understanding how a digital signature is created and how it achieves the same functionality as a handwritten signature is by no means an easy task. This is because the technical concepts involved in creating a digital signature seem far removed from the realm of law, although the objective of affixing a digital signature to an electronic record is purely legal! Digital signatures are an application of asymmetric key cryptography. This chapter traces the roots of cryptography, discusses symmetric and asymmetric key cryptography and ends with a detailed discussion on how asymmetric key cryptography can be used to create a digital signature.

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. One of the landmark developments in the history of cryptography was the introduction of the revolutionary concept of **public-key cryptography**. In 1978, **Ron Rivest, Adi Shamir and Leonard Adleman** discovered the first practical public-key encryption and signature scheme, now referred to as RSA (after the names of its inventors).

2.1 How cryptography works

Cryptography is the **science of using mathematics to encrypt and decrypt data**. Cryptography enables you 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.

While cryptography is the science of securing data, **cryptanalysis** is the science of analyzing and breaking secure communication (breaching security measures). Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis.

A cryptographic algorithm, or **cipher**, is a mathematical function used in the encryption and decryption process. This mathematical function works in combination with a **key** — a very large number — to encrypt the plaintext (the original message).

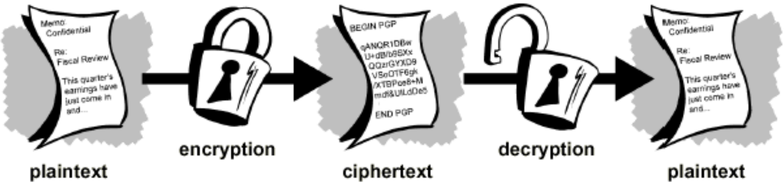
Data that can be read and understood without any special measures is called **plaintext** or clear text. Data which requires some special function to be performed on it before it can be read and understood, is called **cipher text**.

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.

A cryptographic algorithm, plus all possible keys and all the protocols that make it work comprise a **cryptosystem**.

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**.

The figure below illustrates the process of encryption and decryption.



[Image courtesy: An Introduction to Cryptography – PGP Corporation]

The fundamental objective of cryptography is information security. The following are the objectives of information security that cryptography helps to fulfil:

1. **Confidentiality** is used to keep the content of information secret from unauthorized persons. This is achieved through symmetric and asymmetric encryption.
2. **Data integrity** addresses the unauthorized alteration of data. This is addressed by hash functions.
3. **Authentication** is related to identification. This function applies to both - the entities and the information itself. This is achieved through digital signature certificates and digital signatures.
4. **Non-repudiation** prevents someone from denying previous commitments or actions. This is achieved through digital signature certificates and digital signatures.

2.2 Keys

A key is a value that works with a cryptographic algorithm to produce a specific cipher text. Keys are basically **very, very, very big numbers**. Key size is measured in bits. In public key cryptography, the bigger the key, the more secure the cipher text. However, public key size and conventional cryptography's symmetric key size are totally unrelated.

The algorithms used for each type of cryptography are very different and are very difficult to compare.

In public key cryptography, although the public and private keys are mathematically related, it is very difficult to derive the private key by analysing the public key (this is explained later in this chapter). Keys are stored by cryptographic software in an encrypted form. These files are called key rings.

The figure below illustrates a 512-bit RSA public key

```
3048 0241 00FC DBDF 80FA 0121 AD3F 8FFF B101 A19D
52E8 A4A4 E79D E9A2 BE37 EFED 8126 8A03 7130 F4E2
3644 1BE0 5CFE 613B 4400 CEE4 8E27 B971 ECCA 78C5
F714 FAE5 B2A2 1E01 FF02 0301 0001
```

A 512-bit RSA public key

The figures below illustrate a 1024 bit RSA key pair generated using the PGP (Pretty Good Privacy) digital signature and encryption software.

```
-----BEGIN PGP PRIVATE KEY BLOCK-----
lQHgBD5vDDEBBAC+UMHKr9YL1W0OYzL9gK/AERegEtzoFiveSz
beFQtNhxDIOSPJc60Y8v2nTecI0R5Y6Z55uzakcPBZmTJ+kWrFR4
NZPApiOFXhUrkHF0DmrmEpa5UpHjpO3sD+Hlvg84N6jHjAIRMlN
MAyrg/e4i6ABGzAuxYbJCs6ax9mxdrFAQARAQABAwvtDcK53Fr7
j9Ss3v83ZR7g1DgFfY3oo97XWbmJ02BdRGy/C+aIuu3wMRNqmP
o5w1I8VVCjjM02eqSr0+8mbLLX0Dwqbn33QitGW34Upt6EI+fv0
ObKbJRi2Hc628l3mi+jjsskxvQ8oavtSJL2j/xTEtL+wvqObcFxllsyjp
H5N1wY7xQ5BPSNjYLFZr99MXycFhee14V2YdQv0iPZFrJnvCQFW
XLAiX1L9AH5DgwmXLtNCPbIQnRwyLPyWSOT4yH8e6ibqIBvMh
pGe4WOAzuccHL6jjZrokVrBBu50Z6EqGFkzS8X6iygvSATOjr3L/X
9EW7Fw098CcVK3lDB93rpeXR+tU370nV+0FgXQqUzQ3SJ6vZwdl
wy6cmjZOWmd/YrbGLOyyW+zFFSZFdiG480ELozMfMsqp3OJvElv
hRgS/tbA/94jpOtzhWV9Du0pd7otCBBYmhpbmF2IEJoYXR0IDxh
YkBhc2lhbmxhd3Mub3JnPp0B4AQ+bwwyAQQAmkqdApHtWspZ
dNfqeEROxctZKLxdvtXBnaO1J1sS6jKjx2qGj3yxLRnW+N4QUAgm
+eNNsTrqZZjJUP526dOTK8RmxV4QJeh2Q0bsLPs6SXTlPwfBWPp
t+U/kfrSt8ZJF5lWR0jaiJG2hE3dBiuszPa+6cJUDuQnYCVCHZARCK
LcAEQEAAQPT8PBQW4y8b4C7BvhjnGAATQliwRajv6uWmfUFcI+
DPdtAZh3yb9EKWmS8vSkSnz+pWG1dEkuURyvBGJMDxs/FB+CM
ouTQejhA11Ho5tblas8HnoNPeQv1x9Xas+lrs1j2AmfrLWwKEQAu
H9di+d9DRU6YHxy1ocIHZELXR9ECsSP0C1iSeuJn+u4HLP3y4uBH
cGRdihLRIUSCJ0tXd2meRAxw4dsZllDAeb21i2Tj+l0SngTEzFj8fSu
vAxoXRv30gq5VLbH5WDbJah5n688THMAUIUC5dlG8MMXMgmU
e887lwKEqSvLqCk5ymHmCdZiJQQEpAxVbXb9bkKs2UhxN1zRnu
g4OcR411XOqlvlBwsk121yY7606mZ7r+icnXvLLEVezmegXsN8ml
hAnb+p629HPZSMFOSHgX3CwhIwTKDaMxZBft94Fk8w3l/NBuw
QJYg===Emf5
-----END PGP PRIVATE KEY BLOCK-----
```

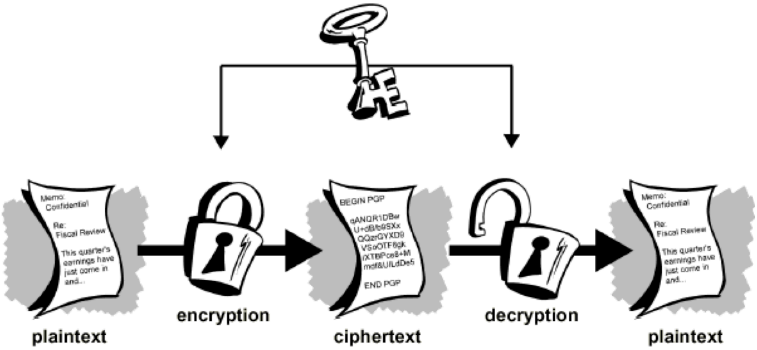
A 1024 bit RSA private key generated using the PGP (Pretty Good Privacy) digital signature and encryption software.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQCNBD5vDDEBBAC+UMHKr9YL1W0OYzL9gK/AERegEtzoFiv
eSzbeFQtNhxDIOSPJc60Y8v2nTecI0R5Y6Z55uzakcPBZmTJ+kW
rFR4NZPApiOFXhUrkHF0DmrmEpa5UpHjpO3sD+Hlvg84N6jHj
AIRMlNMAyrg/e4i6ABGzAuxYbJCs6ax9mxdrFAQARAQABtCBB
YmhpbmF2IEJoYXR0IDxhYkBhc2lhbmxhd3Mub3JnPokAtAQQA
QIAHgUCPm8MMQUJAeKFAAgLAwkIBwIBCgIZAQUbAwAAAAA
KCRDRPtuuStKFCIJwA/9t1Cjpi+hjVaWjJx1BZpoGv4b+t/Qb03J9
ABFUatbypUX5jmMmCUT7h3TgiCgT5F4imvijm4+uCDeoHz0Uj
+nPfvW8guMd805s/+3oU+FT4R2qYvEX6MAQVex67TJ0pHvmi
V55Mn/apNvTdvgSXJbQfHuza9u1QPEUm+LlVdOZx7kAjQQ+bw
wyAQQAmkqdApHtWspZdNfqeEROxctZKLxdvtXBnaO1J1sS6jKj
x2qGj3yxLRnW+N4QUAgm+eNNsTrqZZjJUP526dOTK8RmxV4Q
Jeh2Q0bsLPs6SXTlPwfBWPpt+U/kfrSt8ZJF5lWR0jaiJG2hE3dBi
uszPa+6cJUDuQnYCVCHZARCKLcAEQEAAYkAqAQYAQIAEgUCP
m8MMgUJAeKFAAUbDAAAAAAKCRDRPtuuStKFCADiA/0csZOS
Y9Ztyvw2iVSJqf9g4u3z+ePmEcwy2RK5tuOXU2p7HvEBMKeLlG
9Dxg0xwy7cVvHejjAn4LxMPG9j26TinLCAfqHs7C1og8an1tHstr
M4Icw7pWx5fIRLiqQLqEc/RVFLBKU3nMAjgu0E9wjHicWFwsx
UfeF5qD9kAsI0Og===klTT
-----END PGP PUBLIC KEY BLOCK-----
```

A 1024 bit RSA public key generated using the PGP (Pretty Good Privacy) digital signature and encryption software.

2.3 Symmetric Cryptography

In conventional cryptography, also called secret-key or symmetric-key encryption, the **same key is used both for encryption and decryption**. The figure below is an illustration of the conventional encryption process.



Symmetric Cryptography

[Image courtesy: An Introduction to Cryptography – PGP Corporation]

Caesar's Cipher

When Julius Caesar sent messages to his generals, he didn't trust his messengers. So he replaced every A in his messages with a D, every B with an E, and so on through the alphabet. Only someone who knew the "shift by 3" rule could decipher his messages.

For example, if we want to encode the word "SECRET" using Caesar's key value of 3, we offset the alphabet so that the 3rd letter down, (D), begins the alphabet.

So starting with
ABCDEFGHIJKLMNOPQRSTUVWXYZ

and sliding everything up by 3, you get DEFGHIJKLMNOPQRSTUVWXYZABC

where D=A, E=B, F=C, and so on.

Using this scheme, the plaintext, “SECRET” encrypts as “VHFUHW”. To allow someone else to read the cipher text, you tell him or her that the key is 3.

Key management and conventional encryption

Conventional encryption has certain benefits. It is **very fast**. It is especially useful for encrypting data that is not to be transmitted anywhere. So, if you want to store information so that no one can read it without your authorization, it would be a good idea to use conventional encryption.

For a sender and recipient to communicate securely using conventional encryption, they must **agree upon a key and keep it secret** between themselves. If they are in different physical locations, they must trust a courier or some other **secure communication medium.**

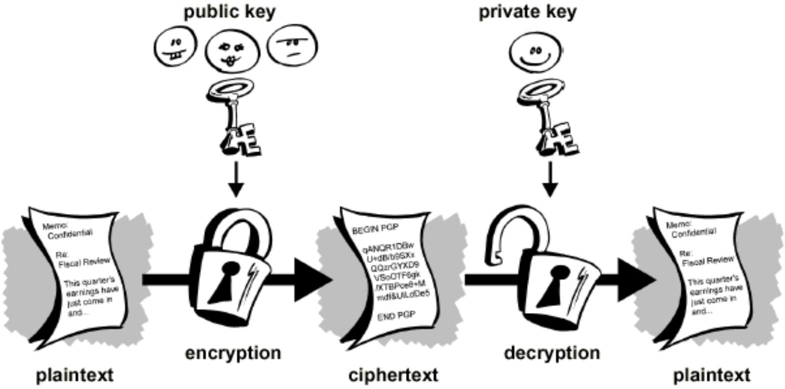
This is to prevent the disclosure of the secret key during transmission. Anyone who overhears or intercepts the key in transit can later read, modify, and forge all information encrypted or authenticated with that key. The persistent problem with conventional encryption is key distribution: how do you get the key to the recipient without someone intercepting it? The problems of key distribution in conventional encryption are solved by public key cryptography, a concept that was introduced by Whitfield Diffie and Martin Hellman in the U.S.A.

2.4 Asymmetric Cryptography

Public key cryptography is an asymmetric scheme that uses a pair of keys: a **public key**, which encrypts data, and a **corresponding private key**, or secret key for decryption.

Each user has a key pair with him. The public key is published to the world while the private key is kept secret. Anyone with a copy of the public key can then encrypt information that only the person having the corresponding private key can read.

It is **computationally infeasible to deduce the private key from the public key**. Anyone who has a public key can encrypt information but cannot decrypt it. Only the person who has the corresponding private key can decrypt the information. The figure below illustrates the process of asymmetric encryption.



Public key encryption - [Image courtesy: An Introduction to Cryptography – PGP Corporation]

The primary benefit of public key cryptography is that it allows people who have no pre-existing security arrangement to exchange messages securely. The need for sender and receiver to share secret keys via some secure channel is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared.

Some examples of public-key cryptosystems are ElGamal (named for its inventor, Taher ElGamal), RSA (named for its inventors, Ron **R**ivest, Adi **S**hamir, and Leonard **A**dleman), Diffie-Hellman (named for its inventors), and DSA, the Digital Signature Algorithm (invented by David Kravitz).

Because conventional cryptography was once the only available means for relaying secret information, the expense of secure channels and key distribution relegated its use only to those who could afford it, such as governments and large banks. Public key encryption is the technological revolution that provides **strong cryptography to the masses**.

The figure below illustrates a simple message.

Dear Sameer,

I am in town on the 11th of this month.

Will it be convenient for you to meet me at the Four Seasons restaurant for dinner?

Pooja

A simple message

The figure below illustrates the encrypted form of the message above.

