OFFICE OF THE CONTROLLER
OF CERTIFICATION AUTHORITIES

GUIDELINES FOR AUDIT
OF CERTIFICATION AUTHORITIES

Table of Contents

1. TRUSTWORTHY SYSTEM

According to Regulation 6(f) of Digital Signature Regulations 1998 ("Regulations"), the person who intends to operate as a CA is required to maintain trustworthy systems for the generation and management keys and certificates; and to ensure the trustworthiness of the entire business operation.

1.1 Definition

- the trustworthy system provides specifications of recommended attributes for computer hardware, software, and related procedures that:
- are reasonably secure from intrusion and misuse;
- provide a reasonable level of availability, and reliability, and correct operation;
- are reasonably suited to performing their intended functions ; and
- adhere to generally accepted security principles.

1.2 Scope

The elements and criteria that constitute a trustworthy system are : -

- technical attributes and requirements of hardware that enable secure and reliable operation of the CA;
- technical attributes and requirements of software that enable secure and reliable operation of the CA; and
- policies and procedures that enable secure and reliable operation of the CA. These high level policies, normally specified in the CA's Certificate Practice Statement ('CPS'), should address
  - Local security policy issues; and
  - Technical security policy issues.

The first two elements are described in detail in ***The Technical requirements for evaluation, operation and audit of Certification Authorities*** document. Security considerations and measures taken into account when designing and implementing the technical components will be covered later in ***Section 3.0 – Suitable security measures***. The third element will be explained under section 1.3 and 1.4.

1.3 Local security policy

The CA should establish local security policies and supporting procedures regarding the use of computers and computer information. For example, policies regarding the handling of confidential, sensitive and proprietary data, as well as the implications of a breach of these policies, such as disciplinary actions. Such policies and procedures provide a means to ensure the integrity, accuracy and completeness of the data being processed. Policies should also ensure that only suitably qualified staff are responsible for operating the computer system.

1.3.1 *Physical and environmental control*

All computer equipment and resources should be physically protected. Access should be restricted to only those staff who are properly authorised. Security precautions should not, however, impede the efficient running of the business operation. Appropriate physical access controls will reduce the risk of computer equipment being stolen or accidentally or deliberately damaged. It will also help to prevent accidental disclosure or theft or sensitive or confidential information such as the CA's private key.

The following security issues should be addressed:

- Security facilities such as use of closed-circuit cameras, monitoring devices, locks and access control devices (keys, token or smart card) should be implemented.

- Guards or receptionists should ensure that only authorised persons may enter the office. If there is more than one entrance to the office, access to all entrances should be controlled.

- Physical access controls are usually applied at two levels: access to the organisation's offices or premises and access to the area within the offices/premises where the CA computer equipment is located.

- Access to the office outside hours should also be regulated. In particular, it may not be desirable for certain grades of staff to have unrestricted access to the premises.

- Ideally, key computer equipment should be physically secured. If , however, it is not practical to keep key computer equipment, such as the network server, in a secure area, then it should be located where it is clearly visible, and where access can be observed (rather than in a secluded area where tampering with the equipment may go unnoticed).

- There should be adequate protection against risks such as fire and flood, for example, conveniently placed and adequately maintained fire extinguishers.

- CA's data center should be kept tidy. Food, and in particular drinks, should not be allowed near computer equipment.

1.3.2 *Procedural controls*

Ideally, no single individual should be able to exercise control over than one functional or business area. A formal separation of duties is crucial due to the high security requirements of the CA operation. Separation of duties reduces the risk of fraudulent activities as controls are easily bypassed when a single individual is empowered to control several functional areas. Separation of duties also reduces an organisation's dependence upon key staff. Where separation of duties is not practicable, compensating controls should be put in place to ensure the trustworthy operation of the CA.

These measures should be considered:

- The roles and responsibilities of the operative personnel should be distinctly defined. The level of authorisation and access privilege of these individuals performing critical CA operation also be clearly stated.

- Privileged access such as supervisor authority should be restricted to one or at most two senior and responsible individuals. This access can potentially be used to delete and corrupt data without leaving any audit trial and therefore should be strictly controlled.

- A suitably senior and key individual should be allocated the responsibility for insuring that appropriate policies and procedures are developed and enforced and that computer security is taken seriously.

- Segregation of duties principle should be implemented. Protection of private-keys value or other secret values that control access to private-key value should involve split knowledge or secret sharing whereby, secret shares are distributed to a number of independent individuals.

