Report on
CA Responsibilities and Liability
For
Cross-Border E-Commerce

July 31 , 2005

Legal Infrastructure Working Group

ASIA PKI Forum

PREFACE

The Legal & Working Group, one of the four working groups of ASIA Public Key Infrastructure (PKI) FORUM, published the "Report on Legal Issues in Cross-Border E-Commerce Transactions" in July 2003. In this report, we looked at how electronic signature acts, electronic transaction acts, and other related laws and regulations of the member country/areas recognize disparities with the UNCITRAL Model E-Commerce (1996) and Electronic Signature (2001) Laws. The UNCITRAL laws recognize digital signatures as an indispensable element of PKI and push forward one of the key objectives of the Asia PKI Forum: to expand PKI use for e-commerce in Asia.

Following the above-mentioned report, we published another report entitled "Dispute Resolutions for Cross-Border E-Commerce" in August 2004. It first provides an overview of the judicial system and alternative dispute resolutions as applied to e-commerce transactions. Next, it addresses hypothetical cases to which member countries/areas provide legal solutions in accordance with present domestic laws and regulations of each country/area. At present, there is no convention or treaty on applicable law and/or international jurisdiction that can be applied to all the member countries/areas of the Asia PKI Forum. Because the report provides a basis for mutual understanding of the institutions of dispute resolutions and private international law, we believe that we may provide business entities and consumers engaged or involved in business activities in Asia with foresight and advance measures regarding cross-border e-commerce dispute resolutions.

With the rising usage of PKI for cross-border e-commerce transactions and government purposes in Asia, disputes involving Certification Authority's responsibilities and liability are likely to arise. The Legal & Infrastructure Working Group has been researching the Certification Authority's responsibilities and liability since August 2004, and during the course of our study, we have conducted comparisons of Certification Practice Statements issued by Certification Authorities in Asia using RFC 3647 4.9.1-15 as the basis, analyzed the validity of those CPSs in each country/area, and looked at other key issues. In addition, we collected information and materials concerning privacy laws in each country/area as the conflict between security and privacy has been a critical legal and social issue recently. Next year, we will study the legal issues arising out of new security technologies in the Asia PKI Forum.

This report would not have been possible without the LIWG members' generous and invaluable support, cooperation, and contributions.

Editor

With contributions from: China PKI Forum, Japan PKI Forum, Korea PKI Forum, PKI Forum Singapore, Chinese Taipei PKI Forum, Hong Kong PKI Forum, Macao Post, Thailand PKI Forum.

Written or contributed by: Legal & Infrastructure Working Group of ASIA PKI FORUM in FY 2005; Jiajun Ning, Dr. Jinqiang Ren, Prof. Zhang Chu (China PKI Forum); Shigeru Kameda, Haruhiko Kato, Kazuhisa Hayashi, Takashi Aoki, Hajime Takatsuka, Yutaka Hori, Hiro Rokugawa-Leader Chair and Editor (Japan PKI Forum); Jae-Il Lee, Seok Lae Lee, Jeonghyun Lee (Korea PKI Forum); NG Yit_Siew, Kenneth Chia (PKI Forum Singapore); Judy Chang-Partner Co-Chair, Arthur Shay, Wei-Jung Lin (Chinese Taipei PKI Forum)

References:

1. “PKI Assessment Guidelines” by Information Security Committee of American Bar Association. pp94-99 http://www.arbanet.org/scitech/ec/isc/pag/pag.html
2. “Certification Authority Liability Analysis” by American Bankers Association http://www.bakernet.com/ecommerce/articles-pki-s.html
3. Directive 1999/93/EC of The European Parliament and of The Council of 13 December 1999 on a Community framework for electronic commerce Article 6.
   Please be advised that the Article 6 only mentions “qualified certificate” and it does not mention general certificates.
4. “Report on Legal Issues in Cross-Border E-Commerce Transactions” by Legal Infrastructure WG of Asia PKI Forum
5. “Dispute Resolutions for Cross Border E-Commerce” by Legal Infrastructure WG of Asia PKI Forum

Table of Contents

ACRONYMS AND DEFINITIONS

CA	**Certification Authority**
CPS	**Certification Practice Statement**

Request 1: (CPS Mapping)

Request 1:(Policy Mapping)

We need to recognize the disparities of Certification Practice Statements issued by the following Certification Authorities in each country/area using Article 3647 Paragraph 4.9.1-16 of "Request for Comments" provided by IETF (The Internet Engineering Task Force) as the basis.

Japan: Japan Certification Services, Inc. (2001)
Korea 1: Korea Information Security Agency(Korea Certification Authority Central : Root CA of Korea) (CPS version 1.2, 2004)
Korea 2: Korea Information Certificate Authority(CPS version 4.1, 2004)
Singapore: Netrust Pte. Ltd (2001)
Chinese Taipei: Taiwan-CA. COM Inc.(2002)
Hong Kong China: Hong Kong Post (2002)
Thailand: ACERTs Ltd. (2001)

RFC3647-4.9 OTHER BUSINESS AND LEGAL MATTERS

This component covers general business and legal matters. Sections 9.1 and 9.2 of the framework discuss the business issues regarding fees to be charged for various services. It also discusses the financial responsibility of participants to maintain resources for ongoing operations and for paying judgments or settlements in response to claims asserted against them. The remaining sections are generally concerned with legal topics.

Starting with Section 9.3 of the framework, the ordering of topics is the same as or similar to the ordering of topics in a typical software licensing agreement or other technology agreement. Consequently, this framework may not only be used for CPs and CPSs, but also associated PKI-related agreements, especially subscriber agreements and relying party agreements. This ordering is intended help lawyers review CPs, CPSs, and other documents adhering to this framework.

With respect to many of the legal subcomponents within this component, a CP or CPS drafter may choose to include in the document terms and conditions that apply directly to subscribers or relying parties. For instance, a CP or CPS may set forth limitations of liability that apply to subscribers and relying parties. The inclusion of terms and conditions is likely to be appropriate where the CP or CPS is itself a contract or part of a contract.

In other cases, however, the CP or CPS is not a contract or part of a contract. Instead, it is configured so that its terms and conditions are applied to the parties by separate documents which may include associated agreements, such as subscriber or relying party agreements. In that event, a CP drafter may write a CP so as to require that certain legal terms and conditions appear (or do not appear) in such associated agreements. For example, a CP might include a subcomponent stating that a certain

limitation of liability term must appear in a CA's subscriber and relying party agreements. Another example is a CP that contains a subcomponent prohibiting the use of a subscriber or relying party agreement containing a limitation upon CA liability inconsistent with the provisions of the CP. A CPS drafter may use legal subcomponents to disclose that certain terms and conditions appear in associated subscriber, relying party, or other agreements in use by the CA. A CPS might explain, for instance, that the CA writing it uses an associated subscriber or relying party agreement that applies a particular provision for limiting liability

RFC3647-4.9.1 Fees

This subcomponent contains any applicable provisions regarding fees charged by CAs, repositories, or RAs, such as:

* Certificate issuance or renewal fees;
* Certificate access fees;
* Revocation or status information access fees;
* Fees for other services such as providing access to the relevant CP or CPS; and
* Refund policy.

Japan:

2.5. Charges

The JCSI will publicize the basic prices of A-Sign public services on the web site of the JCSI. Other charges will be presented by sales personnel of the JCSI whenever necessary.

Korea 1:

2.4 Fees

2.4.1 Fee for Issue, Reissuance and Renewal of Accredited Certificate

KISA may make a charge to the ACA applying for issue, reissuance or renewal of accredited certificate observing fee estimation standard defined by the president of KISA.

2.4.2 Accredited Certificate Access Fee

KISA makes no charge to the relying party reading and confirming accredited certificates.

2.4.3 Access Fee for Suspension and Revocation List of Accredited Certificate

KISA makes no charge to the relying party accessing the suspension and revocation list of accredited certificates.

2.4.4 Fees for Other Service

KISA can make charge for the other practices if needed under the provisions of the Electronic Signature Act.

Korea 2:

6.2 Fees

6.2.1 Certificate Fees

Fee schedules for issuance and re-issuance of certificates by certificate class are as follows:

General-Purpose		Server Operator	Special-Purpose
Individual	Corporation		
・4,000	・100,000	・500,000	To be decided by contract

Note:

1) VAT is excluded.

2) A current schedule of Discount fees and Membership fees will be available from the KICA homepage at <http://www.signgate.com> separately.

6.2.2 Request and Payment of Fees

KICA may impose fees on subscribers when applications for certification services are filed, and subscribers should prepay them. However, corporations, organizations or subscribers for server certification services are allowed to pay them later. In the latter cases, KICA issues Request for Payment of Fees to the parties concerned.

6.2.3 Refund of Fees

Subscribers may request a refund of fees if they decide to cancel their applications based on the quality of certification services at KICA. If the quality is not to the standards of what has been stipulated in the Rules or the Center has failed to perform major duties provided under the Rules then a refund should be requested within 10 days from the date of certificate issuance. In this case, subscribers should fill out the Application for Cancellation or Request for Refund of Fees prepared by KICA before presenting them to KICA by personal visit, or send in an electronically signed Application for Cancellation or Request for Refund of Fees through on-line communication networks.

When the subscriber requests a cancellation of application and for a refund within the given period, KICA may deduct necessary expenses as dictated by the circumstance and refund the balance. On receipt of the refund, the subscriber's certificate is automatically revoked.

Singapore:

2.5 Fees

2.5.1 Netrust charges Subscribers and all such other parties for their use of Netrust's PCS and all Subscribers and all such other parties shall be obliged to pay to Netrust such charges in accordance with its Schedule of Fees and at such times as may be prescribed by Netrust.

2.5.2 All fees are subject to change seven (7) days following their posting in the Netrust web site at http://www.netrust.net or as may be notified by Netrust in any other manner. The fees Netrust charges include:

2.5.2.1 Certificate Subscription or Renewal Fees - refer to Netrust for Schedule of Fees.

2.5.2.2 Certificate Revocation Fees - refer to Netrust for Schedule of Fees.

2.5.2.3 Fees for Other Services such as Policy Information - Schedule of Fees to be determined.

2.5.2.4 Refund Policy - Netrust has a policy where no monies will be refunded under any circumstances whatsoever.

Chinese Taipei:

2.5 Fees

2.5.1 Certificate Issuance or Renewal Fees

The fee calculation framework and fee rates for registration, Certificate application, and renewal between Subscribers and RA are specified in relevant service CP regulations and fee-calculation operating procedures or contract terms.

2.5.2 Certificate Access Fees

The fee calculation framework and fee rates for directory server or database Certificate access between CA and Subscribers are specified in relevant service CP regulations and fee-calculation operating procedures or contract terms.

2.5.3 Revocation or Status Information Access Fees

The fee calculation framework and fee rates for Subscriber Certificate revocation services and Online Certificate Status Protocol (OCSP) services provided by the CA are specified in relevant service CP regulations and fee-calculation operating procedures or contract terms.

2.5.4 Fees for Other Services such as Policy Information

CA shall not collect any service fees when Subscriber downloads the CPS or relevant service CPs from the Internet, CA must, however, charge Subscriber postage and a handling charge when Subscriber requests a printed CPS, CB, or other relevant documents from CA. The fee rate shall be specified in relevant CP specifications and fee-calculation operating procedures or contract terms.

2.5.5 Refund policy

This CPS does not describe operating procedures for refunds. Refund procedures in each service system reflect individual service systems' characteristics and needs. Please refer to the relevant service system CP and certificate operation fee-calculation and refund handbook, or to the service contract.

Hong Kong China:

2.4 Fees

e-Cert (Personal) certificates (for both new and renewal application) are available at the cost of HK$50 per certificate per year.

e-Cert (Organizational) certificates are available at the cost of HK$50 per certificate for first time subscription. Renewal of e-Cert (Organizational) certificates is available at the cost of HK$150 per certificate per year. An additional administration fee of HK$150 per application (irrespective of the number of Authorised User) is payable.

e-Cert (Server) certificates (for both new and renewal application) me available at HK$2,500 per certificate per year.

e-Ceet (Encipherment) cefti1icates (for both new and renewal application) are available at HK$150 per certificate per year. An additional administration fee of HK$150 per application (irrespective of the number of Authorised Unit) is payable.

Thailand:

2.5. Fees and Refund Policy

2.5.1 Fees

ACERTs charges Subscribers and all such other parties for their use of ACERTs' PCS and all Subscribers and all such other parties shall be obliged to pay ACERTs such charges in accordance with its Schedule of Fees and at such times as may be prescribed by ACERTs.

All fees are subject to change seven (7) days following their posting in the ACERTs web site at http://www.ACERTs.net or as may be notified by ACERTs in any other manner. The fees ACERTs charges include:

(a) Certificate Subscription or Renewal Fees – refer to ACERTs web site for Schedule of Fees;
(b) Certificate Revocation Fees – refer to ACERTs web site for Schedule of Fees; and
(c) Fees for Other Services such as Policy Information – Schedule of Fees to be determined by ACERTs.

2.5.2 Refund Policy

Refund policies will be specified in the applicable fee schedule or agreement with ACERTs PCS Participant paying fees. In the absence of such specification, no refunds will be provided.

RFC3647-4.9.2 Financial Responsibility

This subcomponent contains requirements or disclosures relating to the resources available to CAs, RAs, and other participants providing certification services to support the performance of their operational PKI responsibilities, and to remain solvent and pay damages in the event they are liable to pay a judgment or settlement in connection with a claim arising out of such operations. Such provisions include:

* A statement that the participant maintains a certain amount of insurance coverage for its liabilities to other participants;
* A statement that a participant has access to other resources to support operations and pay damages for potential liability, which may be couched in terms of a minimum level of assets necessary to operate and cover contingencies that might occur within a PKI. Examples include assets on the balance sheet of an organization, a surety bond, a letter of credit, or a right under an agreement to an indemnity under certain circumstances; and
* A statement that a participant has a program that offers first-party insurance or warranty protection to other participants in connection with their use of the PKI.

Japan:

2.3. Financial responsibilities

2.3.1. Compensation liabilities

(a) If the JCSI violates any liability set forth in section 2.2.1 of this set of standards and bears any liability for compensating for damages, the limit amount for the subscriber will be the amount set forth in a separate subscriber agreement, and the limit amount for the relying party will be the amount set forth in the relying party agreement. This also provides that the JCSI will not be liable for any damage stemming from any cause not attributable to the JCSI's responsibility, any damage stemming from a special cause regardless of whether the JCSI expected it, or any loss of profit.

(b) If the subscriber fails to implement any obligation set forth in this set of standards or violates any liability set forth in section 2.2.2 of this set of standards, and if this leads to damage on the part of the JCSI, the JCSI may require the subscriber to compensate for the damages.

(c) Concerning the limitations on the use of certificate by subscribers in 2.1.3 (2) of this set of standards, for trouble stemming from the presentation of certificates for uses other than the specified ones by subscribers, the subscribers must bear all liabilities. If such trouble causes any damage to the JCSI, the subscribers must compensate the JCSI for the damages. Concerning the revocation request described in 2.1.3 (5) of this set of standards, the subscriber must bear all liabilities for trouble stemming from impersonation by a third party due to the negligence of the subscriber and/or

stemming from a misjudgement by a relying party. If such trouble causes any damage to the JCSI, the subscriber must compensate for the damages.
(d) Concerning the limitations on the use of certificates described in 2.1.4 (1) of this set of standards, the relying party must bear all liabilities for damages resulting from the use of a certificate for any unspecified use by a relying party, and the JCSI will not take any liability for compensation. A validity check on a certificate by a relying party as described in 2.l.5 (2) of this set of standards is generally automatically conducted by the software employed. Final decisions are the responsibility of the relying party. If there is any damage resulting from any transaction despite the fact that the relying party cannot make a validity check, the JCSI will not take any liability for compensation.
2.3.2. Trust relationship
The JCSI is not an agent or trustee for the financial condition of the customers, subscribers, and relying parties to A-Sign public services. However, the JCSI is in cooperation with NEC Corporation, Hitachi, Ltd., and Fujitsu Ltd. These three corporations participate in running the JCSI as major stockholders. The JCSI commissions work to the three companies.
2.3.3. Accounting principles
As per the business accounting principles based on the Commercial Code of Japan

Korea 1:
2.2 Liability of Korea Information Security Agency

2.2.2 Exemption from Liability
KISA has no responsibility for any delays in certification practice or damages due to force majeure such as warfare and a natural disaster or reasons beyond provisions of the Electronic Signature Act, the Ordinance and the Regulations.

Korea 2:
5.1.2 KICA's Liabilities

5.1.2.1 Liability for Damages
KICA compensates for damages inflicted on subscribers while providing certification service in violation of the Act, its enforcement decrees, regulations, or provisions of these Rules.

5.1.2.2 Limit of Liability

a. KICA is subscribed to insurance in response to damages by the work mistake and negligence of KICA for subscriber and user. KICA shall make compensation on subscriber and user that not exceed the total amount of compensation(1 billion won a year, 0.5 billion a accident) from the insurance that KICA subscribed

b. In case the damage where exceeds the limit of liability, and is accompanied by a judgment of a legal court, KICA shall be responsible only within the above limits and only for cases officially resolved.

Singapore:

2.3 Financial Responsibility

2.3.1 Indemnification by Relying Party and Subscriber

2.3.1.1 Netrust shall be entitled to be indemnified from and against any and all loss, damage or liability and legal fees and costs incurred by Netrust in the event of or as a result of any act or default by any Relying Party making use of or relying on the Certificate or their agents and employees.

2.3.1.2 Without limiting other Subscriber obligations stated in this CPS, Subscribers are liable for any misrepresentations they make in Certificate or in their applications for Certificate to third parties who having verified one or more digital signatures with the Certificate, reasonably rely on the representations contained therein.

2.3.1.3 BY ACCEPTING A CERTIFICATE, THE SUBSCRIBER AGREES TO INDEMNIFY AND HOLD NETRUST, ITS ORA, THEIR AGENTS AND CONTRCTORS HARMLESS FROM ANY ACTS OR OMISSIONS RESULTING IN LIABILITY, ANY LOSS OR DAMAGE AND ANY SUITS AND EXPENSES OF ANY KIND, INCLUDING REASONABLE LEGAL FEES, THAT NETRUST, ITS ORA, THEIR AGENTS AND CONTRACTORS MAY INCUR, THAT ARE CAUSED BY THE USE OR PUBLICATION OF A CERTIFICATE AND THAT ARISES FROM (i) FALSEHOOD OR MISREPRESENTAT10N OF FACT BY THE SUBSCRIBER (OR A PERSON ACTING UPON INSTRUCTIONS FROM ANYONE AUTHORISED BY THE SUBSCRIBER); (ii) FAILURE BY THE SUBSCRIBER TO DISCLOSE A MATERIAL FACT, IF THE MISREPRESENTATION OR OMISSION WAS MADE NEGLIGENTLY ORWITH INTENT TO DECEIVE NETRUST, ITS ORA, THEIRAGENTS AND CONTFLACTORS OR ANY PERSON RECEIVING OR RELYING ON THE CERTIFICATE. OR (iii) FAILURE TO PROTECT THE SUBSCRIBER'S PRIVATE KEY, TO USE A TRUSTWORTHY SYSTEM, OR TO OTHERWISE TAKE THE PRECAUTIONS NECESSARY TO PREVENT THE COMPROMISE, LOSS, DISCLOSURE. MODIFICATION OR UNAUTHORISED USE OF THE SUBSCRIBER'S PRIVATE KEY.

2.3.1.4 When a Certificate is issued by the request of a Subscriber's agent, both the agent and the Subscriber shall jointly and severally indemnify Netrust, its ORA, their agents and contractors pursuant to this CPS. The Subscriber has a continuing duty to notify the issuer of any misrepresentations and omissions made by an agent.

<u>Chinese Taipei:</u>

2.3 Financial Responsibility

With regard to legal specifications in connection with government-authorized Specifications Administration Organization and CA, no financial risk management and compensation insurance risk management specifications have as yet been formulated. 'When such specifications have been formulated, CA must specify financial risk management and compensation insurance risk management specifications in CPS.

2.3.1 Indemnification by Relying Parties and Subscriber

Unless specified in applicable government legal regulations, CA or RA and Relying Party or Subscriber Agreement specifications must state that CA or RA has exemption from liability in the case of financial, characte1 or other injury to a third party due to intentional or negligent action on the part of Relying Party or Subscriber, and not due to the negligence of CA or RA.

If negligence or other circumstances attributable to Relying Party or Subscribers causes financial, character, or other injury to CA or RA, CA or RA may seek compensation from Relying Party or Subscribers in accordance with law.

2.3.2 Fiduciary Relationships

With regard to the Certificates issued under this CPS, the relationships between Subscriber and RA, or between Subscriber and CA, or between RA and CA are all direct relationships, and hence no fiduciary relationships exist.

2.3.3 Administrative Processes

CA is ordinarily exclusively responsible for Certificate management tasks, while RA is exclusively responsible for Subscriber registration tasks. If CA must additionally bear responsibility for Subscriber registration tasks due to service needs, CA will have to increase service charges in light of implementation management costs. In conjunction with various kinds of service operating specifications, this shall be specified in relevant service CP specifications.

Hong Kong China:

2.2.12 Financial Responsibility

An insurance policy is in place to cover the liabilities and claims against reliance limit on the certificates.

Thailand:

2.3 Financial Responsibility

2.3.1 Indemnification by Relying Party

Each Relying Party agrees to indemnify and hold harmless ACERTs PCS Participants for any and all losses or damages arising out of failure of the Relying Party to fulfill its obligations under this CPS, the applicable CP, and all other applicable PKI Documents. **2.3.2 Fiduciary Relationships**

All ACERTs PCS Participants agree that neither the creation and operation of ACERTs PCS by ACERTs, nor the issuance of Certificates by ACERTs CA or RA, shall make ACERTs, ACERTs CA or RA an agent, partner, joint venturer, fiduciary, trustee, or other representative of any Subscriber, or Relying Party.

2.3.3 Administrative Processes

ACERTs shall keep a proper set of accounts and engage an independent third party to audit the accounts in accordance with the laws of Thailand. The audited accounts may be published on a yearly basis as required by the laws of Thailand.

RFC3647-4.9.3 Confidentiality of Business Information

This subcomponent contains provisions relating to the treatment of the exchange of confidential business information, such as business plans, sales information, trade secrets, and information received from a third party under a nondisclosure agreement. Specifically, this subcomponent addresses:

* The scope of what is considered confidential information,
* The types of information that are considered to be outside the scope of confidential information, and
* The responsibilities of participants that receive confidential information to secure it from compromise, and refrain from using it or disclosing it to third parties.

Japan:

2.8. Confidentiality

2.8.1. Confidential information

Regarding A-Sign services, the JCSI and its customers must not disclose or divulge to a third party without the written prior consent of the other party any confidential information (including information about the subscribers) which (i) has been disclosed in a document that is expressly marked as confidential or (ii) has been disclosed orally with an empress statement that it is confidential and whose confidentiality was confirmed in writing within 14 days after the disclosure thereof from the other party. The JCSI and its customers must not use any such information beyond the range of necessity for providing or using A-Sign services.

The JCSI must handle as personal information the information provided or presented with a use application or revocation request from the subscribers and must not use any such information beyond the range of necessity for providing or using A-Sign services.

2.8.2. Non-confidential information

Despite section 2.8.1, the information set forth in the clauses listed below must not be regarded as confidential information:

(1) Information included in the certificate or CRL, except for the subscriber identifiers in the certificates for subscribers.

(2) Information included in this CPS.

2.8.3. Disclosure of information about certificate revocation

When a subscriber certificate is revoked upon request from the subscriber or other party, the CRL will include the reason code and date of revocation. These reasons code and dates of revocation are not regarded as confidential information and will be disclosed to all relying parties. Other details of the revocation will not be disclosed.

2.8.4. Disclosure to the law enforcement officials and other authorities

When a law enforcement official, court, bar association or other legally authorized person makes a non-forcible inquiry to the JCSI, and if it is judged to be a lawful self-defense or urgent escape, confidential information concerning the customers and subscribers may be disclosed to the law enforcement officials.

2.8.5. Disclosure as part of a civil procedure

Included in section 2.8.4.

2.8.6. Disclosure upon request from the user indicated on the certificate:

If the user indicated on the certificate issued files a document stating that his or her right or interest is infringed on or may be infringed on, the JCSI must check that the filer is the user indicated on the certificate or his or her authorized agent, then disclose:

- the use application and attachments,
- materials and records used to authenticate the user,

and

- the contents of the certificate which correspond to the certificate.

Except for cases set forth in 2.8.4 and 2.8.5 of this set of standards, the JCSI will not respond to requests for the disclosure of subscriber information from a relying party.

Regarding the certificate issued, as long as it is effective, only the information about whether the certificate is revoked will be disclosed on the CRL to the relying parties.

2.8.7. Other status of information disclosure:

When the JCSI decommissions part of its work, it may disclose confidential information to the subcontractor. To prevent leakage, a commissioning contract will be established to obligate the

parties to keep the information confidential.

Korea 1:

NO Regulation

Korea 2:

5.1.1.5 Protection of private information and safekeeping of data security

a.With regard to the information pertaining to subscribers obtained in performing certification procedures and the following data generated in operating certification authority, KICA does not use or disclose such private information for purposes other than that for certification service, unless otherwise stipulated by other laws, court order, or consent of the corresponding subscriber.

① Records related to certification application (other than what is recorded in the certificate or information already disclosed). ② Data related to audit and certification services.

b. With regard to one's own private information, subscribers are allowed access to certification management systems through which they may inspect or correct any relevant information.

Singapore:

2.8 Confidentiality

2.8.1 Types of Information to be Kept Confidential

2.8.1.1 The types of information Netrust will keep confidential include agreements, correspondence and business arrangement with its Sponsor, ORA, and Subscriber. These information are considered sensitive and shall not be disclosed without prior consent of the other respective party, unless required bylaw.

2.8.1.2 Any disclosure of subscriber-specific information by Netrust or ORA must be authorized by the Subscriber as defined in 1.3.4.

2.8.1.3 The Subscriber’s private keys are to be kept secret by the Subscriber. Disclosure of these keys by the Subscriber is at Subscriber's own risk.

2.8.1.4 Audit results and information are considered sensitive and wild not be disclosed to anyone other than Netrust authorized and trusted personnel. These information will not be used for any purpose other than audit purposes or where required by law.

2.8.1.5 Information pertaining to Netrust CA operations shall only be disclosed to Netrust authorized personnel on a need-to-know basis.

2.8.1.6 Netrust is not and shall not be obliged to disclose any information pertaining to management of Subscriber's Certificates unless expressly required by law.

2.8.2 Types of Information Not Considered Confidential

2.8.2.1 Notwithstanding any other provisions to the contrary all information revealed to Netrust and the ORA in the application forms are considered and shall be deemed to be not of a confidential nature and Netrust and its OFLA shall be allowed to make use of all such information in such manner as would be required by Netrust and/or the ORA in the conduct of Netrust's or the ORA's business, including without limitation the right to disseminate the aforesaid information to any third party.

2.8.2.2 The types of information that are not considered confidential includes information related to Subscriber's Certificate. Personal or corporate information that appear in public directories or web sites are also not considered confidential.
2.8.3 Disclosure of Certificate Revocation/Suspension Information
2.8.3.1 Netrust publishes the Certificate revocation information in the Netrust Directory.
2.8.4 Release to Law Enforcement Officials
2.8.4.1 In the event that Netrust is required under any provision of any rules, regulations or statutory provisions or by any order of court to release any information that is deemed to be or construed to be of a confidential nature under this CPS, Netrust sham be at liberty to release all such information required to be disclosed under any provision of any said rules, regulations or statutory provisions or by any order of court without any liabilities and any such release sham not be construed as or be deemed to be a breach of any obligations or requirements of confidentiality.
2.8.5 Release as Part of Civil Discovery
2.8.5.1 In the event that Netrust is required, pursuant to any suit or legal proceedings initiated by itself or otherwise, under any provision of any rules, regulations or statutory provisions or by any order of court to release any information that is deemed to be or construed to be of a confidential nature under this CPS, Netrust shall be at liberty to release all such information required to be disclosed under any provision of any said rules. regulations or statutory provisions or by any order of court without any
liabilities and any such release shall not be construed as or be deemed to be a breach of any obligations or requirements of confidentiality.
2.8.6 Disclosure Upon Owner's Request
2.8.6.1 In the event that the owner of any confidential information requests that Netrust reveal or disclose any confidential information owned by the said owner for any reasons whatsoever, Netrust shall only do so if it forms the opinion that the release of any such information will not result in the incurrence of any liability on any other party and Netrust shall not be liable for any damages or Posses arising out of any such revelation or disclosure of such confidential information and the owner of the confidential information shall indemnify Netrust for any and all liabilities, damages, Posses or any and all such liabilities arising out of or pursuant to any such revelation or disclosure of such confidential information.
2.8.7 Other Information Release Circumstances
2.8.7.1 Any and all such other information may be released by Netrust upon such times and under such circumstances as Netrust may at its sole option determine.

Chinese Taipei:

2.8 Confidentiality

2.8.1 Type of Information to be Kept Confidential

CA/RA must protect Subscriber information in accordance with the regulations of the Executive Yuan's "Computer-Processed Personal Information Protection Act" or in accordance with the regulations of other government agencies. Protection of Subscriber information must also conform to OECD data confidentiality protection regulations (OECD; Organization for Economic Co-operation and Development ; Guidelines on the Protection of Privacy and Transborder Flows of Personal Data).

While CA/RA may publicly reveal Subscribers Certificate Profile (for instance, ID card uniform serial number is confidential, protected information, but may be revealed when serving as user

identification information in Certificate Profile), when managing and using Subscriber information, CA/RA must strictly protect other information used at time of registration or Certificate application:

1. Subscriber information used for identity verification (such as Subscriber name, data births, identity verification identifie1 user password or code, contact information, etc.).
2. Confidential transaction-related information given by Subscriber at time of registration, Certificate application, or Certificate revocation
3. Registration forms filled out by Subscriber at time of registration, Subscriber information on contract, and confidential information on identity verification documents (photocopies).

2.8.2 Type of Information Not considered Confidential

Subscriber Certificate information published on directory server, Certificate status (available for Certificate of validity status queries), and CA CP, CPS, and Privacy Policy are considered open, non-confidential information. Detailed information publication functions are specified in service-related CP and operating specifications.

2.8.3 Disclosure of Certificate Revocation/Suspension Information

At present CA temporarily does not provide a Certificate suspension function. In accordance with generation frequency specifications, Certificate revocation information is generated and published in CRL and Certificate database and directory server Detailed information publication functions are specified in service-related CP and Certificate operating specifications.

2.8.4 Release to Law Enforcement Officials

Unless there is special need and:

1. conformance with CPS specifications or CP specifications;
2. conformance with government laws and regulations, and legal authorization from a competent Specification Administration Organization;
3. a court of law has formally applied for information in accordance with lag otherwise capped subscriber registration and Certificate information may not willfully be provided to an authorized Specification Administration Organization or other Subscribers.

2.8.5 Release as Part of Civil Discovery

CA is forbidden to willfully disclose Subscriber registration and Certificate information.

When Subscriber registration and Certificate information must be accessed due to a civil suit resulting from a transaction in which a Certificate was used, the information may be released only when the following conditions obtain:

1. A court has formally applied for relevant documents in accordance with lag or a litigation arbitration organization possessing lega1jurisdiction formally applies for documents;
2. Subscriber has authorized use of documents by means of electronic signature or written signature.

2.8.6 Disclosure upon Owner s Request

CA may provide Subscriber registration and Certificate information to a third party only after Subscriber has submitted an application for the documents using electronic signature or written signature as verification.

2.8.7 Other Information Release Circumstances

Except when required by government laws, or Subscribers has authorized its released, or CA has formally applied for it and wishes to use it lawful1g other Subscriber Certificate-related information may not be willfully provided to any other third party.

Hong Kong China:

2.7 Confidentiality

The restrictions in this subsection apply to HKPost and any HKPost subcontractors performing tasks related to HKPost's system of issuing withdrawing and publishing e-Certs. Information about Subscribers that is submitted as part of an application for an e-Cert certificate under this CPS will be used only for the purposes collected and is kept confidential except to the extent necessary for HKPost to perform 11s obligations under this CPS. Such information will not be released without the prior consent of the Subscriber except when required by a court-issued subpoena or order, or when otherwise required by the laws of Hong Kong SAR. HKPost is specifically precluded from releasing lists of Subscribers or Subscriber information (except for compiled data which is not traceable to an individual Subscriber in accordance with the laws of Hong Kong SAR) unless required by a court-issued subpoena or orde1 or when otherwise required by the laws of Hong Kong SAR.

Thailand:

2.8 Confidentiality

Reasonable steps will be undertaken by ACERTs CA or RA, to protect the Confidential Information of Subscribers that is disclosed to it during the registration, identification and authentication process, or Certificate suspension or revocation process. Confidential Information must not be disclosed in any manner to any third-party without the prior consent of the Subscriber to which the Confidential Information belongs, except where authorised by this CPS, the applicable CP, a Subscriber Agreement, or any other PKI Document.