```
hQCMAztC/6WmKod+AQQAiZmIDTpFg9nC5GmN4Azx2+0
JYo1C70Iux+IhhVvhGy9IA+BuURbxeqFroJPEl665fgAPrTH
HdAHV112eTFieH7BW+LaA0Rt4sLzxb077GJEh+e2wgMhK
kymi6RXYQvlXaswMELm7xVz/F6Kh8Q0MwHIt2jXUc8ayM
pw6i7AWAqKkkb86t2XBUfQNw03ZfFG3z7EZKB+a772HG
pM41MOYc7hY6rjwXHEwu5XtQC81SBAqDBUK9A4gh9dW
sCypB9y/k3LbpyhOGmmJJymG5PmbpLSXXyi7b6Js6ZNk7V
tjv2zrBZYjhvRpxCIu7uwC41KKn7gqsvD2fMXHqhgAyL/av
wkOSREEw/dstAc94zUeowvBlLg==tD2W
```

The encrypted form (using asymmetric encryption) of the message above.

2.5 Hash function

A one-way hash function takes variable-length input – say, a message of any length – and produces a fixed-length output; say, 160-bits. The hash function ensures that, if the information is changed in any way – even by just one bit – an entirely different output value is produced. The table below shows some sample output values using SHA (Standard Hash Algorithm).

sanya	c75491c89395de9fa4ed29affda0e4d29cbad290
SANYA	33fef490220a0e6dee2f16c5a8f78ce491741adc
Sanya	4c391643f247937bee14c0bcca9ffb985fc0d0ba

It can be seen from the table above that the hash value for **sanya** is

c75491c89395de9fa4ed29affda0e4d29cbad290

while the hash value for **SANYA** is

33fef490220a0e6dee2f16c5a8f78ce491741adc

By changing the input from **sanya** to **SANYA**, an entirely different hash value is generated. What must be kept in mind is that irrespective of the size of the input, the hash output will always be of the same size.

Two things must be borne in mind with regard to one-way hash functions:

1. It is computationally infeasible to find two different input messages that will yield the same hash output.

2. It is computationally infeasible to reconstruct the original message from its hash output.

2.6 Digital Signatures

A major benefit of public key cryptography is that it provides a method for employing digital signatures.

Digital signatures enable the recipient of the information to verify the authenticity of the information's origin, and also verify that the information is intact. Thus, **digital signatures provide authentication and data integrity**.

A digital signature also provides **non-repudiation**, which means that it prevents the sender from claiming that he or she did not actually send the information. These features are every bit as fundamental to cryptography as privacy, if not more. A digital signature serves the same purpose as a handwritten signature. However, a handwritten signature is easy to counterfeit. A **digital signature is superior to a handwritten signature** in that it is nearly impossible to counterfeit, plus it attests to the contents of the information as well as the identity of the signer.

Illustration

Sameer uses computer software to generate two keys, a public key and private key. These keys 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.

Sameer will give his public key to the whole world but will keep his private key to himself. Now, Sameer wants to enter into a transaction with Pankaj. He composes an electronic document containing the words

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

U ng his computer Sameer runs this document through a hash function.

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.

When using a particular hash function, the length of the output is always the same, whether the input document is one word or 1-lakh words.

Moreover, 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. That is why it is known as a one-way hash function.

Sameer 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.

Sameer 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 Sameer’s public key. When Pankaj receives Sameer’s email, he runs the original document through the hash function software and generates a hash result.

He compares this hash result with the one that was sent to him by Sameer. If the two hash results are the same, it means that the message is unaltered. Pankaj also verifies whether Sameer’s private key was actually used to sign the hash result. For this Pankaj’s computer uses Sameer’s public key. Only a message signed by Sameer’s private key can be verified using Sameer’s public key.

The public key and private key are basically two very large numbers that are mathematically related to each other. If a particular private key was used to “sign” a message, then only the corresponding public key will be able to verify the “signature”.

The digital signature creation and verification process achieves the following legal requirements:

1. **Signer authentication:** A person’s digital signature cannot be forged unless his private key is stolen. This means that if a digital signature can be verified by Sanya’s public key, then it must have been created by Sanya’s private key. The digital signature verification process thus authenticates the identity of the signer.

2. **Message authentication:** A digital signature is based upon the hash value (or message digest) of the actual message. Thus a digital signature is unique for each message and automatically authenticates the message.

3. **Affirmative act:** The process of digital signature creation requires the signer to use his private key (usually by entering a password). This overt act alerts the signer that he is initiating a transaction that may have legal consequences.

2.7 Digital Signature Certificates

Simply put, a digital signature certificate contains a public key as “certified” by a Certifying Authority (CA).

Let us take a simple illustration. Rohas Nagpal wants to digitally sign emails and electronic contracts. The first step he would take is to generate a private-public key pair. Once he has done that, he can use his private key to sign contracts etc. Anyone can use Mr. Nagpal’s public key to verify his signature. That’s where the problem begins.

How can anyone be sure which is Mr. Nagpal’s public key? What if Mr. Nagpal denies that a particular public key is actually his? To solve this problem digital signature certificates are used.

Mr. Nagpal would apply to a licenced CA for a digital signature certificate. As part of the application process he would submit identification documents (such as passport, PAN card etc). He would also send his public key to the CA. The CA would then “certify” the public key as belonging to Mr. Nagpal and issue a digital signature certificate that contains Mr. Nagpal’s public key along with information identifying him. The digital signature certificate is digitally signed by the CA and is legally recognised under the law.

Note: The detailed procedure for obtaining a digital signature certificate is discussed later in this book.

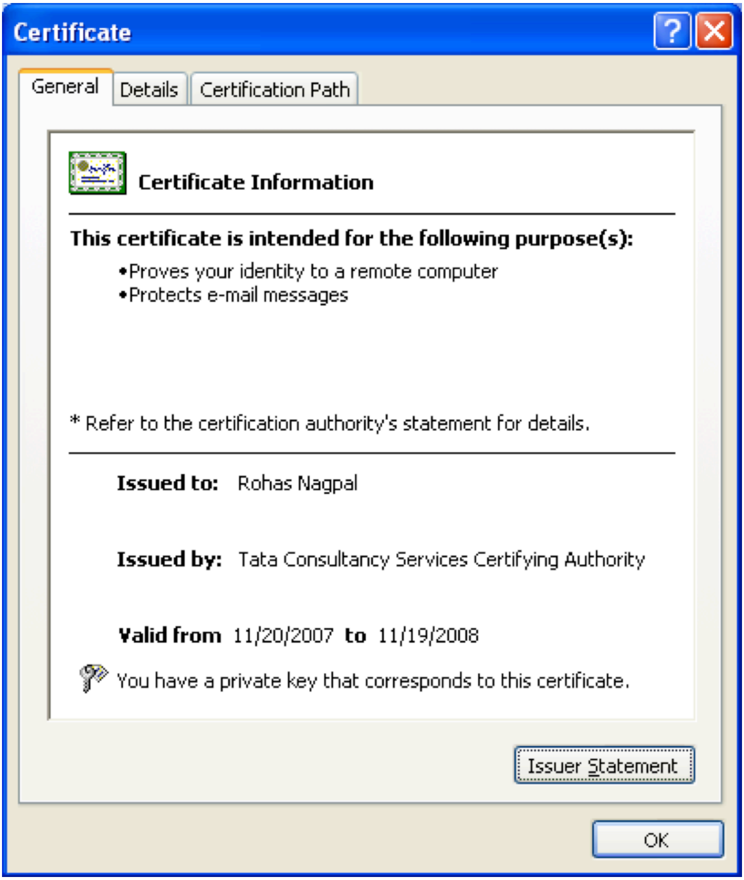
Let us now discuss the contents of a digital signature certificate in detail. For the purposes of this discussion we will discuss the **digital signature certificate issued to Mr. Rohas Nagpal** by the Tata Consultancy Services (TCS) CA.

To view digital signature certificates stored by default on your computer, you can open up the Microsoft Internet Explorer program and click on Tools → Internet Options → Content → Certificates option.

To make this section easy to understand, the language used is in the first person. References to "I", "me" etc refer to "Rohas Nagpal", the author of this book.

Let us discuss my digital signature certificate (DSC) in detail. I have been issued a DSC by TCS CA which is licenced by the Controller of Certifying Authorities of India. The DSC has been imported into my personal computer, which also has the Microsoft Internet Explorer program installed.

To view my DSC, I first open up the Microsoft Internet Explorer program and click on Tools → Internet Options Content → Certificates option.



Certificate Information

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

- Proves your identity to a remote computer
- Protects e-mail messages

* Refer to the certification authority's statement for details.

Issued to: Rohas Nagpal

Issued by: Tata Consultancy Services Certifying Authority

Valid from 11/20/2007 **to** 11/19/2008

You have a private key that corresponds to this certificate.

The first view of the DSC displays the **Certificate Information** which contains the following basic information:

1. Purposes for which the certificate is intended.
2. Person to whom it is issued.
3. Issuer of the certificate.
4. Validity period of the certificate.

As can be seen from figure 1, the certificate is intended to do the following:

1. Prove my identity to another computer
2. Protect email messages

The certificate is issued to me by Tata Consultancy Services Certifying Authority (TCS CA) and is valid from 20th November 2007 to 19th November 2008.

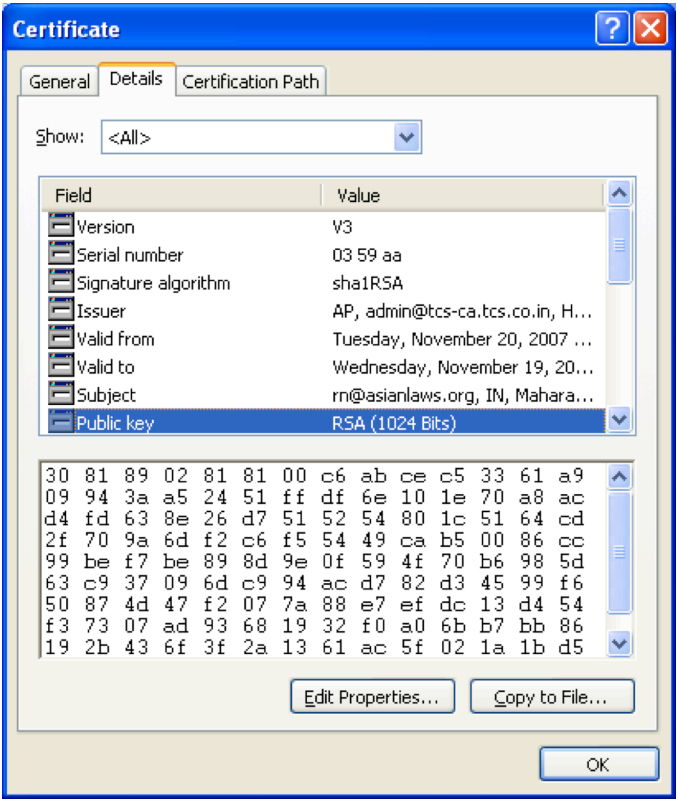
Please notice that the DSC states that "**You have a private key that corresponds to this certificate**". This is because the DSC is on my personal computer and my private key is also on this computer. If you were to download my DSC onto your computer, then this statement would not show up as your computer does not have my private key.

Clicking on the "Issuer Statement" button on the DSC opens up the **Relying Party Agreement** from the TCS website.

The Relying Party Agreement is an agreement between TCS CA and the person relying on a DSC (or verifying a DSC).

The agreement must be read along with the TCS-CA trust network certification practice statement (CPS) posted at the TCS-CA web site (https://www.tcs-ca.tcs.co.in) as amended from time to time.

Clicking on the **Details** tab, displays the certificate details.



Show: <All>

Field	Value
Version	V3
Serial number	03 59 aa
Signature algorithm	sha1RSA
Issuer	AP, admin@tcs-ca.tcs.co.in, H...
Valid from	Tuesday, November 20, 2007 ...
Valid to	Wednesday, November 19, 20...
Subject	rn@asianlaws.org, IN, Mahara...
Public key	RSA (1024 Bits)