- Individuals responsible for system development should be segregated from those having control over computer operations, key management personnel and CA operations personnel.

1.3.3 *Personnel controls*

The management should set out clear policies on the recruitment, assessment, training and dismissal of operative personnel. Bona fide references should be taken up for all recruits, including temporary and contract personnel, to ensure that they are adequately qualified and that they do not present a security risk to the organisation.

These issues should be considered:

- Thorough background checks and clearance procedures should be performed on key operative personnel to ensure integrity.

- All operative personnel, including temporary and contract personnel, who are required to perform core CA operation should be adequately trained. Retraining period and retraining procedures should also be considered.

- Special control measures should be taken for contracting personnel (such as bonding, monitoring, auditing and special contract provisions).

- Sanction against personnel in the event of unauthorised actions of suspected malicious actions.

- Frequency and sequence for job rotation among various roles.

1.3.4 *Disaster recovery and backup*

Data and programs are usually held on hard disks, diskettes, magnetic tape or cartridges. These media are susceptible to damage, theft or loss and consequently the data held on them are vulnerable. Further, the computer hardware itself can damaged, perhaps through failure of a significant component of the system or an external factor such as a fire. Steps should be taken to ensure that the CA can promptly and effectively, recover its data, application programs and computer facilities with minimum disruption to the business if an accident or a "computer disaster" occurs. This is particularly important where the effect of a loss of computing capabilities may have a serious impact over the entire certification process.

Measures to be considered are:

- The management should determine which files, application programs and documentation are critical to the running of the business. Critical certification related information and records such private keys, databases containing certificates and CRLs. They should then establish an appropriate backup strategy based on the findings. Backup and recovery procedures should then be documented and staff should be instructed on their implementation.

- Adequate and frequent backup of data and programs should be taken to ensure than the system can be recovered after a "computer disaster" and before the business is disrupted.

- The management should assign specific individuals to perform backups.

- At least three generations of the backup should be kept. However if daily backups are taken it may be easier administratively to retain six or seven generations, for example Monday's daily backup should be kept until the following Monday when it can be overwritten, etc. Month end and year end copies of files may be retained for longer periods as required. The records required by Regulation 78 should be kept for a period specified in Regulation 80. Records kept in digital form should be digitally signed.

- At least one copy of the most recent backup should be kept off-site and should be securely stored, for example in a fire-proof safe.

- Magnetic tapes, diskettes or cartridges used for backup should be clearly and accurately labeled. Backups should be tested periodically to ensure that they can be restored when ultimately needed.

- Copies of essential documents, such as user manuals, system and applications documentation, should also be kept off-site.

- The management should develop a formal recovery plan setting out specifically what to do in the event of a disaster which results in a prolonged disruption of computing facilities. The management should also consider the impact of such a disaster on their business and outline the necessary recovery procedures.

- Data, including backup copies, held on magnetic media such as diskettes or cartridges should be properly labeled and locked away when not in use.

- Printouts containing confidential or sensitive information should be filed away and, when no longer required, should be carefully disposed of to prevent accidental disclosure of such information. The management should however take preventive measure to ensure that they do not violate the Regulation 80 or any other provision with respect to the retention of records.

1.4 Technical security policy

The management should establish an appropriate strategy regarding the acquisition of computer hardware and software. This would ensure that the computer facilities are able to meet a sufficiently high level of security requirements and to support the business operations.

1.4.1 *Computer security function and assurance*

The management should take the necessary measures to ensure all the security related hardware and software used meet recognized criteria as to security functionality and assurance. A computer security rating for computer systems may be required. The rating could be based, for example, on the Trusted System Evaluation Criteria (TCSEC), Canadian Trusted Products Evaluation Criteria, European Information Technology Security Evaluation Criteria (ITSEC), British standard BS7799 or the Common Criteria. This component can also address requirements for product evaluation analysis, testing, profiling, product certification, and/or product accreditation related activity undertaken.

1.4.2 *System life cycle controls and assurance*

This component addresses system development controls and security management controls. This component can also address life-cycle security ratings based, for example on the Trusted Software Development Methodology (TSDM) level IV and V, independent life-cycle security controls audit, and the Software Engineering Institute's Capability Maturity Model (SEI-CMM).

System development controls include environment security development, personnel security development, configuration management security during product maintenance, software engineering practices, software development methodology, modularity, layering, use of failsafe design and implementation techniques (e.g. defensive programming) and development facility security.

