Team in enhancing ... to prevent the occurrence of cyber crimes is briefly covered in the last section.

15.2 Cyber Crimes

Cyber crimes use computers and networks for criminal activities. Computers can be used for committing a crime in one of the following three ways:

- As a tool
- As a target
- Both as a tool and a target.

The first type of crime is basically an extension of 'real world' crimes, such as forgery, fraud or copyright piracy using computers. Existing laws can be used to bring criminals to justice.

The second type of crime is a real cyber crime in which culprits damage or modify the victims' computer systems and networks through illegal access, and cause heavy loss to the victims. They are unique in that they occur in cyberspace. There is no physical equipment of such a cyber crime, since the target of attack is a computer system. A criminal may launch a virus, worm, or a Trojan to attack a target computer system or network. Existing laws are inadequate to prosecute such crimes. They require special computer crime, and/or misuse laws.

Hackers exploit known vulnerabilities in various systems. They write codes to exploit these vulnerabilities to gain unauthorised entry into systems and networks, and engage in activity that threatens their security. The malicious code created may be in the form of viruses, worms, or Trojans. These have been defined in Chapter 14 on security issues.

The third type of crime is the one in which computers are used both as a tool as well as a target.

A partial list of cyber crimes is as follows:

- Hacking of computer systems and networks
- Cyber pornography involving production and distribution of pornographic material, including child pornography
- Financial crimes such as siphoning of money from banks, credit card frauds, money laundering
- Online gambling
- Intellectual property crimes such as theft of computer source code, software piracy, copyright infringement, trademark violations
- Harassments such as cyber stalking, cyber defamation, indecent and abusing mails
- Cyber frauds such as forgery of documents including currency and any other documents
- Launching of viruses, worms and Trojans
- Denial-of-service attacks
- Cyber attacks and cyber terrorism
- Economic espionage
- Consumer harassment and consumer protection
- Privacy of citizens
- Sale of illegal articles such as narcotics, weapons, wildlife, etc.

Cyber crimes that can generally occur within organisations are as follows:

- E-mail abuse
- Spam mails
- Cyber defamation

- Theft of source code
- Exchange of business secrets and documents
- Insider attacks on personnel databases
- Use of office computer for running other businesses
- Transmission and viewing of pornographic materials
- External cyber attacks on an organisation resulting in denial-of-service
- Information espionage

15.3 Cyber Crimes and the Information Technology Act, 2000

The IT Act, 2000 notified for implementation in October 2000, explicitly deals with the following categories of cyber crimes only:

- Tampering with a computer source code
- Hacking
- Publishing any information which is obscene
- Breach of privacy
- Misrepresentation
- Publishing digital signature which is false in certain particulars or for fraudulent act.

It is obvious that it is silent on many types of cyber crimes. It was probably logical since the Act was written with a view to promote the growth of e-commerce and e-governance as is stated in its preamble. Its primary object was to create trust in the electronic environment by providing electronic authentication through the use of digital signatures based on asymmetric cryptosystems. Some types of crimes which relate to e-commerce and e-governance were included in the Act with a view to increasing trust in the smooth conduct of these activities over the Net. It is not a special Act for preventing abuse and misuse of computer systems using networks in the normal social intercourse of individuals and organisations in the context of the multifarious uses of the Internet. Many countries have

result of the decoding operation).

16.4 The IT Act, 2000

The IT Act defines the following key concepts related to electronic records, digital signatures, and Certifying Authorities*:

- Asymmetric cryptosystem
- Certifying authority

*The IT Act, 2000 has chosen the nomenclature of "Certifying Authority" instead of the international practice of "Certification Authority".

- Certification practice statement
- Computer
- Computer network
- Computer systems
- Data
- Digital signature certificate
- Electronic form
- Electronic record
- Key pair
- Originator
- Private key
- Public key
- Secure system

16.4.1 Legal Recognition to Electronic Records

Section 3 of the IT Act provides for authentication of an electronic record by a person by affixing his digital signature, "which shall be effected by the use of an asymmetric crypto system and hash function." This is explained in detail in Chapter 17 on Public Key Infrastructure (PKI).