2.8.1 Types of Information to be Kept Confidential

Subject to the limitations as set forth in Section 2.8.2, listed below are the categories of information considered Confidential Information for purposes of this CPS.

(a) Private Keys, whether held by Subscriber (including individuals representing Subscriber), ACERTs CA, RAs or any other Organisation, must be held in the strictest confidence. Each party is responsible for keeping its own Private Key confidential and, after Certificate issuance, no other party will have access to or be responsible for another's Private Key;

(b) information held in audit trails, including annual audit results, is confidential to ACERTs CA and will not be disclosed except as authorised in this CPS; and

(c) all personal and corporate information submitted as part of the registration, identification and authentication process, or Certificate suspension or revocation processes, that is not published as part of a Certificate, CRL, CP, or in this CPS is confidential to ACERTs CA or RA and will not be disclosed, except as authorised by this CPS.

2.8.2 Types of Information Not Considered Confidential

Notwithstanding Section 2.8.1, the following categories of information are not considered Confidential Information:

(a) information contained in Certificates, CRLs, and all personal and corporate information appearing on them;

(b) information in the CP or this CPS, provided that nothing in this Section will prevent ACERTs from limiting access to such documents in accord with the provisions of this CPS;

(c) revocation or suspension information relating to the compromise of the Certificate's Private Key; and

(d) any information that:

(i) is lawfully obtained from a third party under no obligation of confidentiality;

(ii) is independently developed without reference to any Confidential Information; or

(iii) is or becomes available to the public without breach of obligation of confidentiality by an ACERTs PCS Participant.

2.8.3 Disclosure of Certificate Revocation/Suspension Information

The revoked/suspended Certificate will include a revocation/suspension reason in the CRL and certificate status entry for the revoked/suspended Certificate. The revocation/suspension is not considered confidential and may be shared with Relying Parties.

2.8.4 Release to Law Enforcement Official

On receipt of a valid judicial order or as otherwise required by law, ACERTs CA and RAs may disclose Confidential Information to law enforcement officials. Unless prohibited by law, ACERTs CA and RAs will to the extent reasonably practical, give all interested persons or parties reasonable prior notice before disclosing such information.

2.8.5 Release as Part of Civil Discovery

During the course of any arbitration, litigation, or any other legal, judicial, or administrative proceeding, ACERTs CA and RAs may disclose Confidential Information. Unless prohibited by law, ACERTs CA and RAs will to the extent reasonably practical, give all interested persons or parties reasonable prior notice before disclosing such information.

2.8.6 Release upon Owner's Request

Upon receipt of a valid request from the appropriate ACERTs PCS Participant that originally provided the Confidential Information, directly or indirectly, or to which the Confidential Information appears to belong, ACERTs CA and RAs, may disclose Confidential Information to third-parties. Reasonable steps will be taken by ACERTs CA or RA to ensure that the Organisation making the request is the owner of the Confidential Information, but ACERTs CA or RA shall have no liability for any errors in disclosure. ACERTs PCS Participants that provide Confidential Information to ACERTs CA or RA in connection with ACERTs PCS agree to indemnify and hold harmless ACERTs CA or RA, as applicable, for any and all losses or damages arising from improper disclosures made to third-parties where ACERTs CA or RA disclosing such information had a reasonable belief that the disclosure request was proper.

2.8.7 Other Information Release Circumstances

ACERTs CA and RA will be entitled to disclose Confidential Information, on a “need-to-know” basis to any of its employees, contractors or agents that are assisting it in the verification of information supplied in Certificate applications or that are assisting it in the operation of ACERTs CA or RA. ACERTs CA and RA will also be entitled to disclose information which is considered to be confidential to third parties, such as legal and financial advisors, assisting in connection with any legal, judicial, administrative, or other proceedings required by law or by this CPS, and to legal counsel, accountants, banks and financing sources and their advisors in connection with mergers, acquisitions, or reorganisations. Any such disclosures will be permissible provided that ACERTs CA or RA use reasonable efforts to ensure that all such third parties will protect the Confidential Information at the same level as such Confidential Information is protected in this CPS.

RFC3647-4.9.4 Privacy of Personal Information

This subcomponent relates to the protection that participants (particularly CAs, RAs, and repositories) may be required to afford to personally identifiable private information of certificate applicants, subscribers, and other participants. Specifically, this subcomponent addresses the following to the extent pertinent under applicable law:

* The designation and disclosure of the applicable privacy plan regarding a participant's activities, if required by applicable law or policy;
* Information that is or is not considered private within the PKI;
* Any responsibility of participants that receive private information to secure and refrain from using and disclosing it to third parties;
* Any requirements as to notices to, or consent from individuals regarding use or disclosure of private information; and
* Any circumstances under which a participant is entitled or required to disclose private information pursuant to judicial, administrative process in a private or governmental proceeding, or in any legal proceeding.

Japan:

2.10. Protection of personal information

The JCSI must protect personal information that it has obtained when providing A-Sign public services as described below,.

(1) Positioning of personal information obtained:

Personal information owned includes information with no right to suspend its use or delete it, according to the provisions of the Digital Signature Law.

(2) Determining a purpose

The JCSI must use personal information about the subscribers that is needed to provide the subscribers with A-Sign public services, for the purpose of providing such services only. The details will be set forth in Chapters 3 and 4 of this set of standards.

Before changing this purpose, the JCSI must check that the change is within the range where it is reasonably considered to have a significant relationship with the current purpose according to the provisions of Chapter 8 as a change of this CPS.

(3) Limitations on the purpose

The JCSI will not use any personal information for any purpose other than that mentioned in the preceding clause. If a third party requests use for a purpose other than that specified, the JCSI will not consent to any such request except in exceptional cases specified in relevant laws.

(4) Appropriate acquisition

The JCSI will not obtain any personal information by fraud or other unlawful means.

(5) Notification of the purpose at the time of acquisition

The JCSI will disclose this set of standards for the purpose in (2) including those specified in the Digital Signature Law according to section 2.6 of this set of standards, and will disclose any changes according to Chapter 8 of this set of standards in order to keep such information publicized. In acquiring personal information, the JCSI will notify the subscribers of these purposes.

(6) Ensuring data accuracy

The JCSI will obtain personal information directly from the subscriber and correct and update it upon request from the subscriber alone. The JCSI will not respond to any request for correction or update from any third party other than the subscriber.

The JCSI will provide a correction application, mail it to the subscriber in advance, and only accept corrections and updates based on that correction application.

(7) Safety controls and supervision of employees and subcontractors

The JCSI will take measures to prevent divulgement, loss, and damage to personal information collected from the subscriber, including the supervision of information-handling personnel and subcontractors, according to section 4.6 and Chapter 5 of this set of standards.

(8) Limitations on provision for a third party

The JCSI will not respond to any third party's request for provision of personal information unless as set forth in relevant laws.

(9) Publication of matters related to owned personal data

The JCSI will set forth the purpose, information disclosure, corrections and other matters in this section in Chapter 1 of this set of standards, and will disclose this set of standards so that all subscribers will know them. No specific notices will therefore be given. (If there is a particular notice, the JCSI will reply as per this section.)

(10) Disclosure and correction

The JCSI will receive requests for disclosure and correction using a disclosure application and a correction application from the subscriber, and will give a notice about the request results with a method to be specified in a separate document.

If a specific correction leads to the revocation of an existing subscriber certificate, an application for certificate revocation must be filed together with a correction application.

(11) Suspension and other operations

Personal data owned by the JCSI is set forth in (I) and ****HIRO WHO IS “ONE”? USERS? COMPANIES? JCSI? PLEASE BE SPECIFIC is obligated to store it under the Digital Signature Law. The JCSI will therefore have no authority to suspend or delete it and cannot respond to a request from the subscriber.

(12) Explanation of the reason, procedure, charges, and ombudsmanship:

If the JCSI takes an action different from the one requested by the subscriber, JCSI will explain to the subscriber the reason why it decided to take that action. When making any such request, the subscriber him or herself must use a disclosure application or correction application. To respond to a request from the subscriber, the JCSI may claim the expenses actually incurred.

Korea 1:

NO Regulation

Korea 2:

5.1.1.5 Protection of private information and safekeeping of data security

a.With regard to the information pertaining to subscribers obtained in performing certification procedures and the following data generated in operating certification authority, KICA does not use or disclose such private information for purposes other than that for certification service, unless otherwise stipulated by other laws, court order, or consent of the corresponding subscriber.

Singapore:

Hong Kong China:

Thailand:

RFC3647-4.9.5 Intellectual Property Rights
This subcomponent addresses the intellectual property rights, including copyrights, patents, trademarks, or trade secrets, that certain participants may have or claim in a CP, CPS, certificates, names, and keys, or are the subject of a license to or from participants.

Japan:

2.9. Intellectual property rights

The copyrights for these standards and for the software and documents to be loaned to the customers by the JCSI will belong to the JCSI. If the customer is to use an A-Sign private service, he or she may use this set of standards in preparing a certification policy or customer CPS. However, if this certification policy or customer CPS is a secondary product under this set of standards, the JCSI will own the rights as the original copyright owner.

Korea 1:

2.6 Intellectual Property Rights

Intellectual property rights listed in below belong to KISA according to the Copyright Act and other related regulations:

- Software and hardware developed by KISA
- Certification Practice Statement of KISA
- the Name of KISA
  - Corporate Name
  - Internet Domain Name
- Key pair created by KISA

Korea 2:

No Regulation

Singapore:

2,9 Intellectual Property Rights

2.9.1 Netrust shall retain sole and exclusive ownership of all right, title and/or interest in and to the Certificate and all software supplied by Netrust. Netrust shall be entitled to continue using the Certificate and all software supplied in whatever form, manner or model it so elects.

2.9.2 All parties are to acknowledge that any and all of the copyrights, trademarks and other intellectual property rights used or embodied in or in connection with any and all Certificate issued and all software supplied by Netrust pursuant to this CPS, including all documentation and manuals relating thereto, is and shall remain the property of Netrust and the parties shall not during or at any time after the revocation, expiry or suspension of any of their Certificate in any way question or dispute the ownership or any other such rights of Netrust.

2.9.3 The parties also acknowledge that such trademarks, copyrights and other rights in the Certificate belongs to Netrust and/or that Netrust has the authority to use all such trademarks, copyrights and all such other rights and shall not be used by the parties unless with the express written consent of Netrust. Upon the termination, revocation, or expiry of any Certificate, the parties shall forthwith discontinue such use, without receipt of compensation for such discontinuation and the parties shall deliver unto Netrust any and all copies of the Certificate and software supplied by

Netrust that it has in its possession or shall at the request of Netrust destroy any and all copies of the Certificate and software supplied by Netrust that it has in its possession and shall render unto Netrust a certification that the parties has so duly done so.

2.9.4 The parties shall not, during or after the expiry, revocation, or termination of any Certificate, without the prior written consent of Netrust, use or adopt any name, trade name, trading style or commercial designation that includes or is similar to or may be mistaken for the whole or any part of any trademark, trade name, trading style or commercial designation used by Netrust.

Chinese Taipei:

2.9 Intellectual Property Rights

Intellectual property rights for hardware/software systems, related equipment, and relevant operating handbooks used by CA in the certificate management system belong to the supplying vendors. CA guarantees that it lawfully possesses right of use in all cases, and in no case in fringes upon the rights of any third party All systems and relevant operating handbooks developed in-house by TaiCA are owned by TaiCA.

TaiCA also owns intellectual property rights for the CPS, CPs, and other certificate management-related documents.

When Subscribers generate private and public keys, the public keys are certified by the CA in Certificate format, and are stored in the directory server or database. CA only provides Subscribers limited right of use of Public Key Certificate, and does not guarantee Subscribers' intellectual property rights.

CA respects Subscriber Registration Name stored as Subscriber Identification Name in X.509 V3 Certificate, but does not guarantee Subscriber's intellectual property right to Subscriber Registration Name. If Subscriber's registered trademark has already been claimed by another user at time of registration, arbitration and resolution of any resulting disputes is not under the CA’s jurisdiction. In that case, Subscribers must apply to the competent authorities for assistance in resolution.

Hong Kong China:

Thailand:

2.9 Intellectual Property Rights

All rights, titles and/or interests in and to the Certificates and all software supplied by ACERTs shall remain the sole and exclusive ownership of ACERTs. ACERTs shall be entitled to continued use of the Certificate and all software supplied in whatever form, manner or model it so elects.

All parties are to acknowledge that all of the copyrights, trademarks and other intellectual property rights used or embodied in or in connection with all Certificates issued and all software supplied by ACERTs pursuant to this CPS, including all documentation and manuals relating thereto, is and shall remain the property of ACERTs and the parties shall not during or at any time after the revocation, expiry or suspension of any of their Certificate in any way question or dispute the ownership or any other such rights of ACERTs.

The parties also acknowledge that such trademarks, copyrights and other rights in the Certificate belongs to ACERTs and/or that ACERTs has the authority to use all such trademarks, copyrights and all such other rights and shall not be used by the parties unless with express written consent of ACERTs. Upon the termination, revocation, or expiry of any Certificate, the parties shall forthwith discontinue such use, without receipt of compensation for such discontinuation and the parties shall

deliver unto ACERTs all copies of the Certificate and software supplied by ACERTs that it has in its possession or shall at the request of ACERTs destroy all copies of the Certificate and software supplied by ACERTs that it has in its possession and shall render unto ACERTs a certification that the parties has duly done so.
The parties shall not, during or after the expiry, revocation, or termination of any Certificate, without the prior written consent of ACERTs, use or adopt any name, trade name, trading style or commercial designation that includes, or is similar to, or may be mistaken for, the whole or any part of any trademark, trade name, trading style or commercial designation used by ACERTs.

RFC3647-4.9.6 Representations and Warranties
This subcomponent includes representations and warranties of various entities that are being made pursuant to the CP or CPS. For example, a CPS that serves as a contract might contain a CA's warranty that information contained in the certificate is accurate.
Alternatively, a CPS might contain a less extensive warranty to the effect that the information in the certificate is true to the best of the CA's knowledge after performing identity authentication procedures with due diligence. This subcomponent can also include requirements that representations and warranties appear in certain agreements, such as subscriber or relying party agreements. For instance, a CP may contain a requirement that all CAs utilize a subscriber agreement, and that a subscriber agreement must contain a warranty by the CA that information in the certificate is accurate. Participants that may make representations and warranties include CAs, RAs, subscribers, relying parties, and other participants.

Japan:

Korea 1:
2.1 Obligations

2.1.1 Korean Information Security Agency Obligations

2.1.1.1 Providing and Notifying Accurate Information
KISA immediately notifies the ACAs and the relying parties of the information as below which can affect the trustworthiness or validity of a accredited certificate in order to help anybody confirming it under the accredited certification practice structure.

Information on an ACA
- ACA nomination
- Suspension or revocation of an ACA certification practice
- Cancellation of an ACA nomination
- Transfer or merger of an ACA

Information about accredited certificate
- Accredited certificate
- Accredited certificate suspension and revocation list

Other certification practice related information

2.1.1.2 Provision of Information through Information and Communication Network
KISA shall publish the KISA's certificate, ACA's accredited certificate, and the accredited certificate suspension and revocation list through information and communication network so that ACA and relying parties can browse them anytime.

2.1.1.3 Measures on Vulnerability of Private Key
KISA revokes the KISA's certificate including public key in accord with private key and reissues the KISA's certificate by creating a new key pair when KISA recognizes that its private key is not secure. After renewal and issuance of an ACA's accredited certificate using a new private key, KISA immediately notifies the matters that everybody can identify and take measures to guarantee the safety and trustworthiness in the management under the accredited certification practice structure.

KISA, when informed of the loss and damage, theft, drain or vulnerability about the private key from an ACA, revokes the accredited certificate issued to the ACA and notifies the matters everybody can identify under the accredited certification practice structure. KISA, when being informed of loss and damage or theft, drain and vulnerability from the ACA of a governmental and municipal authority, immediately inform it to the Director of the National Intelligence Service.

2.1.1.4 Measures on Vulnerability of Digital Signature Algorithm
KISA, when recognizing that its digital signature algorithm is not secure, revokes the KISA's and ACA's accredited certificates issued by using its digital signature algorithm as well as immediately notifies the matters everybody can identify and takes measures to guarantee safety and trustworthiness in the practice under the accredited certification practice structure.

KISA, when informed vulnerability about the digital signature algorithm from an ACA, revokes the accredited certificate issued to the ACA and notifies the matters everybody can identify under the accredited certification practice structure. KISA, when informed vulnerability about the digital signature algorithm from the ACA of a governmental and municipal authority, immediately informs it to the Director of the National Intelligence Service.

2.1.2 Accredited Certification Authority Obligations

2.1.2.1 Providing and Notifying Accurate Information
ACA has to provide accurate information and facts to KISA in the cases below.

- Application for accredited certificate issuance
- Application for an accredited certification suspension and revocation
- Application for accredited certificate reinstatement

ACA has to notify the subscribers and the relying parties of the information as below which can affect the trustworthiness or validity of an accredited certificate in order to help anybody confirming it within the accredited certification practice structure.

- ACA nomination
- Certification suspension and revocation practice of an ACA

- Cancellation of ACA nomination
- Transfer or merger of an ACA
- Information on an accredited certificate
  - Subscriber's accredited certificate
  - Certification suspension and revocation practice of a subscriber
- Other certification practice related information

2.1.2.2 Protecting Private Key
ACA shall create their own digital signature keys using secure and reliable schemes utilizing reliable software or hardware, and manage them with utmost care so that digital signature generation keys will not to be lost/damaged or stolen/leaked by using security modules complying with technical specifications set forth in the Regulations on ACA's Facilities and Equipment.

When ACA generates a digital signature key for subscriber, ACA should apply trustworthy software and/or hardware to generate a digital signature key for a subscriber. In addition, ACA shall encrypt the digital signature key in accordance with Sub-Sec. 1.3 of Sec. 5 of the Regulations on ACA's Facilities and Equipment, store the digital signature key in a storage device along with Message Authentication Code (MAC) information in order to guarantee the integrity of the digital signature generation key, and directly transfer the digital signature key to the subscriber.

2.1.2.3 Using a Certified Private Key
ACA has to use the private key in accord with a KISA-certified public key when providing a certification practice.

2.1.2.4 Notification and Measures about Loss and Damage or Theft or Drain of Private Key
ACA, when its private key is lost, damaged, stolen or drained, takes measures to guarantee safety and trustworthiness by reporting to KISA under Sub-Sec. 3 of Sec.21 of the Electronic Signature Act.

2.1.2.5 Notification and Measures about Vulnerability of Private Key
When recognizing its private key is not secure, ACA immediately reports it to KISA and takes measures to guarantee safety and trustworthiness.

2.1.2.6 Notification and Measures about Vulnerability of Digital Signature Algorithm
When recognizing its digital signature algorithm is not secure, ACA immediately reports it to KISA and takes measures to guarantee safety and trustworthiness.

2.1.3 Relying Party Obligations

2.1.3.1 Understanding of Purpose in Use of Accredited Certificate
Relying party has to understand the purpose in use of accredited certificate issued by KISA under the Accredited Certification Practice Statement '1.6 Accredited Certificate Usage Range and Use'.

2.1.3.2 Confirming Accredited Certificate
Relying party has to verify the accredited certificate's valid period, utilization range, use and

trustworthiness prior to using the accredited certificate.
2.1.3.3 Confirming Suspension and Revocation of Accredited Certificate
Relying party has to verify and confirm the validity of an accredited certificate through the accredited certificate suspension and revocation list prior to using the accredited certificate.

Korea 2:
5.1.1 KICA's Responsibilities

5.1.1.1 Provision of accurate information and public announcement
a. KICA ensures that subscribers and users may verify the reliability and validity of certificates by announcing the following information promptly:

1) Information on KICA:
- Designation and cancellation as licensed certification authority.
- Recess, suspension, or revocation of certification services.
- Transfer, takeover, or merger of certification services.

2) Information concerning subscriber certificates:
- Subscriber certificates.
- Certificate Revocation List(CRL).

3) Certification Practice Statement of KICA.
4) Other information related to certification services.

5.1.1.2 Safekeeping of Private keys
KICA generates Key pair in a secure manner utilizing reliable software or hardware. KICA should securely manage the private key to prevent their loss, damage, theft, or leakage.

5.1.1.3 Measures to maintain security of Private keys
a. KICA informs KISA and a subscriber when KICA discovers any events that may affect reliability or validity of certificates, including loss, damage, theft, or leakage of Private key, or discovers any weaknesses in Key pair or in the algorithms, through communication networks immediately. And also, KICA may revoke subscriber certificates issued using the corresponding Private keys.

b. KICA generates new Private keys, has its Public key certified from KISA, and uses Private keys to re-issue subscriber certificates. KICA then notifies and distributes the corresponding facts through e-mail or communication networks.

c. Further, KICA publicly announces the corresponding facts so that anyone concerned can check them at any time through certification management systems, and can also take measures to secure the reliability and validity of its certification services.

5.1.1.4 Provision of directory service
KICA also provides directory service so that subscribers and users relying on a certificate may search certificate of KICA, subscriber certificates, and Certificate Revocation List (CRL) at any time through on-line communication networks.

5.1.1.5 Protection of private information and safekeeping of data security

a.With regard to the information pertaining to subscribers obtained in performing certification procedures and the following data generated in operating certification authority, KICA does not use or disclose such private information for purposes other than that for certification service, unless otherwise stipulated by other laws, court order, or consent of the corresponding subscriber.

- Records related to certification application (other than what is recorded in the certificate or information already disclosed).
- Data related to audit and certification services.

b. With regard to one's own private information, subscribers are allowed access to certification management systems through which they may inspect or correct any relevant information.

5.2.1 RA's Responsibilities

5.2.1.1 Observance of Certification Practice Statement

In providing licensed certification services, Registration Authorities observe these Rules and (pursuant to 5.3.1 of these Rules) carry out registration functions faithfully.

5.2.1.2 Receipt of applications for Certification services

With regard to issuance of certificates, Registration Authorities accept only those applications with accurate information based on facts, and until verifications are completed applications are not treated as "accepted". For personal identification, Registration Authorities observe specific guidelines set by KICA.

When the reception process is completed, Registration Authorities issue receipt slips prepared by KICA or by the RAs themselves.

c. Registration Authorities are prohibited from refusing receipt of applications for certificate issuance, suspension, revocation, reinstatement, etc. without good reasons. Accordingly, when refusing Registration Authorities should clearly state the reasons why the applications in question cannot be received.

5.2.1.3 Fast, accurate, and secure registration

Registration Authorities, as befitting their role as reliable managers of registration, carry out their responsibilities quickly, accurately, and securely.

5.2.1.4 Protection of private information and safekeeping of data security

Pursuant to 5.2.2.5 of these Rules, Registration Authorities protect the private information obtained in performing certification and safeguard the security of data.

5.2.1.5 Safeguard of facilities and personnel

In performing certification services, Registration Authorities observe security guidelines for facilities and personnel as set by KICA.

5.3.1 Subscribers' Responsibilities

5.3.1.1 Provision of accurate information

Information that subscribers provide, including changes subscribers make subsequently to them, in the following cases, shall always be accurate and based on facts:

a. Information provided for certificate application (issuance, re-issuance, and renewal).
b. Information provided when applying for suspension of certificates.
c. Information provided when applying for reinstatement of certificates.
d. Information provided when applying for revocation of certificates.
e. Changes made to subscribers' identity as recorded in the certificates.

5.3.1.2 Generation of Key pair

Pursuant to 3.1.2 of these Rules, subscribers can generate Key pair.

5.3.1.3. Protection and safekeeping of Private keys

a. Of the generated Key pair, subscribers are responsible for safekeeping of Private keys to prevent their loss, damage, theft, or leakage.

b. On recognizing that the Private keys belonging to them have been lost, damaged, stolen, or leaked, subscribers should immediately notify KICA of the corresponding fact through on-line communication networks, etc.

c. Upon recognition that the Private keys belonging to them have been lost, damaged, stolen, or leaked, subscribers should exert themselves to reduce or confine the damage.

5.3.1.4 Use of Private key

To generate key pair having legal validity, subscribers should use the Private key that matches the Public key contained in the KICA-issued certificate.

5.3.1.5 Verification of Certificates

On receiving new certificates, subscribers should confirm their validity, issuing body, their types, and services before using them.

5.4.1 User relying on a certificate

Users are those who, trusting reliability of the certificates issued by KICA, conduct business with KICA certificate holders.

5.4.2 Responsibilities of the user relying on a certificate

a. Before conducting business with KICA certificate holders, user relying on a certificate should confirm the validity, issuing body, types, and use of the corresponding certificates.

b. Before conducting business with KICA certificate holders, users should verify and confirm whether or not the corresponding certificates are suspended or revoked of their validity, using C.R.L.

c. For damages incurred by not observing confirmation responsibilities of users, the users are exclusively responsible.

Singapore:

Chinese Taipei:

Hong Kong China:

1.2.1.1 Representations by HKPost

By issuing a certificate that refers to this CPS, HKPost represents to Relying Parties who act in accordance with Section 2.1.3 and other relevant sections of this CPS, that HKPost has issued the certificate in accordance with this CPS. By publishing a certificate that refers to this CPS, HKPost represents to Relying Parties who act in accordance with Sections 2.1.3 and other relevant sections of this CPS, that HKPost has issued the certificate to the Subscriber identified in

1.2.2.1 Warranties and Representations by Subscribers

Each Subscriber (represented by the Authorised Representative in the case of applying for an e-Cert (Organizational), e-Cert (Sewer) certificate or e-Cert (Encipherment) certificate) must sign an agreement (in the terms specified in this CPS) which includes a tem by which the Subscriber agrees that by accepting a certificate issued under this CPS, the Subscriber warrants (promises) to HKPost and represents to all other relevant parties (and in particular Relying Parties) that during the operational period of the certificate the following facts are and will remain true:

a) No person other than the Subscriber of the certificates, the authorised users of an e-Cert (Organizational) certificate and the authorised units of an e-Cert (Encipherment) certificate has had access to the Subscriber' s private key.
b) Each digital signature generated using the Subscriber' s private key, which corresponds to the public key contained in the Subscriber's e-Cert (Personal) cefti1icate, e-Cert (Organizational) certificate or e-Cert (Sever) certificate, is the digital signature of the Subscriber.
c) An e-Cert (Encipherment) certificate is to be used only for the purposes stipulated in Section 1.2.3 (d) below.
d) All information and representations made by the Subscriber included in the certificate are true.
e) The certificate will be used exclusively for authorised and legal purposes.
f) All information supplied in the certificate application process does not infringe or violate in any way the trademarks, service marks, trade name, company name, or any other intellectual property rights of any third party.

Thailand:

RFC3647-4.9.7 Disclaimers of Warranties

This subcomponent includes disclaimers of express warranties that may be deemed to exist in an agreement, and disclaimers of implied warranties that may be imposed by applicable law, such as

warranties of merchantability or fitness for a particular purpose. The CP or CPS may directly impose such disclaimers, or the CP or CPS may contain a requirement that disclaimers appear in associated agreements, such as subscriber or relying party agreements.

RFC3647-4.9.8 Limitations of Liability

This subcomponent includes limitations of liability in a CP or CPS or limitations that appear or must appear in an agreement associated with the CP or CPS, such as a subscriber or relying party agreement. These limitations may fall into one of two categories: (1) limitations on the elements of damages recoverable and (2) limitations on the amount of damages recoverable, also known as liability caps. Often, contracts contain clauses preventing the recovery of elements of damages such as incidental and consequential damages, and sometimes punitive damages. Frequently, contracts contain clauses that limit the possible recovery from one party to the other a certain amount or an amount corresponding to a benchmark, such as the amount a vendor was paid under the contract.

RFC3647-4.9.9 Indemnities

This subcomponent includes provisions by which one party makes a second party whole for losses or damage incurred by the second party, typically arising out of the first party's conduct. They may appear in a CP, CPS, or agreement. For example, a CP may require that subscriber agreements contain a term under which a subscriber is responsible for indemnifying a CA for losses the CA sustains arising out of a subscriber's fraudulent misrepresentations on the certificate application under which the CA issued the subscriber an inaccurate certificate. Similarly, a CPS may say that a CA uses a relying party agreement, under which relying parties are responsible for indemnifying a CA for losses the CA sustains arising out of the use of a certificate without properly checking revocation information or the use of a certificate for purposes beyond what the CA permits.

Japan

2.2. Liabilities

2.2.1. Liabilities of the JCSI

In providing A-Sign public services, the JCSI will be in charge of the IA, RA, and repositories described in the preceding clause, and take the responsibilities for:

- the subscriber according to the subscriber agreement and,
- the relying party according to the relying party agreement.

If a corporation establishes an agreement with the JCSI for providing certificate issuance services to more than one specified subscriber, the warranties and liabilities between the corporation and the JCSI must be as per the provisions of the agreement in question and will not be covered in this set of standards. Also, with this agreement, the warranties and liabilities between the subscriber specified by the corporation and the JCSI will be as per the provisions of the special-purpose subscriber agreement (unlike those specified in this set of standards for the specification of the subscriber by the corporation), a statement made by the subscriber that it is specified, and matters regarding charge payments.

(a) The JCSI warrants the following:

- In response to a use application from the subscriber, the RA must perform specified applicant identification and request a certificate.
- If the RA requests a certificate in response to a use application from the subscriber, the IA must

issue a certificate accurately reflecting the contents of the request for a certificate from the RA (such as the subject identifier of the certificate).
- After a key pair (a private key and a public key) is generated by the RA upon the option of the subscriber, it must be handed over securely only to the subscriber who is supposed to own the key pair generated.
- Regarding the CRLs of all subscribers to be issued in A-Sign public services according to Chapter 4 of this set of standards, except for the temporary suspensions for system maintenance and suspensions that are urgent and unavoidable, one must prepare it, register it regularly on the JCSI repository, and keep it disclosed until the expiration of the effective period of the certificate.
- If one checks and receives a revocation request from the subscriber or other party, one must follow a secure revocation procedure on the certificate of the subscriber who has received a revocation request.
- Except for cases where the private keys of all certification authorities are inferred or calculated based on the public keys one must operate the certificate issuing system according to Chapters 5 and 6 of this set of standards, and make sure that there is no compromise due to theft or other cause.
- The certificate, CRL form, and attributes must conform to the provisions of Chapter 7 of this set of standards when respective certificates are issued.
- Various documents and papers including papers examined for subscribers must be stored with a method that is invulnerable to loss, tampering, or other inconvenience for the period set forth in the Digital Signature Law.
(b) Regardless of (a), the JCSI may abort a whole or a part of the A-Sign public services temporarily without notifying the subscriber or relying party, in either of the cases described below:
- When any of the equipment owned by the JCSI for A-Sign public services is maintained urgently.
- When A-Sign public services become no longer available due to a fire, power failure or other reason.
- When A-Sign public services become no longer available due to an earthquake, eruption, flood, tsunami, or other natural disaster.
- When A-Sign public services become no longer available due to a war, disturbance, riot, civil commotion, labor dispute, or other reason.
- In any other case when the JCSI finds it necessary to temporarily suspend providing A-Sign public services for reasons related to administration, technical matters, or contract execution with the customer.
(c) The liabilities that the JCSI has for the subscriber and relying party regarding A-Sign services must be limited to the ranges specified in (a) and (b).
2.2.2. Customer liabilities
As recipients of A-Sign public services, the players other than the JCSI (only the subscribers) must bear the following liabilities:
(a) Subscriber
The subscriber must bear all liabilities for matters indicated in the subscriber agreement regarding the IA, RA, and the JCSI in charge of the repository.
- The subscriber must follow the application formalities as per this set of standards and the subscriber agreement. At that time, he or she must not file a false application.
- If the subscriber to any of the items specified in this set of standards or the subscriber agreement, he or she must promptly apply for a certificate revocation.
- He or she must follow the provisions of this set of standards and subscriber

agreement.

Korea 1:

2.2 Liability of Korea Info 2.2 Liability of Korea Information Security Agency

2.2.1 Liability of Warranties

KISA guarantees the below relevant to the certificate issued by itself.

- The contents in the issued certificate are correct.
- The certificate is issued under the Electronic Signature Act.
- The matters about suspension and revocation of certificate are correct.

2.2.2 Exemption from Liability

KISA has no responsibility for any delays in certification practice or damages due to force majeures such as warfare and a natural disaster or reasons beyond provisions of the Electronic Signature Act, the Ordinance and the Regulations

.

Korea 2:

5.1.2 KICA's Liabilities

5.1.2.1 Liability for Damages

KICA compensates for damages inflicted on subscribers while providing certification service in violation of the Act, its enforcement decrees, regulations, or provisions of these Rules.

5.1.2.2 Limit of Liability

a. KICA is subscribed to insurance in response to damages by the work mistake and negligence of KICA for subscriber and user. KICA shall make compensation on subscriber and user that not exceed the total amount of compensation (1 billion won a year, 0.5 billion a accident) from the insurance that KICA subscribed

b. In case the damage where exceeds the limit of liability, and is accompanied by a judgment of a legal court, KICA shall be responsible only within the above limits and only for cases officially resolved.