Security management controls include execution of tools and procedures to ensure that the operational systems and networks adhere to configure security. These tools and procedures include checking the integrity of the security software, firmware, and hardware to ensure their correct operation.

1.4.3 *Network security control*

All communication affecting security of the Public Key Infrastructure ('PKI') and access to data and software on computer networks should be selectively restricted to authorised personnel. Access should only be granted that is sufficient to enable personnel to perform their duties. Systems can only be considered reliable if it is free from unauthorised changes to either the data or the programs. Adequate safeguards over unauthorised access will protect confidential and sensitive information and prevent unauthorised modifications or corruption of data. They will also reduce the risk of viruses or other malicious programs being introduced into the system.

- A suitable person should be designated Network Security Officer to control and monitor network security and activities, for example, ensuring the list of network users is up-to-date, and following up any unauthorised access attempts.

- Each network user should be assigned a unique identifier, often referred to as a user-ID that has an associated user profile and an associated password. Users should change their initial passwords immediately when they log on to the network for the first time.

- Users should keep their IDs, profiles and passwords secret, and should regularly change their passwords. Guidelines concerning passwords should be properly set out. For example, the frequency of password change, the length of the password, which should ideally be at least six characters long, and guidance regarding the format to ensure that the passwords cannot be easily guessed.

- Special security features provided by a network operating system should be applied where appropriate. For example, users profiles can and should be disabled after a certain number of unauthorised access attempts, or the date and time of when each users is able to log on to the system should, if possible, be pre-defined.

- The network administrator profile should be constantly monitored. It is also advisable to keep passwords of key users in sealed envelopes for emergency use. The envelopes should be securely stored and passwords should be changed immediately after each emergency access.

- Where dial-up access is permitted using modems and telephones lines, the network administrator should consider the use of dial-back procedures thus exercising some degree of control over telephone access.

- The network administrator should adequately control and supervise the maintenance of hardware and software applications, especially when this work is performed by the respective vendors. This is to prevent accidental corruption or disclosure of sensitive data and applications.

- The network administrator should set up monitoring software that can alert the presence of attack against the network. The network administrator should also record the IP addresses of the source computers and determine the source of attacks in order to take legal measures (Computer Crime Act 1997) to stop the problem.

1.4.4 *Cryptographic module Engineering controls and assurance*

The security measures should focus on the functions and characteristics of hardware or software cryptographic modules, for example, conformance to FIPS140-1 or its equivalent.

2. APPROVED DIGITAL SIGNATURE SCHEME

2.1 Purpose of digital signature

Digital signature can be used for many purposes, including signing certificates, signing Certificate Revocation List (CRL), signing contracts, signing email messages, signing various data in Internet Security Association and Key Management Protocol (ISAKMP), Secure Socket Layer (SSL), Secure Electronic Transaction (SET), Transport Layer Security (TLS), or other protocol exchanges.

The digital signature can be used to provide several security services such as:

- data integrity,
- data origin authentication,
- entity authentication
- non-repudiation

2.2 Recommended Digital Signature Scheme

We recommend a digital signature scheme that fulfills the requirement specified in, Regulation 29 of Regulations. The recommended scheme:

- uses a secure public-key algorithm for the generation of the key pair and a secure public-key algorithm and hash function for the creation of the digital signature.

- creates digital signature that is not capable of being modified to contain a subliminal channel.

In the context of signing an electronic document, the digital signature created must have characteristics that satisfy the following conditions:

- The signature must be authentic and must convince the document's recipient that the signer deliberately signed the document.
- The signature must be unforgeable and must serve as a proof that the signer and no one else deliberately signed the document.
- The signature must not be reusable and must be part of the document. Any unscrupulous person cannot move the signature to a different document.
- The signed document cannot be modified after the document is signed. The signature will not be verified if the document is altered.
- The signature cannot be repudiated. The signature and the document are physical things that the signer cannot later claim that he or she did not sign it.

A public-key based digital signature scheme is recommended as opposed to biometrics or handwritten signature because it permits detailed statutory alignment and policy making in the context of the known capabilities or weaknesses. The public-key cryptosystem is proven to be the most prominent and widely used technology available today. It provides a high degree of certainty with regard to the authentication of parties to communications, message integrity and non-repudiation. It also provides evidentiary presumptions relating an organisation to the message digitally signed with its private key.