Section 4 of the Act provides legal recognition to records, while Section 5 provides legal recognition to digital signatures. Section 6 allows filing of electronic records in the form of electronic forms, with digital signatures of persons, to be filed with Government organisations in lieu of paper-based forms, when prescribed by any of them.

Section 7 of the Act provides legal recognition to electronic records that are stored in the original formats in which they were generated. Retention of electronic records has thus been legalised. The Government has been further authorised to have an Official Electronic Gazette which will have the same legal recognition as the paper gazette for all rules, regulations, orders, bye-laws, notifications, or any other matter published in it.

Chapter 17
Public Key Infrastructure

The most well-known and almost universally accepted method of electronic authentication is the one based on asymmetric cryptosystems, which has already been discussed in the previous chapter. This is also known as public key cryptography, and is the basis for creating digital signatures. Digital signatures created and verified by using public key cryptography that is based on the concept of a key-pair, generated by a mathematical algorithm—the public and private keys has already been discussed in Chapter 14.

The main challenge faced in implementing digital signatures based on asymmetric cryptosystems was in making all the public keys widely available while ensuring that the relying party can be assured that the corresponding private key has indeed been used to create the digital signature.

Electronic authentication using digital signatures requires Certifying Authorities (CAs), who act as trusted third parties or electronic notaries in cyberspace, to issue Digital Signature Certificates or Public Key Certificates (PKCs) to individuals to establish their identity in the cyberspace by binding a public key with attributes such as name, address, telephone number, passport number, etc. while ensuring that the entity possessing these attributes owns the corresponding private key. The CAs and the regime governing their operations are together known as Public Key Infrastructure (PKI). PKI is thus the foundation for secure transactions in cyberspace.

17.1 PKI and Certifying Authorities (CAs)

A CA is a trusted third party which issues digital certificates, the PKCs, that bind a public key to its owner. The digital signature created by using a private key gets verified by the corresponding public key in such a PKC. The PKC contains critical information which is signed by the CA. The CA as a trusted third party, performs the function of identity verification of the applicant before issuing a PKC to him. The distinguished name is a set of values that identifies the entity being certified. This includes country, organisation, organisation unit, name, etc. Additionally, other attributes describing the entity being certified such as address, telephone number, passport number, driving licence, election card number, etc., can also be included in the PKC. The public key belonging to this entity being certified is of course, a part of this PKC. The CA's digital signature on the certificate imparts it security and trust. A valid digital signature on a certificate is a guarantee of its integrity. Since the CA has signed the certificate with its private key, anyone verifying the CA's signature on the certificate is guaranteed that only the CA could have created and signed the user's certificate. Finally, the CA with strict security criteria for securing his own private key cannot deny having signed the certificate.

A CA therefore performs the following functions:

1. Reliably identifies persons applying for digital signature certificates,
2. Confirms the attribution of a public key to an identified physical person by means of a digital signature certificate,
3. Issues digital signature certificates and Certificate Revocation Lists,
4. Always maintains online access to certificates and CRLs,
5. Takes measures to operate its infrastructure in conformance with the IT Act, and as per its approved Certification Practice Statement (CPS), and
6. Provides the desired level of assurance for its various classes of certificates; undertakes liability as per the approved CPS.