```
30 81 89 02 81 81 00 c6 ab ce c5 33 61 a9
09 94 3a a5 24 51 ff df 6e 10 1e 70 a8 ac
d4 fd 63 8e 26 d7 51 52 54 80 1c 51 64 cd
2f 70 9a 6d f2 c6 f5 54 49 ca b5 00 86 cc
99 be f7 be 89 8d 9e 0f 59 4f 70 b6 98 5d
63 c9 37 09 6d c9 94 ac d7 82 d3 45 99 f6
50 87 4d 47 f2 07 7a 88 e7 ef dc 13 d4 54
f3 73 07 ad 93 68 19 32 f0 a0 6b b7 bb 86
19 2b 43 6f 3f 2a 13 61 ac 5f 02 1a 1b d5
```

Figure 2: Details

The following are some of the details of the certificate:

1. **Version:** This is stated as V3. This signifies that the DSC is based on the X509 version 3 technology standards.

2. **Serial number:** The serial number is a positive integer assigned by the CA to each DSC issued by it. This number is unique for each DSC issued by the CA. **Note:** “03 59 aa” is a hexadecimal number that corresponds to the decimal number 50696362

3. **Signature Algorithm:** This field identifies the mathematical algorithm used by the CA to sign the certificate [sha1RSA is this case]. **sha1** stands for Secure Hash Algorithm 1 while **RSA** stands for Rivest Shamir Adleman.

4. **Issuer:** This field identifies the CA who has issued this DSC. The table below summarizes the information as contained in the DSC and the brief explanation of what that information stands for.

Information on DSC	**Explanation**
S = AP	State = Andhra Pradesh
E = admin@tcs-ca.tcs.co.in	Email = admin@tcs-ca.tcs.co.in
L = Hyderabad	Location = Hyderabad
CN = Tata Consultancy Services Certifying Authority	Common Name = Tata Consultancy Services Certifying Authority
OU = TCS CA	Organizational-unit = TCS CA
O = India PKI	Organization = India PKI
C = IN	Country = India

5. **Valid From:** This indicates that the DSC is valid from 11:31:07 AM on Tuesday, November 20, 2007.

6. **Valid To:** This indicates that the DSC is valid till 11:31:07 AM on November 19, 2008.

7. **Subject:** The subject field identifies the person to whom this DSC has been issued by the CA – Rohas Nagpal in this case. The table below summarizes the information as contained in the DSC and the brief explanation of what that information stands for.

Information on DSC	**Explanation**
E = rn@asianlaws.org	Email = rn@asianlaws.org
C = IN	Country = India
S = Maharashtra	State = Maharashtra
L = Pune	Location = Pune
O = Tata Consultancy Services - Certifying Authority	Organisation = Tata Consultancy Services - Certifying Authority
OU = Class 3 Certificate	Organization Unit = Class 3 Certificate[1]
OU = Individual - Others	Organization Unit = Individual - Others[2]
OU = TCS-CA - Registration Authority	Organization Unit = TCS-CA - Registration Authority
CN = Rohas Nagpal	Common Name = Rohas Nagpal

[1] Class-3 Certificates are legally recognized digital signatures as per the IT Act, 2000.

[2] The basic options are Company user, Government user and Individual user. Under Individual user the options are Banking, Government and Others.

8. **Public Key:** This field specifies my public key (see below), the algorithm used by me to generate the key (RSA) and the key size (1024 bits)

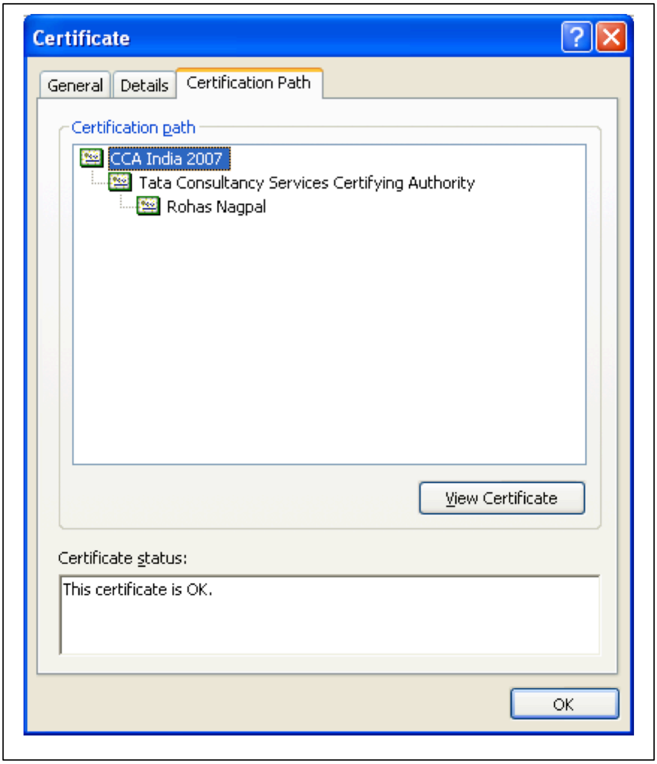
```
30 81 89 02 81 81 00 c6 ab ce c5 33 61 a9 09 94 3a a5 24 51 ff df 6e 10 1e 70
a8 ac d4 fd 63 8e 26 d7 51 52 54 80 1c 51 64 cd 2f 70 9a 6d f2 c6 f5 54 49 ca
b5 00 86 cc 99 be f7 be 89 8d 9e 0f 59 4f 70 b6 98 5d 63 c9 37 09 6d c9 94 ac
d7 82 d3 45 99 f6 50 87 4d 47 f2 07 7a 88 e7 ef dc 13 d4 54 f3 73 07 ad 93 68
19 32 f0 a0 6b b7 bb 86 19 2b 43 6f 3f 2a 13 61 ac 5f 02 1a 1b d5 52 e5 70 24
16 fa 5d 83 79 02 03 01 00 01
```

9. **CRL Distribution Points:** A certificate revocation list (CRL) is a list of serial numbers of those digital signature certificates which should not be relied upon because they:
    1. have been revoked, or
    2. are no longer valid.

    This field indicates the URL from where the relevant Certificate Revocation List can be downloaded, which in this case is-http://www.tcs-ca.tcs.co.in/crl_2785.crl

Clicking on the **Certification Path** tab, displays the certification path.

Figure 3: Certification Path

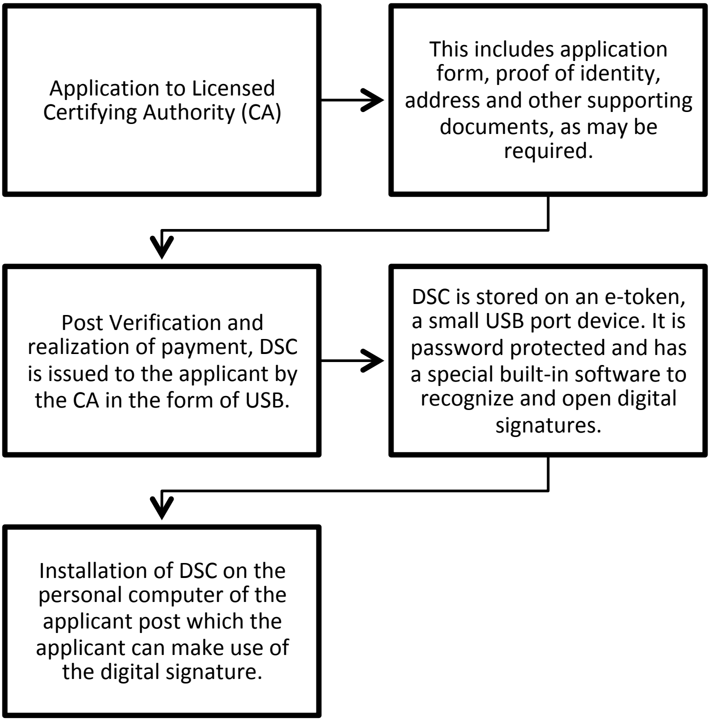


CCA India 2007
Tata Consultancy Services Certifying Authority
Rohas Nagpal

Certificate status:
This certificate is OK.

This shows that my digital signature certificate has been issued by TCS CA. It also shows that the TCS CA digital signature certificate has been issued by the Controller of Certifying Authorities.

2.8 How to acquire a digital signature certificate?



Application to Licensed Certifying Authority (CA)

This includes application form, proof of identity, address and other supporting documents, as may be required.

Post Verification and realization of payment, DSC is issued to the applicant by the CA in the form of USB.

DSC is stored on an e-token, a small USB port device. It is password protected and has a special built-in software to recognize and open digital signatures.

Installation of DSC on the personal computer of the applicant post which the applicant can make use of the digital signature.

2.9 Types of Digital Signature Certificates

Each class of digital signature certificate is associated with certain security features and reflects distinct levels of trust. The classes under which a digital signature certificate is issued are stated as below:-

Class 1 Certificate: Class 1 certificates are issued to individuals/private subscribers. These certificates confirm that the user's name and e-mail address form an unambiguous subject within the Certifying Authorities database.

Class 2 Certificate: These certificates are issued for both business and private purposes and can be issued to individuals or corporates. These certificates provide a higher level of assurance than Class 1 certificate. A Class 2 certificate is generally used for e-filings with authorities such as Ministry of Corporate Affairs and Income Tax. It is generally issued for a period of one to two years and can be renewed upon expiry.

Class 3 Certificate: This type of certificate can be issued to both individuals as well as organizations. As these have higher assurance certificates than Class 1 and Class 2 certificates, they are usually used for e-commerce applications such as e-tendering, patents and trademark filing, etc. It is generally issued for a period of one to two years and can be renewed upon expiry.

Class 3 digital signature certificate is issued under two categories - Individual User (Class 3A) and Authorized Professional of the company (Class 3B).

Aadhaar eKyc - OTP: Aadhaar OTP class of certificates are issued for individual use based on OTP authentication of subscriber through Aadhaar eKyc.

Aadhaar eKyc - biometric: Aadhaar biometric class of certificates are issued based on biometric authentication of subscriber through Aadhaar eKyc service.

The abovementioned Aadhaar based certificates confirm that the information in Digital Signature Certificate provided by the subscriber is same as information retained in the Aadhaar databases pertaining to the subscriber as Aadhaar holder.

THREE

3. Electronic & Digital Signatures - legal issues

The technical concepts relating to digital signatures have been discussed in detail in the previous chapter. Let us take an overview of this concept using a simple illustration.

Illustration

Sanya uses a digital signature software (e.g. PGP) installed on her computer, to generate a public and private key pair. Simply put, these keys are very large numbers.

She then stores her private key very securely on her computer. She uploads her public key to the website of a licensed certifying authority (CA). She also couriers a filled-in application form and photocopies of her passport and Income Tax PAN card to the CA.

After following some verification procedures, the CA sends Sanya a hardware device by post. This device contains Sanya's digital signature certificate. The digital signature certificate contains Sanya's public key along with some information about her and the CA. Sanya then has to accept her digital signature certificate.

All digital signature certificates are stored in the online repository maintained by the Controller of Certifying Authorities (e.g. at www.cca.gov.in)

Each Certifying Authority stores digital signature certificates issued by it in an online repository.

In order to digitally sign an electronic record, Sanya uses her private key.

In order to verify the digital signature, any person can use Sanya's public key (which is contained in her digital signature certificate).

In case Sanya had originally generated her private key on a smart card or USB Crypto Token then the subsequent signatures created by her would be **secure digital signatures**.

Note: The smart card / crypto token have a chip built into it, which has technology to enable the signing operation to happen in the device itself. The private key does not come out of the device in its original form.

In case Sanya had generated and stored her private key on a hard disk, floppy, CD, pen drive etc then subsequent signatures are not secure digital signatures.

The IT Act took a "technology dependent" approach to the issue of electronic authentication. This was done by specifying digital signatures as the means of authentication. Digital signatures are one type of technology coming under the wider term "electronic signatures".

The defect in this approach is that the law is bound by a specific technology, which in due course of time may be proven weak. The advantage of using a technology neutral approach is that if one technology is proven weak, others can be used without any legal complexities arising out of the issue.

> An example of this is the MD5 hash algorithm that at one time was considered suitable. MD5 was prescribed as suitable by Rule 6 of the Information Technology (Certifying Authorities) Rules, 2000[3].
>
> MD5 was subsequently proven weak by mathematicians. In fact, Asian School of Cyber Laws had filed a public interest litigation in the Bombay High Court on the same issue.
>
> Subsequently, the Information Technology (Certifying Authorities) Amendment Rules, 2009[4] amended the Rule 6 mentioned above and MD5 was replaced by SHA-2.

The Information Technology (Amendment) Act, 2008 amends the technology dependent approach and introduces the concept of electronic signatures in addition to digital signatures.

[3] "Rule 6. Standards.—The Information Technology (IT) architecture for Certifying Authorities may support open standards and accepted de facto standards; the most important standards that may be considered for different activities associated with the Certifying Authority's functions are as under:.....Digital Hash Function: MD5 and SHA-1.

[4] Gazette notification dated 5th August, 2009 issued by the Department of Information Technology, Ministry of Communications and Information Technology.

3.1 Authentication using digital signatures

<u>According to section 3 of the IT Act</u>

3. (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.

Let us examine some of the terms used in this section:

Subscriber is a person in whose name the Digital Signature Certificate is issued.

Authenticate means “to give legal validity to”, “establish the genuineness of”.

> **Illustration:** Pooja has issued a certificate stating that Sameer has been employed in her company for 3 years. Pooja affixes her digital signature to this certificate. Pooja has authenticated the certificate.

Electronic record means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.

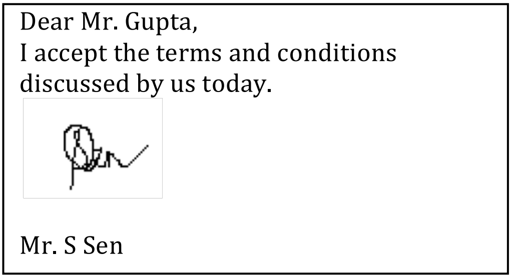
Affixing digital signature means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature.

Asymmetric crypto system is a system of using mathematically related keys to create and verify digital signatures. The key pair consists of a **private key** and a **public key**. The private key pair is used in conjunction with a one-way hash function to create digital signatures. The public key is used to verify the digital signatures created by the corresponding private key.

A one-way **hash function** takes variable-length input – say, a message of any length – and produces a fixed-length output; say, 160-bits. The hash function ensures that, if the information is changed in any way – even by just one bit – an entirely different output value is produced.

In interpreting this provision, the term "digital signature" must not be compared to "signature" in the conventional sense. This is because although **a person usually has one conventional handwritten signature for all messages**, he will have a **different digital signature for every message** that he signs.

Illustration: Mr. Sen writes a message as under:



Dear Mr. Gupta,
I accept the terms and conditions
discussed by us today.

Mr. S Sen

Figure 1: Conventionally signed message

Here, Mr. Sen's signature is as marked in the above message. Every document he signs will bear this signature.

However, his digital signature for this message could be

iQA/AwUBO0BCsFPnhMicaZh0EQJllgC
gt1qtfqazO2ppYNdZN685h2QtYQsAo
OgZ eH3gqHf5Tisz1C7tzvHC09zx
=g/BR

Figure 2: Digital Signature

Although his digital signature for the message in Figure 1 is as shown in Figure 2, his digital signature for any and every other message will be different.

E.g. if he changes the word “today” in the message in Figure 1 to “yesterday”, his digital signature for the new message could be:

```
iQA/AwUBO0BDdlPnhMicaZh0EQIOB
QCgiu0vAT47Q7VJsgeQYWU69OtV+M
MAoL772XDQBvzPYOKSWDS6wjucho
1T
```

Figure 3: New Digital Signature

What the law implies here is that a person may authenticate an electronic record by means of a digital signature, which is unique to the message being digitally signed.

The public key and private key are basically two very large numbers that are mathematically related to each other. If a particular private key was used to “sign” a message, then only the corresponding public key will be able to verify the “signature”.

The law also lays down that the private key and public key are unique to each subscriber. This implies that no two subscribers should have the same public and private key pair. This is practically achieved by using very large numbers (hundreds of digits) as keys. The probability of two persons generating the same key pair is thus extremely remote.

3.2 Authentication using electronic signatures

According to section 3A of the IT Act

3A. Electronic Signature.-
(1) Notwithstanding anything contained in section 3, but subject to the provisions of sub-section (2), a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which –

(a) is considered reliable; and

(b) may be specified in the Second Schedule.

(2) For the purposes of this section any electronic signature or electronic authentication technique shall be considered reliable if –

(a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and to no other person;

(b) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;

(c) any alteration to the electronic signature made after affixing such signature is detectable;

(d) any alteration to the information made after its authentication by electronic signature is detectable; and

> *(e) it fulfils such other conditions which may be prescribed.*
>
> *(3) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated.*
>
> *(4) The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the Second Schedule:*
>
> *Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable.*
>
> *(5) Every notification issued under sub-section (4) shall be laid before each House of Parliament.*

Electronic signature is a wide term that includes various methods. According to UNCITRAL[5], electronic authentication and signature methods may be classified into the following categories:

1. those based on the knowledge of the user or the recipient (e.g. passwords, personal identification numbers (PINs)),

[5] UNCITRAL publication titled "Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods".

2. those based on the physical features of the user (e.g. biometrics),
3. those based on the possession of an object by the user (e.g. codes or other information stored on a magnetic card),

4. types of authentication and signature methods that, without falling under any of the above categories, might also be used to indicate the originator of an electronic communication (such as a facsimile of a handwritten signature, or a name typed at the bottom of an electronic message).

According to the UNCITRAL Model Law on Electronic Signatures, technologies currently in use include:

1. digital signatures within a public key infrastructure (PKI),

2. biometric devices,

3. PINs,

4. user-defined or assigned passwords,

5. scanned handwritten signatures,

6. signature by means of a digital pen,

7. clickable "OK" or "I accept" boxes,

8. hybrid solutions based on a combination of different technologies.

3.3 Secure electronic & digital signature

According to section 15 of the IT Act, a secure digital signature should satisfy the following conditions:

1. **It should be unique to the subscriber affixing it.** A digital signature is unique and is based upon the message that is signed and the private key of the signer.

2. **It should be capable of identifying such subscriber.** What this implies is that the digital signature should be verifiable by the public key of the signer and by no other public key.

3. **It should be created in a manner or using a means under the exclusive control of the subscriber.** This implies that the signer must use hardware and software that are completely free of any unauthorized external control.

4. **It should be linked to the electronic record to which it relates in such a manner that if the electronic record were altered, the digital signature would be invalidated.** All standard software programs used to create digital signatures contain this feature. Without this feature, the whole purpose of creating digital signatures would be defeated.

According to notification G.S.R. 735 (E), notified by the Central Government on the 29th of October, 2004, a secure digital signature is one to which the following security procedure has been applied:

(a) a **smart card**[6] or **hardware token**[7], as the case may be, with **cryptographic module**[8] in it, is used to create the key pair;

(b) the private key used to create the digital signature always remains in the smart card or hardware token as the case may be;

(c) the hash of the content to be signed is taken from the host system to the smart card or hardware token and the private key is used to create the digital signature and the signed hash is returned to the host system;

(d) the information contained in the smart card or hardware token, as the case may be, is solely under the control of the person who is purported to have created the digital signature;

(e) the digital signature can be verified by using the public key listed in the Digital Signature Certificate issued to that person;

(f) the standards referred to in rule 6 of the Information Technology (Certifying Authorities) Rules, 2000 (as amended from time to time) have been complied with, in so far as they relate to the creation, storage and transmission of the digital signature; and

(g) the digital signature is linked to the electronic record in such a manner that if the electronic record was altered the digital signature would be invalidated.

[6] a device containing one or more integrated circuit chips.

[7] means a token which can be connected to any computer system using a Universal Serial Bus (USB) port.

[8] This can be understood as the software, e.g., PGP, used to generate the key pair used for creating and verifying a digital signature.

This section has been amended by the Information Technology (Amendment) Act, 2008. Accordingly, an electronic signature shall be deemed to be a secure electronic signature if –

a. the **signature creation data**, at the time of affixing signature, was under the exclusive control of signatory and no other person; and

b. the signature creation data was stored and affixed in such exclusive manner as may be prescribed.

The signature creation data is basically the data using which the signature is created e.g. in case of a digital signature, the "signature creation data" means the private key of the subscriber. In case of a 'biometric signature', the signature creation data may be the retina or fingerprint of the person.

3.4 Digital Signature Certificates

Any person can make an application[9] to the Certifying Authority (CA) for the issue of a Digital Signature Certificate. The Information Technology (Amendment) Act, 2008 has amended the Information Technology Act, 2000 so that most of the provisions relating to digital signatures now apply to electronic signatures also.

Each application is required to be accompanied by:

1. The prescribed fee (not exceeding twenty-five thousand rupees) to be paid to the CA.[10]
2. A certification practice statement or a statement containing specified particulars[11].

On receipt of an application the Certifying Authority may grant the Digital Signature Certificate or for reasons to be recorded in writing, reject the application.

A Digital Signature Certificate cannot be granted unless the Certifying Authority is satisfied that:

1. The applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate,

2. The applicant holds a private key, which is capable of creating a digital signature,

[9] Schedule IV of the Information Technology (Certifying Authorities) Rules, 2000 prescribes the form for this.

[10] Different fees may be prescribed for different classes of applicants.

[11] As per Executive order dated 12th September 2002 issued by Ministry of Communications and Information Technology, every application for the issue of a Digital Signature Certificate shall not be required to be accompanied by a certification practice statement.

3. The public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant.

The Certifying Authority cannot reject an application unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

Representations upon issuance of Digital Signature Certificate

While issuing a Digital Signature Certificate a Certifying Authority must certify that:

1. It has complied with the provisions of the IT Act and allied rules.

2. It has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it.

3. The subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate.
4. The subscriber's public key and private key constitute a functioning key pair.

5. The information contained in the Digital Signature Certificate is accurate.

6. It has no knowledge of any material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the representations made in (1) to (4) above.

Suspension of Digital Signature Certificate

The Certifying Authority, which has issued a Digital Signature Certificate, may suspend such Digital Signature Certificate:

1. on a request from the subscriber listed in the Digital Signature Certificate,

2. on a request from any person duly authorized to act on behalf of that subscriber,

3. if it is of the opinion that the Certificate should be suspended in public interest.

A Digital Signature Certificate cannot be suspended for a period exceeding 15 days unless the subscriber has been given an opportunity of being heard in the matter.

On suspension of a Digital Signature Certificate the Certifying Authority shall communicate the same to the subscriber.

Revocation of Digital Signature Certificate

A Certifying Authority can revoke a Certificate issued by it on the:

1. request of the subscriber, or

2. request of any person authorized by him, or

3. upon the death, dissolution or winding up of the subscriber.

A Certifying Authority may revoke a Digital Signature Certificate issued by it at any time, if it is of the opinion that:

1. a material fact represented in the Digital Signature Certificate is false or has been concealed,

2. a requirement for issuance of the Digital Signature Certificate was not satisfied,

3. the Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability,

4. the subscriber has been declared insolvent or dead, has been dissolved, wound-up or otherwise ceased to exist.

A Digital Signature Certificate may not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

On revocation of a Digital Signature Certificate under this section, the Certifying Authority is required to communicate the same to the subscriber.

Notice of suspension or revocation

In case of suspension or revocation of a digital signature certificate, the Certifying Authority is required to publish a notice of such suspension or revocation in the repository specified in the Digital Signature Certificate for publication of such notice.

Where more than one repository has been specified, the Certifying Authority will publish notices of such suspension or revocation in all such repositories.

3.5 Duties of subscribers

Generating key pair

A subscriber must apply relevant security procedure while generating his key pair. The key pair consists of the private key and the public key.

The public key will be sent to the Certifying Authority for inclusion in the subscriber's Digital Signature Certificate.

Acceptance of Digital Signature Certificate

A subscriber is deemed to have accepted a Digital Signature Certificate if:

1. He publishes the certificate to others or to a repository.

2. He authorises the certificate's publication to others or to a repository.

3. He demonstrates his approval of the Digital Signature Certificate in any manner.

Upon accepting a Digital Signature Certificate the subscriber certifies that:

- ✓ He holds the private key corresponding to the public key listed in the Certificate and is entitled to hold the same,

- ✓ All representations made by him to the Certifying Authority and all material relevant to the information contained in the Certificate are true

- ✓ All information in the Certificate is true to the best of his knowledge.

Control of private key

Every subscriber is required to:

1. Exercise reasonable care to retain control of his private key.

2. Take all steps to prevent its disclosure to an unauthorized person.

If this private key has been compromised, then, the subscriber is required to communicate the same without any delay to the Certifying Authority in the prescribed manner.

The subscriber is liable till he has informed the Certifying Authority that his private key has been compromised.

3.6 Regulation of Certifying Authorities

The IT Act empowers the Controller of Certifying Authorities to regulate licenced Certifying Authorities in India.

<u>Appointment of Controller and other officers</u>

The Central Government is empowered to appoint:

1. A Controller of Certifying Authorities,

2. Deputy Controllers, and

3. Assistant Controllers.

   The Controller is required to discharge his functions subject to the general control and directions of the Central Government.

   The Deputy Controllers and Assistant Controllers are required to function under the general superintendence and control of the Controller.

The Central Government is also empowered to prescribe the:

1. qualifications, experience & terms and conditions of service of the Controller, Deputy Controllers and Assistant Controllers,

2. places where the Head Office and Branch Office of the office of the Controller are to be located.

Functions of Controller

The Controller is empowered to supervise the activities of the Certifying Authorities (CAs), certify their public keys, lay down the standards to be maintained by them and specify the qualifications and experience, which their employees should possess. The Controller is empowered to specify the following:

1. The conditions subject to which the CAs should conduct their business,
2. The contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key,
3. The form and content of a Digital Signature Certificate and the key,
4. The form and manner in which accounts are required to be maintained by the CAs,
5. The manner in which the CAs are to conduct their dealings with the subscribers, and
6. The terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them.

The Controller is also empowered to:

1. facilitate the establishment of any electronic system by a CA (solely or jointly),
2. to regulate such systems,
3. resolve any conflict of interests between the CAs and the subscribers,
4. lay down the duties of the CAs and
5. maintain a database of disclosure records of every CA[12].

[12] This database may contain particulars accessible to the public.

Recognition of foreign certifying authorities

The Controller is authorised to recognize any foreign Certifying Authority as a Certifying Authority for the purposes of the IT Act. However, such approval:

- ✓ requires the previous approval of the Central Government, and
- ✓ is required to be notified in the Official Gazette.

The Digital Signature Certificate issued by a recognized foreign Certifying Authority will be valid for the purposes of the IT Act.

If the recognized foreign Certifying Authority contravenes any of the conditions and restrictions subject to which it was granted recognition, the Controller is empowered to revoke such recognition. The reasons for such revocation are required to be recorded in writing and the revocation is required to be notified in the Official Gazette.

Controller to act as repository

The Controller is the repository of all Digital Signature Certificates issued under the IT Act. To ensure the secrecy and security of the digital signatures, the Controller is required to:

1. make use of hardware, software and procedures that are secure from intrusion and misuse,
2. observe standards prescribed by the Central Government.

The Controller is also required to maintain a computerized database of all public keys. This database should be maintained in such a manner that the public keys are available to any member of the public. This provision is removed by the Information Technology (Amendment) Act, 2008.

License to issue Digital Signature Certificates

A Certifying Authority can make an application, to the Controller, for a license to issue Digital Signature Certificates in India. The person making such an application is required to fulfil the requirements prescribed by the Central Government[13]. Such a license will be:

1. valid for a prescribed period[14],