5.1.2.3 Exemption of Liability

KICA does not assume responsibility for damages caused by the following reasons:

a. Damages that are caused by using the certificates beyond specific restrictions imposed by KICA on the scope of their application or use.

b. Damages that resulted from causes not attributable to KICA, including communication failures in providing such certification services as issuance, re-issuance, and renewal of certificates or in announcing lists of suspended or revoked certificates, or failures of subscribers' system.

c. Damages caused by not checking and verifying on the part of user relying on a certificate, as required under "5.5.2 Responsibilities of user relying on a certificate" of these Rules.

d. Damages other than those that are direct and compensatory caused in connection with KICA's certificates and certification services.

e. Damages caused by fraudulent information provided by subscribers or other illegal means.

f. Damages caused by revised information that subscribers failed to provide due to negligence or intention.

Damages caused by careless management of Private keys on the part of subscribers.

Damages caused by reasons other than those stipulated in the Act or in the Certification Practice Statement.

5.1.2.4 Limitation on warranty

KICA does not warrant the matters such as subscribers' credit or the integrity of information related to subscribers that are not provided under the Act and these Rules.

5.1.2.5 Security for Liability for Damages

As a security for its Liability for Damages, KICA is carrying a policy of public liability insurance.

5.2.2 RA's Liabilities

a. In case Registration Authorities cause subscribers and users to suffer damages by violating provisions of the Act, its enforcement decrees, regulations, and these Rules in performing certification functions, RAs shall be subject to the same liabilities as those applicable to KICA, as shown in "5.2.4 KICA's Liabilities."

b. As a security for such Liability for Damages, Registration Authorities may subscribe to public liability insurance.

5.3.2 Subscribers' Liabilities

In case subscribers cause KICA to suffer damages by violation of subscribers' responsibilities pursuant to these Rules or in the process of using certification services then subscribers are liable to compensate for the damages inflicted on KICA..

Singapore:

2.2 Liability

2.2.1 CA Liability

2.2.1.1 Warranties and Limitations on Warranties

NETRUST MAKES NO OTHER WARRANTIES EXPRESS OR IMPLIED AND HAVE NO FURTHER OBLIGATIONS UNDER THIS CPS AND EXCEPT AS EXPRESSLY PROVIDED IN THE FOREGOING, NETRUST DISCLAIMS ALL WARRANTIES AND OBLIGATIONS OF ANY TYPE, INCLUDING, BY WAY OF EXAMPLE AND NOT OF LIMITATION; (i) ANY WARRANTY OF MERCHANTABILITY; (ii) ANY WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE; (iii) THAT THE USE OF THE CERTIFICATE OR ANY SOFTWARE PROVIDED AND/OR SUPPLIED HEREUNDER AND/OR PURSUANT TO THIS CPS WILL NOT INFRINGE ANY PATENT, COPYRIGHT OR TRADEMARK OR OTHER PROPRIETARY RIGHTS OF OTHERS; (iv) AND ANY WARRANTY OF THE ACCURACY OF INFORMATION PROVIDED, AND FURTHER DISCLAIM ANY AND ALL LIABILITY FOR NEGLIGENCE AND LACK OF REASONABLE CARE.

Netrust does not warrant the accuracy, authenticity, reliability, completeness, currentness, merchantability or fitness of purpose in relation to any information contained in Certificate or otherwise compiled, published or disseminated by or on behalf of Netrust and Netrust disclaims all liabilities for representations of information contained in a Certificate, and Netrust does not warrant "non-repudiation" of signature on any electronic communication or transaction (as mentioned above in Clause 1.3.6 above).

2.2.1.2 Kinds of Damages Covered

Netrust shall not be liable for any loss or damage whatsoever or howsoever caused arising directly or indirectly in connection with the use or reliance on any Certificate by any parties.

Notwithstanding any other provisions to the contrary, Netrust is to and/or has expressly excluded liability for all indirect, special, incidental and consequential loss or damage, howsoever caused including without limitation, negligence, default or any acts of Netrust, its employees, agents, contractors, representatives, including but not limited to loss or damage to other equipment or property or for loss of profit, business, revenue, goodwill or anticipated savings pursuant to the use or reliance of any Certificate or any other transactions, services offered or contemplated by this CPS even if Netrust has been advised of the possibility of such damages. No action arising pursuant to the use or reliance of any Certificate, regardless of form, may be brought by any parties more than one (1) year after such cause of action has arisen.

2.2.1.3 Loss Limitations

Subject to the provisions of this clause, in the event that (i) any limitation or provision contained in this Agreement is held to be invalid for any reason; and (ii) Netrust breaches any of its obligations pursuant to Clause 2.1 above, and Netrust becomes liable for loss or damage that would otherwise have been excluded hereunder or excludable in law, (a) Netrust's total liability shall be limited to the aggregate amount of its liability under any insurance policies that it subscribes to for each Certificate currently at the level set out below for each Certificate within each of its class or such other applicable liability cap for such Certificate as may be further and/or subsequently amended by Netrust; and (b) Netrust shall only be liable for any such loss or damages if such loss or damage arose or is incurred during the paid subscription period.

This limitation on damages applies to loss and damages of all types, including but not limited to direct, compensatory, indirect, special, consequential, exemplary or incidental damages incurred by any person, including without limitation a Subscriber, an applicant, a recipient or a Relying Party that are caused by reliance on or use of a Certificate Netrust issues, manages, uses, or revokes or such a Certificate that expires. This limitation on damages applies as well to liability under contract,

tort and any other form of liability claim. The liability cap on each Certificate shall be the same regardless of the number of digital signatures, transactions or claims related to such Certificate. For each class of Certificate, the liability cap is stipulated in its respective CP. In the event that the liability cap is exceeded, the available liability cap shall be apportioned first to the earliest claims to achieve final dispute resolution, unless otherwise ordered by a court of competent jurisdiction. In no event shall Netrust be obligated to pay more than the aggregate liability cap for each Certificate, regardless of the method of apportionment among claimants to the amount of the liability cap.

2.2.1.4 Other Exclusions

Netrust's PCS are not designed, intended or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities. aircraft navigation or communication systems, air traffic control systems or weapons control systems, where failure could lead directly to death, personal injury or severe environmental damage.

2.2.2 ORA Liability

2.2.2.1 The liabilities of the ORA are addressed in the appropriate and applicable ORA Agreement entered into between the applicable ORA and Netrust.

Chinese Taipei:

2.2 Liability

The certification service items provided by TaiCA and their content are uniformly specified in item 1.3 of this CPS and service-related CP specifications. TaiCA shall bear no liability for content not specified in this CPS, such as transaction system used by Subscribers and Relying Party.

2.2.1. CA Liability

· With regard to CA processing of Subscriber registration data and Certificate issuance tasks, unless CA has caused Subscribers losses through operations in accordance with this CPS, CP and relevant operating regulations, or through negligence attributable to CA, CA shall under no circumstances be held liable for damages.

· If the issued Certificate causes Subscribers losses through interruption of Internet transmission, equipment malfunction, other nature disaster (such as war or earthquake), or other circumstances not involving the negligence or malicious intent of CA operating staff CA shall under no circumstances be held liable for damages.

· If, due to the negligence or malicious intent of operating staff or through failure to comply with regulations of this CPS, CP, or relevant operating specifications, CA's implementation of registration, Certificate issuance, and revocation tasks causes injury to Subscribers, CA must, in accordance with regulations, compensate Subscribers for their direct losses, but shall not be held liable for other associated losses. Holders of electronics certificates may receive the following maximum compensation during the year:

	Type of Entity	Amount of compensation (units: NT$)
1	Natural persons	NT $ 250,000
2	Corporate entities	NT $ 1,000,000
3	SSL server (128 buts, 40bit)	According to contract terms
4	Merchant	NT $ 600,000
5	Gateway	NT $ 1,500,000

· The length of time during which Subscribers may pursue compensation shall be set in accordance MOEA regulations and other legal requirements. Other service-related liabilities shall be specified in relevant CP specifications and contracts.

2.2.2 RA Liability

· RA and its operating staff must fulfill their obligation to protect Subscriber registration data and relevant information, and avoid the disclosure, misuse, falsification, and willful use of relevant information. If an error on the part of the RA and its operating staff while processing Subscriber registration and related data, or while applying to CA for a Subscriber Certificate, causes injury to Subscribers or other parties, That RA and its operating staff must bear liability for compensation.

· Other service-related liabilities shall be specified in relevant service-related CP specifications, RA and CA service contract stipulations, and RA and Subscriber service contract stipulations.

2.2.3 User (or Subscriber) Liability

· If a Subscribe1 either intentionally negligently or with dishonest intent, provides false information while applying to RA for registration, causing injury to RA, CA, or any third party that Subscriber must bear liability for all damages.

· Subscribers must adequately protect their private key and password, and not reveal or transfer them to another person for that person's use. If Subscriber, either intentionally or negligently so causes injury to RA, CA, or any third party, that Subscriber must bear liability for all damages.

· If Subscriber violates this CPS, CP, relevant operating specifications, or other certificate use service scope not specified in this CPS when applying to use Certificate or use Relying Party Certificate, Subscriber must bear liability for all damages.

· Other service-related liabilities shall be specified in relevant service-related CP and contract specifications.

Hong Kong China:

2.2.3 Limitation of Liability

2.2.3.1 Reasonableness of Limitations

Each Subscriber and Relying Pap must acknowledge and agree that the PKI initiative and HKPost's role as a CA within that initiative me new and innovative ventures, in which the sum received by HKPost from Subscribers is modest compared to the burden that could be placed upon HKPost if HKPost were liable to Subscribers and Relying Parties without limit for damages under or in connection with Subscriber Agreements or the issue by HKPost of certificates under the PKI. Accordingly, each Subscriber and Relying Party must agree that it is reasonable for HKPost to limit its liabilities as set out in the Subscriber Agreements and in this CPS.

2.2.3.2 Limitation on Types of Recoverable Loss

In the event of HKPost' s breach of the Subscriber Agreements or of any duty of care, and in particular, of its duty under the Subscriber Agreements to exercise reasonable skill and care and/or duties that may arise to a Subscriber or Relying Party when any certificate issued by HKPost under the PKI is relied upon or used by a Subscriber or Relying Party or anyone else or otherwise howsoever whether a Subscriber or Relying Party suffers loss and damage as a Subscriber or as a Relying Party as defined by the CPS or otherwise howsoeve1 **HKPost shall not be liable for any damages or other relief in respect of (l) any direct or indirect: loss of profits or revenue, loss or injury Co reputation or goodwill, loss of any opportunity or chance, loss of projects; or the loss or loss of use of any data, equipment or software or**

(2) for any indirect, consequential or incidental loss or damage even i[in respect of the latter, HKPost has been advised of the likelihood of such loss or damage in advance.

2.2.3.3 HK $ 500,000 and HK $ 250,000 Limit

Subject to the exceptions that appear below, in the event of HKPost's breach of a Subscriber Agreement or of any duty of care, and in particular, of any duff under the Subscriber Agreements, under this CPS or in law to exercise reasonable skill and care and/or breach of any duties that may arise to a Subscriber or Relying Party when any certificate issued by HKPost under the public key infrastructure initiative is relied upon or used by a Subscriber or Relying Party or anyone else or otherwise howsoever, whether a Subscriber or Relying Party suffers loss and damage as a Subscriber or as a Relying Party as defined by the CPS or otherwise howsoever the liability of HKPost to any Subscriber and any Relying Party, whether as Subscriber or Retying Party as defined by the CPS or in any other capacity at all, is limited to, and shall not under any circumstances exceed, HK $500,000 in respect of one e-Cert (Personal) certificate, e-Cert (Organizational) certificate or e-Cert (Server) certificate or HK $250,000 in respect of one e-Cert (Encipherment) certificate.

2.2.3.4 Time Limit For Making Claims

Any Subscriber or Relying Party who wishes to make any legal claim upon HKPost arising out of or in any way connected with the issuance, withdrawal or publication of an e-Cert must do so within one year of the date upon which Chat Subscriber or Relying Party becomes aware of any facts giving rise to the right to make such a claim or (if earlier) within one year of the date when, with the exercise of reasonable diligence, they could have become aware of such facts. For the avoidance of doubt, ignorance of the legal significance of those facts is immaterial. After the expiration of this one-year time limit the claim shall be waived and absolutely barred.

2.2.3.5 Hong Kong Post Office Personnel

Neither the Hong Kong Post Office nor any officer or employee or other agent of the Hong Kong Post Office is to be a party to the Subscriber Agreements, and the Subscriber and Relying Parties must acknowledge to HKPost that, as far as the Subscriber and Relying Parties are aware, the Hong Kong Post Office and none of such officers, employees or agents voluntarily accepts or will accept any personal responsibility or duty of care to the Subscriber or Relying Parties in connection with any action or omission done in good faith by any of them in any way connected either with the performance of HKPost of a Subscriber Agreement or any certificate issued by HKPost as a CA and each and every Subscriber and Relying Party accepts and will continue to accept that and undertakes to HKPost not to sue or seek any form of recovery or redress by other legal means whatsoever from any of the foregoing in respect of any act or omission done by that person in good faith (whether done negligently or not) in any way connected with either the performance of HKPost of a Subscriber Agreement or any certificate issued by HKPost as a CA and acknowledges that HKPost has a sufficient legal and financial interest to protect these individuals from such actions.

2.2.3.6 Liability For Wilful Misconduct, Personal Injury or Death

Any liability for fraud or wilful misconduct personal injury and death is not within the scope of any limitation or exclusionary provision or notice of this CPS, any Subscriber Agreement or certificate issued by HKPost and is not limited or excluded by any such provision or notice.

2.2.3.7 Liability to Consumers

In respect of subscribers who do not enter into Subscriber Agreements in the course of a business or held themselves out as doing so, it is possible that, as a matter of law some or all of the limitations of liability that apply in the event of HKPost's failure to carry out the Subscriber Agreements with them with reasonable skill and care do not apply to any claim they may have.

2.2.3.8 Certificate Notices, Limitations and Reliance Limit

Certificates issued by HKPost shall contain the following reliance limit and/or limitation of liability notice:

"The Postmaster General acting by the officers of the Hong Kong Post Office has issued this certificate as a CA under the Electronic Transactions Ordinance upon the terms and conditions set out in the Postmaster General's Certification Practice Statement (CPS) thal applies lo this certificate.
Accordingly, any person, before relying upon this certificate should read the CPS which may the HKPost C.4 web site at http//www. hongkongpost. gov. hk. The laws of Hong Kong SAR applies to this certificate ahd Relying Parties mast submit any dispute or issue arising as a result of their reliance upon this certificate to the non-exclusive jurisdiction of the Courts of Hong Kong SAR.

If you, as a Relying Party, do not accept the terms and conditions upon which this certificate is issued, then do not rely upon it.

The Postmaster General (by the Hong Kong Post Office, its officers, employees and agents) issues this certificate without undertaking any responsibility or duty of care to Relying Parties save as set out in the CPS.

Relying Parties, before relying upon this certificate are responsible for:-

a) Relying on it only when relation is reasonable and in good faith in the light of all the circumstances known to the Relying Party at the time of reliance:
b) Before relying upon this certificate, determining that the use of the certificate is appropriate for its purposes under the CPS:
c) Checking the status of this certificate Oh the Certificate Revocation List prior to reliance; and
d) Performing all appropriate certificate validation procedures.

If, despite the exercise of reasonable skill and care by the Postmaster General and the Hong Kong Post Office, its officers, employees or agents, this certificate is in any way inaccurate or misleading, the Postmaster General, Hong Kong Post Office, its officers, employees or agents, accept no responsibility for any loss or damage to the Relying Parties and the applicable reliance limit that applies to this certificate under the Ordinance in these circumstances is HK $0.

If this certificate is in any way inaccurate or misleading and this is the result of the negligence of the Postmaster General, Hong Kong Post Office, its officers, employees or agents, then the Postmaster General will pay a Relying Party up to HK $ 500,000 or, if this certificate is an e-Cert (Encipherment) certificate, HK $ 250,000, in respect of

proved loss caused by reasonable reliance upon such inaccurate or misleading matters in this certificate where such losses are not and do not include (I) any direct or indirect loss of profits or revenue, loss or injury to reputation or goodwill, loss of any opportuniity or chance, loss of projects, or the loss or loss of use of any data, equipment or software or (2) any indirect, consequential or incidental loss or damage even if; in respect of the latter, HKPost has beer' advised of the likelihood of such loss or damage in advance. The applicable reliance limit that applies to this certificate under the Ordinance in these circumstances is HK $500,000 or, if this certificate is an e-Cert (Enciphermemi) certificate, HK $250,000, and in all cases in relation to categories of loss (1) and (2), is HK $ 0.

Neither the Hong Kong Post Office nor any Officer, employee or agent of the Hong Kong Post Office undertakes any duty of care to Relying Parties in any circumstances in relation to this certificate.

Time Limit For Making Claims

Any Relying Party who wishes to make any legal claim upon the Postmaster General arising out of or in any way connected with the issuance, withdrawal or publication of this e-Cert must do so within one year of the date upon which that Relying Party becomes aware of any facts giving rise to the right to make such a claim or (if earlier) within one year of the date when, with the exercise of reasonable diligence, they could have become aware of such facts. For the avoidance of doubt, ignorance of the legal significance of those facts is immaterial. After the expiration of this one-year time limit the claim shall be waived and absolutely barred.

If this certificate contains any international or reckless misrepresentation by the Postmaster General the Hong Kong Post Office, its officers, employees or agents. this certificate does not impose any limit upon their liability to Relying Parties who suffer loss it, consequence of reasonable reliance upon such misrepresentation in this certificate.

The limits of liability contained here in do not apply in the (unlikely) event of liability for personal injury or death".

2.2.4 HKPost's Liability for Defective e-Cert Customer Kit or CD-ROM (or alternative storage medium) or Floppy Disk or other Storage Medium and for Accepted but Defective Certificates

2.2.4.1 Notwithstanding the limitation of liability set out above, if the e-Cert Customer Kit or CD-ROM (or alternative storage medium) or floppy disk or other storage medium "kit") referred to in Sections 3.1.7 or 4.3 (as applicable) below is defective so that the certificate in respect of which the same was supplied cannot be completed or accepted properly or at all, and the Subscriber to whom they were supplied notifies HKPost of this immediately to permit the supply (if desired) of a replacement "kit", then if such notification has occurred within 3 months of the Subscriber being sent the "kit" and the Subscriber no longer wants a certificate, HKPost, on being satisfied of the existence of any such defect, will refund the fee. If the Subscriber waits longer than 3 months after the date upon which the "kit" was sent to him before notifying HKPost of any such defect, the fee will not be refunded as of right, but only at the discretion of HKPost.

2.2.4.2 Notwithstanding the limitation of HKPost's liability set out above, if after acceptance of the certificate, a Subscriber finds that, in respect of e-Cert (Personal) certificates, e-Cert (Organizational) certificates and e-Cert (Server) cefti1icates, because of any error in the private key or public key of the certificate, no transactions contemplated by the PKI can be completed properly or at all, or, in respect of an e-Cert (Encipherment) certificate, no enciphered electronic communications can be completed properly or at all, and that Subscriber notifies HKPost of this immediately to permit the certificate to be revoked and (if desired) re-issued, then, if such notification has occurred within 3 months of the acceptance of the certificate and the Subscriber no longer wants a certificate, HKPost, on being satisfied of the existence of any such error will refund the fee. If the Subscriber waits longer than 3 months after acceptance before notifying HKPost of any such error, the fee will not be refunded as of right, but only at the discretion of HKPost.

Thailand

2.2 Liability

2.2.1 CA Liability

Subject to the provisions of this clause, in the event that:

(a) any limitation or provision contained in this Agreement is held to be invalid for any reason; and

(b) ACERTs breaches any of its obligations pursuant to Clause 2.1.1 above, and ACERTs becomes liable for loss or damage that would otherwise have been excluded hereunder or excludable in law.

ACERTs' total liability shall be limited to the aggregate amount of its liability under any insurance policies that it subscribes to for each Certificate currently at the level set out in the respective CP for each Certificate within each of its class or such other applicable liability cap for such Certificate as may be further and/or subsequently amended by ACERTs. ACERTs shall only be liable for any such loss or damages if such loss or damage arising or is incurred during the paid subscription period.

This limitation on damages applies to loss and damages of all types, including but not limited to direct, compensatory, indirect, special, consequential, exemplary or incidental damages incurred by any person, including without limitation a Subscriber, an applicant, a recipient or a Relying Party that are caused by reliance on or use of a Certificate ACERTs issues, manages, uses, or revokes or such a Certificate that expires. This limitation on damages applies as well to liability under contract, tort and any other form of liability claim. The liability cap on each Certificate shall be the same regardless of the number of digital signatures, transactions or claims related to such Certificate. For each class of Certificate, the liability cap is stipulated in the respective CP. In the event that the liability cap is exceeded, the available liability cap shall be apportioned first to the earliest claims to achieve final dispute resolution, unless otherwise ordered by a court of competent jurisdiction. In no event shall ACERTs be obligated to pay more than the aggregated liability cap for each Certificate, regardless of the method of apportionment among claimants to the amount of the liability cap.

ACERTs CA shall have no liability whatsoever for any loss:

(a) incurred between the time a Certificate is revoked and the next scheduled issuance of a CRL;

(b) due to the unauthorised issuance or use of Certificates, or use of Certificates beyond the limits set forth in this CPS and the applicable CP;

(c) caused by fraudulent or negligent use (other than by ACERTs CA) of Private Keys, Certificates,

and/or information obtained from the Repository;

(d) resulting from interruptions in services that are not the sole fault of ACERTs CA (e.g. acts of God or other causes beyond its control). These interruptions may be caused by, but not limited to, strikes, or other labour disputes, riots, civil disturbances, actions or in actions of suppliers, acts of God, war, fire, explosion, earthquake, flood or other catastrophes; and

(e) incurred as a result of the performance or non-performance of any RA, or for actions taken outside the scope of the RA's authority, as set forth in this CPS, the applicable CP and RA Agreement.

ACERTs CA SHALL HAVE NO LIABILITY FOR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES INCLUDING, BUT NOT LIMITED TO ANY LOSS OF PROFITS, LOSS OF DATA OR ANY OTHER INDIRECT OR CONSEQUENTIAL OR PUNITIVE DAMAGES ARISING FROM OR IN CONNECTION WITH THE CA SERVICES, ITS PERFORMANCE OF ITS OBLIGATIONS UNDER THIS CPS, ANY CP, SUBSCRIBER AGREEMENT, OR THE PERFORMANCE OR NON-PERFORMANCE OF ANY RA. EXCEPT AS EXPRESSLY PROVIDED IN THIS CPS, ACERTs CA DISCLAIMS ALL OTHER WARRANTIES AND OBLIGATIONS OF ANY TYPE, INCLUDING ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR ACCURACY OF INFORMATION PROVIDED.

2.2.2 RA Liability

Each RA is fully and solely responsible for all claims or losses related to the performance or non-performance of its obligations, and for actions taken outside the scope of the RA's authority, as set forth in this CPS, the applicable CP and RA Agreement. However, no RA shall have any liability for any indirect, special, incidental, or consequential damages, including but not limited to lost profits, loss of data, or punitive damages.

Each RA agrees to indemnify and hold harmless ACERTs PCS Participants for any and all losses or damages arising out of:

(a) performance or non-performance of the RA's obligations;

(b) actions taken by the RA outside of the RA's authority, as set forth in this CPS, and the applicable CP and RA Agreement; and

(c) any use of the RA's Private Keys other than as expressly set forth in this CPS, and applicable CP and RA Agreements.

Notwithstanding the foregoing, in those cases where the RA function is performed directly by ACERTs CA, the limitation on the RA's liability shall be as specified in Section 2.2.1 above.

2.2.3 Subscriber Liability

Each Subscriber is fully and solely responsible for all claims or losses related to the performance or non-performance of its obligations, as set forth in this CPS, the applicable Subscriber Agreement, and any other applicable PKI Documents. Any further liabilities of the Subscriber shall be more specifically set forth in the applicable Subscriber Agreement.

Each Subscriber agrees to indemnify and hold harmless ACERTs PCS Participants for all losses or damages arising out of:

(a) performance or non-performance of the Subscriber obligations, as set forth in this CPS, the applicable Subscriber Agreement, and any other applicable PKI Documents;

(b) the use of any name infringing upon third-party trademark rights, as set forth in Section 3.1.6, below; and

(c) any use of the Subscriber's Private Keys other than as expressly set forth in this CPS, the

applicable CP, Subscriber Agreements and any other applicable PKI Documents.

2.2.4 Relying Party Liability

Each Relying Party is fully and solely responsible for all claims or losses related to the performance or non-performance of its obligations, as set forth in this CPS, the applicable CP, and any other applicable PKI Documents.

RFC3647-4.9.10 Term and Termination

This subcomponent can include the time period in which a CP or a CPS remains in force and the circumstances under which the document, portions of the document, or its applicability to a particular participant can be terminated. In addition or alternatively, the CP or CPS may include requirements that certain term and termination clauses appear in agreements, such as subscriber or relying party agreements. In particular, such terms can include:

* The term of a document or agreement. That is, when the document becomes effective and when it expires if it is not terminated earlier
* Termination provisions stating circumstances under which the document, certain portions of it, or its application to a particular participant ceases to remain in effect.
* Any consequences of termination of the document. For example, certain provisions of an agreement may survive its termination and remain in force. Examples include acknowledgements of intellectual property rights and confidentiality provisions. Also, termination may trigger a responsibility of parties to return confidential information to the party that disclosed it.

Japan

4.9. Termination of the CA

The CA for A-Sign public services will be terminated if the authorization under the Digital Signature Law cannot be renewed due to the revision of laws related to the Digital Signature Law or a change in the provisions of sections 2.2 through 2.4 of this set of standards and the JCSI's business principles. This termination will start to be disclosed on the JCSI's website two months before the termination until six months afterwards, unless it is absolutely impossible, and a termination notice will be mailed to the subscriber two months before the termination. When the CA is terminated, the JCSI will completely initialize or physically destroy and abort using the certificate signature key and its backup storage medium, but will not revoke the CA certificate corresponding to the certificate signature key. The JCSI will abort the issuance (including the renewed issuance) of a new certificate. All certificates still effective and unrevoked at that time will be revoked with the termination of the CA. The JCSI will also mail a revocation notice to the subscriber. The JCSI will update the last CRL on which this collective revocation is to be added and will publicize that CRL on the URL indicated in the certificate for six months. Even if the CA is to be terminated, the JCSI will continue to store the various documents and data on paper and in digital form for the storage period for forms set forth in the Digital Signature Law. The provisions about the successive controller of such stored information will be included in the contents publicized when the CA is terminated, if it is

Korea 1

8.2 Enforcement Procedure

KISA reports the established and revised Accredited Certification Practice Statement to the Minister of Information and Communication.

When newly instituting or amending the Certified Certification Practice Statement, KISA shall officially notify individually all ACAs and all other parties concerned as per Section 1.4.2 'Certificate Practice Related Information' of the Accredited Certification Practice Statement.

The established and revised Accredited Certification Practice Statement is in force since the day of report.

Korea 2

10.1.5 Subscriber's Agreement

Unless subscribers file their formal objections, within 2 weeks of announcement of changed Rules, in writing or by electronically signed documents using the Private key that matches the certificate issued by KICA, the corresponding subscribers will be recognized by KICA to have agreed on the changed Rules.

10.1.6 Enforcement

This CPS comes into effect from June 12, 2004

Singapore

Chinese Taipei

4.9 CA Termination

If CA terminates system operation for some cause, it must reduce risk to service system to a minimum. CA must therefore stably transfer certification services to another secure, fair and objective CA.

If services normally expire, or if contract is terminated, or if company is reorganized, and no security concerns are present:

- Subscribers shall be notified three months in advance by letter or other formal document that CA will terminates system operation for some cause.
- Following discussion and negotiation with TaiCA PKI Subscribers, terminated certification , services shall be transferred to a successor CA for continued operation.
- Private Keys of the CA to revoke and terminate operations shall be transferred to the successor CA in a highly secure and uncompromised operating environment.
- Subscriber Certificates and CRLs of the directory services to be terminated shall be transferred to the successor CA in a highly secure operating environment.
- Relevant Private Keys shall be completely deleted, and a formal announcement made to Subscribers that certification services have been transferred to a successor CA for continued operation. Successor CA shall be rendered all possible assistance in implementing PKI Certificate issuance tasks.
- All Certificate service transaction records, audit logs, relevant documents and data preserved by terminated CA shall be transferred to successor CA, in any case be preserved no less than 7 yeas.

After conclusion of service abnormality (court declaration of bankruptcy or illegality)
Apart from notifying Subscribers three months in advance by letter or other formal document (CA must still notify Subscribers as soon as possible), CA must also implement the same operating procedures as in the case of normal termination of services, and must reduce impact on Subscriber service system operation to a minimum.

Hong Kong China:

4.9 CA Termination

In the event that HKPost ceases to operate as a CA, notification to the Director of Information Technology Services and public announcement will be made in accordance with the procedures set out in the HKPost termination plan. Upon termination of service, HKPost will properly archive the CA records including certificates issued, root certi1icates, Certification Practice Statements and Certificate Revocation Lists for a period of7 years after the date of service termination.

Thailand:

4.9 CA Termination

In the event that it is necessary to terminate operation of ACERTs CA, ACERTs CA will undertake the following steps to minimise the impact of the termination as much as possible in light of the prevailing circumstances:

(a) providing practicable and reasonable prior notice to all of ACERTs Subscribers to whom ACERTs CA has issued Certificates, and all affected RAs;
(b) assisting with the orderly transfer of service, and operational records, to a successor CA, if any; and
(c) preserving any records not transferred to a successor CA.

All Certificates issued by ACERTs CA will be revoked no later than the time of termination.
In cases where the termination of ACERTs CA is voluntary, and no successor CA is contemplated, no less than ninety (90) days' notice will be provided to all applicable ACERTs PCS Participants.

RFC3647-4.9.11 Individual notices and communications with participants

This subcomponent discusses the way in which one participant can or must communicate with another participant on a one-to-one basis in order for such communications to be legally effective. For example, an RA may wish to inform the CA that it wishes to terminate its agreement with the CA. This subcomponent is different from publication and repository functions, because unlike individual communications described in this subcomponent, publication and posting to a repository are for the purpose of communicating to a wide audience of recipients, i.e., all relying parties. This subcomponent may establish mechanisms for communication and indicate the contact information to be used to route such communications, such as digitally signed e-mail notices to a specified address, followed by a signed e-mail acknowledgement of receipt

Japan:

2.6.2. Frequency of publication

(1) The disclosure of this set of standards is set forth in Chapter 8.

(2) Revocation information will start to be disclosed on the JCSI in the CRL form within 24 hours of the revocation procedure.
(3) Revocation information will continue to be disclosed on the JCSI repository until the certificate expires.
(4) Other information will be updated and disclosed whenever appropriate, upon the JCSI's discretion.

Korea 1:

2.1.1.1 Providing and Notifying Accurate Information

KISA immediately notifies the ACAs and the relying parties of the information as below which can affect the trustworthiness or validity of a accredited certificate in order to help anybody confirming it under the accredited certification practice structure.

- Information on an ACA
  - ACA nomination
  - Suspension or revocation of an ACA certification practice
  - Cancellation of an ACA nomination
  - Transfer or merger of an ACA
- Information about accredited certificate
  - Accredited certificate
  - Accredited certificate suspension and revocation list
- Other certification practice related information

2.1.1.2 Provision of Information through Information and Communication Network

KISA shall publish the KISA's certificate, ACA's accredited certificate, and the accredited certificate suspension and revocation list through information and communication network so that ACA and relying parties can browse them anytime.

2.1.1.3 Measures on Vulnerability of Private Key

KISA revokes the KISA's certificate including public key in accord with private key and reissues the KISA's certificate by creating a new key pair when KISA recognizes that its private key is not secure. After renewal and issuance of an ACA's accredited certificate using a new private key, KISA immediately notifies the matters that everybody can identify and take measures to guarantee the safety and trustworthiness in the management under the accredited certification practice structure.

KISA, when informed of the loss and damage, theft, drain or vulnerability about the private key from an ACA, revokes the accredited certificate issued to the ACA and notifies the matters everybody can identify under the accredited certification practice structure. KISA, when being informed of loss and damage or theft, drain and vulnerability from the ACA of a governmental and municipal authority, immediately inform it to the Director of the National Intelligence Service.

2.1.1.4 Measures on Vulnerability of Digital Signature Algorithm

KISA, when recognizing that its digital signature algorithm is not secure, revokes the KISA's and ACA's accredited certificates issued by using its digital signature algorithm as well as immediately notifies the matters everybody can identify and takes measures to guarantee safety and

trustworthiness in the practice under the accredited certification practice structure.

KISA, when informed vulnerability about the digital signature algorithm from an ACA, revokes the accredited certificate issued to the ACA and notifies the matters everybody can identify under the accredited certification practice structure. KISA, when informed vulnerability about the digital signature algorithm from the ACA of a governmental and municipal authority, immediately informs it to the Director of the National Intelligence Service.