The contents of a digital signature certificate are as follows:

1. Version
2. Serial number of the certificate
3. Signature algorithm used for signing
4. CA's distinguished name
5. Validity period of the Certificate
6. Distinguished name of the user
7. Public key of the user
8. Signature of the CA
9. Extensions

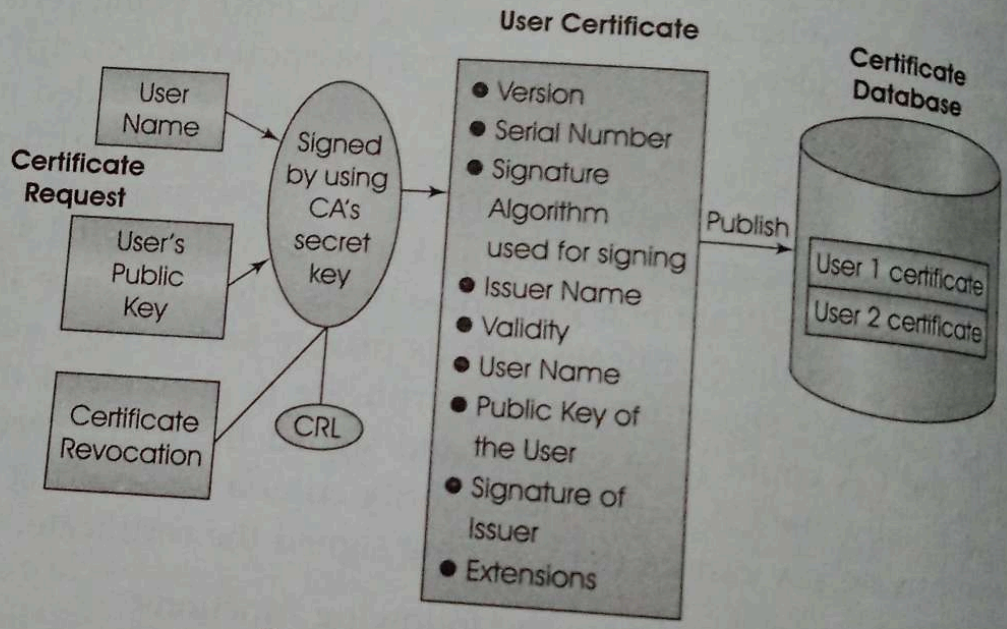

Fig. 17.1 *CA Operations*

One of the main functions of a CA is to make available all the certificates issued by it online, in the form of a directory, to its subscribers and relying parties. Relying parties wishing to enter into a contract with a subscriber of a CA can confirm the validity of the certificate from the CA's directory, and through it, the identity of the subscriber and other credentials that may be part of the certificate.

In the event of compromise of a subscriber's private key, he may request the revocation of his digital signature certificate.

The CA is obliged to issue a Certificate Revocation List (CRL) as and when such a request is received. There may be other circumstances that can warrant the revocation of a certificate. This includes circumstances wherein facts come to light, which, if known earlier, would have resulted in the non-issuance of the certificate.

The CA is also expected to perform some other functions that include time-stamping service, and making available reliable cryptographic software to subscribers for generating key-pairs.

The CA is expected to inspire confidence among its subscribers on the security of its infrastructure, the practices followed in its operations, and the liability that it is willing to take in respect of the digital signature certificates issued. This is done by the CA through its Certification Practice Statement (CPS)—a document published as the sum total of the practices followed by it. The CPS deals with practices with regard to certificate issuance and user registration, certificate lifetime and revocation, identity verification procedure, classes of certificates, certification publishing practices, and liability issues. On the basis of the recommendations of the Internet Engineering Task Force as contained in the document RFC 2527, the CAs normally cover the following areas in their CPs:

1. General Provisions including Obligations, Liability, Financial Responsibility, Interpretation and Enforcement, Fees, Publication and Repositories, Compliance Audit, Policy of Confidentiality and Intellectual Property Rights
2. Identification and Authentication
3. Operational Requirements
4. Physical, Procedural and Personnel Security Controls
5. Technical Security Controls
6. Certificate and CRL Profiles
7. Specification Administration.

A PKI manages the generation and distribution of key-pairs, and publishes the public keys as part of the PKCs and CRLs in open repositories such as X.500 directories. Subscribers and

relying parties can access these directories to verify the credentials of a person before completing a transaction in cyberspace.