2. will not be transferable or heritable and

3. will be subject to specified terms and conditions.

Application for license

The application is required to be in prescribed form[15] and is to be accompanied by:

1. a certification practice statement,
2. a statement including the procedures with respect to identification of the applicant,
3. a prescribed fee,[16]
4. other prescribed documents.[17]

[13] See the Information Technology (Certifying Authorities) Rules, 2000

[14] This period is 5 years as per Rule 13(1) of the Information Technology (Certifying Authorities) Rules, 2000

[15] The form is provided in Schedule I of the Information Technology (Certifying Authorities) Rules, 2000

[16] The maximum fees is Rs. 25,000 under Rule 11 of the Information Technology (Certifying Authorities) Rules, 2000

Renewal of license

Section 23 provides that an application for renewal of a license must be:

1. in the prescribed form,
2. accompanied by the prescribed fees,[18]
3. made not less than 45 days before the expiry of the license.

Procedure for grant or rejection of license

The Controller is empowered to grant the license or reject the application after considering the documents accompanying the application and such other factors, as he deems fit. However, no application can be rejected unless the applicant has been given a reasonable opportunity of presenting his case.

Suspension of license

The Controller may revoke the license of a Certifying Authority if he is satisfied (after due inquiry) that the Certifying Authority has:

1. made a false or incorrect statement in, or in relation to, the application for the issue or renewal of the license,

[17] See Rule 10 of the Information Technology (Certifying Authorities) Rules, 2000

[18] Rs. 5,000 as per Rule 11 of the Information Technology (Certifying Authorities) Rules, 2000

2. failed to comply with the terms and conditions subject to which the license was granted,

3. failed to maintain the specified standards,[19]

4. contravened any provisions of the IT Act or allied rules, regulations or orders.

However, no license can be revoked unless the Certifying Authority has been given a reasonable opportunity of **showing cause** against the proposed revocation.

The Controller may suspend the license of a Certifying Authority pending the completion of any inquiry ordered by him. However, no license can be suspended for a period exceeding ten days unless the Certifying Authority has been given a **reasonable opportunity** of showing cause against the proposed suspension.

The Certifying Authority whose license has been suspended **cannot issue** any Digital Signature Certificate during such suspension.

Notice of suspension or revocation of license

Section 26 deals with the notice of suspension or revocation of license. Where the license of the Certifying Authority is suspended or revoked, the Controller is required to publish notice of such suspension or revocation in the database maintained by him.

In the event that one or more repositories are specified, the Controller is required to publish notices of such suspension (or revocation) in all such repositories. The database

[19] These standards are prescribed under section 20(2)(b) of the IT Act.

containing the notice of such suspension (or revocation) is to be made available through a web site accessible round the clock. The Controller may publicize the contents of the database in appropriate electronic or other media.

Power to delegate

The Controller is authorised to delegate any of his powers to the Deputy Controller, Assistant Controller or any officer.

Access to computers and data

The IT Act contains provisions relating to access to computers and data in the event that the Controller (or any person authorized by him) has reasonable cause to suspect that any **contravention** of the provisions of the IT Act (or allied rules or regulations) has been committed.

In such cases, the Controller can have **access** to any computer system for obtaining any information or data contained in the computer system.

The Controller may order any person in charge of the computer system to provide him with the necessary reasonable **technical and other assistance**.

Certifying Authority to follow certain procedures

Certifying Authorities are required to:

1. make use of hardware, software and procedures that are secure from intrusion and misuse,

2. provide a reasonable level of reliability in their services which are reasonably suited to the performance of intended functions,

3. adhere to security procedures to ensure that the secrecy and privacy of the digital signature are assured, and

4. observe other specified standards.

Certifying Authority to ensure compliance with the IT Act, etc.

Every person employed or engaged by a Certifying Authority should **comply with the provisions of the IT Act** (and allied rules) in the course of his employment or engagement.

Display of license

Every Certifying Authority is required to **display it's license** at a conspicuous place of the premises in which it carries on it's business.

Surrender of license

Every CA whose license is suspended or revoked is required to immediately surrender the license to the Controller. Failure to surrender a license is an offence punishable with **imprisonment** up to 6 months and / or **fine** up to Rs 10,000.

Disclosure

Every Certifying Authority is required to disclose the following in the prescribed manner:

1. its Digital Signature Certificate which contains its public key corresponding to the private key used by it to digitally sign another Digital Signature Certificate,

2. certification practice statement,

3. notice of the revocation or suspension of its Certifying Authority certificate, if any,

4. any other fact that materially and adversely affects either the reliability of a Digital Signature Certificate, which it has issued, or its ability to perform its services.

5. if any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Digital Signature Certificate was granted, then, the Certifying Authority must:

   - use reasonable efforts to notify any person who is likely to be affected by that occurrence, or

   - act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

3.7 Certifying Authority (Procedure Rules)

The Information Technology (Certifying Authorities) Rules, 2000 were published in the Official Gazette on 17th October, 2000 and have come into force from that date.

Rule 3 provides for the use of public key cryptography to authenticate information by means of digital signatures. **Rule 4** and **Rule 5** contain provisions relating to the creation and verification of digital signatures.

Rule 6 lays down that the Information Technology (IT) architecture for Certifying Authorities may support open standards and accepted de facto standards. It also provides the most important standards that may be considered for different activities associated with the Certifying Authority's functions.

These are as under:

1. Public Key Infrastructure - PKIX

2. Digital Signature Certificates and Digital Signature revocation list - X.509. version 3 certificates as specified in ITU RFC 1422

3. Directory (DAP and LDAP) - X500 for publication of certificates and Certification Revocation Lists (CRLs)

4. Database Management Operations - Use of generic SQL

5. Public Key algorithm - DSA and RSA

6. Digital Hash Function - SHA-2 [earlier it was MD-5 and SHA-1]

7. RSA Public Key Technology - PKCS#1 RSA Encryption Standard (512, 1024, 2048 bit), PKCS#5 Password Based Encryption Standard, PKCS#7 Cryptographic Message Syntax standard, PKCS#8 Private Key Information Syntax standard, PKCS#9 Selected Attribute Types, PKCS#10 RSA Certification Request, PKCS#12 Portable format for storing/transporting a user's private keys and certificates.

8. Distinguished name - X.520

9. Digital Encryption and Digital Signature - PKCS#7

10. Digital Signature Request Format - PKCS#10

Rule 7 provides for the conformance of Digital Signature Certificates to the ITU X.509 version 3 standard. All Digital Signature Certificates are required to contain the following information:

1. Serial number assigned by Certifying Authority to distinguish it from other certificates,

2. Signature Algorithm Identifier, which identifies the algorithm used by Certifying Authority to sign the digital signature certificate,

3. Name of the Certifying Authority who issued the Digital Signature Certificate,

4. Validity period of the Digital Signature Certificate,

5. Name of the subscriber whose public key the Certificate identifies,

6. Public key information of the subscriber.

Rule 8 lays down detailed provisions relating to the licensing of certifying authorities. Indian citizens having a capital of five crores of rupees or more and companies having paid up capital of not less than five crores of rupees or net worth of at least rupees fifty crores, may apply for grant of a license to issue Digital Signature Certificates.

Companies in which the equity share capital held in aggregate by the Non-resident Indians, Foreign Institutional Investors, or foreign companies, exceeds forty-nine per cent of the capital, shall not be eligible for grant of license.

In case a newly formed company (whose main object is to act as Certifying Authority) applies for grant of license, the net worth referred to above will be the aggregate net worth of its majority shareholders holding at least 51% of paid equity capital, being Hindu Undivided Families, firms or companies. These majority shareholders shall not include Non-resident Indian, foreign national, Foreign Institutional Investor and foreign company.

The majority shareholders are restricted from selling or transferring equity shares unless the company acquires or has its own net worth of not less than fifty crores of rupees. In other cases, the prior approval of the Controller must be acquired for selling or transferring shares.

A firm having capital subscribed by all partners of not less than five crores of rupees or net worth of not less than fifty crores of rupees may also apply for grant of a license to issue Digital Signature Certificates. Firms in which the capital held in aggregate by any Non-resident Indian, and foreign national, exceeds forty-nine per cent of its capital, will not be eligible for grant of license.

In the case of a firm that has been registered under the Indian Partnership Act during the preceding financial year or in the financial year during which it applies for grant of license and whose main object is to act as Certifying Authority, the net worth referred to above will be the aggregate net worth of all of its partners (not including non-resident Indians and foreign nationals).

These partners are restricted from selling and transferring capital held in the firm. They can do so if the firm has acquired or has its own net worth of not less than fifty crores of rupees. In other cases, the prior approval of the Controller will be needed.

The Central Government or any State Government or any of the Ministries or Departments, Agencies or Authorities of such Governments can also apply for grant of a license to issue Digital Signature Certificates.

Applicants are required to submit a performance bond or furnish a banker's guarantee from a scheduled bank in favour of the Controller for an amount of not less than rupees five crores. The performance bond or banker's guarantee will remain valid for a period of six years from the date of its submission.

Companies and firms having net worth of rupees 50 crore and above but not having paid up capital of Rs 5 crore or more are required to submit a performance bond or furnish a banker's guarantee for rupees ten crores.

This bond or guarantee may be invoked on suspension of the license, for payment of an offer of compensation made by the Controller, for payment of liabilities and rectification costs attributed to the negligence of the Certifying Authority or its employees, for payment of the costs incurred in the discontinuation or transfer of operations of the licensed Certifying Authority, or for any other default made by the Certifying Authority.

Rule 9 provides that the infrastructure associated with all functions of generation, issue and management of Digital Signature Certificates as well as maintenance of Directories containing information about the status, and validity of Digital Signature Certificates will be installed at any location in India.

Rule 10 provides that every application for a licensed Certifying Authority must be made to the Controller in the prescribed form. The documents and information required to be submitted along with the form include:

1. A Certification Practice Statement (CPS),

2. A statement including the procedures with respect to identification of the applicant,

3. A statement for the purpose and scope of anticipated Digital Signature Certificate technology, management, or operations to be outsourced,

4. Certified copies of the business registration documents

5. A description of any event, particularly current or past insolvency, that could materially affect the applicant's ability to act as a Certifying Authority;

6. An undertaking by the applicant that to the best of its knowledge and belief it can and will comply with the requirements of its Certification Practice Statement;

7. An undertaking that the Certifying Authority's operation would not commence until its operation and facilities associated with the functions of generation, issue and management of Digital Signature Certificates are audited by the auditors and approved by the Controller,

8. An undertaking to submit a performance bond or banker's guarantee within one month of the Controller indicating his approval for the grant of license.

Rule 11 provides for a non-refundable fee of twenty-five thousand rupees to be paid along with the application for grant of license. For renewal of license a non-refundable fee of five thousand rupees is payable. The fee is not refundable in the event of suspension or revocation of the license.

Licensed Certifying Authorities are required to have arrangements for cross certification with other licensed Certifying Authorities within India. Such arrangements have to be submitted to the Controller before the commencement of operations.

Rule 12 provides that any dispute arising as a result of an arrangement between the Certifying Authorities or between the Certifying Authority and the subscriber must be referred to the Controller for arbitration or resolution.

Provisions relating to licensing, location of facilities, submission of application, fee, cross certification and validity of license shall also apply in the case of an application for renewal of a license. An application for renewal of license is required to be submitted not less than forty-five days before the date of expiry of the period of validity of license and may be submitted in the form of electronic record.

Rule 13 lays down that the license issued to a certifying authority will be valid for a period of 5 years from the date of issue and that the license is not transferable.

Rule 14 empowers the Controller to suspend the license in accordance with the provisions of section 25(2) of the IT Act.

Rule 15 contains provisions relating to renewal of the licence of a certifying authority. A certifying authority is required to submit an application for the renewal of its licence at least 45 days prior to the expiry of the validity period of the licence.

Rule 16 contains provisions relating to Issuance of Licence. The Controller may, within four weeks from the date of receipt of the application grant or renew the licence or reject the application. This period of 4 weeks may be extended to a maximum of eight weeks under special circumstances.

On approval of the application the applicant will be required to submit the performance bond or banker's guarantee within one month from the date of such approval and execute an agreement with the Controller binding himself to comply with the terms and conditions of the licence and the provisions of the Act and the allied rules.

Rule 17 empowers the Controller to refuse to grant or renew a licence if-

1. The applicant has not provided the Controller with such information relating to its business, and to any circumstances likely to affect its method of conducting business, as the Controller may require; or

2. The applicant is in the course of being wound up or liquidated; or

3. A receiver and / or manager have been appointed by the court in respect of the applicant; or

4. The applicant or any trusted person has been convicted, whether in India or out of India, of an offence the conviction for which involved a finding that it or such trusted person acted fraudulently or dishonestly, or has been convicted of an offence under the IT Act or rules framed thereunder; or

5. The Controller has invoked performance bond or banker's guarantee; or

