

SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

Version 2.0

September 2003

(Total number of pages: 32)

No part of this document shall be reproduced, in any form or by means, without permission in writing from the Infocomm Development Authority of Singapore.

The Infocomm Development Authority of Singapore makes no warranty of any kind with regard to this material and shall not be liable for errors contained herein or for incidental or consequential damages in connection with the use of this material.

TABLE OF CONTENTS	PAGE
PREFACE	5
1. INTRODUCTION	6
1.1 PURPOSE.....	6
1.2 SCOPE.....	6
1.3 PUBLIC KEY INFRASTRUCTURE FRAMEWORK	7
1.4 TERMINOLOGY	7
1.5 DEFINITION OF TERMS	7
2. MANAGEMENT GUIDELINES	11
2.1 OBLIGATIONS	11
2.2 LIABILITY	12
2.3 CERTIFICATE POLICY AND CERTIFICATION PRACTICE STATEMENT.....	12
2.4 SECURITY MANAGEMENT.....	12
2.5 RISK MANAGEMENT.....	13
2.6 PERSONNEL CONTROL	14
2.7 MAINTENANCE OF SUBSCRIBERS' DATA	14
2.8 INCIDENT MANAGEMENT	15
2.9 BUSINESS CONTINUITY PLANNING	16
3. CERTIFICATE MANAGEMENT GUIDELINES	17
3.1 CERTIFICATE ATTRIBUTES	17
3.2 REGISTRATION	17
3.3 GENERATION	18
3.4 ISSUANCE	18
3.5 PUBLICATION	18
3.6 RENEWAL.....	19
3.7 CERTIFICATE SUSPENSION	19
3.8 CERTIFICATE REVOCATION	19
3.9 ARCHIVAL.....	21
3.10 AUDIT TRAILS.....	21
4. KEY MANAGEMENT GUIDELINES	22
4.1 GENERATION	22
4.2 DISTRIBUTION	22
4.3 STORAGE.....	22
4.4 USAGE.....	22
4.5 BACKUP.....	23
4.6 KEY CHANGE.....	23
4.7 DESTRUCTION	23
4.8 KEY COMPROMISE	23
4.9 CA KEY AND SUBSCRIBER ENCRYPTION KEY ARCHIVAL	24
4.10 CRYPTOGRAPHIC ENGINEERING	24
5. SYSTEMS AND OPERATIONS GUIDELINES	25
5.1 PHYSICAL SECURITY	25
5.2 SYSTEMS AND SOFTWARE INTEGRITY AND CONTROL	26
5.3 CHANGE AND CONFIGURATION MANAGEMENT	26
5.4 NETWORK AND COMMUNICATIONS SECURITY	26
5.5 MONITORING AND AUDIT LOGS	27
6. APPLICATION INTEGRATION GUIDELINES	29
6.1 INTEGRITY OF SIGNING AND VERIFICATION FUNCTIONS.....	29

6.2	PROTECTION OF PRIVATE KEY	29
6.3	VERIFICATION OF CERTIFICATES	29
7.	REFERENCES	31
8.	ACKNOWLEDGEMENTS	32
9.	VERSIONS.....	32



SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

Preface

In electronic transactions performed over an open network such as the Internet, there is a need for the parties involved to be assured of the identities of the transacting parties in the electronic environment. There is also a need to ensure that the electronic transactions are reliable and have not been tampered with.

Public key technology provides the capabilities for transacting parties in an electronic environment to authenticate each other's identities and ensure non-repudiation of electronic transactions through the use of digital signatures.

A certification authority acts as a trusted party to facilitate the confirmation of the relationship between a public key and a named entity. The certification authority issues digital certificates that can be used for authentication and digital signatures. The certification authority also performs certificate management services such as publication and revocation of digital certificates.

As certification authorities play a vital role in facilitating secure electronic transactions, there needs to be assurance that the certification authorities perform their roles and duties with high levels of integrity and security.

This document defines the security guidelines for the management, systems and operations of a certification authority. It is intended for use by the management, security, technical and operational personnel of a certification authority. It is assumed that the reader has basic understanding of public key technology and certification authority. The document makes reference to the BS 7799-1:2000 on general IT systems and operations.

The Controller of Certification Authorities (henceforth referred to as "the Controller") is the regulatory authority that supervises the activities of certification authorities in Singapore. Certification authorities that intend to be licensed by the Controller shall comply with the mandatory requirements stated in this document.

Where applicable, the provisions in the Electronic Transactions Act 1998 and the Electronic Transactions (Certification Authority) Regulations 1999 or any future versions thereof shall take precedence over the Security Guidelines.

This document will be reviewed on an ongoing basis to take into account the evolution of security and other related technologies.

Comments on this document can be forwarded to:

Controller of Certification Authorities
c/o Infocomm Development Authority of Singapore
8 Temasek Boulevard
#14-00 Suntec Tower Three
Singapore 038988
Email: cca@ida.gov.sg
Website: <http://www.cca.gov.sg/>



SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

1. Introduction

1.1 Purpose

The purpose of this document is to define security guidelines for the management, systems and operations of licensed certification authorities (CAs). The guidelines are aimed at protecting the integrity, confidentiality and availability of certification services, data and systems.

The security guidelines shall apply to licensed CAs and potential licensees that perform the role of trusted third parties to verify and vouch for the identities of entities in the electronic environment. The CAs perform the following certificate management functions:

- Verification of registration, suspension and revocation requests;
- Generation, issuance, suspension and revocation of certificates; and
- Publication and archival of certificates, suspension and revocation information.

1.2 Scope

The scope of this document covers the basic role and functions of a CA, i.e. identity verification and certificate management. It does not address extended functions such as electronic notary and trusted time-stamp service.

This document does not address the requirements for a hierarchy of CAs, e.g. the CA's relationship with a higher-level CA and a cross-certification entity. The security guidelines do not cover interoperability requirements across CAs, e.g. certificate formats and certificate management protocols.

SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

1.3 Public Key Infrastructure Framework

This document defines the security guidelines for the functions, systems and operations of a generic Public Key Infrastructure (PKI) as illustrated in Figure 1:

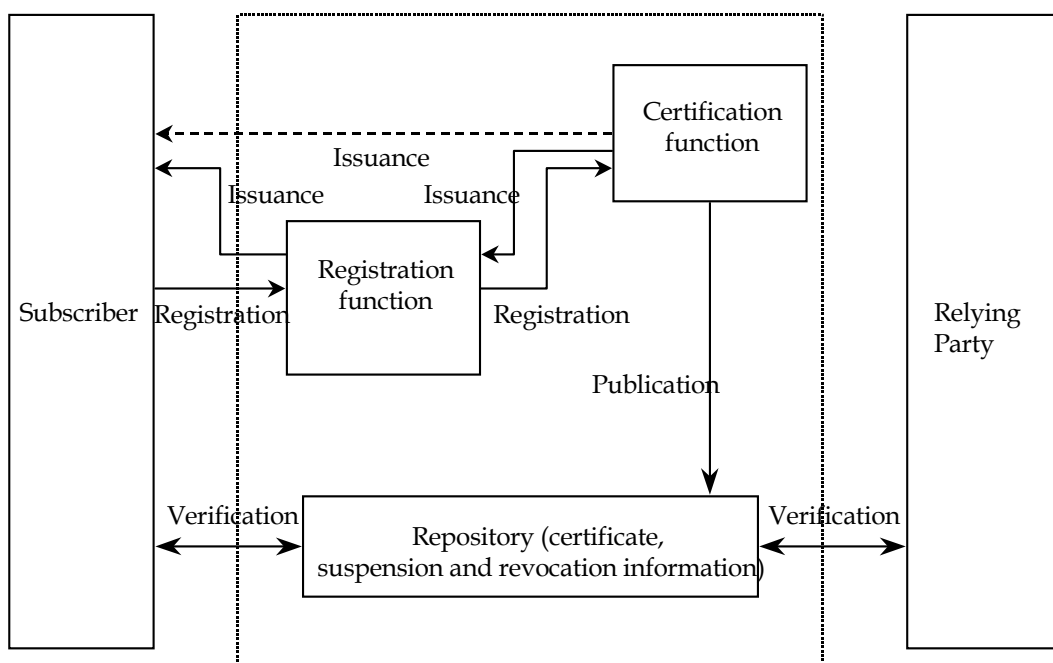


Figure 1: Logical Representation of PKI Entities and Processes

1.4 Terminology

The following terminologies used in the security guidelines are to be interpreted as follows:

- ❑ Shall: The guideline defined is a mandatory requirement, and therefore must be complied with.
- ❑ Should: The guideline defined is a recommended requirement. Non-compliance shall be documented and approved by the management. Where appropriate, compensating controls shall be implemented.
- ❑ May: The guideline defined is an optional requirement. The implementation of this guideline is determined by the CAs' requirements.

1.5 Definition of terms

CA certification key	The CA's private key that is used to sign certificates, suspension and revocation information.
CA operator	The technical personnel that operate the systems associated with the CA's function.
CA systems	The systems that perform or support the registration, certification and repository functions of a CA.
Certificate	Digital document verifying the correspondence between a public key and a named entity. It contains certain digitally signed information, including

SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

	the identification information of the entity, the public key, purpose and scope of the usage of the key, name of certification authority, etc.
Certificate generation	The process of approving a user's registration request and the production of a certificate associated with the request.
Certificate Policy	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.
Certificate revocation	<p>There are 2 main categories of certificate revocation:</p> <p>Permissive revocation: The invalidation of a certificate within the validity period of that certificate as a result of a request by the subscriber or subscriber-authorized representative.</p> <p>Required revocation: The invalidation of a certificate within the validity period of that certificate because:</p> <ul style="list-style-type: none"> • information on the certificate is no longer valid. • the private key associated with the certificate, or the media holding the private key, has been or is suspected of being compromised. • the subscriber is no longer a member of the community that is subject to the Certificate Policy. • the issuer determines that the certificate was not properly issued in accordance with the Certificate Policy and/or any other applicable practice documents. • the CA ceases operations. In such an event, all certificates issued by the CA shall be revoked prior to the date its operations cease.
Certification	The process of generating/signing certificates, suspension and revocation information for individuals, corporations, equipment, etc.
Certification Authority (CA)	The relied-upon entity that issues, publishes, suspends and revokes a certificate. The CA's basic role is to verify and vouch for the identity of the subscriber and to provide certificate management services. The CA may delegate the registration and publication functions to a registration authority or repository service provider. References to CA include RA and repository service provider unless otherwise stated.
Certification Practice Statement	A statement of the practices that a CA employs in issuing and managing certificates, and addressing its general business liability and service availability.
Certification system	The system that is used to perform the certification or CA signing function.
Compromise	A case where the private key and related security information have been or may be stolen or leaked or where secrecy has been or may be lost by a third party's decryption.
Confidentiality key pair	A cryptographic key pair generated specifically for the purpose of encryption and decryption purposes.
Certificate expiry	The invalidation of a certificate when its specified validity period defined by the issuer has been exceeded. An expired certificate cannot be re-instated.
Certificate issuance	The process of issuing a certificate whose contents have been verified and signed by the CA to the certificate applicant.
Certificate issuer	The entity that issues certificates to CA applicants. In an open PKI model, the certificate issuer' is typically the certification authority whereas in an outsource model, the certificate issuer may outsource the backend certification operations to another entity.
Key custodian	A person who is entrusted to maintain custody of the secret keys for the



SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

	CA operations. The person must not be directly involved in performing the CA operations.
Key generation system	The system that is used to generate cryptographic keys.
Key loading	The process by which a key is manually or electronically transferred into a secure cryptographic device.
Physical notice	Physical notices may include a writing delivered by hand or certified or registered mail.
Policy Management Authority	The Policy Management Authority is the authority on policies relating to the PKI and is responsible for developing the Certificate Policy.
RA operator	The personnel that operate the systems associated with the registration function.
Registration Authority (RA)	The entity that performs the registration functions, e.g. verification of the certificate applicant's identification information.
Registration function	Registration services consist of registering and managing individual data, and carrying out the authentication necessary for the issuance or revocation of certificates, on behalf of the CA.
Registration system	The system that is used to perform the registration function
Regulations	The Electronic Transactions Act 1998 and the Electronic Transactions (Certification Authority) Regulations 1999 and any future versions thereof.
Relying party	A recipient of a certificate who acts in reliance on that certificate and/or digital signature verified using that certificate.
Repository	The system that enables the user community to retrieve information pertaining to certificates, certificate suspension and revocation information.
Signature key pair	A cryptographic key pair generated specifically for the purpose of digital signature creation and signature verification.
Split control	The process of utilising two or more persons, who are operating in concert, to protect sensitive functions or information. No single person is to be able to access or to utilise the protected entity.
Subscriber	An entity (e.g. person, organisation) that has been issued a certificate by the CA. In this document, the subscriber is simply referred to as a user unless otherwise stated.
Suspension	The temporary invalidation of a certificate within the validity period of that certificate. Suspended certificates can be re-instated if the certificate information is valid and the secret key associated with the certificate has not been compromised.
User community	The users of the certification services. The user community typically includes the certificate subscribers and relying parties.
Validity	The certificate is deemed valid if it : <ul style="list-style-type: none"> • has not expired, • is not being suspended, • has not been revoked.
Verification	The process of checking the authenticity of certificates used by subscribers and relying parties.
Virtual notice	Insecure: Insecure electronic methods of delivery such as fax and unsigned electronic mail. Secure: Notice by secure electronic methods such as digitally signed messages, should be the primary means of providing notification to all parties. The CA Certificate Policy should require parties to obtain a



SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

	<p>registered electronic mail address, which would be considered a secure and reliable place to send and receive notification from all related parties. If registered electronic mail addresses are used, then a CA may deem a message sent to a registered electronic mail address as received.</p>
--	--

SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

2. Management Guidelines

A CA plays an important role in a PKI as a trusted party which digital certificates derive legitimacy. It is essential to ensure that the management of a CA is proper and secure. The scope of the management guidelines includes personnel, material, financial and information management guidelines.

2.1 Obligations

2.1.1 Any CA function or service that is outsourced shall comply with the security guidelines. The outsourced function or service shall be audited for compliance with the guidelines.

2.1.2 Accurate and complete records and transaction logs pertaining to the CA's business and operations shall be maintained. The records and logs shall be retained for the minimum period as specified in the applicable laws.

2.1.3 Any "force majeure" provision in the CPS or other contractual agreement that relieves the CA of its obligations from events that are beyond reasonable control shall be brought to the attention of the user community.

2.1.4 The user community shall be informed of the procedures for certificate registration, issuance, suspension and revocation.

2.1.5 The subscribers shall be informed of their responsibility to verify the accuracy of the information contained in their certificates upon issuance.

2.1.6 The subscriber's explicit consent shall be given before the CA can publish his certificate on the repository.

2.1.7 Adequate information on the measures to protect the subscribers' private keys shall be provided to the subscribers. The implications of the different protection measures shall be brought to the attention of the subscribers.

2.1.8 The subscribers' records shall be kept current and any changes in the information contained in the subscribers' certificates shall be updated promptly.

2.1.9 The relying party shall be informed of the reasonable steps to be taken to verify the authenticity and validity of a certificate. The steps shall include verification of the following information in the certificate:

- Issuer's signature
- Policy parameters;
- Usage parameters;
- Validity period; and
- Revocation or suspension information.

SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

- 2.1.10 The user community shall be informed of the time intervals between each update and publication of the certificate suspension, certificate revocation and certificate revocation list information. The publication of such information shall conform to the time intervals specified.
- 2.2 Liability
- 2.2.1 The user community shall be informed of the scope and limitations of CA's liabilities with respect to the expected reliance to be placed in the information contained in the certificates.
- 2.3 Certificate Policy and Certification Practice Statement
- 2.3.1 The user community shall be informed of the CA's Certificate Policy and Certification Practice Statement and any updates thereafter. The significance and implications of the Certificate Policy and Certification Practice Statement shall be brought to the attention of the user community.
- 2.3.2 A Certificate Policy shall be defined for each class of certificates that have common assurance levels and usage requirements.
- 2.3.3 Each Certificate Practice Statement shall be referenced by a unique object identifier (OID) approved by the Controller.
- 2.4 Security Management
(Refer to additional guidelines defined in section 3 of the BS 7799-1:2000).
- 2.4.1 The IT security policy for the CA organisation shall be defined and approved by the top management. The policy shall be communicated to all personnel and widely published throughout the organisation to ensure that the personnel are aware and reminded of the policy.
- 2.4.2 Personnel shall be provided with the information security policy upon employment. It shall be the responsibility of each personnel to read and understand it. Security notices, pamphlets, posters and signs shall be used to provide updates and reminders of the security policy.
- 2.4.3 An information security awareness program shall be implemented and conducted on at least an annual basis to ensure that all personnel are informed of the potential security risks and exposures in the CA operations and systems. In particular, personnel, especially those in the frontline service, shall be informed of typical social engineering attacks and the safeguards against them.
- 2.4.4 All personnel shall be educated on basic IT principles and safeguards. Personnel responsible for security areas (e.g. systems and operations security administrator) shall be trained on advanced IT security principles and safeguards. The security personnel shall be trained in the security features and vulnerabilities of the systems and operations.

SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

- 2.4.5 Procedures shall be documented and implemented to ensure that when personnel or contractors are transferred by appointment, assignment or deployment, all access privileges to IT systems, information and assets are reviewed, modified or revoked accordingly.
- 2.4.6 Procedures or a mechanism shall be established and implemented so that access rights of all registered users, their levels of access and their continued requirement for access can be checked on a regular basis (re-authentication).
- 2.4.7 Procedures shall be established and implemented to actively keep track of security vulnerabilities and attacks that are reported by reputable sources and develop countermeasures or correct them promptly. The procedures should include an incident response capability to provide active defence and corrective actions against security exploits and attacks.
- 2.4.8 Incident response procedures shall be established for documenting an event as a basis for subsequent action including forensics where necessary.
- 2.5 Risk Management
(Refer to additional guidelines defined in sections 4.2 and 4.3 of the BS 7799-1:2000).
- 2.5.1 The components of the CA infrastructure (e.g. cryptographic algorithm and its key parameters, physical security, system security, operating system, etc.) shall be reviewed every year for new technology risks and appropriate action plans of the components shall be developed to manage the risks identified.
- 2.5.2 Comprehensive CA system review, in the event of a hardware configuration change, software (operating system or layered product) update, network change (hardware, network operating system software or configuration), application update (new application or revised existing application) or changes made to the environment (physical or business) in which the CA functions, shall be conducted periodically.
- 2.5.3 Risk management policies and procedures shall be reviewed periodically as part of a comprehensive risk management approach.
- 2.5.4 Network and system security audits shall be performed periodically using automated audit tools to help identify new security vulnerabilities.
- 2.5.5 Network penetration tests shall be performed periodically to help identify gaps that may have been introduced in the network perimeter defences.
- 2.5.6 Intrusion detection systems shall be used to provide real time detection of network attacks.
- 2.5.7 Risk analysis and protection policies shall be reviewed periodically for all incidents (real or suspected) or when the perceived threat level changes (technical, physical or personnel).

SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

- 2.5.8 Results and action plans, from the regular security audits and network penetration tests conducted by a suitably qualified independent party, shall be submitted to the Controller annually
- 2.6 Personnel control
(Refer to additional guidelines defined in section 6 of the BS 7799-1:2000).
- 2.6.1 All job applicants shall be subjected to security screening prior to being employed. The screening shall ensure that the applicant does not have any criminal records that may jeopardise the trustworthiness of the CA functions
- 2.6.2 All personnel shall be required to sign a confidentiality agreement as part of their initial terms and conditions of employment prior to being given access to the CA services and processes facilities.
- 2.6.3 Confidentiality or non-disclosure agreements shall be reviewed when there are changes to the terms of employment or contract, particularly when employees are due to leave the organization or contracts are due to end.
- 2.6.4 All personnel shall be subjected to security re-screening at the point of re-licensing in the case of a licensed CA, to ensure that they continue to be trustworthy.
- 2.6.5 Personnel performing trusted roles or security-sensitive functions shall be subjected to stringent security screening (e.g. character profile).
- 2.6.6 Dual control and segregation of duties shall be implemented for critical CA services and processes. In particular, technical personnel involved in critical CA services and processes such as the CA system administrators and operators shall not be given security related roles.
- 2.6.7 Security related roles shall be given to dedicated personnel who are adequately trained to perform the job without any conflict of interest.
- 2.6.8 Job responsibilities and access rights shall be designed and reviewed yearly to ensure proper segregation of duties and alignment of access rights to business functions, i.e. certificate registration, issuance, suspension and revocation. In addition, periodic cross checks on personnel performing trusted roles or security sensitive functions for incompatible duties or interests (internal or external) shall be conducted.
- 2.6.9 All personnel shall be adequately trained in their designated tasks and functions. Personnel who have not been adequately trained shall not be allowed to independently operate the CA functions without the presence or supervision of trained personnel.
- 2.7 Maintenance of subscribers' data
- 2.7.1 Procedures and security controls to protect the privacy and confidentiality of the subscribers' data under the CA's custody shall be implemented. Confidential information provided by the subscriber must not be disclosed to a third party without the

SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

subscribers' consent, unless the information is required to be disclosed under the law of the Republic of Singapore or a court order.

2.7.2 Data on the usage of the certificates by the subscribers and other transactional data relating to the subscribers' activities generated by the CA in the course of its operation shall be protected to ensure the subscribers' privacy.

2.7.3 Information resources shall be monitored to minimise risk of corruption and unauthorised disclosure, access, modification or deletion.

2.7.4 Database management tools shall be used to manage and monitor information resources and master files.

2.8 Incident Management

2.8.1 An incident management plan shall be developed and approved by the management. The plan shall include but not limited to the following areas:

- RA key compromise;
- CA certification key compromise;
- User certificate compromise;
- Systems and network penetration;
- Breach of physical security;
- Infrastructure availability; and
- Fraudulent registration and generation of certificates, certificate suspension and revocation information.

2.8.2 An incident response action plan shall be established and periodically tested to ensure the readiness of the CA to respond to incidents. The plan shall include but not limited to the following areas:

- Compromise control;
- Notification to user community; (if applicable)
- Revocation of affected certificates; (if applicable)
- Personnel incident handling responsibilities;
- Service disruption procedures and investigation;
- Monitoring and audit trail analysis; and
- Media and public relations.

2.8.3 The CA's certificate shall be revoked immediately in the event of loss or compromise of the CA certification key or its storage device. All certificates signed using the CA's certification key shall be revoked.

2.8.4 All incidents shall be reported to the Controller within 24 hours.



SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

2.9 Business Continuity Planning

(Refer to additional guidelines defined in section 11 of the BS 7799-1:2000).

2.9.1 Business continuity and disaster recovery planning shall be developed and tested periodically to ensure the continued availability of critical services in the event of a disaster or computer failure.