There are a number of public-key cryptography based digital signature schemes available today such as RSA, DSA, GOST, ESIGN and EIGamal. Among the most widely used are RSA and DSA. RSA reversible digital signature scheme is based on RSA public-key cryptosystem. RSA is also the international digital signature standard defined in ISO9796 and is used in the information annex to ISO9594-8 (ITU-T X.509). The French banking community standardised on RSA, as have the

Australians. DSA, as specified in US Federal Information Processing Standard 186 and in Part 1 of ANSI standard X9.30 digital signature scheme, is based on irreversible public key cryptosystem. The US NSA (National Security Agency) developed DSA. There have been allegations that the US government prefers the DSA because it is only a digital signature algorithm and cannot be used for encryption. GOST is a Russian digital signature standard that is very similar to DSA. ESIGN is a digital signature scheme from NTT Japan. It is touted to be at least as secure and considerably faster that either RSA or DSA, with similar key signature length.

The lack of viable digital signature technology for the past decade has made RSA a de facto standard. Many large international organisations such as Microsoft, Netscape, Motorola, Nortel, Apple, Lotus, Novell and IBM have incorporated RSA algorithm into their products.

DSA[1], although is known to be capable of containing subliminal channel[2], will likely be a strong competitor to RSA digital signature schemes for some time to come. In terms of the function provided and cryptographic strength, the scheme seems essentially equivalent. The choice between them will therefore rest on factors such as performance, licensing issues and political acceptability. Subliminal channel allows someone to insert a secret message in his signature that can only be read by another person who has the key. Subliminal channel can also be added to the following public-key algorithms ElGamal and ESIGN.

---

[1]G.J Simmons, "The subliminal Channels of the US Digital Signature Algorithm (DSA)," *Proceedings of the third symposium on: State and progress of Research in Cryptography, Rome: fondazone Ugo Bordoni, 1993* **PP 35-54**

[2]G.J Simmons, "The Subliminal Channel and Digital Signatures", *Advances in Cryptology: Proceedings of EUROCRYPT 84, Springer-Verlag, 1985 pp 364-378*

Elliptic curve cryptosystem (ECC), a relatively new technology, is becoming increasingly accepted as basis of digital signature systems. Having the ability to perform the same functions as RSA and DSA, the Elliptic curve based digital signature system has more efficient implementations. The generation and verification of ECC digital signature is faster than that of the RSA and DSA. It has been studied for several years and has been implemented in some commercial products.

Several initiatives, such as the World Wide Web Consortium (W3C), the World Trade Organisation (WTO), the Organisation for Economic Cooperation and Development (OECD), and the UN, are working on international standards for digital signature schemes. Results will only be obvious in the next few years.

2.3 Recommended Key Length

The criterion for choosing the key length correlates with the value transaction in which the signature is used. The longer the key, the more protection it offers but at a cost of computing resources. As such key length must be weighed against the value of the transaction it serves to protect. Comparison and recommendation of appropriate key length is beyond the scope of this paper. Simple comparison of key length is not appropriate since different key algorithm requires different key length for comparable strength. The controller of CA must continually evaluate appropriate key length as increase in computer power and development of advanced mathematics continue to degrade strength of keys over time. A key length that is appropriate today will likely not meet the needs of the subscribers tomorrow.

3. SUITABLE SECURITY MEASURES

In deriving the technical components that will be used in operating CA, suitable security measures of those technical components should be defined to support the reliability, integrity, and the accountability of the CA services.

3.1 Objectives

The objectives of the security measures are to:

- minimise business damage by preventing and minimising the impact of security incidents; and

- reduce the risks associated with threats to the services provided arising directly and indirectly from human error or deliberate subversion.

3.2 Key pair generation

In deriving the key pairs, these issues should be addressed:

- The application forms submitted should be documented (in the case whereby the CA generates the subscriber's keys upon request).

- The successful applications must be approved by the registration officer.

- The key generation systems should allow the authorised registration officer to generate the key pairs. The user identification (user-IDs) and passwords should be supplied. Alternatively, a smart card system could be used to achieve a higher level of security.

- The key pairs should have unique identifiers.

- The key generation systems should not:
  - accept the creation of the key pairs that have been improperly generated;
  - duplicate the existing key pairs; and
  - derive the corresponding public key by using the private key.