6. A Certifying Authority commits breach of, or fails to observe and comply with, the procedures and practices as per the Certification Practice Statement; or

7. A Certifying Authority fails to conduct, or does not submit, the returns of the audit in accordance with rule 31; or

8. The audit report recommends that the Certifying Authority is not worthy of continuing Certifying Authority's operation; or

9. A Certifying Authority fails to comply with the directions of the Controller.

Rule 18 lays down that the Certification Practice Statement of the Certifying Authority will comply with and be governed by Indian laws.

Rule 19 lays down the security guidelines for Certifying Authorities. Certifying Authorities have the sole responsibility of integrity, confidentiality and protection of information and information assets employed in its operation, considering classification, declassification, labelling, storage, access and destruction of information assets according to their value, sensitivity and importance of operation.

The Information Technology Security Guidelines and Security Guidelines for Certifying Authorities aimed at protecting the integrity, confidentiality and availability of service of Certifying Authority are prescribed.

Certifying Authorities shall formulate their own Information Technology and Security Policy, for operation, complying with the guidelines, and submit them to the Controller before commencement of operation. Any change made by the Certifying Authority in the Information Technology and Security Policy is required to be submitted by it within two weeks to the Controller.

Rule 20 provides that the licensed Certifying Authority will not commence commercial operation of generation and issue of Digital Signature Certificates before –

1. confirming to the Controller the adoption of Certification Practice Statement,

2. generation of its key pair,

3. audit of installation of facilities and infrastructure associated with all functions of generation, issue and management of Digital Signature Certificate,

4. submission of the arrangement for cross certification with other licensed Certifying Authorities within India to the Controller.

Rule 21 contains provisions relating to the requirements prior to cessation as Certifying Authority. Before ceasing to act as a Certifying Authority, a Certifying Authority is required to give notice to the Controller of its intention to cease acting as a Certifying Authority. The notice has to be made ninety days before ceasing to act as a Certifying Authority or ninety days before the date of expiry of licence.

The Certifying Authority is also required to advertise his intention sixty days before the expiry of licence or ceasing to act as Certifying Authority in daily newspapers or newspapers specified by the Controller. The Certifying Authority is also required to notify its intention to the subscriber and Cross Certifying Authority of each unrevoked or unexpired Digital Signature Certificate issued by it.

The notice is required to be given sixty days before ceasing to act as a Certifying Authority or sixty days before the date of expiry of unrevoked or unexpired Digital Signature Certificate, as the case may be. The notice is required to be sent to the Controller, affected subscribers and Cross Certifying Authorities by digitally signed e-mail and registered post.

The Certifying Authority is also required to revoke all Digital Signature Certificates that remain unrevoked or unexpired at the end of the ninety days' notice period. Such revocation is required irrespective of whether or not the subscribers have requested revocation.

The Certifying Authority is required to make a reasonable effort to ensure that discontinuing its certification services causes minimal disruption to its subscribers and to persons duly needing to verify digital signatures by reference to the public keys contained in outstanding Digital Signature Certificates.

The Certifying Authority is also required to make reasonable arrangements for preserving the records for a period of seven years and to pay reasonable restitution (not exceeding the cost involved in obtaining the new Digital Signature Certificate) to subscribers for revoking the Digital Signature Certificates before the date of expiry.

After the date of expiry mentioned in the licence, the Certifying Authority is required to destroy the certificate–signing private key and confirm the date and time of destruction of the private key to the Controller.

Rule 22 provides that the Controller has to maintain a database of the disclosure record of every Certifying Authority, Cross Certifying Authority and Foreign Certifying Authority. This database is required to contain the following details:

1. The name of the person / Directors, nature of business, Income-tax Permanent Account Number, web address, if any, office and residential address, location of facilities associated with functions of generation of Digital Signature Certificate, voice and facsimile telephone numbers, electronic mail address(es), administrative contacts and authorized representatives;

2. The public key(s), corresponding to the private key(s) used by the Certifying Authority and recognized foreign Certifying Authority to digitally sign Digital Signature Certificate;

3. Current and past versions of Certification Practice Statement of Certifying Authority;

4. Time stamps indicating the date and time of -

- Grant of licence;

- Confirmation of adoption of Certification Practice Statement and its earlier versions by Certifying Authority;

- Commencement of commercial operations of generation and issue of Digital Signature Certificate by the Certifying Authority;

- Revocation or suspension of licence of Certifying Authority;

- Commencement of operation of Cross Certifying Authority;

- Issue of recognition of foreign Certifying Authority;

- Revocation or suspension of recognition of foreign Certifying Authority.

Rule 23 says that the Digital Signature Certificate can be granted only after a Digital Signature Certificate application in the form provided by the Certifying Authority has been submitted by the subscriber to the Certifying Authority and the same has been approved by it. The application form is required to contain the prescribed particulars.

The rule further says that no interim Digital Signature Certificate can be issued and that the Digital Signature Certificate must contain one or more repositories in which revocation or suspension of the Digital Signature Certificate will be listed, if the Digital Signature Certificate is suspended or revoked.

The subscriber identity verification method employed for issuance of Digital Signature Certificate is required to be specified in the Certification Practice Statement of the Certifying Authority.

The rule contemplates situations where a new Digital Signature Certificate is issued to a person on the basis of another valid Digital Signature Certificate held by that person.

If subsequently the older Digital Signature Certificate has been suspended or revoked, the Certifying Authority that issued the new Digital Signature Certificate is required to conduct investigations to determine whether it is necessary to suspend or revoke the new Digital Signature Certificate.

The Certifying Authority is required to provide a reasonable opportunity for the subscriber to verify the contents of the Digital Signature Certificate before it is accepted.

Once a subscriber accepts the issued Digital Signature Certificate, the Certifying Authority is required to publish a signed copy of the Digital Signature Certificate in a repository.

If the Digital Signature Certificate has been issued by the licensed Certifying Authority and accepted by the subscriber, and the Certifying Authority comes to know of any fact that affects the validity or reliability of such Digital Signature Certificate, it is required to notify the same to the subscriber immediately.

All Digital Signature Certificates are to be issued with a designated expiry date.

Rule 24 contains provisions relating to the generation of Digital signature certificates. The process will entail:

1. receipt of an approved and verified Digital Signature Certificate request,

2. creating a new Digital Signature Certificate,

3. binding the key pair associated with the Digital Signature Certificate to a Digital Signature Certificate owner,

4. issuing the Digital Signature Certificate and the associated public key for operational use,

5. allotting a distinguished name associated with the Digital Signature Certificate owner, and

6. using a recognized and relevant policy as defined in the Certification Practice Statement.

Rule 25 says that before the issue of the digital signature certificate, the Certifying Authority will be expected to:

1. Confirm that the user's name does not appear in its list of compromised users;

2. Comply with the procedure as defined in his Certification Practice Statement including verification of identification and/or employment;

3. Comply with all privacy requirements;

4. Obtain consent of the person requesting the Digital Signature Certificate, that the details of such Digital Signature Certificate can be published on a directory service.

Rule 26 contains provisions relating to the life of a digital signature certificate. A Digital Signature Certificate has to be granted with a designated expiry date. It expires automatically upon reaching the designated expiry date at which time it must be archived.

It cannot be reused after expiry. The period for which a Digital Signature Certificate has been issued cannot be extended, but a new Digital Signature Certificate may be issued after the expiry of such period.

Rule 27 says that Certifying Authorities are required to archive the following for a minimum period of seven years:

1. Applications for issue of digital signature certificates,
2. Registration and verification documents of generated Digital signature certificates,
3. Digital signature certificates,
4. Notices of suspension,
5. Information of suspended Digital Signature Certificates,
6. Information of revoked Digital Signature Certificates,
7. Expired Digital Signature Certificates

Rule 28 lays down provisions relating to compromise of Digital Signature Certificates. A Digital Signature Certificate is deemed to be compromised when the integrity of the private key associated with it is in doubt or when the Digital Signature Certificate owner is in doubt, as to the use, or attempted use of his key pairs, or otherwise, for malicious or unlawful purposes.

Digital Signature Certificates that become compromised while in operational use are to be revoked in accordance with the procedure defined in the Certification Practice Statement. A Digital Signature Certificate can remain in the compromised state for only such time as it takes to arrange for revocation.

Rule 29 provides for revocation of digital signature certificates. A Digital Signature Certificate may be revoked and become invalid for any trusted use, where –

1. There is a compromise of the Digital Signature Certificate owner's private key;

2. There is a misuse of the Digital Signature Certificate;

3. There is a misrepresentation or errors in the Digital Signature Certificate;

4. The Digital Signature Certificate is no longer required

Revoked Digital Signature Certificates are to be added to the Certificate Revocation List.

Rule 30 lays down the fees for issue of digital signature certificate. The Central Government can prescribe the fees that Certifying Authorities can charge for the issue of Digital Signature Certificates.

The rule allows Certifying Authorities to levy fees for access to its X.500 directory for certificate downloading, certificate revocation and status information. Certifying Authorities are required to provide an up-to-date fee schedule to all their subscribers and users.

The rule allows publishing of the fee schedule on a nominated web site. No fee can be levied for access to Certification

Practice Statement via Internet. Certifying Authorities can charge fees for providing printed copies of their Certification Practice Statements.

Rule 31 says that Certifying Authorities must get their operations audited annually by an auditor. The audit must include the following:

1. Security policy and planning;
2. Physical security;
3. Technology evaluation;
4. Certifying Authority's services administration;
5. Relevant Certification Practice Statement;
6. Compliance to relevant Certification Practice Statement;
7. Contracts / agreements;
8. Regulations prescribed by the Controller;
9. Policy requirements of Certifying Authorities Rules, 2000;
10. Certifying Authorities are also required to conduct half yearly audit;
11. Security Policy, physical security and planning of their operations and quarterly audit of their repositories.

Certifying Authorities are required to submit copies of each audit report to the Controller within four weeks of the completion of such audit. In the event that an irregularity is found, the Certifying Authority is required to take immediate appropriate action to remove such an irregularity.

Rule 32 provides that the auditor has to be independent of the Certifying Authority being audited and cannot be a software or hardware vendor which is, or has been providing services or supplying equipment to the said Certifying Authority.

The auditor and the Certifying Authority are not to have any current or planned financial, legal or other relationship, other than that of an auditor and the audited party.

Rule 33 says that the following information must be kept confidential:

1. Digital Signature Certificate application, whether approved or rejected,

2. Digital Signature Certificate information collected from the subscriber or elsewhere as part of the registration and verification record but not included in the Digital Signature Certificate information,

3. Subscriber agreement

Rule 34 lays down that the access to confidential information, by the operational staff of a Certifying Authority, is to be on a "need-to-know" and "need-to-use" basis. The rule further provides that paper based records, documentation and backup data containing all confidential information as prescribed in rule 33 must be maintained in secure and locked container or filing system, separately from all other records.

The rule further provides that the confidential information is not to be taken out of the country except in a case where a properly constitutional warrant or other legally enforceable document is produced to the Controller and he permits to do so.

Schedule I specifies the form for application for grant of licence to be a certifying authority.

Schedule II contains Information Technology Security Guidelines.

Schedule III contains security guidelines for Certifying Authorities.

Schedule IV specifies the form for application for issue of digital signature certificates.

Schedule IV contains a glossary of terms.

3.8 List of licenced CAs

The list of licenced Certifying Authorities in India include can be obtained from the website of the Controller of Certifying Authorities at: www.cca.gov.in

FOUR

4. Electronic Contracts

Contracts have become so common in daily life that most of the time we do not even realize that we have entered into one. Right from hiring a taxi to buying airline tickets online, innumerable things in our daily lives are governed by contracts.

The **Indian Contract Act, 1872** governs the manner in which contracts are made and executed in India. It governs the way in which the provisions in a contract are implemented and codifies the effect of a breach of contractual provisions.

Within the framework of the Indian Contract Act, parties are free to contract on any terms they choose. Indian Contract Act consists of limiting factors subject to which contract may be entered into, executed and enforced.

It only provides a framework of rules and regulations which govern formation and performance of contract. The rights and duties of parties and terms of agreement are decided by the contracting parties themselves. The court of law acts to enforce agreement, in case of non-performance.

Electronic contracts (contracts that are not paper based but rather in electronic form) are born out of the need for speed, convenience and efficiency.

Imagine a contract that an Indian exporter and an American importer wish to enter into. One option would be that one party first draws up two copies of the contract, signs them and couriers them to the other, who in turn signs both copies and couriers one copy back. The other option is that the two parties meet somewhere and sign the contract.

In the electronic age, the whole transaction can be completed in seconds, with both parties simply affixing their digital signatures to an electronic copy of the contract. There is no need for delayed couriers and additional travelling costs in such a scenario.