Korea 2:

5.1.1.1 Provision of accurate information and public announcement

a. KICA ensures that subscribers and users may verify the reliability and validity of certificates by announcing the following information promptly:

1) Information on KICA:

- Designation and cancellation as licensed certification authority.
- Recess, suspension, or revocation of certification services.
- Transfer, takeover, or merger of certification services.

2) Information concerning subscriber certificates:

- Subscriber certificates.
- Certificate Revocation List(CRL).

3) Certification Practice Statement of KICA.

4) Other information related to certification services.

5.1.1.2 Safekeeping of Private keys

KICA generates Key pair in a secure manner utilizing reliable software or hardware. KICA should securely manage the private key to prevent their loss, damage, theft, or leakage.

5.1.1.3 Measures to maintain security of Private keys

a. KICA informs KISA and a subscriber when KICA discovers any events that may affect reliability or validity of certificates, including loss, damage, theft, or leakage of Private key, or discovers any weaknesses in Key pair or in the algorithms, through communication networks immediately. And also, KICA may revoke subscriber certificates issued using the corresponding Private keys.

b. KICA generates new Private keys, has its Public key certified from KISA, and uses Private keys to re-issue subscriber certificates. KICA then notifies and distributes the corresponding facts through e-mail or communication networks.

c. Further, KICA publicly announces the corresponding facts so that anyone concerned can check them at any time through certification management systems, and can also take measures to secure the reliability and validity of its certification services.

Singapore:

8.2.1 All items in Netrust CP and this CPS are subject to the publication and notification requirement.

8.2.2 All publication and notification will be done via the Netrust web site at http://vvww.netrust.net

unless the notification has great impact to Netrust, Sponsor, ORA, Subscriber and Relying Party, e.g. termination of CA services.
8.2.3 Netrust may digitally sign each publication and notification before they are posted at the Netrust web site.
8.2.4 Netrust will, from time to time, suggest and make available to, publish or will notify the Subscriber of what may be constituted as adequate private key protection measures.
8.2.5 Netrust will make available to, publish or will notify the Subscriber of risks associated with the use of any Certificate, issued by Netrust to the Subscriber, based on any technologies used by Netrust which have been discontinued or superceded.
2.4.2.5 Any notice required or permitted to be given to Netrust shall be in writing and shall be sent to its registered office from time to time. Any such notice shall be delivered personally or sent in a letter by the recorded delivery service and shall be deemed to have been served if by personal delivery when delivered and if by recorded delivery 24 hours after receipt by Netrust. Any such notice may be sent to Netrust via electronic mail ("e-mail") and such notices shall only be deemed to be valid if such e-mail notices are confirmed in writing by the Subscriber to Netrust within 24 hours of the receipt of the e-mail notice by Netrust.

Chinese Taipei:

Hong Kong China:

Thailand:

RFC3647-4.9.12 Amendments
It will occasionally be necessary to amend a CP or CPS. Some of these changes will not materially reduce the assurance that a CP or its implementation provides, and will be judged by the policy administrator to have an insignificant effect on the acceptability of certificates. Such changes to a CP or CPS need not require a change in the CP OID or the CPS pointer (URL). However, some changes to a specification will materially change the acceptability of certificates for specific purposes, and these changes may require corresponding changes to the CP OID or CPS pointer qualifier (URL).
This subcomponent may also contain the following information:
* The procedures by which the CP or CPS and/or other documents must, may be, or are amended. In the case of CP or CPS amendments, change procedures may include a notification mechanism to provide notice of proposed amendments to affected parties(such as subscribers and relying parties), a comment period; a mechanism by which comments are received, reviewed and incorporated into the document, and a mechanism by which amendments become final and effective.
* The circumstances under which amendments to the CP or CPS would require a change in CP OID or CPS pointer (URL).

Japan:
8. Specification administration
This chapter is designed to describe specification administration for the A-Sign public service

standards. The specification administration of standards in A-Sign private services will be prepared by the customer. The customer may refer to this chapter.
The JCSI will aggressively monitor the latest trends in security technology and, whenever necessary, reflect them in the form of redesigns in this set of standards in order to maintain security.
8.1. Policy for procedures for redesign
The JCSI will own the right to revise this set of standards without the prior consent of the customer or relying party.
The revision of this set of standards will be conducted after a revision draft is considered at the specification administration committee set up in the JCSI and its reasonability is confirmed.
(1) Minor changes will be made whenever necessary at the discretion of the specification administration committee.
(2) Important updates that need update certification must be considered at the specification administration committee. Update certification will then be obtained and this set of standards will then be revised.
8.2. Policy for publication and notification
This set of standards is revised by disclosing the revised version of standards or disclosing a change notice (excerpts of only the revised portion of this set of standards) in the notice in this company's repository. This change notice will have the same effect as an actual change in this set of standards and will be reflected on the disclosure of the next version of this set of standards. Changes and revisions of this set of standards will be identified by version number and issue date representing the revision history.
Change notices will be made by disclosing a change notice or a revised version of this set of standards. The date when a redesign will become effective will vary according to the importance and urgency of the contents to be changed. The JCSI will make decisions about the importance and urgency of the change according to the Digital Signature Law as follows:
(1) Important updates will become effective within 15 days (a notification time) after the notice. Customers and relying parties will visit this company's repository regularly and must understand the additions and changes in the A-Sign service specifications. During the notice period, the JCSI may post up a notice in this company's repository to that effect, thus aborting the change.
(2) Urgent important changes will become effective immediately after a notice is posted. Here, "urgent" means that a part or a whole of A-Sign services may become compromised unless the particular change is made immediately.
(3) Non-important changes will become effective immediately after a notice is given.
8.3. Procedure for specification certification
If this set of standards is revised, the revised version of this set of standards indicated in this company's repository will be applied regardless of the date of issuance of the subscriber certificate.
The customer will be construed as having consented to a specific change made by the JCSI unless they apply for revocation of the certificate. If a relying party cannot consent to this change, they will abort using the certificate obtained.
8.4. Preservation of this set of standards
The JCSI will preserve each version of this set of standards and its revision history while the authentication project is certified.

Korea 1:

8. Accredited Certification Practice Statement Administration

8.1 Revision Procedure

When the Minister of Information and Communication orders an alteration of the Accredited Certification Practice Statement, KISA revises the rule.
When the Director of KISA decides an alteration of the Accredited Certification Practice Statement, KISA revises the rule.

KISA maintains the revision-related record of the Accredited Certification Practice Statement including the belows:

- Version of the Accredited Certification Practice Statement
- Overview of the applied practice and range
- Revision record of the Accredited Certification Practice Statement
  - Previous provisions of the Accredited Certification Practice Statement
  - Revised contents
  - Reason of the revision

8.2 Enforcement Procedure

KISA reports the established and revised Accredited Certification Practice Statement to the Minister of Information and Communication.

When newly instituting or amending the Certified Certification Practice Statement, KISA shall officially notify individually all ACAs and all other parties concerned as per Section 1.4.2 'Certificate Practice Related Information' of the Accredited Certification Practice Statement.

The established and revised Accredited Certification Practice Statement is in force since the day of report.

Korea 2:

10.1 Management of Certification Practice Statement

10.1.1 Formulation and Revision of Certification Practice Statement
When formulating or revising this Certification Practice Statement or the Rules, KICA reports to the Minister of Information & Communications of the fact, pursuant to Article 6 Clause 1 of the Electronic signature Act.

10.1.2 Reasons for Revision of Certification Practice Statement
a. When the Minister of Information & Communications orders a revision, pursuant to Article 6 Clause 2 of the Electronic signature Act.

b. When the President of KICA deems it necessary to revise the Rules.

10.1.3 Maintenance of Records Related to Revision of Certification Practice Statement
Whenever these Rules are revised, KICA should maintain records containing the following:

a. Version of rules.
b. Scope of application and outline.
c. Records related to revision.
① Existing provisions before revision.
② Particulars of revision.
③ Reasons for revision, etc.

Singapore:

8.1 Specification Change Procedure

8.1.1 Prior to making any changes in Netrust CP and this CPS, Netrust will document the list of proposed changes. The list will be circulated to ORA, CA whom Netrust has directly cross-certified with, and the Controller of Certificate Authority of Singapore, for comments. The comment period will be thirty days unless otherwise specified.

8.1.2 All comments wild be consolidated and reviewed by Netrust management. The decision to implement the proposed changes are at the sole discretion of Netrust, or subject to regulatory government body approval, where appropriate. A decision for the final change will be announced within two weeks.

8.1.3 Netrust will adhere to its change management control procedures such that all changes made to the CP and CPS are tracked and version controls are in place.

Chinese Taipei

8.1 Specification Change Procedure

The authorized Specification Administration Organization in this CPS is the TaiCA PAA. The TaiCA PAA must review these operating specifications at least once per year to insure security specifications comply with international standards. Operating specifications may be revised and rekeyed at any time in response to modification of Certificate operation management system platform or functions, to comply with service system needs, to comply with service needs and international standards, to remedy errors, or in accordance with Subscribers' suggestions.

If it is recommended that these operating specifications be rekeyed, detailed relevant documents must be sent by e-mail or postal delivery to Contact Person specified in section 1.4, and must undergo TaiCA PAA review.

8.2 Publication and Notification Policies

After TaiCA PAA has reviewed and approved CPS specifications or updated version specifications, the new version must be published on the CA Certificate management system website at least one month before it is to take effect. Subscribers must be notified to obtain a new version from the CA website.

8.3 CPS Approval Procedures

The TaiCA PAA is the approving organization for these CPS specifications. After the government has enacted the Electronic Signature Act, and the authorized Specification Administration Organization (MOEA) has drafted CA and CPS management regulations, the CPS must be reviewed and approved by the Specification Administration Organization.

Hong Kong China:

8. CPS ADMINISTRATION

All changes to this CPS must be approved and published by HKPost. The CPS changes will be effective upon publication by HKPost in the HKPost CA web site at hilp://www.hongkongpost.gov.hk or in the HKPost repository and are binding on all applicants for new certificates and upon all holders of existing certificates as those certificates are renewed. HKPost will notify the Director of Information Technology Services any subsequent changes to this CPS as soon as practicable. A copy of this CPS and its predecessors are available for viewing by Subscribers and Relying Parties on the HKPost CA web site at http://www.hongkongpost.gov.hk or in the HKPost repository. Paper copies of this CPS are also available for viewing by Subscribers and Relying Parties at any of Post Offices.

Thailand:

8.1 CPS Change Procedures

All ACERTs PCS Participants understand and agree that the CPS may require modifications from time-to-time, and that ACERTs has the authority to modify this CPS. Any suggestions as to modifications should be communicated to the Contact Persons listed in Section 1.4.2 of this CPS.

8.1.1 Items that can Change Without Notification

Changes to this CPS which, in the judgement of ACERTs, will have no or only a minimal effect on Certificate or CRL use or management, may be made without requiring the issuance of a new version of the CPS and without notification to ACERTs PCS Participants. Examples of these types of changes include typographical corrections and changes to contact information.

8.1.2 Changes with Notification

Changes which, in the judgement of ACERTs may have a significant impact on Certificate or CRL use or management will be made only with prior notice to ACERTs PCS Participants. In such event, a new version of the CPS will be published and made available to current ACERTs PCS Participants. The new version will supersede all previous versions and is binding on all ACERTs PCS Participants.

8.2 Publication and Notification Policies

Prior to significant changes, as set forth in Section 8.1.2, to this CPS, notification of such changes will be posted on ACERTs web site http://www.ACERTs.net.

Upon publication of this information, ACERTs Subscriber may revoke their Certificate(s) within fifteen (15) days without obligating ACERTs Subscriber to the terms of the new version of the CPS. An ACERTs Subscriber’s decision not to revoke its Certificate(s) within the fifteen (15) days following the first posting of the new version of the CPS on the web site, constitutes acceptance of the terms of the new CPS.

8.2.1 Access Controls

8.2.1.1 External Access Control

ACERTs CPS is available to all Applicants, Subscribers and Relying Parties for reading only.

8.2.1.2 Internal Access Control

Only ACERTs Corporate Security Officer may authorise replacement or removal of this CPS from ACERTs Internet site or Intranet.

RFC3647-4.9.13 Dispute Resolution Procedures

This subcomponent discusses procedures for resolving disputes arising out of the CP, CPS, and/or agreements. Examples of such procedures include requirements that disputes be resolved in a certain forum or by alternative dispute resolution mechanisms

RFC3647-4.9.14 Governing Law

This subcomponent sets forth a statement that the law of a certain jurisdiction governs the interpretation and enforcement of the subject CP or CPS or agreements.

RFC3647-4.9.15 Compliance with Applicable Law

This subcomponent relates to stated requirements that participants comply with applicable law, for example laws relating to cryptographic hardware and software that may be subject to the export control laws of a given jurisdiction. The CP or CPS could purport to impose such requirements or may require that such provisions appear in other agreements.

RFC3647-4.9.16 Miscellaneous Provisions

This subcomponent contains miscellaneous provisions sometimes called "boilerplate provisions" in contracts. The clauses covered in this subcomponent may appear in a CP, CPS, or agreements and include:

(1) An entire agreement clause, which typically identifies the document or documents comprising the entire agreement between the parties and states that such agreements supersede all prior and contemporaneous written or oral understandings relating to the same subject matter;

(2) An assignment clause, which may act to limit the ability of a party to an agreement to assign its rights under the agreement to another party (such as the right to receive a stream of payments in the future) or the ability of a party to delegate its obligations under the agreement;

(3) A severability clause, which sets forth the intentions of the parties in the event a court or other tribunal determines that a clause within an agreement is, for some reason, invalid or unenforceable, and whose purpose is frequently to prevent the unenforceability of one clause from causing the whole agreement to be unenforceable; and

(4) An enforcement clause, which may state that a party prevailing in any dispute arising out of an agreement is entitled to attorneys' fees as part of its recovery, or may state that a party's waiver of one breach of contract does not constitute a continuing waiver or a future waiver of other breaches of contract.

(5) A force majeure clause, commonly used to excuse the performance of one or more parties to an agreement due to an event outside the reasonable control of the affected party or parties. Typically, the duration of the excused performance is commensurate with the duration of the delay caused by the event. The clause may also provide for the termination of the agreement under specified circumstances and conditions. Events considered to constitute a "force majeure" may include so-called "Acts of God," wars, terrorism, strikes, natural disasters, failures of suppliers or vendors to perform, or failures of the Internet or other infrastructure. Force majeure clauses should be drafted so as to be consistent with other portions of the framework and applicable service level agreements. For instance, responsibilities and capabilities for business continuity and disaster recovery may place some events within the reasonable control of the parties, such as an obligation to maintain backup electrical power in the face of power outages.

Japan:

2.4. Interpretation and execution

2.4.1. Governing laws

This Certificate Practice Statement (CPS) must be interpreted according to the domestic laws and rules of Japan.

2.4.2. Severability, survival, merger, and notice:

If A-Sign public services are to be segmented, to integrate another service, or to be integrated into another service, the JCSI will do its utmost to continue A-Sign public services in real terms. If the above necessitates a change in the standards in this CPS, the change will be managed according to the provisions of Chapter 8 of this set of standards.

2.4.3. Dispute resolution procedures

If a lawsuit or legal act occurs between a customer, subscriber or relying party on the one hand and the JCSI on the other, the Tokyo District Court will be an exclusive agreed jurisdictional court. All matters not covered in this document or the agreement and all discrepancies in the interpretation of any of those documents must be discussed and settled in good faith by the two parties.

Korea 1:

2.3.1 Applicable Law

The Accredited Certification Practice Statement is interpreted and applied under the Electronic Signature Act and relevant regulations.

2.3.2 Competent Court

Seoul District Court is the competent court to mediate a dispute relating to certification practices between KISA and an ACA or a relying party.

2.3.3 Dispute Resolution

Minister of Information and Communication can order a corrective action at the same time with guiding them to mutual consent by suggesting a mediation plan through requesting related materials to KISA and to an ACA and investigating the observance of the Electronic Signature Act and the Accredited Certification Practice Statement.

Korea 2：

10.2.1 Applicable Laws

This Certification Practice Statement will be interpreted and applied pursuant to the Electronic Signature Act and related laws of the Republic of Korea.

10.2.2 Jurisdiction of Litigation Court

All litigation concerning certification services between KICA and subscriber or user relying on a certificate shall be referred to the Seoul District Court.

10.2.3 Mediation of Disputes

a. Should there arise a dispute between subscriber and user relying on a certificate, KICA may present a plan for mediation or recommend an agreement by requesting the related parties to present relevant material and investigating their compliance with the Electronic Signature Act and Certification Practice Statement.

b. Should there arise a dispute between KICA and its subscriber or user relying on a certificate, KICA may request The Korea Information Security Authority (KISA) to mediate the dispute. KISA may present a plan for mediation or recommend corrective measures by requesting related parties to present relevant material and investigating their compliance with the Electronic Signature Act and Certification Practice Statement.

Singapore

2.4 Interpretation and Enforcement

In the event of any conflict or inconsistencies between this CPS and other rules, guidelines or contracts, the provisions herein this CPS shall prevail over such other rules, guidelines or contracts, except as to other contracts either (i) predating the first public release of the CPS; or (ii) expressly superseding this CPS for which such contract shall govern as to the parties thereto and except to the extent that the provisions of this CPS are prohibited by law.

2.4.1 Governing Law

2.4.1.1 This CPS shall be governed by and construed in all respects in accordance with the laws of the Republic of Singapore.

2.4.2 Severability, Survival, Merger, Notice

2.4.2.1 In the event that any or any part of the terms, conditions or provisions contained in this CPS are determined invalid, unlawful or unenforceable to any extent such term, condition or provision shall be severed from the remaining terms, conditions and provisions which shall continue to be valid and enforceable to the fullest extent permitted by the Governing Law.

2.4.2.2 This CPS shall supersede any and all previous negotiations, agreements, memoranda and commitments in relation to the subject matter. Netrust shall be entitled to amend, modify and change any of the terms, conditions or provisions herein contained at any time and without prior notice to any parties. Netrust sham be entitled to place and/or publish amendments in the Netrust repository either (i) in the form of an amended version of the CPS; (ii) in the Netrust website at http://www.netrust.net; (iii) in such other manner as may be determined by Netrust. All amendments, modification and changes sham, unless otherwise expressly stated in such amendments, modification and changes be effective immediately upon placement and/or publication. The subscriber's decision not to request revocation of his Certificate within fifteen (15) days following such placement and/or publication shall constitute agreement to the amendments, modification and changes.

2.4.2.3 Netrust's failure or forbearance to enforce any right or claim against any party arising hereunder shall not be deemed to be a waiver by Netrust to such right or claim. Any of Netrust's waiver of a breach of any provision of this CPS shall not operate or be construed as a waiver of any subsequent breach or breaches of the same or any other provision.

2.4.2.4 Any notice required or permitted to be given to a Subscriber shall be in writing and shall in the case of a recipient being (i) a company be sent to its registered office from time to time; (ii) an individual be sent to its address as set out in its application. Any such notice shall be delivered personally or sent in a letter by the recorded delivery service and shall be deemed to have been served if by personal delivery when delivered and if by recorded delivery 48 hours after posting. lf Netrust so elects, Netrust shall be entitled to send any such notice to the Subscriber via electronic mail("e-mail") to the e-mail address designated by the Subscriber at the time of application for the Certificate.

2.4.2.5 Any notice required or permitted to be given to Netrust shall be in writing and shall be sent to its registered office from time to time. Any such notice shall be delivered personally or sent in a

letter by the recorded delivery service and shall be deemed to have been served if by personal delivery when delivered and if by recorded delivery 24 hours after receipt by Netrust. Any such notice may be sent to Netrust via electronic mail ("e-mail") and such notices shall only be deemed to be valid if such e-mail notices are confirmed in writing by the Subscriber to Netrust within 24 hours of the receipt of the e-mail notice by Netrust.

2.4.2.6 Each of the Certificate and all the terms and provisions of this CPS are personal to each of the Subscriber and the Subscriber shall not assign their Certificate to any other parties.

2.4.2.7 The headings contained in this CPS are inserted for convenience of reference only and are not intended to be part of or to affect the meaning or interpretation of any of the terms, conditions or provisions of this CPS.

2.4.2.8 Export of certain software used in conjunction with Netrust's PCS may require the approval of appropriate Netrust and/or government authorities. Au parties shall conform to applicable export laws and regulations as may or may not have been advised by Netrust.

2.4.3 Dispute Resolution Procedures

2.4.3.1 All questions or differences whatsoever which may at any time hereafter arise hereto touching or concerning the CPS or its construction or effect or as to the rights, duties or liabilities of the parties hereunder under or by virtue of this CPS or otherwise as to any other matter connected with or arising out of or in relation to the subject matter of this CPS shall if such questions disputes or differences cannot be amicably resolved by the parties, be referred to arbitration in Singapore in accordance with the Arbitration Rules of the Singapore International Arbitration Centre ("SIAC Rules") for the time being in force which rules are deemed to be incorporated by reference into this CPS. The arbitrators' decision shall be final and binding upon the parties and shall provide the sole and exclusive remedies of the parties. All arbitration proceedings shall be in the English language and judgment upon the award so rendered may be entered in any court having jurisdiction or application may be made to such court for a judicial acceptance of the award or orders of enforcement.

Chinese Taipei:

2.4 Interpretation and Enforcement

2.4.1 Governing Law

This CPS is governed by the laws in force in Taiwan, ROC, and is subordinate to and controlled by the relevant legal regulations of the ROC. For instance, it is managed and overseen by the relevant legal regulations of the Commerce Department, MOEA, and Ministry of Finance. If the need arises for international or inter-regional service integration, apart from accommodating service integration needs, this CPS shall continue to take the laws of the ROC as its governing law.

2.4.2 Severability of Provisions, Survival, Merger and Notice

If certain terms in this CPS are found to be invalid and must be revised, the requirements of other terms shall continue to be valid, and shall not be affected by the invalid regulations. Until the time that a new version has been modified and published for use, the modifying of the invalid portion shall be performed in accordance with the regulations of item 1.4 of this CPS.

When the relationship between Subscriber and Relying Party expires or ceases because of other factors, relevant Subscriber rights and obligations in this CPS and relevant service CPs shall continue to have force, and shall not lose force due to the end of the above relationship. (For instance, a bank subscriber who uses certificates in an online banking transfer system may cancel his relationship with the bank after the transaction has been completed. In that case the relevant rights

and obligations of the subscriber and bank shall continue to be valid, and do not lose force due to the end of the relationship.)

In accordance with the specifications of this CPS and relevant service CPs, transmission of information and notification between CA and Subscribers or RA may be performed by the following means:

1. Electronic transmission The transmitting party shall transmit the information after signing it using the Certificate issued under this CPS and relevant service CP. After receiving the information, the recipient shall complete signature authentication.
2. Printed documents -The documents or forms must possess the names and contact addresses of operating personnel of the transmitting and receiving parties. Items sent by ordinary post must be mailed at least three days before they are expected to arrive (or at least one week in advance in the case of overseas airmail). When information is sent by fax, apart from contact information for the transmitting and receiving parties, the item must possess a fax machine identification number Whether service-related personnel at the transmitting party must personally sign the item shall be determined by the importance of the information, and is not specified in this CPS.

2.4.3 Dispute Resolution Procedures

The dispute resolution provisions described in this section, including dispute arbitration processes and procedures for resolving disputes arising from Public Key Certificate or Private Key problems, are the default provisions to be applied in all circumstances. In the case of service-related problems, please refer to service-related contracts and specifications.

Both parties in a dispute should do their utmost to negotiate a reasonable resolution in the spirit of good faith.

If the two parties cannot negotiate a reso1ution to the dispute within 14 days, they must agree to joint negotiations and must appoint a fair and competent third party arbitrator to arbitrate and resolve the dispute. In addition, the two parties must consent to the arbitrator's negotiation reasonable resolution within one month, the dispute shall be submitted to the Taipel District Court as a suit.

If a dispute arises between Subscribers and RA or CA, the Subscribers and RA or Subscribers and CA must attempt to negotiate a resolution in the spirit of good faith. If a lawsuit is initiated, the two parties agree to take Taipei District Court as the court of first instance. If a dispute arises between RA and CA, the two parties must attempt to negotiate a resolution in the spirit of good faith. If a lawsuit is initiated, the two parties agree to take Taipel District Court as the court of first instance. The sharing of costs that arise due to the resolution of the suit shall be handled on the basis of negotiations or relevant legal requirements. In the case of an international or inter-regional dispute, if the dispute cannot be resolved by the above means, it must be handled in accordance with arbitration regulations for relevant international or inter-regional disputes.

Hong Kong China:

2.3 Interpretation and Enforcement (Governing Law)

2.3.1 Governing Law

The laws of Hong Kong SAR govern this CPS. Subscribers and Relying Parties agree to submit to the non-exclusive jurisdiction of the Courts of Hong Kong SAR.

2.3.2 Severability, Survival, Merger, and Notice

If any provision of this CPS is declared or found to be illegal, unenforceable, or void, then any offending words in it will be deleted to the extent necessary to make it legal and enforceable while

preserving its intent me unenforceability of any provision of this CPS will not impair the enforceability of any other provision of this CPS.

2.3.3 Dispute Resolution Procedures

The decisions of HKPost pertaining to matters within the scope of this CPS are final. No alternative dispute resolution procedures regarding Subscriber or Relying Party disputes will be implemented by HKPost. Any claims should be submitted to HKPost at the fF11owing address:

Electronic Services Division
Hongkong Post
2 Connaught Place, Central
Hong Kong
Email: enquiry@hongkongpost.gov.hk

2.3.4 Interpretation

Where there is a conflict of interpretation of wording between the English and Chinese versions of this CPS, the English version shall prevail.

Thailand:

2.4 Interpretation and Enforcement

2.4.1 Governing Law

This CPS is governed by the applicable laws of Thailand.

2.4.2 Severability, Survival, Merger, Notice

This CPS, the applicable CP and all other applicable PKI Documents, as amended from time to time, constitute the entire statement with respect to the rights, obligations, and responsibilities of ACERTs PCS Participants.

If part of any provision in this CPS is held to be illegal, invalid, or unenforceable by a court or other decision making authority of competent jurisdiction, then the remainder of the provision shall be enforced so as to effect the intentions of ACERTs, and the validity and enforceability of all other provisions in the CPS shall not be affected or impaired. Waiver of any one default of any provisions herein by ACERTs shall not waive subsequent defaults of the same or different kind.

In the event of a conflict between the most current version of this CPS or any CP, and the respective version of such document that was in effect on the date of a Certificate issuance, the version in effect on the date of issuance prevails with regard to issuance of that Certificate and the most current version prevails with regards to the use, management, and revocation of that Certificate.

All notices and requests in connection with this CPS shall be deemed received as of the day they are actually received, when delivered either by messenger, nationally recognised delivery service, or first class Thailand mail, postage pre-paid, certified or registered, return receipt requested, and addressed to the Contact Persons set forth in Section 1.4.2, above.

The terms of this CPS may be modified from time to time by ACERTs, in accordance with Section 8.1 of this CPS.

2.4.3 Dispute Resolution Procedures

Upon the demand of any ACERTs PCS Participant, any Dispute with respect to ACERTs' compliance with the CPS, or with respect to ACERTs PCS operations and Certificates issued pursuant to the CPS and other applicable PKI documents, shall be resolved by binding arbitration in accordance with the terms of this Section 2.4.3. A "Dispute" shall mean any action, dispute, claim or controversy of any kind, whether in contract or tort, statutory or common law, legal or equitable, now existing or hereafter arising under or in connection with, or in any way pertaining to ACERTs

PCS. Any party may, by summary proceedings, bring an action in court to compel arbitration of a Dispute. Any party who fails or refuses to submit to arbitration following a lawful demand by any other party shall bear all costs and expenses incurred by such other party in compelling arbitration of any Dispute.

Arbitration proceedings shall be administered by the Consumer Protection Board ("CPB") or such other administrator as the parties shall mutually agree upon. Arbitration shall be conducted in accordance with the Consumer Protection Act and the Intellectual Property Act. If there is any inconsistency between the terms hereof and any such rules, the terms and procedures set forth herein shall prevail. All Disputes submitted to arbitration shall be resolved in accordance with the Consumer Protection Act and the Intellectual Property Act. The arbitration shall be conducted at a location in Thailand selected by the CPB or other administrator. All statutes of limitation applicable to any Dispute shall apply to any arbitration proceeding. All discovery activities shall be expressly limited to matters directly relevant to the Dispute being arbitrated.

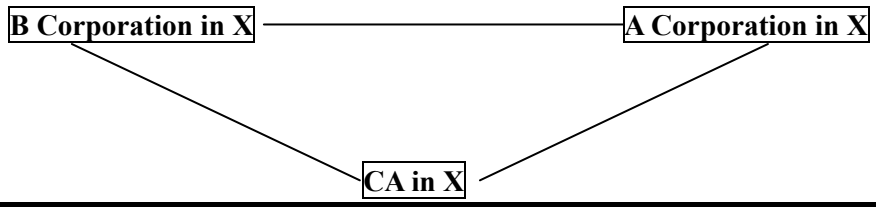
No provision hereof shall limit the right of any party to obtain provisional or ancillary remedies, including without limitation injunctive relief, attachment or the appointment of a receiver, from a court of competent jurisdiction before, after or during the pendant of the arbitration or other proceeding. The exercise of any such remedy shall not waive the right of any party to compel arbitration or reference hereunder.

The arbitrator(s) will have no authority to award damages in excess of those allowed by this CPS. Any award in an arbitration under this Section shall be limited to monetary damages and shall include no injunction or direction to any party other than the direction to pay a monetary amount.

To the maximum extent practicable, the CPB, the arbitrators and the parties shall take all action required to conclude any arbitration proceeding within 90 days of the filing of the Dispute with the CPB. No arbitrator or other party to an arbitration proceeding may disclose the existence, content or results thereof, except for disclosures of information by a party required in the ordinary course of its business, by applicable law or regulation, or to the extent necessary to exercise any judicial review rights set forth herein. This arbitration provision shall survive termination, amendment or expiration of the all PKI documents that are applicable to the dispute or any relationship between the parties. +

Request 2: (Domestic E-Commerce using PKI)

Suppose that there is a company called A Corporation in your country/area which we will call X. A Corporation would like to supply computer goods to B Corporation in X. Exchange of contracts and communications between those corporations are to be conducted using PKI. The both Corporations have agreed to use the CA in X in common.



Request 2-1: Authentication

1 Can the CA in X, a corporation duly incorporated in accordance with corporate laws in X, issue a certificate to the A corporation in X without permission or accreditation of the government in X? Is it required for a CA to obtain permission or accreditation in order to issue a certificate? What are the requirements to issue a certificate?

2. How long is the term or duration per electronic certificate?

China:

1.No. Corporations that wish to issue electronic certificates are required to receive accreditation of Chinese government. These corporations have to apply MII (Ministry of Information Industry) for CA service.

According to Article 17 of Electronic Signature Law of PRC, certification service providers should:(1) have professionals and management employees that can meet with certification service. (2)have the right place to supply service and enough money to support the service.(3)have relevant technology and equipment confirmed by the government. (4) with the government's permission to use passwords in their service. (5) other conditions ruled by laws and regulations.

2. Five years at most.

Japan:

1. Yes. Corporations that wish to issue electronic certificates are not required to receive accreditation by the Japanese government. Section 4.1 of the Japan's Electronic Signatures and Certification Services Act of 2000 provides that "A person seeking to perform or has been performing designated certification services may receive an accreditation from the related ministers."

While "certification service" means a service that, in compliance with either the request of a person who uses such service ("user") with regard to the electronic signature that they personally provide or the request of another person, certifies that an item used to confirm that the user performed an electronic signature belongs to the user. "Designated certification service" means a certification service that is performed with regard to those electronic signatures that conform to the standards prescribed by the ordinance of the related ministries as ones that, according to the method thereof, can only be substantially performed by that

person.(Sections 2.2 and 2.3 of Japan's Electronic Signatures and Certification Services Act of 2000.)

CA that has not received accreditation of the Japanese government can issue any kind of electronic certificates.

However, any CA that seeks for the accreditation is required to submit required documents and to meet with a number of provisions of The Implementation Regulation of Japan's Electronic Signatures and Certification Services Act of 2000.

For instance, the requirements of an "electronic certificate" to be issued by an "accredited certification service provider" are as follows in accordance with Sec. 6-4, 6-5, 6-6 of The Implementation Regulation of Japan's Electronic Signatures and Certification Services Act of 2000.

(1) The term of validity of electronic certificates shall not exceed five years.
(2) Electronic certificates should list the following particulars: (a) Name and issue number of issuer of concerned electronic certificate; (b) Date of issue and expiration date of term of validity of concerned electronic certificate; (c) Name of user of concerned electronic certificate; and (d) Identifiers of user signature verification codes of concerned electronic certificate and algorithms related to concerned user signature verification codes.
(3) Measures shall be taken to verify an issuer and to comply with the standards of Article 2 of The Implementation Regulation of Japan's Electronic Signatures and Certification Services Act of 2000 for the electronic certificates.