- In creating the key pairs, these security requirements should be documented and implemented:

- Keys are generated using a random or pseudo-random process. It is not feasible to determine the probability of the key from the set of the all possible keys. In addition, in generating the key, it must not be in the form that could be interpreted by humans.
- The CA's signing key pair should be at least 1024 bit if RSA digital signature scheme is used.

3.3 Key usage and loading

In using the CA's private key, these should be addressed:

- The user could be identified through either the personal identification number or other data used for identification as long as it is comparable with the data storage medium for the private key of the user.
- The private key should not be disclosed.
- No function of deriving the private key from the digital signature.
- Certificates issued by the CA should contain the *keyUsage* extension restricting the purpose to which the certificate can be applied.
- The signing private key should only be used to sign certificates and CRLs issued by the CA.

Key loading should be handled in a secure manner, procedures to ensure these security features below should be maintained, documented and implemented:

- Prior to loading, inspect the secure cryptographic devices for signs of tampering and there is no leakage on the interface that could disclose the transferred key components.
- The key components are only possessed physically by the designated owner and only for the minimum practical time.
- Hardware used for the key loading function are properly controlled and maintain in secured manner. Use of the equipment is monitored and a log of all key

loading activities maintained. All cable attachment is monitored of all key loading activities maintained. All cable attachments are examined before each application. This examination should be documented and signed by the appropriate person.

- Devices that transferred the key from the generation to the use of key is the secure cryptographic device. This transfer device does not retain any information after the key has been transferred.

- More than one individual are required to enable the use of the CA'S root private key which is used to sign other lower class CA certificates.

- The key pairs that are used for system testing purposes should not be shared or substituted with the keys used for the system production. Keys used for prototyping or pilots should not be used for production.

3.4 Key Protection/ Storage

In ensuring the confidentiality, integrity and the availability of the private key, the suggested security measures are:

- The CA private key should be stored using physically and environmentally secure and separate locking containers that only appropriate key owners or custodian could accessed.

- The private keys and its components should not exist as hard copy unless in encrypted form.

- The CA signing private keys and most subscriber signing private keys are generated in software, within the cryptographic module. In the case of hardware tokens (e.g. microprocessor based smart cards), the token may or may not produce the private signing key the end-entity. If the hardware token is a storage only device, the private signing key is generated in software and injected onto the device encrypted. In both hardware tokens and software cases, the keys are decrypted only at the time at which they are actually being used.

- If the CA's private key is stored on a hardware token, and a personal identification number (PIN) or similar mechanism is used to access the token, then only that token's owner (or designated backup) ever has possession of both the token and its corresponding PIN.

- If the CA's private key (or fragment) is stored in a secure cryptographic device or hardware token, the key should not be intentionally presented outside of the physically secure environment used to certificate processing, other than for backup purposes.

- Backup copies of private keys are subject to the same greater level of security controls as keys currently in use. Backups are securely stored offsite with proper access controls and under at least dual control. The offsite facility must be sufficiently remote from the primary location so as to not be subject to the same potential threat or disaster as the primary facility. Backup copies of private keys held in secure cryptographic devices are controlled by positive user identification (e.g. access identifier and password or other methods) to prevent unauthorised use of the key.

- If the private key is split so as to generate signatures separately (with the signature combined to form a signature identical to the one that would be created by the unfragmented key), then the key fragments of at least level 2 of ANSI X9.66. Secure cryptographic devices storing an unfragmented private key meet at least level 3 of ANSI X9.66.

3.5 Key Destruction

- The hardware token or secure cryptographic device used to generate a private key should be destroyed, if the private key is distributed as secret shares (fragments) to other secure cryptographic devices for creating signatures.

- Instances of private keys that are no longer actively used or that have been replaced by a new key are destroyed. Keys destroyed at one location may continue to exist at another for archival purposes. Private key information

necessary to recreate the keys for active use may exist at the operational location until deletion or termination.

- Deletion of private keys when are no longer required for operational use. Deletion occurs when all instances of the key and the information from which the key may be reconstructed are destroyed at the operational storage/ use location. After deletion, the keys shall only exists for archival purposes.

- Private keys are terminated when there is no further need to verify the legitimacy of transactions occurring prior to their destruction exists. No information exists from which the keys can feasibly be reconstructed.

3.6 Key Compromise

- Contingency plan for key compromise should address who is notified and what actions are taken with system software and hardware, symmetric and asymmetric keys, previously generated signatures, encrypted data, etc.