2.9.2 The planning shall include continuity plans in the event of CA certification key loss and compromise.

2.9.3 The personnel in the recovery team shall be provided with adequate training to deal with the crisis.

2.9.4 The CA shall provide backup procedures and eliminate service failures as a result of “force majeure” not excluded from their obligations.

2.9.5 Redundant systems and devices shall be available to ensure continued operation of critical services in a timely manner.

2.9.6 The “hot” disaster recovery location shall have adequate security in place.

2.9.7 Business continuity plans shall be reviewed for relevance and adequacy every six months to assure the continuity of business in the event of an emergency. Evidence of the review shall be documented for management review.

SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

3. Certificate Management Guidelines

The certificate management processes include certificate registration, generation, issuance, renewal, suspension and revocation, as well as the publication of certificates, certificate suspension and revocation information. The objective is to establish integrity and accountability of the certificate management processes and the certificates.

3.1 Certificate Attributes

3.1.1 A certificate shall be uniquely identifiable within its user community.

3.1.2 A certificate shall indicate certificate policy and usage parameters to allow relying parties to check the acceptable use of a certificate.

3.1.3 A certificate shall indicate expiration parameters to allow relying parties to verify validity of the certificate.

3.1.4 The certificate should include parameters declaring the policy mapping as well as any constraints to policy maps.

3.1.5 Sensitive personal information on the certificate user should not be provided in the certificate attributes such as in the distinguished names fields so as to protect the privacy of the user against potential social engineering infringements.

3.1.6 Certificate extensions may be labelled as critical. The relying party shall be provided with the applications to verify and process any critical certificate extensions or reject the certificate.

3.1.7 Certificate extensions should be used to:

- Identify the policies under which a certificate is issued;
- Map equivalent policies in different user communities or domains;
- Require subsequent certificates in a certification path to include specific policy identifiers or policy mappings;
- Limit the subject name space for subsequent certificates in the certification path;
- Restrict key usage;
- Limit number of subsequent certificates; and
- Distinguish between a CA certificate and a user certificate.

3.2 Registration

3.2.1 The authentication method to verify the identity of the certificate applicant shall commensurate with the level of assurance accorded by the certificate. Where possible, face-to-face authentication of the applicant should be employed. A pre-existing trust relationship between the RA and the applicant may also be employed.



SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

- 3.2.2 The authenticity of attribute information of an applicant shall be verified against official documents issued by authorised organisations.
- 3.2.3 Adequate documents and logs for each registration shall be maintained to enable post verification of the certificate applications.
- 3.3 Generation
- 3.3.1 Procedures shall be defined to ensure that the subscribers' certificates generated are in accordance with the Certificate Policy.
- 3.3.2 The accuracy (e.g. the information in the certificate is correct) and integrity (e.g. the correct association of the key pair with the certificate information) of the certificate shall be ensured.
- 3.4 Issuance
- 3.4.1 A secure communication channel between the CA and its subscribers shall be established to ensure the authenticity, integrity and confidentiality of the exchanges (e.g. transmission of certificate, password, private key) during the certificate issuance process.
- 3.4.2 The CA shall require the subscriber to explicitly acknowledge the receipt and acceptance of the certificate upon issuance.
- 3.5 Publication
- 3.5.1 The CA shall publish its certificate and the location(s) of its CPS and repository to its user community using a reliable and trustworthy channel. (e.g. secure online mechanism or on a reputable newspaper).
- 3.5.2 The CA shall publish at least the following information to allow its user community to verify the authenticity of the establishment operating the CA:
- Company name and registration number;
 - X.500 name;
 - Internet address;
 - Telephone hotline number;
 - CA certificate (or fingerprint of the certificate)
 - Location(s) of the repository
- 3.5.3 Publication of the subscribers' certificate information in the repository shall be subject to the subscribers' explicit consent.
- 3.5.4 The contents in the repository shall be protected from unauthorised modification, insertion and deletion. Strong authentication mechanisms shall be used to validate identity of parties amending the repository contents. Where required,



SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

appropriate access controls to the contents of the repository shall be implemented to restrict access solely to the user community or to protect subscribers' privacy.

3.5.5 Adequate backup and redundancy measures shall be implemented to ensure that the availability of the certificate repository conforms to the service level guaranteed to the user community.

3.6 Renewal

3.6.1 The CA shall provide prior notice to the subscribers on the expiry date of their certificates so that they have sufficient time to apply for renewal or termination.

3.6.2 Certificate renewal requests shall be submitted using a secure communication channel. A secure channel may include the use of an online renewal request that is digitally signed by the subscriber as long as the certificate is still valid.

3.6.3 The certificate generation and issuance guidelines in this section shall apply in the generation and issuance of a new certificate to replace an expired certificate.

3.7 Certificate suspension

3.7.1 A certificate shall be suspended in the event of suspected compromise of a subscriber's private key. A suspended certificate should only be reactivated when investigations established that no compromise has occurred.

3.7.2 Certificate suspension requests shall be submitted using a secure communications channel to verify the identity of the requester so as to minimise risk of sabotage with unauthorised disruption of service or with malicious requests for suspension.

3.7.3 Certificate suspension information in the certificate revocation list shall include the reason and time of the suspension so that relying parties can determine the point at which the certificate cease to be valid.

3.7.4 Certificate suspension information in the certificate revocation list shall be digitally signed by the CA to enable the relying parties to verify the authenticity and integrity of the information.

3.7.5 Certificate suspension information in the certificate revocation list shall be published once the suspension request has been verified to be valid.

3.7.6 Certificate suspension information in the certificate revocation list shall be protected from unauthorised modification and deletion.

3.7.7 The subscriber whose certificate has been suspended shall be notified once the suspension takes effect.

3.8 Certificate Revocation

SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

3.8.1 Permanent revocation occurs when a subscriber requests revocation for any reason. The CA shall state in its Certificate Policy whether an authorised representation of the policy making body or another member of the community that is subject to the Certificate Policy should be permitted to request the revocation of a certificate issued under the Certificate Policy. For example, the RA may be permitted to trigger the revocation of a certificate.