Advantages of accreditation from the Japanese government and obtaining an accredited certification service provider are as follows: (1) an accredited certification service provider may place a mark to the effect that its service has received accreditation on an electronic certificates; and (2) it will be presumed that the public key on issue is the original or authentic pubic key belonged to the registered person.

2. Five years at most. (Sec. 6-4 of The Implementation Regulation of Japan's Electronic Signatures and Certification Services Act of 2000).

Korea:

1. Yes. Corporations that wish to issue electronic certificates are not required to receive accreditation of Korean government. CA that has not received accreditation of the Korean government can issue any kind of electronic certificates.

However, CA that seeks for the accreditation is required to submit required documents and to meet with a number of provisions of Electronic Signature Act of 2001. CAs should follow the Art. 15 of the Electronic Signature Act in order to issue accredited certificates.

*** Article 15 (Issuance of accredited certificates, etc.)**

- An accredited certification authority issues an accredited certificate to those who desire to be issued an accredited certificate. In such event, the accredited certification authority shall verify the identification of the applicant.
- An accredited certificate issued by an accredited certification authority shall contain

each of the following:

1. The subscriber's name (legal name);
2. The subscriber's electronic signature verification data;
3. The type of electronic signature used by the subscriber and the accredited certification authority;
4. The serial number of the accredited certificate;
5. The effective period of the accredited certificate;
6. Data able to identify an accredited certification authority, such as the name of the accredited certification authority;
7. Matters relating to any limitation as to the scope of usage or uses of an accredited certificate;
8. Matters required when a subscriber acts on behalf of a third party or when a statement of occupational qualification is requested; and
9. Mark proving an accredited certificate.

- <Deleted>
- Upon the request of an applicant for an accredited certificate, the accredited certification authority may issue an accredited certificate restricting the scope of its usage or uses.
- The accredited certification authority shall determine an appropriate effective period for the accredited certificate, taking into account the scope of intended usage and uses and the integrity and reliability of the technology used.
- Other matters pertaining to the identification procedure and method required for issuing an accredited certificate shall be determined by the Decree of the Ministry of Information and Communication.

In addition, the entity that desires to be accredited as a certification authority should get accredited by the Ministry of Information and Communication following the Art. 4 of the Electronic Signature Act.

*** <u>Article 4 (Accreditation of certification authorities)</u>**

- The Ministry of Information and Communication may accredit an entity, deemed to be capable of carrying out accredited certification practice (hereinafter "certification practice") in a secure and reliable manner, such as an accredited certification authority.
- The entity that can be accredited as a certification authority shall be limited to central government agencies, local government agencies and legal persons.
- The entity that desires to be accredited as a certification authority must possess the technical and financial capabilities, facilities and equipment prescribed by Presidential Decree and satisfy other requirements therein.
- Licensing procedures and other necessary provisions shall be established by Presidential Decree.

2. It depends on the CA’s Certificate Policies and kinds of certificates. (Art. 15 of The Korea’s Electronic Signatures Act of 2001).

*** Article 15 (Issuance of accredited certificates, etc.)**

- The accredited certification authority shall determine an appropriate effective period for the accredited certificate, taking into account the scope of intended usage and uses and the integrity and reliability of the technology used.

Valid periods of Electronic Certificates are following;
- The Certificate of Root CA is valid within 10 years.
- The Certificate of CA is valid within 5 years.
- The Certificate of OCSP and TSP is valid within 3 years.
- The Certificate for personal users is valid within 1 years

Singapore:

1. The CA in Singapore, a corporation duly incorporated in accordance with corporate laws in Singapore, can issue a certificate to the A corporation in Singapore without permission or accreditation of Singapore government. It is not required for a CA to obtain permission or accreditation in order to issue a certificate. The digital signatures used will enjoy the presumptions given to secure electronic records and signatures under s18 provided that it constitutes a "commercially reasonable security procedure agreed to by the parties involved" which has been properly applied.

The requirements to issue a certificate are set out in s29

"Issue of certificate
29.
(1) A certification authority may issue a certificate to a prospective subscriber only after the certification authority —

(a) has received a request for issuance from the prospective subscriber; and

(b) has —

(i) if it has a certification practice statement, complied with all of the practices and procedures set forth in such certification practice statement including procedures regarding identification of the prospective subscriber; or

(ii) in the absence of a certification practice statement, complied with the conditions in subsection (2).

(2)In the absence of a certification practice statement, the certification authority shall confirm by itself or through an authorised agent that —
(a)the prospective subscriber is the person to be listed in the certificate to be issued;

(b)if the prospective subscriber is acting through one or more agents, the subscriber authorised the agent to have custody of the subscriber's private key and to request issuance of a certificate listing the corresponding public key;

(c)the information in the certificate to be issued is accurate;

(d)the prospective subscriber rightfully holds the private key corresponding to the public key to be listed in the certificate;

(e)the prospective subscriber holds a private key capable of creating a digital signature; and

(f)the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the prospective subscriber."

2. There is no maximum term or duration per electronic certificate set by law.

Chinese Taipei:

1. The Electronic Signature Act in Taiwan does not impose strict restrictions on entities intending to provide certification services. Only necessary requirements are set out to ensure the protection of consumers. CAs are free to set up business or offer services without prior authorization. However, there are some specific requirements for CAs that provide services to the public.

Prior to issuing certificates to the public, a CA shall file a certification practice statement to the competent authority for approval. In addition, after the approval, the CA shall publish the approved certification practice statement on its website for public reference. (Article 11 of the Electronic Signature Act)

There is no bright rule on the methods or procedures for authentication a CA shall adopt regarding the certification application in Taiwan. However, a CA is required to state the identification and authentication requirements and procedures for certificate applicants in the CPS as required under Article 18 of the Regulation on Required Information for Certification Practice Statement. And CAs shall scrutinize the authenticity of application forms in accordance with the CPSs.

Paragraph 1, Article 11 of the Electronic Signature Act in Taiwan:
Prior to providing services for issuing certificates to the public, a CA shall file the certification practice statement (CPS) stating its operational processes related to the practice or certification services of the CA to the competent authority for approval. After the approval, the CA shall publish the approved CPS on its Internet website to the general public for reference. The preceding rule shall also apply in the event that there is any modification in the CPS.

2. For information regarding the cost of a Public Key Certificate for Digital Signature, or the duration of a Certificate, please refer to a specific CA that provides corresponding certificate service.

Request 2-2: Negligence in authentication→CA's Liability

The CA in X did not conduct an authentication on B Corporation with reasonable care.
In this case, "P Corporation" impersonated the B Corporation.
Due to this spoofing (impersonation), the CA issued a Certificate to the "P Corporation " that was impersonating B Corporation.
Relying on the certificate issued to "B Corporation", the A Corporation supplied computer goods to "B Corporation".
However, "B Corporation" (actually P Corporation) never paid the price for the computer goods and disappeared. B Corporation negated the contract formation between A Corporation and B Corporation.
The A Corporation in X would like to file a suit before a court in X seeking damage against the CA in X.

1 What types of liabilities will the CA in X bear? What will the requirements for the A Corporation be to win the case against the CA in X? Will the CA bear strict liability?
2 Will P Corporation be penalized?
3 (1) Suppose there is an escape clause in CPS of the CA in X that "The CA does not assume any liability over 2,000 US dollars." The A Corporation suffered damages of 200,000 US dollars. Is such escape clause valid? Can the A Corporation win the 200,000 US dollars?
(2) Suppose there is an escape clause in CPS of the CA in X that "The CA does not assume any liability in any event." Is this indemnification clause valid? Can the A Corporation win the case?
4 Suppose there is a statute of limitation clause in CPS of the CA in X that "The party shall claim to the CA within one year after the event occurred." Can A Corporation file a suit before a court in X against the CA in X beyond the one year limitation after suffering damages?
5 Is there any difference with respect to the scope and degree of liability of CA in X if its CPS provides that (1) CA shall conduct authentication with scrutiny; or (2) CA does not need to conduct authentication with reasonable care?
6 Can A Corporation win the case against B Corporation if B Corporation was negligent in retaining B Corporation's Private Key?

China:

1. This is a case of inadequate personal identification.
   (1) Principle: Tort Liability

In cases where CA issues an electronic certificate without carrying out adequate personal identification, if another party (A Corporation) receives and trusts the certificate but suffers damage, the CA bears tort liability to the recipient (A Corporation) of the certificate, if CA can not proof that it was no fault. In this case, the recipient (A Corporation) bears the burden of proof as to the negligence (inadequate personal identification) of the CA.

   (2) Exception: Contract Liability

Since there is usually no contractual relationship between the CA and the recipient (A Corporation),

the CA, in principle, bears no contractual liability.
However, in cases where a third party (A Corporation) receives the certificate, if the CA shows its CPS and the recipient (A Corporation) acknowledges it, a contractual relationship might be recognized between them. If a contractual relationship is recognized, the CA is obliged to abide by the CPS. If it does not follow the personal identification procedure prescribed in the CPS, it will have to bear contractual liability for the failure to meet with this obligation. In this case, the CA bears the burden of proof as to the absence of fault on its side.

(3) CA does not bear strict liability.

In this case, as the both A and B Corporations have agreed to use the CA in X in common, it is highly expected that the Corporation has received a electronic certificate from the CA. If so, the A Corporation can seek its damage in accordance with contractual liability against the CA.

2.P Corporation will be penalized. According to Article 20 of the Electronic Signature Law of PRC, corporations who apply for CA certification should supply true, full and trustable personal information.

3(1)Its validity has to be discussed.
In cases where no contractual relationship is recognized between the recipient (A Corporation) and the CA, the parties concerned are not bound by the clause at all. A Corporation can seek for its damage against the CA in accordance with the Tort Law. But the escape clause could reduce the scope of the liability,
In cases where a contractual relationship is recognized between the recipient (A Corporation) and the CA, the parties concerned are bound, in principle, by the clause. However, the surrounding conditions are also important, they will impact the validity of the escape clause.

I this case, a contractual relationship is recognized between the A Corporation and the CA. Therefore, a corporation can seek for its damage against the CA if it can proof that CA made mistake in it's service.

3(2) Same as the above-mentioned answer.

4 No. In accordance with the statute of limitation provisions in the Chinese Civil Code, the statute of limitation for contractual liability claim between businesses is 2 years and that for tort liability is 2 years, too. However, in case for business-business transactions, an agreement to shorten the limitation period is valid.

5 It is said that CA cannot make any rules in its CPS and that CA shall meet with the security standards required by the society. Accordingly, the degree of reasonable care will not be low although the CPS provides "the CA does not need to conduct authentication with reasonable care."

6 A Corporation can seek for B Corporation's tort liability because B Corporation was negligent in retaining B Corporation's Private Key.

Japan:

2. This is a case of inadequate personal identification.

(1) Principle: Tort Liability

In cases where CA issues an electronic certificate without carrying out adequate personal identification, if another party (A Corporation) receives and trusts the certificate but suffers damage because the effects of his transaction with the spoofer do not belong to the principal (B Corporation--the name of the electronic signature), the CA bears tort liability to the recipient (A Corporation) of the certificate. In this case, the recipient (A Corporation) bears the burden of proof as to the negligence (inadequate personal identification) of the CA.

(2) Exception: Contract Liability

Since there is usually no contractual relationship between the CA and the recipient (A Corporation), the CA, in principle, bears no contractual liability.

However, in cases where a third party (A Corporation) receives the certificate, if the CA shows its CPS and the recipient (A Corporation) acknowledges it, a contractual relationship might be recognized between them. If a contractual relationship is recognized, the CA is obliged to abide by the CPS. If it does not follow the personal identification procedure prescribed in the CPS, it will have to bear contractual liability for the failure to meet with this obligation. In this case, the CA bears the burden of proof as to the absence of fault on its side.

(3) CA does not bear strict liability.

In this case, as the both A and B Corporations have agreed to use the CA in X in common, it is highly likely that the A Corporation has received a electronic certificate from the CA in X and its CPS. If so, the A Corporation can seek its damage in accordance with contractual liability against the CA.

2 P Corporation will be penalized. Sec.41 of Japan's Electronic Signature and Certification Service Act provides that: "a person who makes a false application before an accredited certification service provider or accredited foreign certification service provider in connection with its accredited certification service and thereby causes an untrue certification shall be punished with penal servitude for not more than three years or a fine of not more than two million yen."

3(1)

There are cases where a CA limits the amount of its liability for compensation in its CPS (escape clause) and its validity has to be discussed.

(1) Cases where no contractual relationship is recognized between the recipient (A Corporation) and the CA:

The parties concerned are not bound by the clause at all. A Corporation can seek damages against the CA in accordance with the Japanese Tort Law.

However, as it should be noted that the escape clause might have an impact to reduce the scope of the liability, the escape clause is not meaningless even in tort cases.

(2) Cases where a contractual relationship is recognized between the recipient (A Corporation) and the CA:

The parties concerned are bound, in principle, by the clause.

However, in consumer contracts, for example, the escape clause of the CA will be judged invalid if it totally exempts or partly exempts the CA (on condition that there is no knowledge or gross negligence on the part of the CA) from the liability to compensate for

damage resulting from the non-performance of an obligation or from a tort committed during the performance of an obligation (Article 8 of the Consumer Contract Act). There will be other cases where the validity of the escape clause is called into question when considering the surrounding conditions.

In this case, a contractual relationship is recognized between the A Corporation and the CA. In addition, Japan's Consumer Protection Act does not apply to this case because this case is not a case between a business and a consumer. Therefore, A Corporation is bound by the clause. A Corporation cannot seek damages against the CA.

3(2) Same as the above-mentioned answer.

4 No. In accordance with the statute of limitation provisions in the Japanese Civil Code, the statute of limitation for contractual liability claim between businesses is 5 years and that for tort liability is 3 years. However, in case for business-business transactions, an agreement to shorten the limitation period is valid.

5 It is said that CA cannot make any rules in its CPS and that CA shall meet with the security standards required by the society. Accordingly, the degree of reasonable care will not be low although the CPS provides "the CA does not need to conduct authentication with reasonable care."

6 A Corporation can seek for B Corporation's tort liability because B Corporation was negligent in retaining B Corporation's Private Key.

Korea:

1. This is a case of inadequate personal identification.

The liabilities of an accredited certification authority are divided into the contract liability and the tort liability. Contract liability refers to the liability for damages claimed in case the contract entered into by the parties to the contract was not fulfilled, whereas the tort liability refers to the liability for damages claimed by a third party, who sustained the damages, against the person who caused the damages in case the former has no legal relationship with the latter.

Article 26 of the Electronic Signature Act of Korea preferentially applies to the damages resulting in relation to the accredited certification practices of a certification authority.

*** Article 26 (Liability for damages)**

The accredited certification authority shall be liable for damages incurred by a subscriber or any user relying on an accredited certificate in connection with the performance of certification services. If, however, such damages resulted from a force majeure event, the liability shall be reduced, and if the accredited certification authority is proven not liable for such damages, the liability shall be exempted.

Therefore, if the CA cannot prove that its own personal identification was without any negligence, Corporation A can be indemnified for damages. In this case, the burden of proof

rests with the CA in accordance with Article 26 of the Electronic Signature Act. The injured party, A, may only prove his/her damages.

On the other hand, if the CA was not negligent in the process of personal identification, but the simulation of Corporation P was elaborate, the injured party, A, may hold Corporation P liable for its unlawful act.

CA does not bear strict liability.

In case the CA is proven faultless in accordance with Article 26 of the Electronic Signature Act, the liability shall be exempted, and in case of force majeure, the liability shall be reduced.

2. P Corporation will be penalized. The Art. 31 of Electronic Signature Act provides that: "Any person who falls under any of the following Subparagraphs herein shall be subject to imprisonment of up to 3 years or fines of up to thirty million (30,000,000) won: 3. One who has been issued an accredited certificate in the name of another person or aids…."

3.(1) It is valid in principle. In case the CA specified the limits of damages for different types of certificates by means of a CPS or agreement, as it is a schedule of damages, the CA shall, in principle, be liable for the damages within the limits.
However, as CA's bear, in some cases, tort liability for damages to users of certificates without a contractual relationship, the CA of Korea shall purchase a certification service insurance policy in provision for liabilities for damages. Therefore, the insurance company shall indemnify for damages.
In this case, however, according to the provision pertaining to liability for damages in Article 26 of the Electronic Signature Act of Korea, there is no limit to the damages the CA will be liable for. So the CA shall be liable for the entire amount of the damages, and the Court shall determine whether there was any negligence involved.

3.(2) The escape clause is invalid. According to the 'Act on Restriction of Agreements' of Korea, agreements with provisions excluding the legal liabilities resulting from intention or grave negligence of the employers, servants or employees, or provisions limiting the employer's liabilities for damages or transferring the risks, which must be borne by the employer, to customers without any good reasons shall be invalid.(Article 7)
In this case, as the provision on liabilities for damages in Article 26 of 'the Electronic Signature Act' of Korea stipulates that the CA should make reparation for damages in case a subscriber or a user who trusted certificates (Corporation A) incurred damages in relation to performance of certification services, Corporation A will win the lawsuit against the CA.

4. Yes. In accordance with the statute of limitation provisions in the Korean Civil Code, the statute of limitation for contractual liability claim(Article 162) is 10 years and that for tort liability(Article 766) is 3 years(from the day to know the event), and 10years(from the day to do the act).

5. Yes. The Electronic Signature Act of Korea stipulates that certification be performed strictly.

Compliance with (1) shall make the certificate valid. If (2) is stipulated, it may be effective as a private certificate in Korea pursuant to the agreement between the parties concerned.

6. Yes. Corporation A can seek for Corporation B's tort liability because Corporation B was negligent in retaining Corporation B's Private Key. As it is equivalent to causing damage to the other party as a result of its own negligence, it falls under Article 766 of the Civil Act of Korea. Therefore Corporation B must indemnify Corporation A for damages.

Singapore:

1 What types of liabilities will the CA in Singapore bear? What will the requirements for the A Corporation to win the case against the CA in Singapore ? Will the CA bear strict liability?

By issuing the certificate, the CA in Singapore represents to any person who reasonably relies on the certificate or a digital signature verifiable by the public key listed in the certificate (ie A Corporation) that the certification authority has issued the certificate in accordance with any applicable certification practice statement incorporated by reference in the certificate, or of which the relying person has notice.

Assuming that the CA in X has complied with all of the practices and procedures set forth in its certification practice statement including the procedures regarding identification of the prospective subscriber, the CA could still be liable for :

a) negligence, if A Corporation can show that the CA failed to exercise reasonable care notwithstanding its compliance with its practices, e.g. because it accepted a clearly forged document; or

b) misrepresentation, if A Corporation can show the facts represented in the digital certificate were false and it relied on the misrepresentation and CA cannot prove that it had reasonable ground to believe and did believe up to the time the contract was made that the facts represented were true .

CA will not be strictly liable.

2 Will P Corporation be penalized?

Yes, P Corporation can be liable for fraud.

It will also commit an offence under s26 of the ETA

> False or unauthorised request
> 26. Any person who knowingly misrepresents to a certification authority his identity or authorisation for the purpose of requesting for a certificate or for suspension or revocation of a certificate shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 6 months or to both.

3 (1)Suppose there is an escape clause in CPS of the CA in X that "The CA does not assume any liability over 2,000 US dollars." The A Corporation suffered the damage of 200,000 US dollars. Is such escape clause valid? Can the A Corporation win the 200,000 US dollars?

Yes, if the CA is licensed it can limit its liability to the amount specified in the certificate as its recommended reliance limit, i.e. US$2000.00.

If the CA is not licensed in Singapore, it can limit its liability only to the extent is it reasonable as the Unfair Contracts Terms Act will apply.

3(2)Suppose there is an escape clause in CPS of the CA in X that "The CA does not assume any liability in any event." Is this limitation of liability clause valid? Can the A Corporation win the case?

Section 45 of the ETA appears to provide the ability for a CA licensed in Singapore to specify a $0 reliance limit in its CPS.

> "Liability limits for licensed certification authorities
> 45. Unless a licensed certification authority waives the application of this section, a licensed certification authority -
>
> (a) shall not be liable for any loss caused by reliance on a false or forged digital signature of a subscriber, if, with respect to the false or forged digital signature, the licensed certification authority complied with the requirements of this Act;
>
> (b) shall not be liable in excess of the amount specified in the certificate as its recommended reliance limit for either -
>
> (i) a loss caused by reliance on a misrepresentation in the certificate of any fact that the licensed certification authority is required to confirm; or
>
> (ii) failure to comply with sections 29 and 30 in issuing the certificate."

For non-licensed CA's, it can limit its liability only to the extent is it reasonable. Having no liability at all may be unreasonable unless the CA can show very clearly that it brought the limitation of liability clause to the attention of the persons seeking to rely on its digital certificate, and it was reasonable in those circumstances (eg free certificate, obtained over the net, limited purpose) to assume no liability.

4 Suppose there is a limitation of liability clause in CPS of the CA in X that "The party shall make a claim to the CA within one year after the event occurred." Can A Corporation file a suit before a court in X against the CA in X one year after it suffered damage?

Such a provision would be construed as a limitation of liability clause and be subject to the

Unfair Contracts Terms Act, i.e. the CA will have to show that the time bar is reasonable. There has been a case in Singapore which has held that such a clause was unreasonable but a court could still find that in this case the time bar is reasonable since each case will be decided on its facts.

5 Is there any difference with respect to the scope and degree of liability of CA in X if its CPS provides that (1) CA shall conduct authentication with scrutiny; or (2) CA does not need to conduct authentication with reasonable care?

The latter provision appears to be a clause excluding the CA's liability for negligence in performing the authentication, and will be valid only if reasonable.

6 Can A Corporation win the case against B Corporation if B Corporation was negligent in retaining B Corporation's Private Key.

Yes, if A Corporation can show B Corporation was negligent, ie failed to exercise reasonable care to retain control of its private key.

> Control of private key
> 39. —(1) By accepting a certificate issued by a certification authority, the subscriber identified in the certificate assumes a duty to exercise reasonable care to retain control of the private key corresponding to the public key listed in such certificate and prevent its disclosure to a person not authorised to create the subscriber's digital signature.
>
> (2) Such duty shall continue during the operational period of the certificate and during any period of suspension of the certificate.

Chinese Taipei:

1. Article 14 of the Electronic Signature Act in Taiwan deals with the liability of CAs. A CA shall be liable for any damage caused by its operation or other certification-related process to the parties, or to a bona fide person who relies on the certificate, unless the CA proves that it has not acted negligently.

In other words, a CA in Taiwan will bear a kind of modified negligent liability. In situations where a party suffers damages arising out of the use of the certificate service provided by a CA, the CA is presumed being negligent. The CA will thus bear the burden of proof for its not acting negligently in providing the certificate service, and rebut the negligence presumption for not being held liable.

A CA will not bear strict liability regarding its operation or other certification-related process in Taiwan. Unlike the legal doctrine of strict liability, a CA is not held liable as long as it can prove its not acting negligently in causing the damages of the suffering parties.

2. The Electronic Signature Act in Taiwan does not regulate the conduct of wrongful impersonation. It may be panelized under traditional law of Taiwan.

3. To facilitate the development of electronic certification industry, the Electronic Signature Act allows CA to manage their risk by specifying the use of certificates. Under Paragraph 2 of Article 14, the Electronic Signature Act in Taiwan states that: where a CA clearly specifies the limitation for the use of the certificate, it shall not be liable for any damage arising from a contrary use.

In other words, A CA may limit its liability by clearly specifying the limitation or restriction on the use of the certificate it issued. Any claim against a CA for the use of certificate that was utilized not in compliance with the limitation will not be upheld for the damage compensation.

Under Article 222 of the Civil Code in Taiwan, a party shall not waive its liability from intentional or gross negligent liability by agreement. A CA may limit its liability by specifying the limitation on the use of the certificate pursuant to the Electronic Signature Act. However, in its indemnification clause, the CA may not simply state that it does not presume any liability in any event since the Civil Code restricts a party to be exempted from intentional or gross negligent liability by agreement.

In sum, under Article 14 of the Electronic Signature, a CA may limit its liability on the use of the certificate and the compensation cap. A CA that has clearly specified the limitation for the use of the certificate will not be liable for any consequent damages arising from a contrary use. A CA may use an indemnification clause to limit its liability on the amount of compensation, or specify the appropriate application of a certain type of certificate it issued.

4. Yes. Statute of limitation, in general, is regulated by procedure laws and involved public policy concerns. Under Article 147 of the Civil Code in Taiwan, the statute of limitation is non-waivable nor modifiable. Thus, even though a CA may set a shorter term on statute of limitation in the CPS, such agreement does not overwrite the procedure law regulations and will serve very limited purpose.

5. The parties are free to contract the duty of care each party shall exercise under the contract law in Taiwan. Thus, a CA may specify in its CPS that it shall conduct authentication with scrutiny. Considering the liability exoneration clause, a CA may limit its liability under the civil law except to the exemption from international or gross negligent liability, as discussed in the previous question. However, if the failure of a CA to authenticate a certificate user with reasonable care is considered to be gross negligent, it may not in its CPS include the exoneration clause that it does not need to conduct authentication with reasonable care.

6. Under theory of tort law, a party may sue another party regardless whether privity of contract exists. Thus, A Corporation may sue B Corporation under torts liability.

Request 2-3: Cipher breaking

The CA in X conducted authentication of the both A and B Corporations with reasonable care and issued certificates to the both Corporations. The CA met the security standards.
However, a corporation "P" broke the cipher and impersonated the B Corporation.
Due to this cipher-breaking and spoofing (impersonation), the CA in X was driven to issue a certificate to the corporation "P" that was impersonating the B corporation.
As the A Corporation relied on the certificate issued to "B Corporation", it supplied computer goods to "B Corporation ".
However, "B Corporation", actually P Corporation, never paid the price for the computer goods and disappeared. B Corporation negated the contract formation between A Corporation and B Corporation.
The A Corporation would like to file a suit before a court in X seeking damages against the CA in X.
1 What types of liabilities will the CA in X bear? What will be the requirements for A Corporation in X to win the case? Will the CA bear strict liability as to this case?
2 (1) Suppose there is an indemnification clause in CPS of the CA in X that "The CA does not assume any liability over 2,000 US dollars." The Corporation in X suffered damages of 200,000 US dollars. Is such escape clause valid? Can A Corporation in X win the 200,000 US dollars?
(2) Suppose there is an indemnification clause in CPS of the CA in X that "The CA does not assume any liability unless the CA authenticated and issued certificates with willful misconduct or gross negligence." Is this escape clause valid? Can A Corporation in X win the case?
3 Suppose there is a statute of limitation clause in CPS of the CA in X that "The party shall claim to the CA within one year after the event occurred." Can A Corporation in X file a suit before a court in X against the CA in X after one year it suffered damage?

China:

1 Tort Liability OR Contractual Liability. In this case, A corporation has to proof that the CA does not conducted its reasonable care and CA has negligence. CA does not bear strict liability.

2 As the same as the previous answer, in this case, a contractual relationship is recognized between A Corporation and the CA. A Corporation can seek for its damage against the CA but it must supply enough relating evidence.

3 Same as previous answer.

Japan:

1 Tort Liability and Contractual Liability. (Previous Answer). In this case, the CA conducted its reasonable care and there is no negligence on the CA. CA does not bear strict liability. Therefore, the CA does not bear liability for A Corporation's damage.

2 As the same as the previous answer, in this case, a contractual relationship is recognized between A Corporation and the CA. In addition, Japan's Consumer Protection Act does not

apply to this case because this case is not a case between a business and a consumer. Therefore, A Corporation is bound by the clause. A Corporation cannot seek damages against the CA.

3 Same as previous answer.

Korea:

1. Same as the previous answer. It bears tort liability and contractual liability. In this case, as the CA acted with reasonable caution, it was not negligent. The CA does not bear strict liability. However, in accordance with Article 26 of the Electronic Signature Act of Korea, the CA is obligated to prove that it was not negligent, and if it cannot prove that it was not intentional or negligent, it shall be held liable for damages.

2.(1) Same as the previous answer.

2.(2) Article 26 of the Electronic Signature Act stipulates that, if the CA cannot prove it was not negligent in performance of certification service, or if it caused damages to the subscriber or the user (Corporation A) who trusted the certificate due to force majeure, it must make reparation for damages. Therefore, Corporation A may win the lawsuit against the CA. However, speaking from the realistic point of view, since PKI is so secure that no existing technology can decipher it, the question seems misguided.

Singapore:

[It is not clear what "cipher" was broken. The problem goes on to state "Due to this cipher-breaking and spoofing (impersonation), the CA in X was driven to issue a certificate to the corporation "P" that was impersonating the B corporation". Does this mean that B/P was wrongly authenticated or that P created a "false or forged digital signature of a subscriber" ?]

[If the latter, Section 45 provides that unless a licensed certification authority waives the application of this section, a licensed certification authority shall not be liable for any loss caused by reliance on a false or forged digital signature of a subscriber, if, with respect to the false or forged digital signature, the licensed certification authority complied with the requirements of this Act.

Remaining answers as above, i.e it will depend whether the CA was licensed, and if not whether the limitation of liability clauses was reasonable.]

Chinese Taipei:

1. Assuming the CA is not negligent here: subsection 5, Section 1, Chapter 1, Part II of the Civil Code of Taiwan regulates the tortious acts of a party. A party is not liable for a third party's act in general, unless otherwise specified by laws to impose vicarious liability when certain relationship between the party and the third party exists. Absent such relationship, a party is not liable for another's wrongful act. Thus, a CA will not bear any vicarious liability for a third person absent any special relationship the existing law imposed on it.

On the other hand, a CA may be liable under contract liability if it voluntarily assumes any such kind of liability by agreement.

2. Same as previous answers. Please refer to the above-mentioned information (answers to 2-2) for liability, indemnification clause and statute of limitation issues.

3. Same as previous answers. Please refer to the above-mentioned information (answers to 2-2) for liability, indemnification clause and statute of limitation issues.

Request 2-4: Private Information
The private information written in the application forms submitted by Corporation A retained by CA was leaked due to the negligence of an employee of the CA in X. If A Corporation files a suit against CA in X due to invasion of privacy, what liabilities will the CA in X bear?

China
the person who leaked the personal information and the CA itself shall be penalized in accordance with Article 31 of Electronic Signature Law of PRC. CA should correct it's negligence immediately, if not, it's right to issue certifications would be canceled and it the following 10 years it can not provide such service again.

Japan:
If the CA is the Entity handling Personal Information defined in the Personal Information Protection Act of 2003 and did not comply with the obligations provided in such Act, the person who leaked the personal information and the CA itself shall be penalized in accordance with Sec. 58 of Japan's Personal Information Protection Act of 2003.
In addition, the CA will bear contractual liability because it is highly likely that the CA and A Corporation have entered into a confidentiality agreement. The CA breached the confidentiality agreement.

Korea:
The person who leaked the personal information and the CA itself shall be penalized in accordance with The Act on Promotion of Information and Communication Network Utilization and Information Protection, etc.

The Electronic Signature Act of Korea provides it as follows:

* **Article 24 (Protection of Personal Data)**

Certification authorities shall protect personal data in when carrying out all certification services.

Articles 22 through 32, Paragraph of Article 36 and Articles 54, 55, 62, 66 and 67 of The Act on Promotion of Information and Communication Network Utilization and Information Protection, etc. shall be applied mutatis mutandis to the protection of personal data under Paragraph herein In this case, "information and communication service provider" shall be replaced by "accredited certification authority," and "user" shall be replaced by "subscriber."

Singapore:

There is no general privacy law in Singapore, so A Corporation will have to rely on the general laws relating to breach of confidence, and/or if there is a confidentiality agreement between the parties, by bringing an action for breach of contract.

The CA's licence may contain a condition requiring the CA to keep user data confidential, however A Corporation cannot rely on this as a third party (assuming that the Contracts (Rights of Third Parties) Act does not apply or is excluded).

Chinese Taipei:

Article 15 of the Regulation on Required Information for Certification Practice Statement in Taiwan states that, a CA shall specify in its CPS the types of personal information entitled to protection and the methods the CA will adopt to keep such information confidential. Therefore, a CA in drafting its CPS shall make clear what information it will disclose at the repository and what to be keep confidential that collected from its subscribers.

Under the Civil Code of Taiwan, a party may have a claim against another for serious privacy invasion that was attributed to such person's wrongful act. The suffering party may further seek for redress even if such damages are not purely pecuniary (Article 195 of the Civil Code). On the other hand, the Computer-Processed Personal Data Protection Law in Taiwan also deals with the liability of a public or private sectors in a privacy invasion suit.

For violation of privacy protection, a CA may be held liable under negligent tort liability.

Request 2-5: Certificate Revocation List (CRL)

Although the Certificate of B Corporation has been revoked, the CA in X did not provide the revocation information to CRL.

Due to such negligence of the CA, the transaction between A Corporation and B Corporation suddenly ceased. A Corporation suffered damage. Can A Corporation seek for damage against the CA in X?

China:

Yes. A Corporation can seek for its damage against the CA in accordance with Contractual Liability or Tort Liability.

Japan:

Yes. A Corporation can seek damages against the CA in accordance with Contractual Liability or Tort Liability.

Korea:

Yes. A Corporation can seek for its damage against the CA in accordance with Contractual Liability or Tort Liability. First of all, the article 26 of the Electronic Signature Act will apply.