There was initially an apprehension amongst the legislatures to recognize this modern technology, but now many countries have enacted laws to recognize electronic contracts.

The conventional law relating to contracts is not sufficient to address all the issues that arise in electronic contracts. The IT Act solves some of the peculiar issues that arise in the formation and authentication of electronic contracts.

4.1 Essentials of an electronic contract

As in every other contract, an electronic contract also requires the following necessary ingredients:

1. An offer needs to be made

In many transactions (whether online or conventional) the offer is not made directly. The consumer ‘browses’ the available goods and services displayed on the merchant’s website and then chooses what he would like to purchase.

The offer is not made by a website displaying items for sale at a particular price. This is actually **an invitation to offer** and hence is revocable at any time up to the time of acceptance. The offer is made by the customer on placing the products in the virtual ‘basket’ or ‘shopping cart’ for payment.

2. The offer needs to be accepted

As stated earlier, the acceptance is usually undertaken by the business after the offer has been made by the consumer in relation with the invitation to offer. An offer is revocable at any time until the acceptance is made.

Procedures available for forming electronic contracts include:

1. **E-mail:** Offers and acceptances can be exchanged entirely by e-mail, or can be combined with paper documents, faxes, telephonic discussions etc.

2. **Web Site Forms:** The seller can offer goods or services (e.g. air

tickets, software etc.) through his website. The customer places an order by completing and transmitting the order form provided on the website. The goods may be physically delivered later (e.g. in case of clothes, music CDs etc.) or be immediately delivered electronically (e.g. e-tickets, software, mp3 etc.).

3. **Online Agreements:** Users may need to accept an online agreement in order to be able to avail of the services e.g. clicking on “I accept” while installing software or clicking on “I agree” while signing up for an email account.

3. There has to be lawful consideration

Any contract to be enforceable by law must have lawful consideration, i.e. when both parties give and receive something in return. Therefore, if an auction site facilitates a contract between two parties where one person provides a pornographic movie as consideration for purchasing an mp3 player, then such a contract is void.

4. There has to be an intention to create legal relations

If there is no intention on the part of the parties to create legal relationships, then no contract is possible between them. Usually, agreements of a domestic or social nature are not contracts and therefore are not enforceable, e.g., a website providing general health related information and tips.

5. The parties must be competent to contract

Contracts by minors, lunatics etc are void. All the parties to the contract must be legally competent to enter into the contract.

6. There must be free and genuine consent

Consent is said to be free when there is absence of coercion, misrepresentation, undue influence or fraud. In other words, there must not be any subversion of the will of any party to the contract to enter such contract.
Usually, in online contracts, especially when there is no active real-time interaction between the contracting parties, e.g., between a website and the customer who buys through such a site, the **click through procedure** ensures free and genuine consent.

7. The object of the contract must be lawful

A valid contract presupposes a lawful object. Thus a contract for selling narcotic drugs or pornography online is void.

8. There must be certainty and possibility of performance

A contract, to be enforceable, must not be vague or uncertain and there must be possibility of performance. A contract, which is impossible to perform, cannot be enforced, e.g., where a website promises to sell land on the moon.

4.2 Relevant IT Act provisions

The Information Technology (Amendment) Act, 2008 has introduced a new section 10A into the IT Act. This section relates to the validity of contracts formed through electronic means. As per this section:

> *Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.*

This section is in conformance with Article 8(1) of the United Nations Convention on the Use of Electronic Communications in International Contracts which states that:

> *A communication or a contract shall not be denied validity or enforceability on the sole ground that it is in the form of an electronic communication.*

Attribution of Electronic Records

<u>According to section 11 of the IT Act</u>

> *11. An electronic record shall be attributed to the originator—*
>
> *(a) if it was sent by the originator himself;*
>
> *(b) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or*

(c) by an information system programmed by or on behalf of the originator to operate automatically.

According to section 2(1)(za) of the IT Act, **originator** is a person who:

1. sends, generates, stores or transmits any electronic message or
2. causes any electronic message to be sent, generated, stored or transmitted to any other person.

The term originator **does not include an intermediary**.

Illustration
Pooja uses her gmail.com email account to send an email to Sameer. Pooja is the originator of the email. Gmail.com is the intermediary.

This section can best be understood with the help of suitable illustrations.

Illustration 1
Pooja logs in to her web-based gmail.com email account. She composes an email and presses the "Send" button, thereby sending the email to Sameer. The electronic record (email in this case) will be attributed to Pooja (the originator in this case) as Pooja herself has sent it.

Illustration 2
Pooja instructs her assistant Siddharth to send the above-mentioned email. In this case also, the email will be attributed to Pooja (and not her

assistant Siddharth). The email has been sent by a person (Siddharth) who had the authority to act on behalf of the originator (Pooja) of the electronic record (email).

Illustration 3

Pooja goes on vacation for a week. In the meanwhile, she does not want people to think that she is ignoring their emails. She configures her gmail.com account to automatically reply to all incoming email messages with the following message:

"Thanks for your email. I am on vacation for a week and will reply to your email as soon as I get back".

Now every time that gmail.com replies to an incoming email on behalf of Pooja, the automatically generated email will be attributed to Pooja as it has been sent by an information system programmed on behalf of the originator (i.e. Pooja) to operate automatically.

Acknowledgment of Receipt

<u>According to section 12(1) of the IT Act</u>

Where the originator has not agreed with the addressee that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by—

(a) any communication by the addressee, automated or otherwise; or

(b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

According to section 2(1)(b) of the IT Act, **Addressee** means a person who is intended by the originator to receive the electronic record but does not include any intermediary.

Illustration

Pooja uses her gmail.com email account to send an email to Sameer. Pooja is the originator of the email. Gmail.com is the intermediary. Sameer is the addressee.

This sub-section provides for methods in which the acknowledgment of receipt of an electronic record may be given, provided no particular method has been agreed upon between the originator and the recipient.

One method for giving such acknowledgement is any communication (automated or otherwise) made by the addressee in this regard.

Illustration

Let us go back to the earlier example of Pooja going on vacation for a week. She has configured her email account to automatically reply to all incoming email messages with the following message:

"Thanks for your email. I am on vacation for a week and will reply to your email as soon as I get back".

The incoming message is also affixed at the bottom of the above-mentioned message.

Now when Siddharth sends an electronic record to Pooja by email, he will receive Pooja's pre-set message as well as a copy of his own message.

This automated communication will serve as an acknowledgement that Pooja has received Siddharth's message.

Another method is any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received. Let us take another illustration.

Illustration

Rohit sends an email to Pooja informing her that he would like to purchase a car from her and would like to know the prices of the cars available for sale. Pooja subsequently sends Rohit a catalogue of prices of the cars available for sale.

It can now be concluded that Pooja has received Rohit's electronic record. This is because such conduct on the part of Pooja (i.e. sending the catalogue) is sufficient to indicate to Rohit (the originator) that his email (i.e. the electronic record) has been received by the addressee (i.e. Pooja).

According to section 12(2) of the IT Act

Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic *record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.*

Illustration

Suppose Pooja wants to sell a car to Sameer. She sends him an offer to buy the car. In her email, Pooja asked Sameer to send her an acknowledgement that he has received her email. Sameer does not send her an acknowledgement. In such a situation, it shall be assumed that the email sent by Pooja was never sent.

<u>According to section 12(3) of the IT Act</u>

Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

Illustration

Rohit sends the following email to Sameer:

Further to our discussion, I am ready to pay Rs 25 lakh for the source code for the PKI software developed by you. Let me know as soon as you receive this email.

Sameer does not acknowledge receipt of this email. Rohit sends him another email as follows:

I am resending you my earlier email in which I had offered to pay Rs 25 lakh for the source code for the PKI software developed by you. Please acknowledge receipt of my email latest by next week.

Sameer does not acknowledge the email even after a week. The initial email sent by Rohit will be treated to have never been sent.

Time and place of despatch and receipt

According to section 13(1) of the IT Act

Save as otherwise agreed to between the originator and the addressee, the despatch of an electronic record occurs when it enters a computer resource outside the control of the originator.

Illustration

Pooja composes a message for Rohit at 11.56 a.m. At exactly 12.00 noon she presses the "Submit" or "Send" button. When she does that the message leaves her computer and begins its journey across the Internet. It is now no longer in Pooja's control. The time of despatch of this message will be 12.00 noon.

According to section 13(2) of the IT Act

Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely:—

(a) if the addressee has designated a computer resource for the purpose of receiving electronic records,—

> *(i) receipt occurs at the time when the electronic record enters the designated computer resource; or*
>
> *(ii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;*

(b) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.

Illustration:

The marketing department of a company claims that it would make the delivery of any order within 48 hours of receipt of the order. For this purpose they have created an order form on their website. The customer only has to fill in the form and press submit and the message reaches the designated email address of the marketing department.

Now Suresh, a customer, fills in this order form and presses submit. The moment the message reaches the company's server, the order is deemed to have been received.

Karan, on the other hand, emails his order to the information division of the company. One Mr. Sharma, who is out on vacation, checks this account once a week. Mr. Sharma comes back two weeks later and logs in to the account at 11.30 a.m. This is the time of receipt of the message although it was sent two weeks earlier.

Now suppose the company had not specified any address to which orders can be sent by email. Had Karan then sent the order to the information division, the time of receipt of the message would have been the time when it reached the server of the company.

According to section 13(3) of the IT Act

Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be despatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

Illustration

Sameer is a businessman operating from his home in Pune, India. Sameer sent an order by email to a company having its head office in New York, USA.

The place of despatch of the order would be Sameer's home and the place of receipt of the order would be the company's office.

<u>According to section 13(4) of the IT Act</u>

The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).

Illustration

Let us consider the illustration mentioned above of Sameer and the New York based company. Even if the company has its mail server located physically at Canada, the place of receipt of the order would be the company's office in New York, USA.

<u>According to section 13(5) of the IT Act</u>

For the purposes of this section,—

(a) if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business;

(b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;

(c) "usual place of residence", in relation to a body corporate, means the place where it is registered.

Illustration

Sameer sent an order by email to a company having its head office in New York, USA. The company has offices in 12 countries. The place of business will be the principal place of business (New York in this case). Sameer is a businessman operating from his home in Pune, India. He does not have a separate place of business. Sameer's residence will be deemed to be the place of business.

P.R. Transport Agency vs. Union of India & others

AIR2006All23, 2006(1)AWC504

IN THE HIGH COURT OF ALLAHABAD

Civil Misc. Writ Petition No. 58468 of 2005

Decided On: 24.09.2005

Appellants: P.R. Transport Agency through its partner Sri Prabhakar Singh Vs.

Respondent: Union of India (UOI) through Secretary, Ministry of Coal, Bharat Coking Coal Ltd. through its Chairman, Chief Sales Manager Road Sales, Bharat Coking Coal Ltd. and Metal and Scrap Trading Corporation Ltd. (MSTC Ltd.) through its Chairman cum Managing Director

Background of the case

Bharat Coking Coal Ltd (BCC) held an e-auction for coal in different lots. P.R. Transport Agency's (PRTA) bid was accepted for 4000 metric tons of coal from Dobari Colliery.

The acceptance letter was issued on 19th July 2005 by e-mail to PRTA's e-mail address. Acting upon this acceptance, PRTA deposited the full amount of Rs. 81.12 lakh through a cheque in favour of BCC. This cheque was accepted and encashed by BCC.

BCC did not deliver the coal to PRTA. Instead it e-mailed PRTA saying that the sale as well as the e-auction in favour of PRTA stood cancelled "due to some technical and unavoidable reasons".

The only reason for this cancellation was that there was some other person whose bid for the same coal was slightly higher than that of PRTA. Due to some flaw in the computer or its programme or feeding of data the higher bid had not been considered earlier.

This communication was challenged by PRTA in the High Court of Allahabad. [Note: Allahabad is in the state of Uttar Pradesh (UP)]

BCC objected to the "territorial jurisdiction" of the Court on the grounds that no part of the cause of action had arisen within U.P.

Issue raised by BCC

> The High Court at Allahabad (in U.P.) had no jurisdiction as no part of the cause of action had arisen within U.P.

Issues raised by PRTA

1. The communication of the acceptance of the tender was received by the petitioner by e-mail at Chandauli (U.P.). Hence, the contract (from which the dispute arose) was completed at Chandauli (U.P). The completion of the contract is a part of the "cause of action".

2. The place where the contract was completed by receipt of communication of acceptance is a place where 'part of cause of action' arises.

Points considered by the court

1. With reference to contracts made by telephone, telex or fax, the contract is complete when and where the acceptance is received. However, this principle can apply only where the transmitting terminal and the receiving terminal are at fixed points.

2. In case of e-mail, the data (in this case acceptance) can be transmitted from anywhere by the e-mail account holder. It goes to the memory of a 'server' which may be located anywhere and can be retrieved by the addressee account holder from anywhere in the world. Therefore, there is no fixed point either of transmission or of receipt.