The relying party, on receiving a public key certificate, authenticates the public key by virtue of its having been certified by a CA. If the relying party does not possess an assured copy of the public key of the CA who issued the certificate in question, a certificate containing the issuing CA's public key must be obtained. This process continues up the hierarchy until the verifying key is one of the widely trusted public keys. The trust path thus established would normally lead up to the root of the trust chain for a PKI.

Having established the trust path, the relying party has to decide how much a specific certificate can be trusted. This could depend on knowledge about the security controls, practices, identification and authentification methods, etc., followed by the CA in issuing these public key certificates. While practices and security controls are part of the Certification Practice Statement, the relying party should also be able to find out whether the certificate is adequate for the current requirement. Certificate policies are defined in X.509 recommendations as 'a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements specifically meeting this need of the relying party.' Certificates may be issued by a CA under different certificate policies, while there may be a single CPS. However, multiple CAs may support the same policy.

For a relying party to trust the certificate, a mechanism is required to link the certificate to the applicable certificate policy. In X.509 Version 3, certificate policy information is included through the optional certificate extensions. Certificate policies applicable to a specific certificate are indicated by unique registered object identifiers.

The relying party may also be faced with the need for evaluating different certificate policies. Comparison is normally based on factors such as forbidden applications, the required minimal

length of signature keys, public key protection methods and the verification methods of private key possession.

Certificate policies play a central role in public key infrastructure. Since certificates are issued by CAs for a variety of purposes, the certificate policies also constitute a critical component of the basis of the trust reposed by relying parties in a Public Key Certificate.

The trust chain from a subscriber of a CA to a subscriber of another CA can be formed through cross-certification arrangements between the two CAs. When two CAs enter into such an arrangement, each vouches for the certificates issued by the other. From a technical perspective, the process involves the creation of 'cross-certificates' between two CAs. When a CA cross-certifies another CA, he actually creates and digitally signs a certificate containing the public key of the latter. In a similar manner, the second CA creates and signs the public key of the former CA. The users in one domain are thus assured of the trust extended by their CA to the CA of another domain. Since cross-certification extends third party trust, the CAs entering into such an arrangement are expected to be completely comfortable with each other's security policies and practices employed in issuing certificates and in carrying out their operations.

A PKI enables such arrangements. It comprises CAs, certificate and CRL repositories, key management, back-up and recovery systems, timestamping services, cross-certification arrangements, client-side software for users interfacing with their applications and certificates in a consistent and trustworthy manner. The standards for the operations of CAs, certificates, CRLs, protection of their private keys in hardware security modules, standards for physical security of the infrastructure, audit standards, CPS framework and so on, are also part of the definition of a given PKI.

The PKI thus has the following features:

1. It allows parties to have free access to the signer's public key available in the directories of CAs

2. Public keys are freely distributed while private keys are securely held by the owners
3. It entails an assurance that the public key corresponds to the signer's private key, implying:
   —Trust between parties as if they know one another
4. Parties with no prior agreements, operating on open networks, can have the highest level of trust in one another.

The central issue governing the operation of CAs is whether they are to be licensed or accredited by the government or some voluntary association or a central body. The extent to which the government exercises some sort of regulatory authority over CAs tends to increase the level of trust that the subscribers can repose in e-transactions, especially in developing countries, since the legislation invariably provides for their smooth operation. This is the case in India. It will be discussed in the next section.

Liability is one of the most complicated issues surrounding PKI. What is the extent to which the law should define or limit the liabilities of the following players: the person who digitally signs the message, the person who relies on its validity, and the CA who vouches for the identity or some other attribute of the sender? The CA may be liable for any inaccuracies or misrepresentations in the certificate that may have been used by a relying party in trusting the sender for a transaction. The CA may also be liable if he has not revoked a certificate in time. It is for the CA to verify the identity of the subscriber, through a thorough investigation, before issuing a digital certificate. Depending on the class of certificate issued by the CA, digital signatures may be used for high value transactions. This can increase the risk of a CA, and hence his potential liability. A CA has to declare in his CPS the liability he is willing to accept for different classes of certificates.