3.8.2 Required revocation occurs when any party reasonably determines that a certificate is unreliable. A certificate shall be revoked under the following circumstances:

- Whenever any information marked with the extension “critical” on the certificate is no longer accurate;
- Whenever the private key associated with the certificate or the media holding the private key is, or is suspected of having been, compromised;
- Whenever the subscriber is no longer a member of the community that is subject to the Certificate Policy (e.g. cessation of employment or death);
- Upon the request of the subscriber;
- If the CA determines that the certificate was not properly issued in accordance with the CPS;
- If the certificate issuer or CA ceases operation; and
- If the CA certification key is compromised.

3.8.3 Certificate revocation requests shall be submitted using a secure communication channel to verify the identity of the requester so as to minimise risk of sabotage with unauthorised revocation.

3.8.4 The certificate revocation information shall at least contain the following:

- Reason code for revocation; and
- Revocation date and time.

3.8.5 Certificate revocation information shall be digitally signed by the CA to enable the relying party to verify the authenticity and integrity of the information.

3.8.6 Certificate revocation information shall be published once the revocation request has been verified to be valid. It should include provisions for:

- Online certificate revocation checking; and
- Distribution points certificate revocation information.

3.8.7 Certificate revocation information shall be protected from unauthorised modification and deletion.

3.8.8 The subscriber who certificate has been revoked shall be notified once the revocation takes effect

SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

- 3.8.9 Revoked certificates shall not be re-activated.
- 3.9 Archival
- 3.9.1 All certificate suspension and revocation information, certificates and their registration documents shall be archived for a minimum retention period of seven years in accordance with the applicable regulatory requirements so as to facilitate verification of digital signatures corresponding to certificates that have expired.
- 3.9.2 Digital archives shall be indexed, stored, preserved and reproduced so as to be accurate, complete, legible and accessible to authorised persons. The integrity and availability of the digital archives shall be ensured.
- 3.10 Audit trails
- 3.10.1 Audit trails of certificate registration, generation, issue, renewal, suspension and revocation shall be maintained.
- 3.10.2 The integrity and availability of the audit trails shall be ensured.
- 3.10.3 A reviewer tasked with the operational oversight role shall periodically review the certificate management audit trails to ensure normal operation and investigate suspicious activities.
- 3.10.4 Audit trails shall be archived for a minimum period of twelve months or longer, in accordance with the applicable regulatory requirements.

SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

4. Key Management Guidelines

This section defines the guidelines to manage risk at each phase of key management to ensure confidentiality and integrity of cryptographic keys. It covers technical and administrative security requirements to manage risk of cryptographic key compromise. The scope includes cryptographic keys used by the certification authority (including registration functions) and the user community. The principle of split control is to be applied to the handling of CA keys.

4.1 Generation

4.1.1 The subscriber's key pair shall be generated by the subscriber or on a key generation system. If the subscriber generates his own key pair, the CA shall approve the key generation system used.

4.1.2 The CA keys shall be generated and stored under split control by parties who are not involved in the set-up and maintenance of the CA systems and operations.

4.1.3 Separate key pairs for digital signature and encryption should be generated.

4.1.4 The key generation process shall generate statistically random key values for the generation of a strong (unique) key.

4.2 Distribution

4.2.1 Keys shall be transferred from the key generation system to the storage device (if the keys are not stored on the key generation system) using a secure mechanism that ensures end-to-end confidentiality and integrity.

4.3 Storage

4.3.1 The CA should provide the subscriber with the equipment and programs to securely store the subscriber's private key in an encrypted form.

4.3.2 CA keys shall be stored in tamper-proof devices and can only be activated under split control by parties who are not involved in the set-up and maintenance of the CA systems and operations. The CA key may be stored in a tamper-proof cryptographic module or split into sub-keys stored in tamper-proof devices under the custody of the key custodians.

4.3.3 The CA key custodians shall ensure that the CA key component or the activation code is always under his sole custody. Change of key custodians shall be approved by the CA management and documented. In the event that the key custodian is unavailable, CA should put in place a system of checks to ensure that there is no single point of failure.

4.4 Usage

4.4.1 A system and software integrity check shall be performed prior to CA key

SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

- loading.
- 4.4.2 Custody of and access to the CA keys shall be under split control. In particular, CA key loading shall be performed under split control.
- 4.5 Backup
- 4.5.1 CA private keys shall be backed up to prevent a CA's operation from stopping due to accidental deletion or corruption of keys.
- 4.5.2 CA private key backups shall be protected with the same guidelines as required for CA private key storage.
- 4.5.3 Separate key custodians shall be assigned to protect each component of the backup key.
- 4.5.4 CA private key backups should be stored in a separate secure storage facility, at a different location from where the original key is stored.
- 4.6 Key change
- 4.6.1 CA and subscriber keys shall be changed or recertified periodically.
- 4.6.2 Key change shall be processed as per Key Generation guidelines.
- 4.6.3 The validity period shall be defined as per guideline 4.10.5.
- 4.6.4 The CA shall provide reasonable notice to the subscriber's relying parties of any change to a new key pair used by the CA to sign certificates.
- 4.6.5 The CA shall define a CA key change process that ensures reliability of the process by showing how the generation of key interlocks – such as signing a hash of the new key with the old key.
- 4.6.6 The CA shall notify the subscriber or the owner of the digital certificates of any type of key change that are performed automatically either through a secure application program or outsourced mode.
- 4.7 Destruction
- 4.7.1 Upon termination of use of a CA signature private key, all components of the private key and all its backup copies shall be securely archived and stored in a secure location.
- 4.8 Key compromise
- 4.8.1 A procedure shall be pre-established to handle cases where a compromise of the CA certification key has occurred. (See section 2.8 - Incident Management)

SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

- 4.8.2 The CA shall immediately revoke all affected subscriber certificates in the case of CA certification private key compromise.
- 4.8.3 The CA shall immediately revoke the affected keys and certificates in the case of subscriber private key compromise.
- 4.9 CA key and Subscriber encryption key archival
- 4.9.1 CA Public keys shall be archived permanently to facilitate audit or investigation requirements.
- 4.9.2 All subscriber encryption keys should be archived for a reasonable period of time to safeguard users from any compromise or misplacement of keys that may result in their own denial of service.
- 4.9.3 Archives of CA public keys and subscriber encryption keys shall be protected from unauthorised modification.
- 4.10 Cryptographic engineering
- 4.10.1 The cryptographic processes for the CA operations shall be performed in a hardware cryptographic module that minimally conforms to FIPS 140-1 Security Level 3 or FIPS 140-2 Security Level 3.
- 4.10.2 If the RA's operations are separate from the CA, its cryptographic processes shall minimally conform to FIPS 140-1 Security Level 2 or FIPS 140-2 Security Level 2.
- 4.10.3 The cryptographic processes for the subscriber's operations shall minimally conform to FIPS 140-1 Security Level 1 or FIPS 140-2 Security Level 1.
- 4.10.4 All cryptographic algorithms, protocols and their implementations shall be reviewed by a suitably qualified independent party to ensure that the cryptographic components are sufficiently secure and correctly implemented. The components that require certification include all modules and components involved in key generation, key storage, key transport and key usage.
- 4.10.5 The cryptographic keys and algorithms shall be sufficiently strong to protect the cryptographic result (e.g. digital signature) from attacks for the life span of the keys.
- 4.10.6 The asymmetric cryptographic algorithms used should conform to the IEEE Standard Specifications for public key cryptography [IEEE1363].

SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

5. Systems and Operations Guidelines

Design, configuration, operation and maintenance of systems and networks are critical to the security of IT-enabled businesses, especially a CA whose core business revolves around the use of computer systems and networks to provide trusted services for digital certificates. The guidelines listed here are intended to be specific to the CA services and to supplement the general IT security controls addressed in the BS 7799-1:2000. The scope includes availability, confidentiality, integrity and access control of critical CA systems and operations.

5.1 Physical Security

(Refer to additional guidelines defined in section 7 of the BS 7799-1:2000)

5.1.1 Responsibilities for the physical security of the CA systems shall be defined and assigned to named individuals.

5.1.2 The location of the CA system shall not be publicly identified.

5.1.3 Physical access security systems shall be installed to control and audit access to the certification system.

5.1.4 Dual control over the inventory and access cards/keys shall be in place. An up-to-date list of personnel who possess the cards/keys shall be maintained.

5.1.5 Cryptographic keys under the custody of the key custodians shall be physically secured from unauthorised access, use and duplication.

5.1.6 Loss of access cards/keys shall be reported immediately to the security administrator; who shall take appropriate actions to prevent unauthorised access.

5.1.7 CA systems should be located in an area away from strong sources of magnetic or radio frequency interference.

5.1.8 Systems performing the certification function shall be located in a dedicated room or partition to facilitate the enforcement of physical access control.

5.1.9 Entry and exit of the room or partition shall be automatically logged with time-stamps and be reviewed by the CA security administrator daily.

5.1.10 Access to infrastructure components essential to functioning of CA systems such as power control panels, communications risers and cabling shall be restricted to authorised personnel.

5.1.11 Adequate approval procedures and compensating controls shall be in place at times (e.g. during emergency situations) when it is necessary to temporarily bypass or de-activate normal physical security arrangements.

5.1.12 Bypass or de-activation of normal physical security arrangements shall be authorised and recorded by security personnel.

SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

- 5.1.13 Suitable intrusion detection systems installed to professional standards and periodically tested shall be used to monitor and record physical access to the certification system during after hours. Unoccupied areas should be alarmed at all times and cover should be provided for all other areas.
- 5.2 Systems and Software Integrity and Control
(Refer to additional guidelines defined in sections 8.7, 9 and 10 of the BS 7799-1:2000)
- 5.2.1 Systems performing the certification function shall be dedicated to that function and not be used for other purposes (e.g. web surfing, word processing).
- 5.2.2 Systems and application software shall be verified for integrity before each execution.
- 5.2.3 Systems and application software shall minimally conform to Common Criteria EAL4 or equivalent security level.
- 5.2.4 Systems shall enforce strong authentication mechanisms that are not susceptible to prediction, dictionary attacks or replay.
- 5.2.5 The security-critical software, that includes, but not limited to, software that has a crypto module embedded, shall be reviewed by a suitably qualified independent party.
- 5.2.6 Personnel shall be appropriately trained on the secure and proper operation of CA applications.
- 5.2.7 Automatic time-out for terminal inactivity should be implemented. For sensitive systems, the time-out should be not longer than 10 minutes.
- 5.3 Change and Configuration management
(Refer to additional guidelines defined in section 10.5 of the BS 7799-1:2000)
- 5.3.1 Executables of questionable sources or where trustworthiness cannot be ascertained shall not be installed or run on CA systems.
- 5.3.2 Software updates and patches shall be reviewed, thoroughly tested and proven for security implications before being implemented
- 5.3.3 Software updates and patches to rectify security vulnerabilities in critical systems shall be promptly reviewed and implemented.
- 5.3.4 The information on the software updates and patches and their implementation shall be clearly and properly documented.
- 5.4 Network and Communications Security
(Refer to additional guidelines defined in section 8 of the BS 7799-1:2000)



SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

5.4.1 CA systems shall be protected to ensure network access control to critical systems and services from other systems.

5.4.2 Network connections to external networks (if required) from the CA systems shall be restricted to only the connections that are essential to facilitate CA functional processes and services.