Singapore:

Yes, A Corporation can bring a claim for negligence and possibly breach of statutory duty against the CA. The CA has a duty under s35 ETA to publish a notice of revocation.

> Notice of revocation
> 35. —(1) Immediately upon revocation of a certificate by a certification authority, the certification authority shall publish a signed notice of the revocation in the repository specified in the certificate for publication of notice of revocation.
>
> (2) Where one or more repositories are specified, the certification authority shall publish signed notices of the revocation in all such repositories.

Chinese Taipei:

A Corporation may seek for damages under contract or tort liability. Please refer to the answers to 2-2 for liability issues.

Request 2-6: Certificate

1 Can the CA in X issue a certificate under a pseudonym?

2 Are information on electronic certificates required to comply with X. 509 version 3 by ISO?

China:

1.No.

2.(1)yes.

(2) To be described.

(3) To be described.

Japan:

1 No. Sec.5 of the Implementation Order of the Japan's Electronic Signature and Certification Services Act provides that "Persons applying to use the certification services are required to submit a copy of their resident card, certified copy of family register or abstract thereof, certificate of items described in the original registration prescribed in Article 4-3 of the Alien Registration Law".

3. Yes.

Korea:

1. No.
2. (1) Yes.
2. (2) As shown below

Cert Type / Extension Field	Root Cert	CA Cert	OCSP Cert	TSP Cert	User Cert
Authority Key	Root Cert	Root Cert	Root Cert	Root Cert	CA Cert

Identifier	Public key's Hash value	Public key's Hash value	Public key's Hash value	Public key's Hash value	Public key's Hash value
Subject Key Identifier	Root Cert Public key's Hash value	Subject Public key's Hash value	Subject Public key's Hash value	Subject Public key's Hash value	Subject Public key's Hash value
Key Usage	Certificate Signing, CRL Signing	Certificate Signing, CRL Signing	Digital Signature, Non-Repudiation	Digital Signature, Non-Repudiation	Digital Signature, Non-Repudiation
Private Key Usage Period	Not recommended	Not recommended	Not recommended	Not recommended	Not recommended
Certificate Policy	Policy Identifier	Policy Identifier	Policy Identifier, Policy Qualifier Id (Notice Text)	Policy Identifier, Policy Qualifier Id (Notice Text)	Policy Identifier, Policy Qualifier Id (Notice Text)
Policy Mapping	Optional	Optional	Not defined	Not defined	Not defined
Subject Alternative Name	User Real Name	User Real Name	User Real Name	User Real Name	User Real Name & VID
Issuer Alternative Name	Issuer Real Name	Issuer Real Name	Issuer Real Name	Issuer Real Name	Issuer Real Name
Subject Directory Attributes	Not recommended	Not recommended	Not recommended	Not recommended	Not recommended
Basic Constraints	Subject Type=CA, Path Length=1	Subject Type=CA, Path Length=0	Not recommended	Not recommended	Not recommended
Name Constraints	Optional	Optional	Not defined	Not defined	Not defined
Policy Constraints	Optional	Optional	Not defined	Not defined	Not defined
Extended Key Usage	Optional	Optional	OCSP Signing	Timestamp Signing	Optional
CRL Distribution Points	Distribution Point Name	Distribution Point Name	Distribution Point Name	Distribution Point Name	Distribution Point Name
Authority Information Access	Optional	Optional	Optional	Optional	Access Method, Alternative Name

2. (3) Information related to credit information is not in the extension field of the certificate, but

the resident registration number and random number are hashed twice and saved in the Subject Alternative Name field (VID).

Singapore:

1. Possibly. Under s29(2) of the ETA, in the absence of a certification practice statement ("CPS"), the certification authority must confirm by itself or through an authorised agent that the prospective subscriber is the person to be listed in the certificate to be issued. If the CA has a CPS, it must comply with all of the practices and procedures set forth in such CPS including procedures regarding identification of the prospective subscriber. Under para 19(4) of the ETA (CA) Regulations, the subscriber identity verification method employed for issuance of certificates must be specified in the CPS and is subject to the approval of the Controller during the application for a licence by the CA.

2 (1). Every licensed certification authority is required to use the Internet draft of the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, adopted by the Internet Engineering Task Force and reproduced by the Controller on its Internet website, as a guide for the preparation of its certification practice statement. This is currently RFC 3647, November 2003 version.

2(2).Not specified. This is up to the CA to decide.

2(3).Not specified. This is up to the CA to decide.

Chinese Taipei:

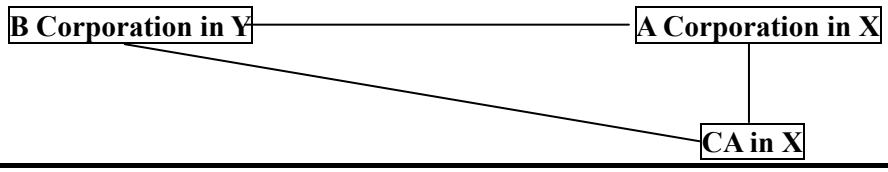
1. Technically speaking, a CA may issue a certificate under a pseudonym. However, current regulation is silent on whether such certificate may be entitled legal effect or recognition.

2. In general, Yes.

Request 3: (Cross-border business using PKI)

Suppose that there is a company called A Corporation in your country/area which we will call X. A Corporation would like to supply computer goods to B corporation in another country/area which we will call Y.

Exchange of contracts and communications between the A Corporation in X and the B Corporation in Y are to be conducted using PKI. A and B Corporations have agreed to use the CA in X.



Request 3-1. Contract

CA is going to issue an electronic certificate to A Corporation in accordance with its agreement between the CA and A Corporation. Is it required for the three parties to enter into one integrated agreement?

China:

No. they are independent agreements. An agreement between the CA and A Corporation and the agreement between the CA and B Corporation can be separated.

Japan:

No. An agreement between the CA and A Corporation and the agreement between the CA and B Corporation can be separate, because they are independent agreements.

Korea:

No. An agreement between the CA and A Corporation and the agreement between the CA and B Corporation can be separated, because they are independent agreements.
B Corporation in Y is a Relying party. B Corporation may request the CA to verify the certificate without a contract.

Singapore:

No. The CA in X does not need to be a party to the agreement between A and B, unless the parties wish to impose additional contractual obligations on the CA in X.

Chinese Taipei:

There is no requirement that all the parties entered into an integrated agreement. Every independent agreement suffices as long as they fit parties' needs.

Request 3-2. Authentication

1 Can the CA in your country/area X issue a certificate to a corporation in foreign country/area Y? are there any regulations?

2 What are the requirements for authentication to issue a certificate to the Corporation in foreign country/area Y?

3 How can the CA implement the authentication? Will the CA directly request the company in Y to provide materials for authentication or ask A Corporation in X to pass its request to B Corporation in Y?

China:

1. Yes. The CA in China can issue a electronic certificate to a foreign corporation in foreign country/area..

2. There are same requirements as well as domestic Chinese corporations.

3. CA in China can directly request the company in Y to provide the material for authentication, and the Electronic Signature Law of PRC also accept CA in foreign countries if it's certifications have

been checked by MII according to relevant treaties or principle of equation.

Japan:

1. Yes. The CA in Japan can issue an electronic certificate to a foreign corporation in foreign country/area.
2. The same requirements pertain to domestic Japanese corporations as well.

The CA in X (Japan) can decide either way.

Korea:

1. No. The CA in Korea can't issue an electronic certificate to a foreign corporation in foreign country/area yet. But, if a foreigner or local branch of foreign company is in Korea, he/she can be issued an electronic certificate in accordance with the article 13-2 of the Enforcement Ordinance of the Electronic Signature Act of Korea. The provisions regarding the issuance of certificates to foreign corporations located overseas are scheduled to be newly established when the said Enforcement Ordinance is revised.

Article 13.2(Standards and Method for Verifying the Identity) An accredited certification authority shall verify the identity of the applicant for issuance of an accredited certificate pursuant to the regulation prescribed at the end of Paragraph of Article 15 of the Act by checking real information of the applicant as follows:

1. Person

1) The name and resident registration no. on a copy of family residential registration papers. But the name on a passport and the passport no. for overseas residents (for those overseas residents for whom passports has not been issued, the name and registration no. on the register for overseas residents according to the Overseas Resident Registration Law).

2) The name and registration no. on the registered foreigner record by the Immigration Control Law for foreigners. But, the name and no. on the passport or an ID card for those foreigners for which a forefinger registration card is not issued.

2. Juridical Person (including corporate juridical persons regarded as juridical persons by the Basic Law for Taxes)

The name and business registration no. on the business registration card issued according to the Corporation Tax Law. But, the name and tax payment no. of the juridical person written on the document to which the tax payment no. is given according to the Corporation Tax Law for those juridical persons for whom business registration cards have not been issued.

2. see 1. answer.

Singapore:

1. Yes
2. There are no specified requirements, except that the subscriber identity verification method for the issuance, suspension, revocation and renewal of a certificate must be specified in the certification practice statement.
3. It is up to the CA but the CA may issue a certificate to B Corporation only after the CA has received a request for issuance from B Corporation.

Chinese Taipei:

There is no specific regulation on a domestic CA issuing certificates to a foreign user. A domestic CA is subject to the regulation set forth under Article 11-14 of the Electronic Signature Act in Taiwan.

Article 11 of the Electronic Signature Act states:
Prior to providing services for issuing certificates to the public, a certification service provider shall file the certification practice statement stating its operational processes related to the practice or certification services of the certification service provider to the competent authority for approval. After the approval, the certification service provider shall publish the approved certification practice statement on its Internet website to the general public for reference. The preceding rule shall also apply in the event that there is any modification in the certification practice statement.

A certification practice statement shall include the following information:

1. significant information that could affect the trustworthiness of a certificate issued by the certification service provider or the certification service provider's operation;
2. grounds for the certification service provider to revoke a certificate without being requested;
3. retention of the information related to the verification of the content of a certificate;
4. methods and procedures implemented to protect the personal information; and
5. other important information mandated by the competent authority.

A certification service provider that has been providing services for issuing certificates prior to the effective date of this Act shall file a certification practice statement to the competent authority for approval within six months after the effective date of this Act. In such case, the certification service provider may continue providing services for issuing certificates before obtaining the competent authority’s approval.

The competent authority shall publish a list of the certification service providers whose certification practice statements have been approved.

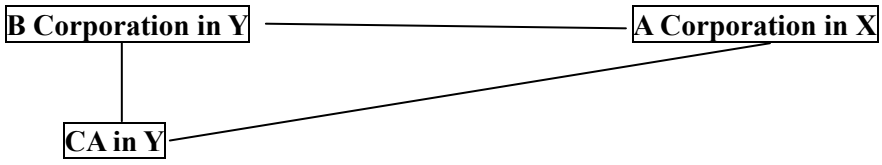
Article 14 of the Electronic Signature Act states:
A certification service provider shall be liable for any damage caused by its operation or other certification-related process to the parties, or to a bona fide person who relies on the certificate, unless the certification service provider proves that it has not acted negligently.

Where a certification service provider clearly specifies the limitation for the use of the certificate, it shall not be liable for any damage arising from a contrary use.

Request 4: (Cross-border business using PKI)

Suppose that there is a company called A Corporation in your country/area which we will call X. A Corporation would like to supply computer goods to B Corporation in another country/area which we will call Y.

A Corporation in X and the B Corporation in Y have agreed to conduct their exchange of contracts and communications using PKI. Both corporations have agreed to use a Certification Authority in country/area Y in common.



Request 4-1: Foreign Certificate

1 Is the certificate issued by the CA in Y valid in your country/area X, although the CA in Y has not obtained permission or accreditation by the government in X?

2 Can a certificate issued by the CA in Y deserve legal authentication presumption?

China:

1 Yes, it is valid. Chinese companies can use an electronic certificate issued by foreign CA although the CA in Y has not obtained permission or accreditation by the Chinese government.

CA in China can directly request the company in Y to provide the material for authentication, and the Electronic Signature Law of PRC also acknowledge CA in foreign countries when it's certifications have been checked by MII according to relevant international treaties or principle of equation.

2. As the answer above.

Japan:

1 Yes, it is valid. Japanese companies can use an electronic certificate issued by a foreign CA even if the CA in Y has not obtained permission or accreditation by the Japanese government.

But, a foreign CA can apply to receive accreditation by the Japanese government. Sec. 15 of Japan's Electronic Signature and Certification Services Act of 2000 provides that: "a person seeking to perform the designated certification service by means of an office located in a foreign country may receive the accreditation from the related ministers."

There are some differences between domestic accredited certification service provider (accredited domestic CA) and accredited foreign certification service provider (accredited foreign CA).

As for accredited domestic CA, the related ministers shall perform on-site investigations of the system involved in the implementation of the service applied for accreditation. On the other hand, an accredited foreign CA is required to file documents that state facts prescribed by the ordinance of the related ministries instead of the investigation. (Sec. 6 and 15-3 of Japan's Electronic Signature and Certification Services Act of 2000).

In addition, accredited domestic CA will be penalized with a fine of not more than three hundred thousand yen if it fails to file a report pursuant to the provisions of Article 35, if it files

a false report, refuses, obstructs, or evades an inspection, or refuses to answer or provides false answers (Sec. 44-3 of Japan's Electronic Signature and Certification Services Act of 2000). On the other hand, accredited foreign CA will not be penalized but merely have its accreditation revoked (Sec 16-1-5 and 6 of said Act).

2 Sec.3 of Japan's Electronic Signature and Certification Services Act of 2000 provides that: "an electro-magnetic record which is made in order to express information shall be presumed to be authentic if an electronic signature (limited to those that, if based on the proper control of the codes and objects necessary to perform the signature, only that person can substantially perform) is performed by the principal in relation to information recorded in the electro-magnetic record." If A Corporation uses a certificate issued by the CA in Y, and the CA in Y is not the accredited foreign CA, then the certificate issued by the CA in Y shall meet the requirements of Sec.3 if A Corporation wishes the legal presumption for authentication.

Korea:

1. They shall have the effect of a private certificate, not that of a accredited certificate. The Electronic Signature Act of Korea stipulates "Any electronic signatures other than accredited electronic signatures shall have the same legal effect as the signatures or signature-seals by an through agreement between parties involved." **Article 3 (Legal Effect of Electronic signatures, etc.)**.

2. If Country Y and Country X enter into a mutual recognition agreement in accordance with Article 27-2 of the Electronic Signature Act of Korea, the certification authority of Country Y(foreign country) or the certificates issued by a foreign country's certification authority may have the same legal status as the CA or the certificates according to the Electronic Signature Act.

Article 27.2 (Mutual Recognition)

- The Government may enter into an agreement with a foreign government for mutual recognition of electronic signatures.
- The agreement entered into pursuant to Paragraph hereof may shall grant the same legal status or effect to a foreign certification authority or a certificate issued by a foreign certification authority as an accredited certification authority, or an accredited certificate issued by an accredited certification authority under this Act.
- When an agreement with a foreign government for mutual recognition of electronic signatures is executed, the Ministry of Information and Communication shall make known the contents thereof by public notice pursuant to Paragraph hereof.
- When an agreement with a foreign government for mutual recognition of electronic signatures or certificates is executed pursuant to Paragraph hereof, the electronic signatures or certificates issued by a the foreign certification authority shall have the same legal effect as accredited electronic signatures or accredited certificates issued by an accredited certification authority under this Act.

Singapore:

1.Yes

2. Yes since the parties have expressly agreed between themselves (sender and recipient) to use

digital signatures as a security procedure, and the digital signature was properly verified by reference to the sender's public key.

Chinese Taipei:

1. There is no specific regulation for a certificate user to receive a certificate from the CA in a foreign country unless the user is using such certificate for satisfaction of written requirement by law. Under such situation, the certificate must be issued from an accredited CA that met the requirement of Article 11 of Electronic Signature Act in Taiwan (please refer to Request 3, Part B for Article 11).

Under the principles of reciprocity and equivalent secure requirements, a certificate issued by a CA organized or registered pursuant to foreign law shall be equivalent to the one issued by a domestic CA, provided that the foreign CA has been permitted by the competent authority. (Article 15 of the Electronic Signature Act)

Moreover, the competent authority has issued the "Regulations Governing Permission of Foreign Certification Service Providers," which describe two ways for a foreign CA to acquire permission: (a) A foreign CA submits required documents to apply for permission; or (b) A foreign CA has been permitted or accredited by other countries, regional organizations, or international organizations with whom the competent authority has signed bilateral or multilateral agreements or arrangements regarding mutual recognition of legal effect of certificates.

Article 15 of the Electronic Signature Act in Taiwan:

Under the principles of reciprocity and equivalent secure requirements, a certificate issued by a certification service provider organized or registered pursuant to foreign law shall be equivalent to the one issued by a domestic certification service provider, provided that the foreign certification service provider has been permitted by the competent authority.

The regulation for permitting the certification service providers specified in the preceding paragraph shall be prescribed by the competent authority.

The competent authority shall publish a list of the certification service providers permitted pursuant to the first paragraph.

2. Under current Electronic Signature Act in Taiwan, there is no legal authentication presumption regardless of what types of electronic signature, or certificate, is used.

Request 4-2: Negligence in Authentication

The CA in Y did not conduct the authentication of the both Corporations with reasonable care and issued certificates to the A Corporations in X and B Corporation in Y.
However, in this case, a "P" impersonated the B Corporation in Y.

Due to this spoofing (impersonation), the CA in Y was driven to issue a certificate the corporation "P" that was impersonating the B Corporation in Y.
As A Corporation in X relied on the certificate issued to "B Corporation in Y", it supplied the computer goods to "B Corporation in Y".
However, "B Corporation in Y", actually P Corporation, never paid the price for the computer goods and disappeared. The B Corporation negated the contract formation between the A Corporation and B Corporation.
1 The A Corporation in X would like to file a suit before a court seeking damages against the CA in Y.
(1) Which law will apply to this case?
(2) Which court will have jurisdiction?
(3) What will be the requirements for the A Corporation in X to win the case?
(4) Suppose there is an escape clause in CPS of the CA in Y that "The CA does not assume any liability over 2,000 US dollars." The A Corporation in X suffered the damage of 200,000 US dollars. Is such indemnification clause valid? Can the A Corporation in X win the 200,000 US dollars?
Or, suppose there is an escape clause in CPS of the CA in Y that "The CA does not assume any liability in any event." Can the A Corporation in X win the case?
(5) Suppose there is a statute of limitation clause in CPS of the CA in X that "The party shall claim to the CA within one year after the event occurred." Can the A Corporation in X file a suit before a court against the CA in Y after one year it suffered damage?

2 The A Corporation in X would like to file an arbitration seeking damages against the CA in Y.
(1) Where will be the place of arbitration?
(2) Which law will apply to the arbitration proceedings?
(3) Suppose that there is an escape clause in CPS of the CA in Y that " The CA does not assume any liability in any event." Can the A Corporation in X receive an arbitral award in favor of the Corporation in X?

China:

1(1) In this case, we think that there is an agreement to use CA in Y between A Corporation and the CA in Y. CPS of the CA in Y may provide the applicable law. In absence of the agreement or provision in the CPS on applicable law between the parties, the law of place having a most closing relationship of conduct the contract shall apply.

(2)If there is an international contractual jurisdiction agreement between the CA in Y and A Corporation in the agreement or CPS, such international jurisdiction agreement will be valid if the substantial requirements are met. They are /is a court of a particular country/area is designated; (b)The existence and content of the agreement is evident. (c) The dispute is not in the scope of the Chinese court's exclusive jurisdiction; and (d) The foreign court must have jurisdiction over the dispute.

(3)A Corporation will seek for CA's contractual liability and tort liability in accordance with Y law or X law.

(4)Legal validity of such escape clause will depend on applicable law.

(5)Legal validity of such clause to shorten the period of statute of limitations will depend on applicable law.

2(1) If there is an agreement to apply CPS between CA in Y and A Corporation and CPS provides an arbitration agreement, the arbitration will be held in such way. We should seek for the parties' express or implied intention.

(2) Arbitration Law of PRC will apply when the place of arbitration is China.

(3)If the arbitration is held in China, Chinese Arbitration Law shall apply in accordance with relating Chinese substantial law. If the arbitration is held in Y, Y's arbitration law shall apply to this case.

Japan:

1(1) In this case, we think that there is an agreement to use CA in Y between A Corporation and the CA in Y. CPS of the CA in Y may provide the applicable law. In absence of the agreement or provision in the CPS on applicable law between the parties, the law of place of conduct shall apply (Horei-The Act concerning the Application of Laws-Sec.7.2).(Dispute Resolutions for Cross-Border E-Commerce by Asia PKI Forum. P34)

1(2)

If there is an international jurisdiction agreement between the CA in Y and A Corporation in the agreement or CPS, such international jurisdiction agreement will be valid if the substantial requirements are met. They are (a) a court of a particular country/area is designated; (b)The existence and content of the agreement is evident. Furthermore, if a foreign court is to have exclusive jurisdiction: (c) The dispute is not in the scope of the Japanese court's exclusive jurisdiction; and (d) The foreign court must have jurisdiction over the dispute (Japanese Supreme Court on Nov. 28, 1975) (Dispute Resolutions for Cross-Border E-Commerce by Asia PKI Forum. P61).

If there is no international jurisdiction agreement between the CA and A Corporation, internal jurisdiction rules shall apply to the determination of international jurisdiction and that the Japanese jurisdiction shall be denied if there is a particular circumstance (Japanese Supreme Court on Octboer16, 1981 and November 11, 1997) (Dispute Resolutions for Cross-Border E-Commerce by Asia PKI Forum. P62). In this case, (a) a court in Japan will have jurisdiction if the CA in Y has an office in X(Japan) (Japanese Civil Procedure Code Sec. 4.5). (b)If the CA in Y does not have an office in Japan, a court in Japan where there is a domicile of the of the representative or principal person in charge of business operation shall have a jurisdiction (Japanese Civil Procedure Code Sec. 4.5). (c)If the CA in Y has neither an office in Japan nor representative or principal person, a court of the place where the obligation is to be performed will have jurisdiction (Japanese Civil Procedure Code Sec. 5.1).

1(3) A Corporation will seek for CA's contractual liability and tort liability in accordance with Y law

or X law.
1(4) Legal validity of such escape clause will depend on applicable law. If Y law shall apply, the validity of such escape clause shall be determined by Y law. If X (Japan) law shall apply, the answer to the Request 2-2-3 will apply.
1(5) Legal validity of such clause to shorten the period of statute of limitations will depend on applicable law. If Y law shall apply, the validity of such clause shall be determined by Y law. If X (Japan) law shall apply, the answer to the Request 2-2-4 will apply.

2(1) If there is an agreement to apply CPS between CA in Y and A Corporation and CPS provides an arbitration agreement, the arbitration will be held in such way. We should seek for the parties' express or implied intention.
2(2) According to Sec. 3.1 of the Japanese Arbitration Act, X (Japan)'s Arbitration Law will apply when the place of arbitration is Japan. Such Section 3.1 follows with the territoriality principle provided in Sec. 2.1 of the UNCITRAL Model Law on International Commercial Arbitration Law (Dispute Resolutions for Cross-Border E-Commerce by Asia PKI Forum. P62).
2 (3) If the arbitration is held in X (Japan), Japanese Arbitration Law shall apply in accordance with Sec. 3.1 of such law.
Sec. 36.1 of Japanese Arbitration Law of 2003 provides that "The arbitral tribunal shall decide the dispute in accordance with such rules of law as are agreed by the parties as applicable to the substance of the dispute. In such case, any designation of the law or legal system of a given State shall be construed, unless otherwise expressed, as directly referring to the substantive law of that State and not to its conflict of laws rule. Sec. 36.2 of such law provides that "Failing agreement as provided in the preceding paragraph, the arbitral tribunal shall apply the substantive law of the State with which the civil dispute subject to the arbitral proceedings is most closely connected."(Dispute Resolutions for Cross-Border E-Commerce by Asia PKI Forum. Appendix P62).
Therefore, the answer to the Request 2-2-3 will apply to this case.
If the arbitration is held in Y, Y's arbitration law shall apply to this case.

Korea:
1.(1) As a contract exists between Corporation A and the CA of Country Y, it shall conform to the governing law on which the contract is based. The governing law of the contract is determined as follows. That is, if the parties concerned specified the governing law implicitly or explicitly, that law shall become the governing law; otherwise, the law of the country most closely related to the contract shall become the governing law.

Even if a contract exists, however, the injured party A may hold the certification authority of Country Y liable for the illegal act. (Contractual liability concerns matters occurring among those who creditors or debtors in accordance with a contract, whereas tort liability concerns matter that may occur among people at any time regardless of whether such a special relationship exists. Since tort liability is likely among people with a contractual relationship at the same time, the prevailing theory and precedents in most countries have it that both can be claimed.)
In that case, according to the private international law, the governing law of tort is the law of the place where the tort was perpetrated (Clause 1 of Article 32 of the international private law). In the case of remote tortious act, i.e. if the place where tort was perpetrated is different from

the place where the result of the tort occurs, both places are regarded as places of tort (Supreme Court March 22, 1983 Judgment 82 Da-Ka 1533 Plenary session decision, etc.). Though there is no Supreme Court decision as to the relationship of both parties, however, some lower court decisions have it that the plaintiff, who is the injured party, can choose a law favorable to him/her, and there is also a predominant support for it. In this case the “place of act” or lexi loci actus is Country Y, and the place of result is Country X, i.e Korea. Therefore, if Corporation A takes the case to a Korean court, Corporation A may choose one of the two laws to its advantage.

(2) If the CA in Y and Corporation A agreed on jurisdiction, this agreement shall be effective in general. If the agreement on jurisdiction is an exclusive agreement, for that to be effective, the case must not fall within the exclusive jurisdiction of the Korean Court, the designated foreign court must have jurisdiction over the case in accordance with the law of that foreign country, and the case in question must have reasonable relevance as to the foreign court (Supreme Court September 9, 1997. 9. 9. Judgment 96 Da 20093 decision).

If there is no agreement on jurisdiction, the international trial jurisdiction shall be determined in accordance with Article 2 of the international private law. However, since Article 2 of the international private law stipulates only abstract principles, those provisions of the Korean Civil Procedure Code related to domestic territorial jurisdiction shall be referred to, and if Korea has territorial jurisdiction, Korea shall have jurisdiction over international trials, unless there is any special reason against it.

In this case, (a) if the CA of Country Y has the main office or agency in Korea, or the person in charge at the CA has an address in Korea, it will have jurisdiction (Korean Civil Procedure Code Sec. 5.2). (b) If the place of duty-fulfillment is Korea, the Korean court will have jurisdiction. (c) Even if the above cases are not applicable, if the CA of Country Y has seizable properties in Korea, the Korean Court shall have general jurisdiction (Korean Civil Procedure Code Sec. 11).

(3) Regardless of whether contractual or tort liability is claimed, the requirements of the applicable proper law must be satisfied.

(4) Such an escape clause must be validated in accordance with the governing law of the applicable liability. If the law of Country X (Korean law) is the governing law, the answer to Request 2-2-3 shall be applied.

(5) The period of extinctive prescription and the effect of expiration of that period shall be determined in accordance with the applicable proper law. If the law of Country X (Korean law) is the governing law, the answer to Request 2-2-4 shall be applied

2(1) If there is an agreement to apply CPS between CA in Y and A Corporation and CPS provides an arbitration agreement, the arbitration will be held pursuant to such arbitration agreement. It should be reviewed whether there is an arbitration agreement between the parties, whether express or implied.

2(2) According to Sec. 2.1 of the Korean Arbitration Act, X (Korea)’s Arbitration Act shall apply when the place of arbitration is in Korea. Section 2.1 follows the territoriality principle provided in Sec. 1.2 of the UNCITRAL Model Law on International Commercial Arbitration of 1985.

2(3) If the arbitration is held in X (Korea), Korean Arbitration Act shall apply in accordance with Sec.2.1 thereof.

Sec. 29.1 of the Korean Arbitration Act of 1999 provides that "The arbitral tribunal shall decide the dispute in accordance with such law as are designated by the parties as applicable to the substance of the dispute. Any designation of the law or legal system of a given state shall be construed, unless otherwise expressed, as directly referring to the substantive law of that state and not to its conflict of laws rules. In addition, Sec. 36.2 of the Korean Arbitration Act provides that "Failing any designation as provided in paragraph 1, the arbitral tribunal shall apply the law of the state with which the subject matter of the dispute is most closely connected."
If the place of arbitration is Korea, regardless of whether contractual or tort liability is claimed, requirements of the applicable proper law as determined by the Arbitration Act of Korea must be satisfied. If the governing law is Korean law, the answer to Request 2-2-3 shall be applied. If arbitration is performed in Country Y, the requirements determined of the governing law as determined by the Arbitration Act of Country Y must be satisfied.

Singapore:

1(1). We assume there is no contract between A Corporation and the CA in Y, and A Corporation merely relied on the digital certificate issued by the CA verifying B Corporation's public key. This is likely to be a tort action (ie for negligence) and most likely to be governed by the law of Y where the majority of the negligent acts occurred (ie the issuance of B Corporation's certificate to P).

1(2). Generally A Corporation will have to sue CA in its home country Y. If A Corporation wants to sue CA in X (Singapore), it will need to serve proceedings on the CA outside of Singapore (ie in Y) with the leave of the court and must thus show that :

> (i) the claim is founded on a tort, wherever committed, which is constituted, at least in part, by an act or omission occurring in Singapore; or
>
> (ii) the claim is wholly or partly founded on, or is for the recovery of damages in respect of, damage suffered in Singapore caused by a tortious act or omission wherever occurring;

1(3). A Corporation will have to prove that CA was negligent.

1(4). Whether the limit of liability clause is valid will depend on the laws of Y if the action is brought in Y.

1(5). Whether the time bar limit clause is valid will depend on the laws of Y if the action is brought in Y.

2. This will depend on the terms of the arbitration agreement between the parties, if any.

Chinese Taipei:

1 (1): Assuming in this case that there is an agreement between A Corporation and the CA in Y regarding the certificate service provided and utilized by both parties, the application of law shall be governed by the agreement or the CPS if it was otherwise specified. In the absence of any agreement

as to the governing law, the applicable law shall be the "place of act" or *lex loci actus* (i.e., execution of contract)(Article 6 of Private International Law)(Please also refer to: Dispute Resolutions for Cross-Border E-Commerce by Asia PKI Forum, Answers to Request 8).

(2): A court in Taiwan has jurisdiction over the matter irrespective of the contract provisions to the contrary if (a) the cause of action arises in torts and the tortious act occurred in Taiwan (Article 15 of Codes of Civil Procedures); or (b) in the case of a claim in contract, the place of execution or breach of contract occurred in Taiwan (Article 12 of Codes of Civil Procedures). (Please also refer to: Dispute Resolutions for Cross-Border E-Commerce by Asia PKI Forum, Answers to Request 17)

(3): A Corporation shall seek for contractual and/or tort liability for claims against the CA.

(4): Issues regarding validity of indemnification clause are subject to the application of governing law. If the law in Taiwan is the governing law, the answers to the Request 2-2 shall apply.

(5): Issues regarding statute of limitations are subject to the application of governing law. If the law in Taiwan is the governing law, the answers to the Request 2-2 shall apply.

2 (1): If there is an agreement between the parties, the place of arbitration shall be the agreed upon place. If, however, the agreement is silent on the place of arbitration, and the claim for arbitration is brought in a Taiwan's arbitration court, the arbitration court shall decide a place of arbitration (Article 20 of the Arbitration Law).

(2): Under Article 19 of the Arbitration Law in Taiwan, the arbitration proceeding shall be conducted in accordance with the agreements of the parties. In the absence of an agreement on arbitration proceedings, the Arbitration Law shall apply. If both the arbitration agreement and the Arbitration Law are silent on rules and procedures for the arbitration, the arbitration court shall have discretion on whether to apply the Codes of Civil Procedure or any other appropriate rules and procedures.

(3): Under Article 31, the rules and procedures of Arbitration Law, the parties may agree to use commercial customs or rules of equity, failing which the panel of arbitrators may agree on the applicable law that they deem appropriate. (Please refer to: Dispute Resolutions for Cross-Border E-Commerce by Asia PKI Forum, Answers to Request 25)

The answers to the Request 2-2 on indemnification clause shall also apply to this case.

Request 4-3: Cipher breaking

The CA in Y conducted authentication of the both Corporations with reasonable care and issued certificates to the A Corporation in X and the B Corporation in Y.
However, a corporation "P" broke the cipher and impersonated the B Corporation in Y. Due to this cipher-breaking and spoofing (impersonation), the CA in Y was driven to issue a certificate the corporation "P" that was impersonating the B Corporation in Y. As the A

Corporation in X relied on the certificate issued to "B Corporation in Y", it supplied computer goods to "B Corporation in Y". However, "B Corporation in Y" never paid the price for the goods and disappeared. B Corporation negated the contract formation between A Corporation and B Corporation.
A Corporation in X would like to file a suit seeking damage against the CA in Y.
(1) Which law will apply to this case?
(2) Which court will have jurisdiction?
(3) What will be the requirements for the A Corporation in X to win the case?
(4) Suppose there is an indemnification clause in CPS of the CA in Y that "The CA does not assume any liability over 2,000 US dollars." The A Corporation in X suffered damages of 200,000 US dollars. Is such indemnification clause valid? Can the A Corporation in X win the 200,000 US dollars?
Or, suppose there is an indemnification clause in CPS of the CA in Y that " The CA does not assume any liability unless the CA authenticated and issued certificates with willful misconduct or gross negligence." Can the A Corporation in X win the case?
(5) Suppose there is a statute of limitation clause in CPS of the CA in Y that "The party shall claim to the CA within one year after the event occurred." Can the A Corporation in X file a suit before a court in X against the CA in Y after one year it suffered damage?