3. Section 13(3) of the Information Technology Act has covered this difficulty of "no fixed point either of transmission or of receipt". According to this section "...an electronic record is deemed to be received at the place where the addressee has his place of business."

4. The acceptance of the tender will be deemed to be received by PRTA at the places where it has place of business. In this case it is Varanasi and Chandauli (both in U.P.)

Decision of the court

1. The acceptance was received by PRTA at Chandauli / Varanasi. The contract became complete by receipt of such acceptance.

2. Both these places were within the territorial jurisdiction of the High Court of Allahabad. Therefore, a part of the cause of action had arisen in U.P. and the court had territorial jurisdiction.

4.3 Browse wrap, shrink wrap and click wrap contracts

Browse wrap, shrink wrap and click wrap are common types of agreements used in electronic commerce.

Under a **Browse wrap agreement**, a hyperlink containing the terms and conditions regarding the usage of the website is posted on the website.

These terms and conditions usually state that by usage of the website, the person has consented to be bound by the terms and conditions stated therein.

For example, electronic commerce websites such as Amazon and Flipkart display a hyperlink on their websites under the tab of "Conditions of Use and Sale" and "Terms of Use" respectively. When one clicks on the hyperlink, it will direct you to a page displaying the terms and conditions in detail. These terms and conditions usually contain a statement to the effect that by accessing, browsing or otherwise using the website, you indicate your consent to all the terms and conditions mentioned therein.

Shrink wrap contracts are license agreements or other terms and conditions which can only be read and accepted by the consumer after opening the product. The term describes the shrink wrap plastic wrapping used to coat software boxes, though these contracts are not limited to the software industry.

A **clickwrap agreement** is mostly found as part of the installation process of software packages. It is also called a "click through" agreement or clickwrap license. The name "clickwrap" comes from the use of "shrink wrap contracts" in boxed software purchases.

Click-wrap agreements can be of the following types:

1. **Type and Click** where the user must type "I accept" or other specified words in an on-screen box and then click a "Submit" or similar button. This displays acceptance of the terms of the contract. A user cannot proceed to download or view the target information without following these steps.

2. **Icon Clicking** where the user must click on an "**OK**" or "**I agree**" button on a dialog box or pop-up window. A user indicates rejection by clicking “**Cancel**” or closing the window.

Upon rejection, the user can no longer use or purchase the product or service. A click wrap contract is a “**take-it-or-leave-it**” type of contract that lacks bargaining power.

The terms of service or license may not always appear on the same webpage or window, but they must always be accessible before acceptance.

Enforceability of Click Wrap Agreement in India

The Income Tax Tribunal, Mumbai recently in 2016 in the case of Capgemini Business Services (India) Ltd. vs. Assistant Commissioner of Income Tax-1(2) (ITA No. 7779/M/2011) made following observations regarding the enforceability of 'Click Wrap' agreements:

1. The Tribunal stated that in an internet license agreement, the end user is supposed to click the icon 'I agree' which means that the end user has agreed to the terms of the license agreement. However, such agreements do not ask the name or address or other

details of the user. It is not mentioned in such type of agreements that who is using the product.

2. It is the computer upon which such software is loaded that can be said to have agreed to abide by the terms of the software license as the user remains unidentifiable.

3. In such type of software licenses, there are certain inbuilt mechanisms made by the buyer preventing the misuse or infringement of the copyright in the product; the moment the end user attempts to violate such conditions, such software becomes inoperative on the computer or sometimes also damages the other data/applications on the computer.

4. However, for the enforceability of such license agreement it is not known who is actual user or which person actually has violated the terms of the agreement.

5. The Tribunal cited an example - Suppose, in case of a company a product is purchased by the staff of the company, for its use in regular course of work or business of the company and an employee of the company while installing the software on the computer in the office of the company clicks the button or the icon 'I agree' and thereafter such an employee or any other employee of the company violates any condition of the license agreement, can such license agreement be enforced against the company or the Directors of the company can be held liable for any such infringement, especially when they are not signatories to such an agreement and nor they have authorized any employee of the company to sign any agreement on behalf of the company and even no

name of the company is written in such type of agreement and even it is also not known as to who actually clicked the button 'I agree'.

6. Under the circumstances as mentioned above, the Tribunal observed that the enforceability of such a license is highly doubtful.

As the above were observations made by a Tribunal, the said proposition is yet to be tested by the High Courts in India.

FIVE

5. How Does E-commerce Work?

Marketing, buying or selling of merchandise or services over the internet is known as electronic commerce or e-commerce. E-commerce includes a series of activities right from display of catalogues of products on the website to back end service. Let us understand in brief how e-commerce works by taking an example –

1. You decide to purchase a phone from Amazon.in, so you create an account on the website and add the phone to the cart. Once, you add the item to the cart, information gets stored on the database of the website.

2. Then you proceed to check out. That is when you enter your credit card number and the information is passed to a payment gateway like CCAvenue, PayPal, Citrus, etc. In order to make sure the transaction takes place in a secure manner, Amazon.in has an arrangement with a payment gateway i.e. a company who in turn has an independent arrangement with the debit or credit card companies to facilitate secure payment methods.

3. Once the payment of the phone takes place, the website directs the purchase order to a central system which connects with the retailer to further process it.

4. The retailer then checks with his stock database regarding the availability of the phone.

5. Once the phone is dispatched, the retailer through a system updates Amazon.in and Amazon.in enables you to track the delivery of the product.

6. And finally you receive the phone!

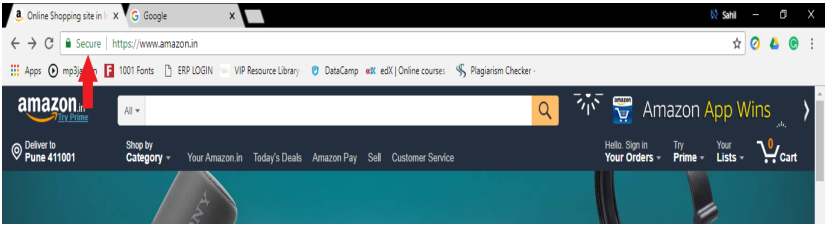
Websites understand that it is imperative to protect the data of the users. In order to ensure that transactions of the website are secure, websites obtain an SSL Certificate i.e. Secure Sockets Layer Certificate. An SSL Certificate ensures the security of all the personal data and credit card details for every user. It ensures the encryption of personal data so that only an intended recipient can access the information. In addition to encryption, SSL also serves as an authentication check, which makes sure that you are sending the information to the genuine server and not an imposter. SSL can be used to verify that data is safe from tampering and eavesdropping.

How to Check SSL Certificate for websites?

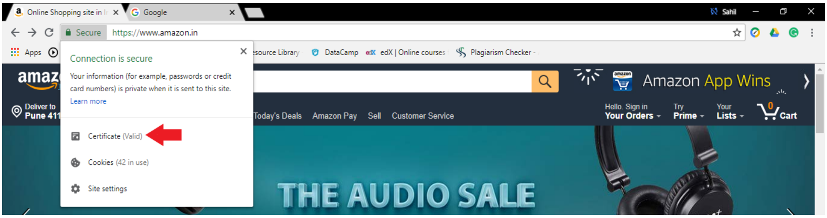
Step 01: Open Google Chrome

Step 02: Open the website for which you want to check the SSL Certificate. Here, we will check the SSL Certificate of Amazon.in

Step 03: Click on the *Secure* tab present on the website address bar located on the top left corner of the webpage



Step 04: A dialog box will appear, click on Certificate to view the Certificate.



Connection is secure

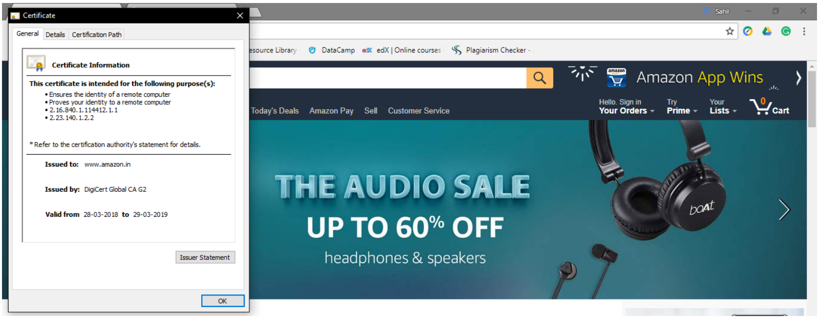
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Certificate (Valid)

Cookies (42 in use)

Site settings

Step 05: View the SSL Certificate, certification path and other details of the website.



Certificate Information

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

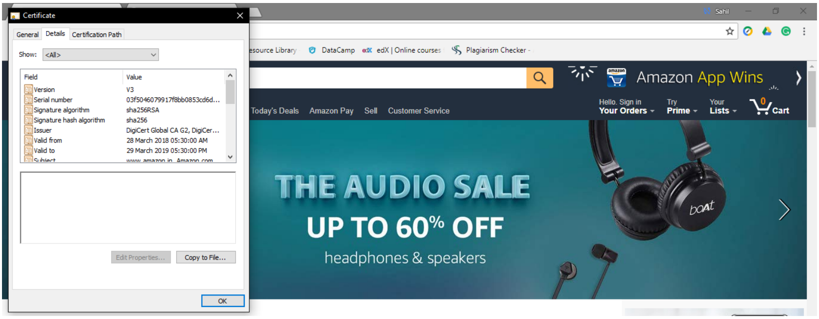
- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 2.16.840.1.114412.1.1
- 2.23.140.1.2.2

* Refer to the certification authority's statement for details.

Issued to: www.amazon.in

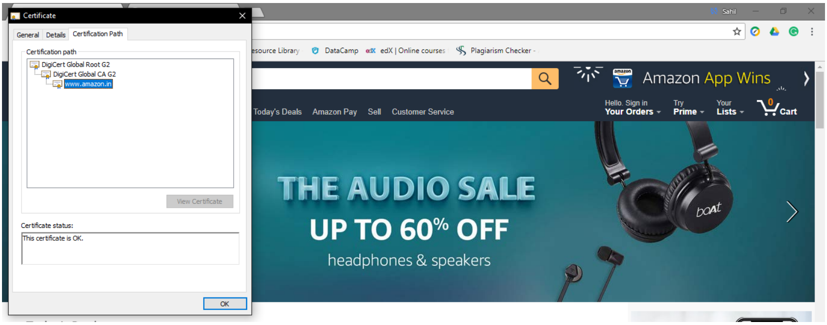
Issued by: DigiCert Global CA G2

Valid from 28-03-2018 **to** 29-03-2019



Show: <All>

Field	Value
Version	V3
Serial number	03f5046079917f8bb0853cd6d...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	DigiCert Global CA G2, DigiCer...
Valid from	28 March 2018 05:30:00 AM
Valid to	29 March 2019 05:30:00 PM
Subject	www.amazon.in, Amazon.com



Certificate

General | Details | Certification Path

Certification path

- DigiCert Global Root G2
  - DigiCert Global CA G2
    - www.amazon.in

View Certificate

Certificate status:

This certificate is OK.

OK

SIX

6. E-money, Bitcoin & the Indian law

With the pervasiveness of technology in almost all major aspects of our lives, even money has taken an electronic form. Popularly known as ‘e-money’, this money is stored in e-payment mechanisms such as e-wallets or digital wallets, and other prepaid e-payment online accounts.

In India in the last few years several digital wallets have cropped up. To name a few – PayZapp by HDFC, Amazon Pay, Airtel Money, Paytm, Ola Money, Jio money are popular digital wallets in India.

The Payment and Settlement Act, 2007 is the nodal legislation which regulates digital wallets and other digital payment systems in India. Under the Payment and Settlement Act, 2007, the Reserve Bank of India has been given the power to supervise and regulate digital payment systems.

What is money?

Our ancestors started off with the barter system—something like “I will give you 2 horses in return for 5 shiny new super-sharp axes”. Soon they realised that the barter system had too many limitations—everyone didn’t want horses, horses were neither divisible (not too many people would want 0.35 horses) nor very portable (imagine having to carry a horse on your shoulders while going shopping).

So they moved on to more acceptable, divisible, homogeneous and portable forms of money—cowry shells, salt, gold, silver and lots more. The Chinese invention of paper eventually led to the birth of paper currency, which was initially backed by gold or other precious metals. Then the world moved on to fiat money—currency that's declared as legal tender by a government but not backed by a physical commodity.

Have a look at a 100-rupee note. It carries a promise signed by the Governor of the Reserve Bank of India (RBI):

I promise to pay the bearer the sum of one hundred rupees.

The RBI gets the power to issue currency notes by section 31 of the Reserve Bank of India Act, 1934. This section states that "*No person in India other than the Bank or, as expressly authorized by this Act, the Central Government shall draw, accept, make or issue any bill of exchange, hundi, promissory note or engagement for the payment of money payable to bearer on demand, or borrow, owe or take up any sum or sums of money on the bills, hundis or notes payable to bearer on demand of any such person…*"

This brings us to an essential question—what is money? Money's a matter of functions four, a Medium, a Measure, a Standard, a Store. So goes the couplet based on William Stanley Jevons analysis of money in 1875. This meant that for something to be called money, it must function as a medium of exchange, a measure of value, a standard of deferred payment and a store of value.

The birth of computers and the Internet brought in many electronic payment systems including debit cards, stored value cards, giro transfers, credit cards, net-banking, electronic bill payments, electronic cheques, mobile wallets, digital gold currencies, digital wallets, electronic funds transfer at point of sale, mobile banking, SMS banking, online banking, payment cards, real-time gross settlement systems, SWIFT, wire transfers and more.

And then came Satoshi Nakamoto's path breaking whitepaper—Bitcoin: A Peer-to-Peer Electronic Cash System in October 2008. This brought the world its first truly peer-to-peer electronic currency.

Virtual & crypto currencies

Bitcoin earned a lot of notoriety primarily because of its use by members of the now shut-down Silk Road—an illegal online marketplace that facilitated the sale of hundreds of millions of dollars' worth of drugs, guns, stolen financial information, counterfeit documents and more. All Silk Road transactions were conducted exclusively in bitcoin.

A lot of crypto-currencies piggybacked on Bitcoin's underlying innovation—the blockchain. In fact, we now have hundreds of virtual currencies being used around the world. And now we have become a world where bankers wake up each morning wondering—"has the meaning of money and banking changed while I slept…".

This rapid change in the global money ecosystem has implications for all of us—from Governments looking to clamp down on money laundering, tax evasion and terrorist funding to banks looking to understand the implications of the blockchain technology. From law enforcement looking to clamp down on the Mafia using Bitcoin to businesses looking for faster and cheaper ways to receive and transfer money globally.

The FATF report on Virtual Currencies—Key Definitions and Potential AML/CFT Risks distinguishes between the terms *Virtual currency* and *Cryptocurrency.*

Virtual currency is a digital representation of value that can be digitally traded and functions as

(1) a medium of exchange; and/or
(2) a unit of account; and/or
(3) a store of value, but does not have legal tender status (i.e. when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction.

It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency.

Virtual currency is distinguished from **fiat currency** (a.k.a. “real currency,” “real money,” or “national currency”), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. **E-money** is a digital transfer mechanism for fiat currency-i.e., it electronically transfers value that has legal tender status.

Cryptocurrency refers to a math-based, decentralised convertible virtual currency that is protected by cryptography.—i.e., it incorporates principles of cryptography to implement a distributed, decentralised, secure information economy.

Cryptocurrency relies on public and private keys to transfer value from one person (individual or entity) to another, and must be cryptographically signed each time it is transferred. The safety, integrity and balance of cryptocurrency ledgers is ensured by a network of mutually distrustful parties (in Bitcoin, referred to as miners) who protect the network in exchange for the opportunity to obtain a randomly distributed fee (in Bitcoin, a small number of newly created bitcoins, called the “block reward” and in some cases, also transaction fees paid by users as a incentive for miners to include their transactions in the next block).

Hundreds of cryptocurrency specifications have been defined, mostly derived from Bitcoin, which uses a proof- of-work system to validate transactions and maintain the block chain. While Bitcoin provided the first fully implemented cryptocurrency protocol, there is growing interest in developing alternative, potentially more efficient proof methods, such as systems based on proof-of-stake.

RBI circular on Virtual Currencies

Reserve Bank has repeatedly cautioned users, holders and traders of virtual currencies, including Bitcoins, regarding various risks associated in dealing with such virtual currencies.

The April 6, 2018 circular titled *Prohibition on dealing in Virtual Currencies* prohibits all commercial & co-operative banks, payments banks, small finance banks, non banking finance companies and payment system providers from dealing in virtual currencies or providing services for facilitating any person or entity in dealing with or settling virtual currencies.

Such services include maintaining accounts, registering, trading, settling, clearing, giving loans against virtual tokens, accepting them as collateral, opening accounts of exchanges dealing with them and transfer / receipt of money in accounts relating to purchase/ sale of virtual currencies.

This circular has been issued under relevant provisions of the *Banking Regulation Act*, *Reserve Bank of India Act* and the *Payment and Settlement Systems Ac*t.