5.4.3 Network connections (if required) should be initiated by the systems performing the certification function to those performing the registration and repository functions but not vice versa. If this is not possible, compensating controls (e.g. use of proxies) shall be implemented to protect the systems performing the certification function from potential attacks

5.4.4 Security testing and evaluation of the network access control of the CA systems shall be reviewed by a suitably qualified independent party before allowing connections to the external network to be made. Mitigating controls shall be put in place for the risks that have been identified.

5.4.5 Systems performing the certification function should be isolated to minimise exposure to attempts to compromise the confidentiality, integrity and availability of the of the certification function.

5.4.6 The CA certification key shall be protected from unauthorised access to ensure its confidentiality and integrity.

5.4.7 Communications between the CA systems over a network shall be secure to ensure confidentiality, integrity and authenticity. For example, communications between the CA systems over a network should be encrypted and digitally signed.

5.4.8 Intrusion detection tools shall be deployed to monitor critical networks and perimeter networks and alert administrators of network intrusions and penetration attempts in a timely manner.

5.5 Monitoring and Audit Logs

5.5.1 The CA should consider the use of automated security management and monitoring tools providing an integrated view of the security situation at any point in time.

5.5.2 Records of the following application transactions shall be maintained:

- Registration;
- Certification;
- Publication;
- Suspension; and
- Revocation.



SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

5.5.3 Records and log files shall be reviewed periodically for the following activities:

- Misuse;
- Errors;
- Security violations;
- Execution of privileged functions;
- Change in access control lists;
- Change in system configuration; and
- Change in software modules.

5.5.4 Review of audit trails shall be performed by personnel tasked specifically with the oversight function.

5.5.5 Audit logs shall be adequately protected from unauthorised access, modification and deletion and backed up periodically in a timely manner for archival purposes.

5.5.6 Audit trail retention for system access records (e.g. Syslog, security-related logs) shall be kept for a minimum of twelve months or longer, in either hard copy or electronic form. Records that are necessary to support litigation or investigation of criminal activities shall be retained permanently or as stipulated by relevant legislations.

5.5.7 Records of applications transactions and significant events shall be retained for a minimum of twelve months or longer, in accordance with the applicable regulatory requirements.

SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

6. Application Integration Guidelines

This section defines guidelines to the certification authority for application toolkits to ensure secure implementation and operation. The scope includes toolkits provided by the CA to the user and developer community. Verification of certificates is addressed in this section and not Certificate Management because it is not a CA function but a function of the applications used by the user community.

6.1 Integrity of signing and verification functions

6.1.1 The application shall inform the user when a private key is being accessed.

6.1.2 The user shall be alerted if its private key is being used for a purpose that is not consistent with that defined as acceptable use by the issuer.

6.1.3 Mechanism shall be available to check the integrity of the applications for unauthorised modifications, esp. the integrity of signing and verification functions.

6.1.4 Application security risk assessment on the CA's software infrastructure should be conducted yearly to ensure that the CA software that manages, issues and revokes certificates is developed to manage the risk identified.

6.1.5 The application should be reviewed by a suitably qualified independent party to ensure safe operations.

6.2 Protection of private key

6.2.1 The RA private keys shall be stored in tamper-evident devices and protected from unauthorised use or copy.

6.2.2 The CA private keys shall be stored in tamper-proof devices and protected from unauthorised use or copy.

6.2.3 Application should securely purge the private key temporarily stored for processing to minimise private key exposure.

6.3 Verification of certificates

6.3.1 The application shall verify the validity and authenticity of the certificate.

6.3.2 The verification process shall trace and verify all the components in the certification path.

6.3.3 The relying party should be informed of what a particular assurance level means, how the private key associated with the certificate is stored, how entities are verified and the issuance process.



SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

- 6.3.4 For validity and authenticity verification, it shall be necessary to verify that:
- The certificate issuer's signature is valid;
 - The certificate is valid (i.e. has not expired, been suspended or revoked); and
 - The certificate extensions flagged as "critical" are being complied with.

SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

7. References

- [DE9804] German Technical Catalogues for Digital Signatures under S16(6) of the Digital Signature Ordinance v2.0a, April 1998
<http://www.iid.de/rahmen/iukdge.html>
- [ECOM9806] ECOM Japan Certification Authorities Guidelines v1.0, June 1998
http://www.ecom.or.jp/ecom_e/cag-smry.html
- [IEEE1363] IEEE P1363 Standard specifications for Public Key Cryptography (draft)
<http://grouper.ieee.org/groups/1363/index.html>
- [IT9710] Italian Digital Signature Technical Catalogues, November 1997
<http://www.notariato.it/forum>
- [ITU509] ITU Recommendations for X.509 Certificate Format
http://www.itu.ch/itudoc/itu-t/rec/x/x500up/x509_27505.html
- [ITUCRL] ITU Recommendations for X.509 Certificate Revocation List Version 2
http://www.itu.ch/itudoc/itu-t/rec/x/x500up/x509_27505.html
- [PKIXCPF] IETF PKIX Certificate Policy and Certification Practices Framework
<http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-part4-03.txt>
- [FIPS 140-1, 140-2] NIST Federal Information Processing Standards (FIPS) Publication 140-2
<http://csrc.nist.gov/cryptval/140-2.htm>
- [BS 7799-1:2000] BS 7799-1:2000 (Information Technology – Code of practice for information security management) <http://www.bsi-global.com>



SECURITY GUIDELINES FOR CERTIFICATION AUTHORITIES

8. Acknowledgements

The following parties are acknowledged for their contributions and inputs to the closed consultation for the Review of the Security Guidelines for CA's, 1999.

- Crimson Logic
- IT Standards Committee (ITSC) Singapore
- LogicaCMG

9. Versions

Version 1.0, IDA Security Guidelines for CA's, September 1999

Version 2.0, IDA Security Guidelines for CA's, September 2003