China:
As same as the answers to the Request 4-2.

Japan:
Same as the answers to the Request 4-2.

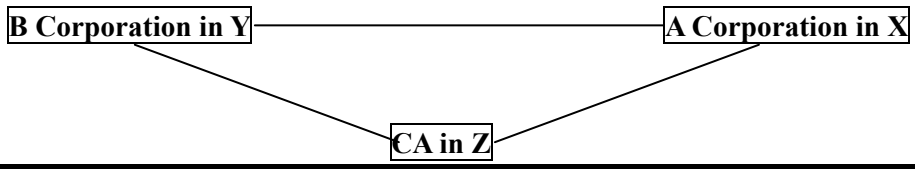
Korea: Same as the answers to Request 4-2.

Singapore:
It appears that the CA was not negligent in the conduct of the initial authentication of both Corporations since it did it with reasonable care. Assuming that the CA was not negligent either when it subsequently issued the certificate to P, then A Corporation may not have a cause of action against the CA, unless under the laws of Y, the CA is strictly liable for any losses suffered by any person, caused by the person's reliance on a certificate issued by a local CA (assuming that A can only sue the CA in Y since under Singapore law the CA is not liable unless it is negligent). Whether the limit of liability clause is valid will depend on the laws of Y if the action is brought in Y.

Chinese Taipei:
Same as the answers to Request 4-2

Request 5: Cross-Border E-Commerce using PKI

Suppose that there is a company called A Corporation in your country/area which we will call X. A Corporation would like to supply computer goods to B Corporation in another country/area which we will call Y. The A Corporation in X and the B Corporation in Y have agreed to conduct their exchange of communications using PKI.



Request 5-1: Negligence in Authentication

The CA in Z did not conduct the authentication of the both Corporations with reasonable care and issued certificates to the Corporations in X and Y.

However, a corporation "P" defrauded the CA in Z and impersonated the B corporation in Y.

Due to this spoofing (impersonation), the CA in Z was driven to issue a certificate the corporation "P" that was impersonating the Corporation in Y.

As the A Corporation in X relied on the certificate issued to "the Corporation in Y", it exported the computer goods to "the B Corporation in Y".

However, "B Corporation in Y" never paid the price for the computer goods and disappeared.

1 The A Corporation in X would like to file a suit before a court seeking damages against the CA in Z.

(1) Which law will apply this case?

(2) Which court will have jurisdiction?

(3) What will be the requirements for the A Corporation in X to win the case?

(4) Suppose that there is an escape clause in CPS of the CA in Z that "The CA does not assume any liability in any event." Can the A Corporation in X win the case?

2 The A Corporation in X would like to file an arbitration seeking damageeeking damages against the CA in Z.

(1) Where will be the place of arbitration?

(2) Which law will apply to the arbitration proceedings?

(3) Suppose there is an indemnification clause in CPS of the CA in Y that " The CA does not assume any liability in any event." Can the A Corporation in X receive an arbitral award in favor of the A Corporation in X?

China:

As same as the answers to the Request 4-2.

Japan:
Same as the answers to the Request 4-2.

Korea:
Same as the answers to Request 4-2.

Singapore:
1(1). We assume there is no contract between A Corporation and the CA in Z, and A Corporation merely relied on the digital certificate issued by the CA verifying B Corporation's public key. This is likely to be a tort action (ie for negligence) and most likely to be governed by the law of Z where the majority of the negligent acts occurred (ie the issuance of B Corporation's certificate to P).

1(2). Generally A Corporation will have to sue CA in its home country Z. If A Corporation wants to sue CA in X (Singapore), it will need to serve proceedings on the CA outside of Singapore (ie in Y) with the leave of the Singapore court and must thus show that :

> (i) the claim is founded on a tort, wherever committed, which is constituted, at least in part, by an act or omission occurring in Singapore; or
>
> (ii) the claim is wholly or partly founded on, or is for the recovery of damages in respect of, damage suffered in Singapore caused by a tortious act or omission wherever occurring;

1(3). A Corporation will have to prove that CA was negligent.

1(4). Whether the limit of liability clause is valid will depend on the laws of Z if the action is brought in Z.

1(5). Whether the time bar limit clause is valid will depend on the laws of Z if the action is brought in Z.

2. This will depend on the terms of the arbitration agreement between the parties, if any.

Chinese Taipei:
Same as the answers to Request 4-2

Request 5-2: Cipher Breaking
The CA in Z conducted the authentication of the both Corporations with reasonable care and issued certificates to the Corporations in X and Y. In this case, a certain corporation "P" broke the cipher and impersonated the B Corporation in Y. Due to this spoofing (impersonation), the CA in Z was driven to issue a certificate the corporation "P" that was

impersonating the corporation in Y. As the A Corporation in X relied on the certificate issued to "the B Corporation in Y", it supplied the computer goods to "the B Corporation in Y". However, "the B Corporation in Y" never paid the price for the computer goods and disappeared.
1 The A Corporation in X would like to file a suit before a court seeking damages against the CA in Z.
(1) Which law will apply to this case?
(2) Which court will have jurisdiction?
(3) What will be the requirements for the Corporation in X to win the case?
(4) Suppose there is an indemnification clause in CPS of the CA in Z that " The CA does not assume any liability unless the CA authenticated and issued certificates with willful misconduct or gross negligence." Can the Corporation in X win the case?
2 The A Corporation in X would like to file an arbitration seeking damages against the CA in Z.
(1) Where will be the place of arbitration?
(2) Which law will apply to the arbitration proceedings?
(3) Suppose there is an indemnification clause in CPS of the CA in Y that " The CA does not assume any liability unless the CA authenticated and issued certificates with willful misconduct or gross negligence." Can the Corporation in X receive an arbitral award in favor of the Corporation in X?

China:
Same as the answer to the Request 4-2

Japan:
Same as the answer to the Request 4-2

Korea:
Same as the answers to Request 4-2.

Singapore:
Same as the answer to the Request 4-2

Chinese Taipei:
Same as the answers to Request 4-2

Request 6: (Cross-Border E-Commerce using "Cross Certificate" determined by Inter-Operability Working Group of ASIA PKI Forum)

Suppose that there is a company called A Corporation in your country/area which we will call X. A Corporation would like to supply computer goods to B corporation in another country/area which we will call Y.
The A Corporation in X and the B Corporation in Y have agreed to conduct their

exchange of contracts and communications using PKI. However, there is neither an agreement between A Corporation and CA in Y nor an agreement between B Corporation in Y and the CA in X.
According to the Inter-Operability Guideline provided by the Asia PKI Forum, the CA in X sends its own self-signed Certificate to CA in Y so as to retain it into CA in Y's repository and vice versa.
When A Corporation in X receives a digital message from B Corporation in Y using PKI, the A Corporation looks into the repository of CA in Y.
If A Corporation finds the self-singed Certificate of CA in X in the repository of the CA in Y, A Corporation can verify the validity of the Certificate issued by CA in Y.
Because CA in X that has entered into an agreement with A Corporation in X exchanges its Certificate pursuant to the mutual agreement between the CA in X and the CA in Y.

<u>Request 6-1: Negligence in authentication, Validity of CPS to Relying Party (Plaintiff: A Corporation in X)</u>
The CA in Y did not conduct authentication of the B Corporation in Y with reasonable care and issued certificates to the B Corporation.
In this case, "P Corporation" impersonated the B Corporation. Due to this spoofing (impersonation), the CA in Y was driven to issue a Certificate to the "P Corporation " that was impersonating B Corporation. As the A Corporation relied on the certificate issued to "B Corporation", it supplied computer goods to "B Corporation".
However, "B Corporation", actually P Corporation, never paid the price for the computer goods and disappeared. B Corporation negated the contract formation between A Corporation and B Corporation.
The A Corporation in X would like to file a suit or suits seeking damages against the CA in Y and CA in X.
1 The A Corporation in X would like to file a suit before a court seeking damages against the CA in Y.
(1) Which law will apply to this case?
(2) Which court will have jurisdiction?
(3) What will be the requirements for the A Corporation in X to win the case?
(4) Suppose there is an escape clause in CPS of the CA in Y that "The CA does not assume any liability over 2,000 US dollars." The A Corporation in X suffered damages of 200,000 US dollars. Is such indemnification clause valid to the A Corporation? Can the A

Corporation in X win the 200,000 US dollars?

Suppose there is an escape clause in CPS of the CA in Y that " The CA does not assume any liability in any event." Can the A Corporation in X win the case?

(5) Suppose there is a statute of limitation clause in CPS of the CA in X that "The party shall claim to the CA within one year after the event occurred." Can the A Corporation in X file a suit before a court against the CA in Y after one year it suffered damage?

2 The A Corporation in X would like to file a suit before a court seeking damages against the CA in X. Can the A Corporation in X to win the case?

China:

1(1) As there is no agreement between A Corporation and the CA in Y, this is a tort case. In this case, A Corporation has suffered its damage result in X (China). Accordingly, X law (Chinese law) shall apply to this case. Governing law of tort in China shall be the law of place where the plaintiff has suffered damage..

(2) As there is no agreement between A Corporation and the CA in Y, this is a tort case. In this case, (a) a court in China will have jurisdiction if the CA in Y has an office in X (China). (b) If the CA in Y does not have an office in China, the conduct or the damage is in China.

(3)A Corporation will seek for the CA's tort liability in accordance with the Chinese law.

(4)This is the case where no contractual relationship is recognized between the recipient (A Corporation) and the CA in Y. In such case, the parties concerned are not bound by the escape clause at all. A Corporation can seek for its damage against the CA in Y in accordance with the Chinese Tort Law. However, an escape clause might have an impact to reduce the scope of the liability.

(5)This is the case where no contractual relationship is recognized between the recipient (A Corporation) and the CA in Y. In such case, the parties concerned are not bound by the escape clause at all. A Corporation can seek for its damage against the CA in Y in accordance with the Chinese Tort Law after one year has passed. Because the statute of limitation is 2 years in accordance with the relating Chinese law.

2 It is difficult to seek for the contractual and tort liability of CA in X(China). Because the CA in X(China) was not negligent.

Japan:

1(1) As there is no agreement between A Corporation and the CA in Y, this is a tort case. Horei (The Act concerning the Application of Laws) Sec. 11.1 provides that: "The formation and effect of obligations due to agency of necessity, unjust enrichment or tort shall be governed by the law of the place where the fact causing the obligation has occurred." Then the issue is what is "the fact causing the obligation." Although "the fact" may include conduct and damage, "the fact causing the obligation" is in general interpreted as suffering damage. Therefore, the governing law for torts in Japan shall be the law of place where the plaintiff has suffered damage. In this case, A Corporation has suffered its damage in X (Japan). Accordingly, X law (Japanese law) shall apply to this case. (Dispute Resolutions for Cross-Border E-Commerce by

Asia PKI Forum. P58).
(2) As there is no agreement between A Corporation and the CA in Y, this is a tort case. As there is no international jurisdiction agreement between the CA and A Corporation, internal jurisdiction rules shall apply to the determination of international jurisdiction and that the Japanese jurisdiction shall be denied if there is a particular circumstance (Japanese Supreme Court on Octboer16, 1981 and November 11, 1997) (Dispute Resolutions for Cross-Border E-Commerce by Asia PKI Forum. P62). In this case, (a) a court in Japan will have jurisdiction if the CA in Y has an office in X (Japan) (Japanese Civil Procedure Code Sec. 4.5). (b) If the CA in Y does not have an office in Japan, a court in Japan where there is a domicile of the representative or principal person in charge of business operation shall have jurisdiction (Japanese Civil Procedure Code Sec. 4.5). (c)If the CA in Y has neither an office in Japan nor representative or principal person, a court of the place where the obligation is to be performed will have jurisdiction (Japanese Civil Procedure Code Sec. 5.1).
(3) A Corporation will seek for the CA's tort liability in accordance with the Japanese law.
(4) This is the case where no contractual relationship is recognized between the recipient (A Corporation) and the CA in Y. In such case, the parties concerned are not bound by the escape clause at all. A Corporation can seek damages against the CA in Y in accordance with the Japanese Tort Law. However an escape clause might have an impact to reduce the scope of the liability. (Answer to the Request 2-2-3(1)).
(5) This is the case where no contractual relationship is recognized between the recipient (A Corporation) and the CA in Y. In such case, the parties concerned are not bound by the escape clause at all. A Corporation can seek damages against the CA in Y in accordance with the Japanese Tort Law after one year has passed as the statute of limitation is 3 years in accordance with the Japanese Civil Code Sec. 724.
2 It is difficult to seek for the contractual and tort liability of CA in X because the CA in X was not negligent.

Korea:

1(1) As there is no contract between Corporation A and the CA of Country Y, it constitutes a tort case. In this case the governing law of tort is the law of the place where the wrongful act was perpetrated (Clause 1 of Article 32 of the international private law). In the case of remote tortious act, i.e. if the place where tort was perpetrated is different from the place where the result of the tort occurs, both places are regarded as places of tort (Supreme Court March 22, 1983 Judgment 82 Da-Ka 1533 Plenary session decision, etc.:1983. 3. 22. 82 1533). Though there is no Supreme Court decision as to the relationship of both parties, however, some lower court decisions have it that the plaintiff, who is the injured party, can choose a law favorable to him/her, and there is also a predominant support for it. In this case the place of act is Country Y, and the place of result is Country X, i.e. Korea. Therefore, if Corporation A takes the case to a Korean court, Corporation A may choose one of the two laws to its advantage.
(2) If there is no agreement on jurisdiction, the international trial jurisdiction shall be determined in accordance with Article 2 of the international private law. However, since Article 2 of the international private law stipulates only abstract principles, those provisions of the Korean Civil Procedure Code related to domestic territorial jurisdiction shall be referred to, and if Korea has territorial jurisdiction, Korea shall have general jurisdiction over international trials, unless there is any special reason against it.
In this case, (a) if the CA of Country Y has the main office or agency in Korea, or the person in

charge at the CA has an address in Korea, it will have jurisdiction (Korean Civil Procedure Code Sec. 5.2). (b) If the place of duty-fulfillment is Korea, the Korean court will have jurisdiction. (c) Even if the above cases are not applicable, if the CA of Country Y has seizable properties in Korea, the Korean Court shall have jurisdiction (Korean Civil Procedure Code Sec. 11).
(3) Regardless of whether contractual or tort liability is claimed, the requirements of the applicable proper law determined in accordance with (1) above must be satisfied.
(4) Such an escape clause must be validated in accordance with the governing law determined by (1) above.
(5) Whether the period of extinctive prescription can be claimed must be decided in accordance with the governing law determined in accordance with (1) above.

Singapore:

We assume that the CA in X (Singapore) cross certified the CA in Y, i.e. when A Corporation checks Y's own certificate, it will see that X has signed Y's certificate, and since it trusts X (which is a licensed CA in Singapore), it can verify Y's identity. The CA in Y remains the issuing CA for P (B) and although A relies on CA Y's certification of P (B), there is no contractual relationship between A and CA Y.

Same answer as 4-2 accordingly since cause of action is for CA Y's negligence.

Chinese Taipei:

1 (1): In the absence of any contractual agreement between A Corporation and the CA in Y, the cause of actions shall be based on tort theory. For actions arising out of the tortious act, the law of the place of the tortious conduct shall be the governing law. However, this shall not apply where such act is not considered to be tortious under the law of Taiwan (Article 9 of Private International Law) (Please also refer to: Dispute Resolutions for Cross-Border E-Commerce by Asia PKI Forum, Answers to Request 15). There is no bright rule on whether the place of tortious conduct refers to the place of the commission of the wrongful act or the place of the damages. The courts in Taiwan seem to accept both theories as the place of tortious conduct.

(2): In the absence of any contractual agreement between A Corporation and the CA in Y, the cause of actions shall be based on tort theory. A court in Taiwan has jurisdiction where the cause of action arises in torts and the tortious act occurred in Taiwan (Article 15 of Codes of Civil Procedures).

(3): A Corporation shall seek for tort liability for claims against the CA.

(4): Assuming the rule of Taiwan applies: there is no bright rule regarding whether the CPS may be enforceable against a relying party. In the absence of any contractual relationship between the A Corporation and the CA in Y, the indemnification clause is not legally enforceable against A Corporation. A Corporation may have cause of actions against the CA in Y based on the tort law. However, if the CPS is construed to bind both the certificate users and the relying party under applicable law, the indemnification clause may be valid against A Corporation. (See also answers to Request 2-2)

(5): Assuming the rule of Taiwan applies: under Article 147 of the Civil Code in Taiwan, the statute of limitation is non-waivable nor modifiable. Under Article 197 of the Civil Code, the statute of limitation for torts is 10 years from occurrence of the tortious conduct, 2 years from plaintiff's identification of the tortfeasor or awareness of the damages suffered from the tortious conduct.
2. In the absence of any finding of negligence on the part of CA in X`, A Corporation probably will not have a triable claim against the CA in X.

Request 6-2: Negligence in authentication, Validity of CPS to Relying Party (Plaintiff: B Corporation in Y)

The CA in X did not conduct the authentication of the A Corporation in X with reasonable care and issued certificates to the A Corporation.

In this case, a certain "P Corporation" impersonated the A Corporation. Due to this spoofing (impersonation), the CA in X was driven to issue a Certificate to the "P Corporation " that was impersonating A Corporation. As the B Corporation relied on the certificate issued to "A Corporation", it remitted the fund for the computer goods to the designated account.

However, "A Corporation", actually P Corporation, never supplied the computer goods and disappeared. A Corporation negated the contract formation between A Corporation and B Corporation.

The B Corporation in Y would like to file a suit seeking damages against the CA in X.

(1) Which law will apply this case?

(2) Which court will have jurisdiction?

(3) What will be the requirements for the A Corporation in X to win the case?

(4) Suppose there is an escape clause in CPS of the CA in X that "The CA does not assume any liability over 2,000 US dollars." The B Corporation in Y suffered damages of 200,000 US dollars. Can the CA in X provide its defense of the validity of such indemnification clause to the B Corporation?

Suppose there is an escape clause in CPS of the CA in X that " The CA does not assume any liability in any event." Can the CA in X provide its defense of the validity of such CPS to the B Corporation?

(5) Suppose there is a statute of limitation clause in CPS of the CA in X that "The party shall claim to the CA within one year after the event occurred." Can the CA in X provide its defense of such statute of limitation after one year the B Corporation suffered damage?

China:

1(1) As there is no agreement between B Corporation and the CA in X, this is a tort case. Therefore, governing law of tort shall be the law of place where the plaintiff has suffered damage. In this case, B Corporation has suffered its damage in Y. Accordingly Y law shall apply to this case.

(2) As there is no agreement between B Corporation and the CA in X, this is a tort case. As there is

no international jurisdiction agreement between the CA and B Corporation, internal jurisdiction rules shall apply to the determination of international jurisdiction. In this case, whether a court in Y will have a jurisdiction over the dispute will depend on Y law.

(3)B Corporation will seek for the CA's tort liability in accordance with Y law.

(4)This is the case where no contractual relationship is recognized between the recipient (B Corporation) and the CA in X. In such case, it will depend on Y law to determine whether the parties concerned are not bound by the escape clause.

(5)This is the case where no contractual relationship is recognized between the recipient (B Corporation) and the CA in X. In such case, it will depend on Y law to determine whether the parties concerned are not bound by the escape clause.

Japan:

1(1) As there is no agreement between B Corporation and the CA in X, this is a tort case. Horei (The Act concerning the Application of Laws) Sec. 11.1 provides that: "The formation and effect of obligations due to agency of necessity, unjust enrichment or tort shall be governed by the law of the place where the fact causing the obligation has occurred." Then the issue is what is "the fact causing the obligation." Although "the fact" may include conduct and damage, "the fact causing the obligation" is in general interpreted as suffering damage. Therefore, the governing law of tort shall be the law of place where the plaintiff has suffered damage. In this case, B Corporation has suffered its damage in Y. Accordingly Y law shall apply to this case. (Dispute Resolutions for Cross-Border E-Commerce by Asia PKI Forum. P58).

(2) As there is no agreement between B Corporation and the CA in X, this is a tort case. As there is no international jurisdiction agreement between the CA and B Corporation, internal jurisdiction rules shall apply to the determination of international jurisdiction. Japanese Civil Procedure Code Sec. 4. provides that: "a suit shall be subject to the jurisdiction of the court governing the place of the defendant's general forum." Sec.4.4 provides that: "The general forum of a judicial person or any other association or foundation shall be determined by the location of its principal office or principal place of business, or when there is no such office or place of business, by the domicile of the representative or principal person in charge of its affairs."

In this case, as A Corporation is a "judicial person," a Japanese court will have a jurisdiction over the dispute if B Corporation files a claim before a Japanese court.

Whether a court in Y will have a jurisdiction over the dispute will depend on Y law.

(3) B Corporation will seek for the CA's tort liability in accordance with Y law.

(4) This is a case where no contractual relationship is recognized between the recipient (B Corporation) and the CA in X. In such a case, it will depend on Y law to determine whether the parties concerned are not bound by the escape clause.

(5) This is a case where no contractual relationship is recognized between the recipient (B Corporation) and the CA in X. In such a case, it will depend on Y law to determine whether the parties concerned are not bound by the escape clause.

Korea:

1(1) As there is no agreement between Corporation B and the CA in X, this is a tort case.

Therefore, the governing law of tort shall be the law of place where the wrongful act was perpetrated (Clause 1 of Article 32 of the international private law). In the case of remote tortious act, i.e. if the place where tort was perpetrated is different from the place where the result of the tort occurs, both places are regarded as places of tort (Supreme Court March 22, 1983 Judgment 82 Da-Ka 1533 Plenary session decision, etc.). Though there is no Supreme Court decision as to the relationship of both parties, however, some lower court decisions have it that the plaintiff, who is the injured party, can choose a law favorable to him/her, and there is also a predominant support for it. In this case the place of action is Country Y, and the place of result is Country X, i.e Korea. Therefore, if Corporation A takes the case to a Korean court, Corporation A may choose one of the two laws to its advantage.

(2) If there is no agreement on jurisdiction, the international trial jurisdiction shall be determined in accordance with Article 2 of the international private law. However, since Article 2 of the international private law stipulates only abstract principles, those provisions of the Korean Civil Procedure Code related to domestic territorial jurisdiction shall be referred to, and if Korea has territorial jurisdiction, Korea shall have general jurisdiction over international trials, unless there is any special reason against it.

The Korean Civil Procedure Code stipulates that, if the corporation has the main office or agency in Korea, Korea shall have general jurisdiction (Korean Civil Procedure Code Sections 2 and 5.1). Therefore, in this case, if the CA of Country X (Korea) has a main office or an agency in Korea, Korea shall have general jurisdiction.

(3) The requirements of the governing law determined in accordance with (1) above must be satisfied.

(4) Such an escape clause must be validated in accordance with the governing law determined by (1) above.

(5) Whether the period of extinctive prescription can be claimed must be decided in accordance with the governing law determined in accordance with (1) above.

Singapore:

We assume that the CA in X (Singapore) cross certified the CA in Y, i.e. when A Corporation checks Y's own certificate, it will see that X has signed Y's certificate, and since it trusts X (which is a licensed CA in Singapore), it can verify Y's identity. The CA in Y remains the issuing CA for P (B) and although A relies on Y's certification of P (B), there is no contractual relationship between A and Y.

In this situation cause of action is for CA X's negligence.

1) a tort action (ie for negligence) is most likely to be governed by the law of X (Singapore) where the majority of the negligent acts occurred (ie the issuance of A Corporation's certificate to P).

2) The Singapore courts will have jurisdiction.

3) B must show that X was negligent in issuing the certificate to P.

4) If CA in X is a licensed CA, it can limit its liability to US$2,000 which is the reliance limit stated in its CPS

5) This will depend whether the one year limit of liability clause is held by the court to be reasonable.

Chinese Taipei:

1 (1): In the absence of any contractual agreement between B Corporation and the CA in X, the cause of actions shall be based on tort theory. For actions arising out of the tortious act, the law of the place of the tortious conduct shall be the governing law. However, this shall not apply where such act is not considered to be tortious under the law of Taiwan (Article 9 of Private International Law) (Please also refer to: Dispute Resolutions for Cross-Border E-Commerce by Asia PKI Forum, Answers to Request 15). There is no bright rule on whether the place of tortious conduct refers to the place of the commission of the wrongful act or the place of the damages. The courts in Taiwan seem to accept both theories as the place of tortious conduct.

(2): In the absence of any contractual agreement between B Corporation and the CA in X, the cause of actions shall be based on tort theory. A court in Taiwan has jurisdiction where the cause of action arises in torts and the tortious act occurred in Taiwan (Article 15 of Codes of Civil Procedures). Also, a court in Taiwan has general jurisdiction against the CA, and the forum will be its principal office in Taiwan (Article 2 of Codes of Civil Procedures).

(3): B Corporation shall seek for torts liability for claims against the CA.

(4): Assuming the rule of Taiwan applies: there is no bright rule regarding whether the CPS may be enforceable against a relying party. In the absence of any contractual relationship between the B Corporation and the CA, the indemnification clause is not legally enforceable against B Corporation. B Corporation may have cause of actions against the CA based on the tort law. However, if the CPS is construed to bind both the certificate users and the relying party, the indemnification clause may be validly enforceable against B Corporation. (See also answers to Request 2-2)

(5): Assuming the rule of Taiwan applies: under Article 147 of the Civil Code in Taiwan, the statute of limitation is non-waivable nor modifiable. Under Article 197 of the Civil Code in Taiwan, the statute of limitation for torts is 10 years from occurrence of the tortious conduct, 2 years from plaintiff's identification of the tortfeasor or awareness of the damages suffered from the tortious conduct.

Request 6-3: Communication failure

There was a communication failure between CA in X and CA in Y due to the negligence of the ISP (Internet Service Provider) with whom the CA in X entered into an agreement.
A Corporation in X suffered damage.
(1) Can the A Corporation win the case against the CA in X?
(2) Can the A Corporation win the case against the CA in Y?

China:

(1)Chinese law applies to this case. A Corporation cannot win the case because CA in X was not negligent.

(2) If Y law applies to this case, it will depend on Y law. If Chinese law applies to this case, A Corporation cannot win the case because CA in Y was not negligent.

Japan:

(1) Japanese law applies to this case. A Corporation cannot win the case because CA in X was not negligent.

(2) If Y law applies to this case, it will depend on Y law. If X (Japan) law applies to this case, A Corporation cannot win the case because CA in Y was not negligent.

Korea:

(1) Korean law applies to this case. A Corporation cannot win the case because CA in X was not negligent.

(2) If Y law applies to this case, it will depend on Y law. If X (Korean) law applies to this case, A Corporation cannot win the case because CA in Y was not negligent.

Singapore:

It is not clear here what effect the communications failure had on the transaction. A (and in the second case B) relied on the issuing CA's certification of P (as B and A respectively). Even if A (or B) had checked the certificate by accessing CA Y's (or CA X's) repository online, it would have arrived at the same answer ie P is B (or A).

Chinese Taipei:

Subsection 5, Section 1, Chapter 1, Part II of the Civil Code of Taiwan regulates the tortious acts of a party. A party is not liable for a third party's act in general, unless otherwise specified by laws to impose vicarious liability when certain relationship between the party and the third party exists. Absent such relationship, a party is not liable for another's wrongful act. Thus, a CA will not bear any vicarious liability for a third person absent any special relationship the existing law imposed on it.

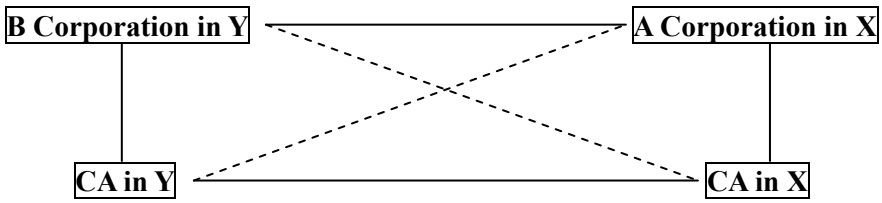
On the other hand, in an extreme case, a CA may be liable for its negligent in entrusting an ISP that has bad reputation in providing the services. If so, under the joint and several liability theory, a CA may be found liable jointly and severally with a third person (the ISP here) if it is found negligent in causing the damages to a party concurrently. The CA may not escape the liability simply because it acting negligently concurrently with a third party.

Other than actions based on tort theory, a CA and its users are free to regulate the liability in their contract agreement.

Request 7: (Cross-Border E-Commerce using "Cross Recognition" provided by Inter-Operability Working Group of ASIA PKI Forum)

Suppose that there is a company called A Corporation in your country/area which we will call X. A Corporation would like to supply computer goods to B Corporation in Y.
The A Corporation in X and the B Corporation in Y have agreed to conduct their exchange of contracts and communications through Internet using PKI.

According to the Inter-Operability Guideline provided by Asia PKI Forum, the CA in X sends its information to CA in Y so as to retain the name of CA in X in the list into CA in Y's repository and vice versa.
When A Corporation in X receives a digital message from B Corporation using PKI, the A Corporation looks into the repository of CA in Y. If the A Corporation finds the name of CA in X in the repository, the A Corporation can verify the validity of the Certificate issued by CA in Y.
Because CA in X with whom the A Corporation in X has entered into an agreement exchanges its Certificate pursuant to the mutual agreement between the CA in X and the CA in Y.
Is there is any difference in legal point of view in comparison to the Request 6?



China:
As the same as the Request 6.

Japan:
There is no difference compared with the Request 6.
.

Korea:
There is no difference compared with the Request 6.

Singapore:
There is no difference compared with the Request 6, since A relies on the Issuing CA's (negligent) certification of P rather than the Cross certifying CA's certification of the Issuing CA.

Chinese Taipei:
There seems no difference as compared with the Request 6.

Request 8: (Privacy Protection)

Please explain the laws or regulations concerning "Privacy Protection" in your country/area in several pages.

(In conducting the study on "Legal issues on new security technologies" from August 2005 till July 2006, it will be necessary to know the status quo of privacy laws in Asia).

China:

There is no specific law or regulation concerning privacy protection. However, there are 24 laws and regulations, including civil procedure code and general principle of civil law, mentioned the privacy protection. In addition, more than 30 judicial interpretations and over 210 department regulations all have the relevant contents about privacy protection.

Japan:

There have been court cases concerning privacy since 1964 in Japan. Invasion of privacy has been regarded as tort set forth in Japanese Civil Code. Japan has enacted Personal Information Protection Act since 2003.

Korea:

Please see the Request 2-4

Korea has "Act on Promotion of Information and Communications Network Utilization and Information Protection, etc." (This law was revised at a last year December 30.)

Singapore:

Chinese Taipei:

The law is attached in the appendix.

(Appendix)

Japan: **Personal Information Protection Act(2003)**

Chinese Taipei: **Computer-Processed Personal Data Protection Law** (1995.08.11 Announced)

Personal Information Protection Act (2003) (Japan)

Table

Chapter 1 General Rules

Article 1 (Purpose)

As highly-networked information and communication society has developed, Personal Information has come to be widely utilized in many sectors. In the circumstances, this Law, while taking into account the usefulness of Personal Information, aims to protect rights and interests of individuals by achieving the proper handling of Personal Information. To attain the purpose, this Law provides for the following matters: definition of the basic ideas, fundamental policy of the government, and other basic matters on the protection of Personal Informationetting of the duties and obligations of the central and local governments; and stipulation of the obligations to be observed by Entity handling Personal Information.

Article 2 (Definitions)

1 As used in this Law, “Personal Information” means information about living individuals that contains names, dates of birth, or other descriptions from which a specific individual can be identified. (Such Information shall also include information that can be easily checked against other information whereby a specific individual can be identified.)

2 As used in this Law, “Personal Information Database” means a group of information incorporating Personal Information, as listed below.

(1) Informationystematically organized so that Personal Information can be retrieved through the use of computers, and

(2) The information designated by cabinet orders as such for the reason of being systematically organized in a way that specific Personal Information can be easily retrieved.

3 As used in this Law, “Entity handling Personal Information” means any person that uses Personal Information Database in business, excepting:

(1) Central government organizations,

(2) Local government organizations,

(3) Independent Administrative Corporations (this term means any independent administrative corporation provided for in Article 2 Item 1 of the "Law for the Protection of Personal Information Possessed by Independent Administrative Corporations" (2003 Law No. 59), and hereinafter the same.), and

(4) Any other person designated by cabinet orders as such for the reason of being not likely to injure rights and interests of individuals in light of the volume of, and the methods of the use of, Personal Information handled by such person.