- In the event of a compromise of a CA's private key(s), the CA should cease issuing certificates under the compromised key(s) or any other use of the compromised key(s) and revoke the CA's certificate(s) pertaining to the compromised key(s); and the CA should verify the validity of digital signatures prior to releasing new certificates.

3.7 System Auditability

- All entries in the audit trail are date time stamped. The audit trail at a minimum includes:

  - All key management operations, such as key generation, backup, recovery, compromise and destruction.
  - Identity of the person authorising the operation and the person handling any key material (such as key components or key stored in portable devices or media).
  - Action taken for the compromise of a private key and the expiration of a certificate.

- Events related to the issuance and revocation of certificates.
- Changes in the custody of keys and of devices or media holding keys. Access to the physically secure environment or any component thereof.
- Physical movement or modifications to any CA related hardware or component thereof.
- Invalid physical or logical access attempts.
- Access to the audit journal.

- Audit trails are maintained in a form which prevents unauthorised modification or destruction of the record.

- Documented procedures exist and are followed to ensure that the audit trails reviewed after each event. The review itself is documented and includes procedures for identifying and reporting violations.

- Documented procedures exist and are followed to ensure that backup of the audit trail occur either daily or for each database access. Backups are physically secured and stored in at least one off-site location. Backup are retained for a period not less than ten years for records pertaining to the issuance or revocation of any certificate as required by Regulation 80.

3.8 CA System Access

- All entities logging on to the CA system must be authenticated.

- If password is used as mean for authentication, stringent set of rules to each password must be applied. Some of the rules on password selection are:

  - it must have at least 8 characters;
  - it must have at least one upper-case letter or digit;
  - it must have at least one lower-case letter;
  - it must not contain many occurrences of the same character;
  - it must not be the same as the entity's profile name; and
  - it must not contain a long substring of the entity's profile name.

3.9 Certificate Issuance Processing

- The on-line enrollment form at the CA web site requires completion of all relevant fields before the form can be submitted the CA for processing.

- All communications between the customer's browser and the CA web server are in SSL during the enrollment process.

- Certificate request are received at the CA operations center and issued only by the CA's authorised employees with the designated authority, after all authentications steps have been performed.

- The CA system should automatically records the date, time and user ID of any record update to certificate applications in an audit trail history.

3.10 Certificate Revocation

- When certificates are revoked either by customer request or directly by the CA, the status of certificate is updated in the CA system to reflect the revoked status. This process occurs in real time. Customers desiring to check the validity of a particular certificate are required to search the repository for the particular certificate to ascertain its status.

- Requests made to revoke a certificate are required to be sent to the CA center on company letterhead by an authorised representative from the certificate holder's organisation, together with the reason for revocation.

- A separate fax machine is used to receive revoke order request to ensure revocation requests are not mislaid and that they are processed on timely basis.

3.11 Management Reporting

- The management reports generated should be timely, accurate and provide sufficient information for management decisions.

- Report are generated for the aggregate number of certificate enrollments received so that staff resourcing issues for the processing of enrollment request can be better defined in the future.

- Network availability reports are available and reviewed by IS management to ensure there are no recurring network problems and to assist in determining future network capacity needs.

3.12 Verification of Digital Signatures

The component to used to verify the digital signatures should:

- detect the fake digital signatures;
- detect falsification of signed data; and
- be capable of preventing of the unauthorised use of private keys.

3.13 Collecting Identification Data

In collecting or transmitting the identification data, the technical components should ensure that the identification data:

- is not capable to be disclosed or revealed; and
- is stored on the storage medium with the private key.

3.14 Representation of the Signed Data

The security measures that should be considered for this technical component are:

- facility to reveal the creation of the digital signature. This is necessary to determine the validity of the sender; and
- allow the matching of the data with the related digital signature.

3.15 Checking Signed Data

The technical component should:

- detect whether there is any unauthorised modification to the signed data;
- determine the data that the digital signature is referring to; and

- identify the private key owner whom the digital signature is attributed to.

3.16 Verifying Certificate

To verify the certificate received, the technical components should be able to detect whether or not the certificate is valid by verifying it with the CA root certificate.

4. CERTIFICATE PRACTICE STATEMENT

The term Certification Practice Statement ('CPS') is defined by the ABA Guidelines as: "A statement of the practices which a CA employs in issuing certificates". A CPS prescribes the practices, procedures, and systems that the CA employs in its operations and in support of the issuance, management, and revocation of a certificate. CPS is often presented by the CA as one of the main elements through which it promotes reliance in the trustworthiness of the certificates it issues and, more generally, as the standard of quality and liability that should govern the relationship between CA and its subscribers.

The practices, procedures and security controls embraced by the CA in authenticating the holder of the key pair will determine the level of trust any relying party has upon a certificate issued by that CA.

Whether a CPS is binding on a relying person depends on whether the relying person has knowledge or notice of the CPS. A relying person has knowledge or at least notice of the contents of the certificate used by the relying person to verify a digital signature, including documents in incorporated into the certificate by reference. It is therefore advisable to incorporated into the certificate by reference. It is therefore advisable to incorporate a CPS into a certificate by reference.

4.1 FORM OF CERTIFICATE PRACTICE STATEMENT

A CPS may take the form of a declaration by the CA of the details of its trustworthy system and practices it employs in its operations and in support of issuance of a certificate, or it may be a statute or regulation applicable to the CA and covering similar subject matter. It may also be part of the contract between the certification

authority and the subscriber. A CPS may also be comprised of multiple documents, a combination of public law, private contract, and/or declaration. The main element, however, is notice to the relying parties.

Certain forms for legally implementing CPS lend themselves to particular relationships. For example, when the legal relationship between a CA and subscriber is consensual, a contract would ordinarily be the means of giving effect to a CPS. The CA's duties to a relying person are generally based on the CA's representations, which may include a CPS.

4.2 CONTENT OF CERTIFICATE PRACTICE STATEMENT

The CPS should contain information or statement that is importance both to the holder who is obtaining the certificate and to the relying parties who will use the certificate issued by the CA as the basis for entering into transactions with the holder.

Although the level of detail may vary among CPSs, they will generally be more detailed than certificate policy definitions. Generally, a CPS should at the least cover the following details:

- description of the precise service offerings;
- procedures used to authenticate the identity of the applicant for a certificate (prior to issuing the certificate);
- the physical, procedural, and personnel controls used by the CA to perform securely the functions of key generation, certificate issuance, certificate revocation, audit, and archiving;
- the security measures taken by the CA to protect its cryptographic keys;
- widely recognized standards to which the CA's practices conform; and
- potential technological compatibility of the certificates issued by the CA with repositories and other systems.

Although such detail may be indispensable to adequately disclose, and to make a full assessment of trustworthiness in the absence of accreditation or other recognized quality metrics, a detailed CPS does not form a suitable basis for interoperability between CAs operated by different organisations. Rather, certificate policies best serve as the vehicle on which to base common interoperability standards and common assurance criteria on an industry-wide (or possibly more global) basis. A CA with a single CPS may support multiple certificate policies (used for different application purposes and/ or by different certificate user communities). Also, multiple different CAs, with non-identical CPS, may support the same certificate policy.

5. ARRANGEMENT WITH REGISTRATION AUTHORITIES ('RA')

There are two models on how the CA could handle subscriber's identity verification. In the first model, the CA itself performs the RA function whereas in the second model the CA issues certificates upon the instruction by its appointed RA(s). There are two scenarios in the second model whereby the RA can be an third party agent appointed by the CA or the RA can be part of the CA such as being a member of the consortium company that forms the CA.

In the second model, the CA should be responsible and liable to its appointed RAs. The CA should, at all time, ensure the trustworthiness of the operations performed by its RAs by observing the following recommended guidelines:

- The CA should developed standards and guidelines to ensure that the relevant section of the CA's CPS are compiled with as well as the Act and Regulations;
- The CA should provide the relevant training to its RAs.
- The CA should have personnel control to ensure trustworthiness of its RAs.
- The CA needs to ensure that it establishes a secure mode of communication with the RAs for accepting certificate request and revocation instruction.
- The CA should keep proper maintenance and storage of books and records related to the validation of certificate request.

- The CA should perform periodic internal review to access its RAs to ensure the operations of its RAs comply with its CPS, the Act and Regulation.

- The CA may consider the existence of external third party audit report such as SAS70 over its RA's operations.

- The CA should have policies and procedures for certificates revocation and suspension process by RA if its RAs perform such activities.

- The CA should provide policies, procedures and other operating manual to its RA or encourage its RAs to develop such documents.

Please note that these guidelines are not comprehensive and the CA should constantly review these guidelines as the market progress.