4 As used in this Law, "Personal Data" means Personal Information that makes up Personal Information Database.

5 As used in this Law, "Retained Personal Data" means Personal Data to which the Entity handling Personal Information is authorized to make correction, addition, deletion, suspension of use, erasure, or stopping of provision to third parties, provided, such Retained Personal Data shall not include any data designated by cabinet orders as such for the reason of being harmful to public or private interests if the existence thereof is disclosed, and any data to be erased within a period of one year or other lesser periods as designated by cabinet orders.

6 As used in this Law, "Specific Person" means, with respect to Personal Information, a specific individual who will be identified by such Personal Information.

Article 3 (Basic Idea)

Personal Information should be carefully handled under the philosophy that individual character must be respected, and thus, Personal Information shall be properly handled.

Chapter 2 Duties and Obligations of Central and Local Governments

Article 4 (Duties and Obligations of Central Government)

In accordance with the intention of this Law, the central government shall work out general measures necessary to secure proper handling of Personal Information, and shall be responsible for implementation of such measures.

Article 5 (Duties and Obligations of Local Governments)

In accordance with the intention of this Law, each local government shall, according to the character of its administrative district, work out general measures necessary to secure proper handling of Personal Information, and shall be responsible for implementation of such measures.

Article 6 (Legislative Actions)

1 The central government shall, with respect to its administrative organizations, in consideration of the nature of Personal Information under possession of such administrative organizations and the purpose of such possession, take legislative actions and other necessary actions to secure proper handling of such Personal Information.

2 The central government shall, with respect to Independent Administrative Corporations, in consideration of the nature of and the content of business of such Independent Administrative Corporations, take legislative actions and other necessary actions to secure proper handling of such Personal Information.

3 In addition to the actions provided for in the preceding two paragraphs, the central government shall, considering the nature of and methods of utilization of Personal Information, take legislative actions and other necessary actions to secure special protection with respect to Personal Information as may be required to be strictly handled in a proper manner for increased protection of rights and interests of individuals.

Chapter 3 Measures for Protection of Personal Information

Section 1 Basic Policy on Protection of Personal Information

Article 7

1 To implement measures for protection of Personal Information in a general and integrated manner, the central government shall work out a basic policy on protection of Personal Information (hereinafter called the "Basic Policy").

2 The Basic Policy shall provide for the following matters.

(1) Basic directions to implement measures for protection of Personal Information.

(2) Detailed matters of actions to be taken by the central government to protect Personal Information.

(3) Basic matters of actions to be taken by local government to protect Personal Information.

(4) Basic matters of actions to be taken by independent administrative corporations to protect Personal Information.

(5) Basic matters of actions for protection of Personal Information to be taken by Entity handling Personal Information and by Authorized Personal Information Protection Organizations provided for in Article 41 Item 1.

(6) Detailed matters of business to smoothly deal with complaints arising from or in relation to the handling of Personal Information.

(7) Other material matters to implement measures for protection of Personal Information.

3 The Prime Minister shall, after hearing opinions from the Social Policy Council, work out a proposed Basic Policy and seek approval by a Cabinet meeting for such Basic Policy.

4 Upon approval by a Cabinet meeting as provided for in the preceding paragraph, the Prime Minister shall publicly announce the Basic Policy without delay.

5 The provisions of the preceding two paragraphs shall also apply, with necessary modifications, to the amendment of the Basic Policy.

Section 2 Measures by Central Government

Article 8 (Support to Local Governments)

To support measures worked out or implemented by local governments in relation to the protection of Personal Information, and to support activities made by people or Entity handling Personal Information in relation to securing the proper handling of Personal Information, the central government shall take necessary actions including but not limited to supply of Informationetting of guidelines for proper and effective implementation of actions to be made by Entity handling Personal Information or by other persons.

Article 9 (Actions to Deal with Complaints)

The central government shall take necessary actions to properly and promptly deal with complaints arising between Entity handling Personal Information and any Specific Person in relation to handling of Personal Information.

Article 10 (Actions to Secure Proper Handling of Personal Information)

Through suitable sharing of functions with local governments, the central government shall take necessary actions to ensure that Personal Information will be properly handled by the Entity handling Personal Information as provided for in the next chapter.

Section 3 Measures by Local Governments

Article 11 (Protection of Personal Information in Possession of Local Governments)

Considering the nature of Personal Information in their possession and the purposes of such possession, local governments shall make efforts to take necessary actions to secure proper handling of such Personal Information.

Article 12 (Support to Entity handling Personal Information in Administrative Districts)

To secure proper handling of Personal Information, local governments shall make efforts to take necessary actions to support Entity handling Personal Information conducting business in and people residing in their administrative districts.

Article 13 (Good Offices for Dealing with Complaints)

To procure that complaints arising between Entity handling Personal Information and any Specific Person in relation to the handling of Personal Information will be dealt with appropriately and promptly, local governments shall make efforts to offer good offices or to take other necessary actions.

Section 4 Cooperation between Central Government and Local Governments

Article 14 The central government and local governments shall cooperate with each other in implementing measures for protection of Personal Information.

Chapter 4　Obligations of Entity handling Personal Information

Section 1　Obligations of Entity handling Personal Information

Article 15 (Definition of Utilization Purposes)

1　In handling Personal Information, the Entity handling Personal Information shall define the purposes to utilize such Personal Information, as clearly as possible (hereinafter called “Utilization Purposes”).

2　In case of making any change to Utilization Purposes, the Entity handling Personal Information shall not make such change beyond the extent considered to have reasonable relationships with such Utilization Purposes.

Article 16　(Limitation of Handling due to Utilization Purposes)

1 The Entity handling Personal Information shall not, without prior consent of Specific Person, handle any Personal Information beyond the extent necessary to achieve the Utilization Purposes defined in the preceding article.

2 Upon receipt of Personal Information from any other Entity handling Personal Information in the course of succession of business due to merger or other events, the Entity handling Personal Information shall not, without prior consent of Specific Person, handle such Personal Information beyond the extent necessary to achieve the Utilization Purposes which were in effect before such succession.

3 The provisions of the preceding two paragraphs shall not apply to the following cases.

(1) Where such handling of Personal Information is done according to laws and ordinances.

(2) Where such handling of Personal Information is needed to protect life or bodily safety of any person while difficult to obtain the Specific Person’s consent.

(3) Where such handling of Personal Information is specifically necessary to improve public health or to promote sound upbringing of juveniles while difficult to obtain the Specific Person’s consent.

(4) Where it is necessary to cooperate with state organizations or local governments, or with any other persons entrusted by them, in implementing the business stipulated by laws and ordinances while the Specific Person’s consent, if obtained, might hinder the implementation of such business.

Article 17　(Lawful Obtaining of Personal Information)

Any Entity handling Personal Information shall not obtain Personal Information by fraud or by other unlawful means.

Article 18　(Notification of Utilization Purposes)

1 The Entity handling Personal Information shall, if it has obtained any Personal Information, promptly notify the Specific Person of Utilization Purposes for such Personal Information or make public announcement of such Utilization Purposes. This provision shall not apply if such Utilization Purposes are publicly announced before obtaining of such Personal Information.

2 Notwithstanding the foregoing provision, the Entity handling Personal Information shall, before obtaining of Personal Information, notify the Specific Person of the Utilization Purposes in the following cases: where it obtains such Personal Information about the Specific Person from written instruments (which include electronic or magnetic records or other records made using such means as is unable to be perceived by humans, and hereinafter the same) produced in relation to any contract with such Specific Person; or where it obtains such Personal Information about the Specific Person from documents directly produced by such Specific Person. This provision, however, shall not apply in emergency cases that may require urgent protection of life, body, or property of any person.

3 In case of any change in Utilization Purposes, the Entity handling Personal Information shall notify the Specific Person of the changed Utilization Purposes or shall publicly announce the changed Utilization Purposes.

4 The provisions of the preceding three paragraphs shall not apply to the following cases.

(1) Where notification to the Specific Person or public announcement of such Utilization Purposes might be detrimental to life, body, property, or other interests of the Specific Person or of any third party,

(2) Where notification to the Specific Person or public announcement of such Utilization Purposes might be detrimental to the rights or legitimate benefits of the Entity handling Personal Information,

(3) Where the Entity handling Personal Information is required to cooperate with state organizations or local

governments in implementing the business stipulated by laws and ordinances while notification to the Specific Person or public announcement of the Utilization Purposes might hinder the implementation of such business, and

(4) Where in light of the circumstances under which Personal Information has been obtained, the Utilization Purposes are considered clearly recognizable.

Article 19 (Assuring the Preciseness of Data)

Within the extent necessary for achieving Utilization Purposes, the Entity handling Personal Information shall make efforts to keep the contents of Personal Data precise and up-to-date.

Article 20 (Actions for Security Control)

The Entity handling Personal Information shall take necessary and appropriate actions for security control of Personal Data it handles, including but not limited to protection from disclosure, loss, or destruction of such Personal Data.

Article 21 (Supervision of Employees)

In case of its employees handling Personal Data, the Entity handling Personal Information shall put such employees under its necessary and appropriate supervision in order to attain the security control of such Personal Data.

Article 22 (Supervision of Subcontractors)

In commissioning any subcontractor to handle Personal Data in whole or in part, the Entity handling Personal Information shall put such subcontractor under its necessary and appropriate supervision in order to attain the security control of such commissioned Personal Data.

Article 23 (Restriction on Provision to a Third Party)

1 The Entity handling Personal Information shall not provide a third party with Personal Data without prior consent of the Specific Person, except in the following cases.

(1) Where such provision is required by laws and ordinances.

(2) Where such provision is necessary to protect life, body, or property of an individual, and for some reason, it is difficult to obtain the Specific Person's consent.

(3) Where such provision is specifically necessary to improve public health or to promote sound upbringing of juveniles while difficult to obtain the Specific Person's consent.

(4) Where the Entity handling Personal Information is required to cooperate with state organizations, local governments, or the commissioned subcontractor in implementing their business provided for in laws and ordinances while the obtaining of the Specific Person's consent might hinder the implementation of such business.

2 Notwithstanding the foregoing paragraph, the Entity handling Personal Information may provide a third party with Personal Data if the Entity handling Personal Information previously agrees to stop, upon request by the Specific Person, providing a third party with Personal Data from which the Specific Person can be identified. This provision, however, shall not apply unless the Entity handling Personal Information previously notifies the Specific Person of the matters listed below or it previously puts such matters in a state that the Specific Person can easily know such matters.

(1) Utilization Purposes (the supply of such Personal Data itself shall be the Utilization Purposes in this case).

(2) Items of Personal Data provided to a third party.

(3) Methods or means of provision to the third party.

(4) Undertakings to stop, upon request by the Specific Person, providing a third party with the Personal Data from which the Specific Person can be identified.

3 In making any change to the matters set forth in Items 2 and 3 of the preceding paragraph, the Entity handling Personal Information shall previously notify the Specific Person of such change or previously put such change in a state that the Specific Person can easily know such change.

4 In the following cases, any person receiving the Personal Data shall not be deemed a third person in application of the preceding three paragraphs.

(1) Where the Entity handling Personal Information commissions such person to handle the Personal Data in whole or in part in the extent necessary to achieve Utilization Purposes.

(2) Where the Personal Data is provided to such person in the course of succession of business due to merger or for any other reason.

(3) Where the Personal Data is commonly utilized with any Specific Person, and the Entity handling Personal Information previously notifies the Specific Person of such common utilization, items of Personal Data commonly utilized, scope of such specific person, Utilization Purposes, and name or trade name of the person responsible for control of the Personal Data or previously puts such matters in a state that the Specific Person can easily know such matters.

5 In making any change to Utilization Purposes of such person, or to the name or trade name of the person responsible for control of the Personal Data, as provided for in Item 3 of the preceding paragraph, the Entity handling Personal Information shall previously notify the Specific Person of such change or previously put such change in a state that the Specific Person can easily know such change.

Article 24 (Public Announcement of the Matters Regarding Retained Personal Data)

1 With respect to the Retained Personal Data, the Entity handling Personal Information shall put the following matters in a state that the Specific Person can know such matters (which include a reply to the request by the Specific Person without delay).

(1) The name or trade name of the Entity handling Personal Information.

(2) The Utilization Purposes of all Retained Personal Data (except in cases coming under Article 18 Paragraph 4 Item 1 to Item 3).

(3) The procedures to respond to the request made under the provisions of the following paragraph, Paragraph 1 of the following article, Article 26 Paragraph 1, or Article 27 Paragraph 1 or Paragraph 2 (which include the amount of fees if such fees are set under Article 30 Paragraph 2).

(4) In addition to the matters set forth in the preceding three items, such matters designated by cabinet orders for reason of the necessity to secure proper handling of Retained Personal Data.

2 Upon request by the Specific Person, the Entity handling Personal Information shall notify the Specific Person without delay of the Utilization Purposes of Retained Personal Data from which the Specific Person can be identified, except in any of the following cases.

(1) Where such Utilization Purposes mentioned in the preceding paragraph are clear.

(2) Where the provisions of Article 18 Paragraph 4 Items 1 to 3 are applicable.

3 Upon decision not to notify such Utilization Purposes requested under the preceding paragraph, the Entity handling Personal Information shall notify the Specific Person to that effect without delay.

Article 25 (Disclosure)

1 Upon request by a Specific Person, the Entity handling Personal Information shall disclose without delay to the Specific Person the Retained Personal Data from which the Specific Person can be identified by means designated in cabinet orders (which include, if applicable, the notification that such Retained Personal Data is not available, and hereinafter the same). In any of the following cases, however, the Entity handling Personal Information may refrain from such disclosure in whole or in part.

(1) Where such disclosure might be detrimental to life, body, property, or other rights and interests of such Specific Person or any third party.

(2) Where such disclosure might substantially hinder the proper implementation of business of the Entity handling Personal Information.

(3) Where such disclosure might violate other laws and ordinances.

2 Upon decision not to disclose such Retained Personal Data, in whole or in part, requested under the preceding paragraph, the Entity handling Personal Information shall notify the Specific Person to that effect without delay.

3 If any provision of other laws and ordinances requires that the Retained Personal Data from which the Specific Person can be identified be disclosed in whole or in part to the Specific Person by means equivalent to those specified in Paragraph 1 of this article, the provision of that paragraph shall not apply to such Retained Personal Data in whole or in part.

Article 26 (Correction)

1 Upon request by the Specific Person for making corrections in, additions to, or deletions of Retained Personal Data (in this article,

hereinafter called “Corrections”) from which the Specific Person can be identified, alleging the incorrectness of the contents of such Retained Personal Data, the Entity handling Personal Information shall make necessary investigations without delay in the extent necessary to achieve the Utilization Purposes unless any other special procedure is provided for in other laws and ordinances in relation to such Corrections, and shall make corrections in the contents of such Retained Personal Data, depending upon the investigation results,

2 If it has made Corrections to the Retained Personal Data in whole or in part as provided for in the preceding paragraph, or if it has decided not to make such Corrections, the Entity handling Personal Information shall notify the Specific Person to that effect in writing without delay (Such notification shall include the contents of Correction, if made).

Article 27 (Stopping of Utilization)

1 With respect to the Retained Personal Data from which a Specific Person can be identified, if requested by such Specific Person to stop utilization of, or make deletion of, such Retained Personal Data for the reasons below (in this article, hereinafter called, “Stopping of Utilization”), and if such request is found to have good cause, the Entity handling Personal Information shall follow such request without delay in the extent necessary to correct such violations: such Retained Personal Data has been handled in violation of Article 16; or such Retained Personal Data has been obtained in violation of Article 17. However, if such Stopping of Utilization of the Retained Personal Data requires a lot of expense, or if it is difficult to do such Stopping of Utilization for other reasons, the Entity handling Personal Information shall not be required to follow such request; provided that it takes other necessary substitute actions to protect the rights and interests of the Specific Person.

2 With respect to the Retained Personal Data from which a Specific Person can be identified, if requested by such Specific Person to stop provision of such Retained Personal Data to a third party for the reason below, and if such request is found to have good cause, the Entity handling Personal Information shall follow such request without delay: such Retained Personal Data has been provided to a third party in violation of Article 23 Paragraph 1. However, if stopping of provision of such Retained Personal Data to a third party requires a lot of expense, or if it is difficult to do so for other reasons, the Entity handling Personal Information shall not be required to follow such request; provided that it takes other necessary substitute actions to protect the rights and interests of the Specific Person.

3 If it has made such Stopping of Utilization of the Retained Personal Data in whole or in part as requested under Paragraph 1 hereof, or if it has decided not to do so, or if it has stopped provision of the Retained Personal Data in whole or in part to a third party as requested under the preceding paragraph, or if it has decided not to do so, the Entity handling Personal Information shall notify the Specific Person to that effect without delay.

Article 28 (Explanation of Reasons)

In case of notifying under Article 24 Paragraph 3, Article 25 Paragraph 2, Article 26 Paragraph 2, or Particle 27 Paragraph 3 that it will not take actions, in whole or in part, requested by the Specific Person or that it will take other actions than those requested by the Specific Person, the Entity handling Personal Information shall make efforts to explain the reasons to the Specific Person.

Article 29 (Procedure to Submit Request for Disclosure)

1 With respect to the request under Article 24 Paragraph 2, Article 25 Paragraph 1, Article 26 Paragraph 1, or Particle 27 Paragraph 1 or Paragraph 2 (in this article, hereinafter called “Request for Disclosure”), the Entity handling Personal Information may, according to cabinet orders, determine the procedure for receiving the Request for Disclosure. In such case, the Specific Person shall follow such procedure in submitting the Request for Disclosure.

2 In receiving the Request for Disclosure, the Entity handling Personal Information may require that the Specific Person produce evidences enough to define the Retained Personal Data covered by the Request for Disclosure. In such case, the Entity handling Personal Information shall provide information helpful to define the Retained Personal Data and take other appropriate actions for convenience of the Specific Person so that the Specific Person can submit the Request for Disclosure without difficulty.

3 The Request for Disclosure may be submitted by any agent of the Specific Person according to the provisions of cabinet orders.

4 In determining the procedure for submitting the Request for Disclosure, the Entity handling Personal Information shall take into account that such procedure will not impose excessive burdens upon the Specific Person.

Article 30 (Fees)

1 For notification of the Utilization Purposes under Article 24 Paragraph 2 or for request for the disclosure under Article 25 Paragraph 1, the Entity handling Personal Information may collect fees to take actions set forth in such paragraph.

2 With respect to the collection of fees under the preceding paragraph, the Entity handling Personal Information shall decide the amounts of such fees within the reasonable limitation by considering the actual expenses incurred in taking such actions.

Article 31 (Dealing with Complaints)

1 The Entity handling Personal Information shall make efforts to properly and promptly deal with complaints arising in relation to the handling of Personal Information.

2 The Entity handling Personal Information shall make efforts to establish necessary systems to achieve the purpose of the preceding paragraph.

Article 32 (Request for Reports)

The competent minister may, within the necessary limitation to enforce the provisions of this section, require the Entity handling Personal Information to submit reports on handling of Personal Information.

Article 33 (Advice)

The competent minister may, within the necessary limitation to enforce the provisions of this section, render necessary advice to the Entity handling Personal Information on handling of Personal Information.

Article 34 (Recommendations and Orders)

1 If the Entity handling Personal Information violates any provision of Articles 16 to 18, Articles 20 to 27, or Article 30 Paragraph 2, the competent minister may, whenever necessary to protect individual's rights and interests, recommend that the Entity handling Personal Information cease such violation or take necessary actions to correct such violation.

2 If notwithstanding the recommendation under the preceding paragraph, the Entity handling Personal Information fails to take necessary actions without good cause, and as a result, the competent minister considers that any individual's rights and interests threaten to suffer material infringements, the competent minister may order the Entity handling Personal Information to take actions according to the recommendation.

3 If notwithstanding the provisions of the preceding two paragraphs, the Entity handling Personal Information violates any provision of Article 16, Article 17, Articles 20 to 22, or Article 23 Paragraph 1, and as a result, the competent minister consider it necessary to take immediate actions because of any threatened material infringement of individual's rights and interests, the competent minister may order the Entity handling Personal Information to cease such violation or to take necessary actions to correct such violation.

Article 35 (Limited Exercise of Powers of the Competent Minister)

1 In requesting reports, rendering advice, making recommendations, or issuing orders under the preceding three articles, the competent minister shall not interfere with any freedom of expression, academic freedom, freedom of conscience, or freedom of political activities.

2 In light of the purpose of the preceding paragraph, the competent minister shall not exercise its powers over any Entity handling Personal Information providing Personal Information to any person listed in each item of article 50 Paragraph 1; provided that such Personal Information is handled for the purpose provided for in each such item.

Article 36 (Competent Minister)

1 The competent minister under this section shall refer to such ministers as listed below. The Prime Minister, however, may appoint a specific minister or the National Public Safety Commission as such competent minister for any specific part of the business conducted by the Entity handling Personal Information relating to the handling of Personal Information (hereinafter called "the Minister") if the Prime Minister considers it necessary to do so for smoothly enforcing the provisions of this section.

(1) With respect to the employment management by the Entity handling Personal Information relating to the handling of Personal Information, the Minister of Health, Labor and Welfare (with respect to the employment management for sailors, the Minister of Land, Infrastructure and Transportation), and the minister holding jurisdiction over the business of such Entity handling Personal Information.

(2) With respect to the other business conducted by the Entity handling Personal Information relating to the handling of Personal Information than stipulated in the preceding item, the minister holding jurisdiction over the business of such Entity

handling Personal Information.

2 If the competent minister is appointed under the proviso of the preceding paragraph, the Prime Minister shall make public notice to that effect.

3 In enforcing the provisions of this section, the competent ministers shall closely communicate and cooperate with each other.

Section 2 Protection of Personal Information by Private Organizations

Article 37 (Authorization)

1 Any corporation (including an unincorporated organization having its authorized representative or manager, and in Item 3 (b) of the following article, the same) which desires to conduct any of the following business for securing the proper handling of Personal Information of the Entity handling Personal Information shall be entitled to authorization by the competent minister.

(1) Dealing with complaints according to Article 42 relating to the handling of Personal Information of the Entity handling Personal Information covered by the business (hereinafter called "Subject Entity").

(2) Provision of information to the Subject Entity in relation to the matters contributable to securing the proper handling of Personal Information.

(3) Any other business than stipulated in the preceding two items, such business being necessary to secure the proper handling of Personal Information of the Subject Entity.

2 Any person who desires authorization under the preceding paragraph shall apply to the competent minister as provided for in cabinet orders.

3 Upon issuance of authorization under Paragraph 1 hereof, the competent minister shall make public notice to that effect.

Article 38 (Incompetency)

Any person to whom any of the following provisions is applicable shall not be entitled to authorization under Paragraph 1 of the preceding article.

(1) A person who was sentenced to any punishment under this Law, and for whom not more than two years have elapsed after execution of such sentence or after relief from such execution.

(2) A person whose authorization was canceled according to Article 48 Paragraph 1, and for whom not more than two years have elapsed after such cancellation.

(3) A person any of whose officers (including an authorized representative or manager of said unincorporated organization) conducting the business of such person is:

a. A person who was sentenced to imprisonment or more severe punishment or sentenced to any punishment under this Law, and for whom not more than two years have elapsed after execution of such sentence or after relief from such execution.

b. In the case of a corporation whose authorization was canceled under Article 48 Paragraph 1, a person who served as an officer at such corporation for not more than 30 days before such cancellation, and for whom not more than two years have elapsed after such cancellation.

Article 39 (Standards of Authorization)

The competent minister shall not issue authorization unless it considers that the application under Article 37 Paragraph 1 satisfies the requirements of all the items below.

(1) The applicant shall propose necessary procedures to properly and reliably conduct business set forth in each item of Article 37 Paragraph 1.

(2) The applicant shall have knowledge, ability, and basic accounting expertise to properly and reliably conduct business set forth in each item of Article 37 Paragraph 1.

(3) Where the applicant is engaged in business other than those set forth in each item of Article 37 Paragraph 1, such engagement shall not be likely to cause unfair implementation of business set forth in each item of Article 37 Paragraph 1.

Article 40 (Notification of Abolition)

1 If a person authorized under Article 37 Paragraph 1 (hereinafter called "Authorized Personal Information Protection Organization") abolishes its authorized business (hereinafter called "Authorized Business"), such person shall notify the competent

minister to that effect in advance according to the provisions in cabinet orders.

2 Upon receipt of such notification under the preceding paragraph, the competent minister shall make public notice to that effect.

Article 41 (Subject Entity)

1 The Authorized Personal Information Protection Organization shall treat as its Subject Entity such Personal Information Protection Handler composing the Authorized Personal Information Protection Organization or any other Personal Information Protection Handler who agrees to handle the authorized business.

2 The Authorized Personal Information Protection Organization shall publicly announce the name or trade name of such Subject Entity.

Article 42 (Dealing with Complaints)

1 Upon receipt of request from any Specific Person for settlement of complaints about handling of Personal Information by any Subject Entity, the Authorized Personal Information Protection Organization shall offer necessary consultation or advice to the Specific Person, investigate the complaints-related circumstances, and notify the Subject Entity of details of the complaints and ask for prompt settlement.

2 Whenever necessary in its opinion with respect to the settlement of complaints under the preceding paragraph, the Authorized Personal Information Protection Organization may request written or oral explanations, or production of materials, from the Subject Entity.

3 Upon request by the Authorized Personal Information Protection Organization under the preceding paragraph, the Subject Entity shall not refuse to follow such request without good cause.

Article 43 (Guidelines for Protection of Personal Information)

1 The Authorized Personal Information Protection Organization shall make efforts to work out and to publicly announce guidelines for the Subject Entity to implement proper handling of Personal Information (hereinafter called “Guidelines for Protection of Personal Information”). Such Guidelines shall be made according to the purpose of this Law by addressing the definition of Utilization Purposes, actions for security control, procedures to accept requests from the Specific Person, and other necessary matters.

2 Upon public announcement of the Guidelines for Protection of Personal Information under the preceding paragraph, the Authorized Personal Information Protection Organization shall make efforts to make directions, recommendations, and other actions to ensure that the Subject Entity will comply with such Guidelines.

Article 44 (Prohibition of Utilization for Other Purposes)

The Authorized Personal Information Protection Organization shall not utilize any information that comes to its knowledge in the course of implementation of Authorized Business for any other purpose than for the Authorized Business.

Article 45 (Restriction on Use of the Name)

Any person that is not the Authorized Personal Information Protection Organization shall not use the name of “Authorized Personal Information Protection Organization” or any other name confusingly similar to such name.

Article 46 (Request for Reports)

In the extent necessary to enforce the provisions of this section, the competent minister may request the Authorized Personal Information Protection Organization to submit reports on its Authorized Business.

Article 47 (Orders)

In the extent necessary to enforce the provisions of this section, the competent minister may order the Authorized Personal Information Protection Organization to improve their methods of conducting Authorized Business, to make a change to the Guidelines for Protection of Personal Information, and to take other necessary actions.

Article 48 (Cancellation of Authorization)

1 If any of the following events occurs to the Authorized Personal Information Protection Organization, the competent minister may cancel authorization of such Organization.

(1) Article 38 Item 1 or 3 has become applicable to the Authorized Personal Information Protection Organization.

(2) The Authorized Personal Information Protection Organization has become nonconforming to any of the items of

Article 39.

(3) The Authorized Personal Information Protection Organization has violated the provision of Article 44.

(4) The Authorized Personal Information Protection Organization has not followed the order provided for in the preceding article.

(5) The Authorized Personal Information Protection Organization has obtained authorization under Article 37 Paragraph 1 by fraudulent means.

2 Upon cancellation of the authorization according to the preceding paragraph, the competent minister shall make public notice to that effect.

Article 49 (Competent Minister)

1 The competent minister under this section shall be such ministers as listed below. The Prime Minister, however, may appoint a specific minister as such competent minister for any specific person that desires to obtain authorization under Article 37 Item 1 if the Prime Minister considers it necessary to do so for smoothly enforcing the provisions of this section.

(1) With respect to the Authorized Personal Information Protection Organization that has received permission or approval for their establishment (such Organization includes the person that desires to obtain authorization under Article 37 Paragraph 1, and hereinafter, the same.), the minister who has issued such permission or approval.

(2) With respect to any other Authorized Personal Information Protection Organization than listed in the preceding item, the minister who has competent jurisdiction over the business conducted by any Subject Entity of such Authorized Personal Information Protection Organization.

2 If the competent minister is appointed under the proviso of the preceding paragraph, the Prime Minister shall make public notice to that effect.

Chapter 5 Miscellaneous Provisions

Article 50 (Exclusion from Application)

1 With respect to any Entity handling Personal Information listed in each item below, if the purpose in whole or in part of their handling Personal Information corresponds to the purpose set forth in each such item respectively, the provisions of the preceding chapter shall not apply.

(1) Broadcasting media, newspaper publishers, news agencies, or other new reporting organizations (including individuals engaging in news reporting business).

Purpose: Using in news reporting.

(2) Persons engaging in writing business.

Purpose: Using in writing books and other works.

(3) Universities and other academic institutions or organizations, or persons belonging to such institutions or organizations.

Purpose: Using in academic research.

(4) Religious organizations.

Purpose: Using in religious activities (including incidental activities).

(5) Political organizations.

Purpose: Using in political activities (including incidental activities).

2 As used in Item 1 of the preceding paragraph, the term “news reporting” means reporting of objective facts to the general public (such reporting shall include statement of opinions or views based upon such objective facts.).

3 The Entity handling Personal Information listed in each item of Paragraph 1 of this article shall take, at its expense, necessary actions to safeguard the Personal Data, to deal with complaints about handling of Personal Information, and to secure other proper handling of Personal Information, and shall make efforts to publicly announce the contents of such actions.

Article 51 (Business Implemented by Local Governments)

The business under the power of the competent minister as set forth in this Law may be delegated to the head or other executive

body of a local government for implementation, as provided for in cabinet orders.

Article 52 (Delegation of Power or Administration)

The business under the power or administrative control of the competent minister as set forth in this Law may be delegated to any personnel under the control of the competent minister, as provided for in cabinet orders.

Article 53 (Public Announcement of the Progress of Enforcement)

1 The Prime Minister may request relevant administrative organs to report on the progress of enforcement of this Law. Such relevant administrative organs shall mean: organs established in the Cabinet (excluding the Cabinet Office) and organs under the control of the Cabinet according to laws; Cabinet Office; Imperial Household Agency; organs provided for in the Cabinet Office Establishment Law (Law of 1999, No. 89) Article 49 Paragraphs 1 and 2; and organs provided for in the National Administrative Organization Law (Law of 1948, No. 120) Article 3 Paragraph 2, and hereinafter, the same.

2 In every fiscal year, the Prime Minister shall compile such reports mentioned in the preceding paragraph and shall publicly announce the summary of such reports.

Article 54 (Communication and Cooperation)

The Prime Minister and heads of administrative organs involved in the enforcement of this Law shall closely communicate and cooperate with each other.

Article 55 (Delegation to Cabinet Orders)

In addition to the matters stipulated in this Law, any necessary matter to enforce this Law shall be provided for in cabinet orders.

Chapter 6 Penal Provisions

Article 56

Any person who has violated orders issued under Article 34 Paragraph 2 or 3 shall be sentenced to six months or less of imprisonment or to 300,000 yen or less of fines.

Article 57 Any person who has failed to report as required by Article 32 or 46 or who has falsely reported shall be sentenced to 300,000 yen or less of fines.

Article 58

1 If any representative of a corporation (including an unincorporated organization having its authorized representative or manager, and hereinafter the same) or any agent, servant, or employee of a corporation or person has committed violations set forth in the preceding two articles in relation to business of such corporation or person, not only shall such actors be punished, but also such corporation or person shall be sentenced to fines according to such two articles.

2 If the provision of the preceding paragraph applies to any unincorporated organization, its representative or manager shall represent such unincorporated organization in relation to relevant proceedings, and in addition, criminal procedure laws applicable to a corporation if such corporation were named as defendant or suspect shall also apply with necessary modifications.

Article 59

Any person set forth below shall be sentenced to non-penal fines in the amount of 100,000 yen or less.

(1) A person who has failed to notify as required by Article 40 Paragraph 1 or who has falsely notified.

(2) A person who has violated the provision of Article 45.

Supplementary Provisions

Article 1 (Date of Enforcement)

This Law shall be enforced on the date of enactment. However, the provisions from Chapter 4 to Chapter 6 and the provisions from Article 1 to Article 6 in these Supplementary Provisions shall be enforced on the date designated by cabinet orders, such date, however, being within two years from the date of enactment.

Article 2 (Transitional Measure about Consent of Specific Person)

If any Specific Person has given any consent in relation to the handling of its Personal Information before enforcement of this Law, and such consent is equivalent to consent to handling the Personal Information for any purpose other than defined in Article 15

paragraph 1, the Specific Person shall be deemed to have given consent provided for in Article 16 Paragraph 1 or 2.

Article 3

If any Specific Person has given any consent in relation to the handling of its Personal Information before enforcement of this Law, and such consent is equivalent to the consent to disclosing to a third party the Personal Data set forth in Article 23 paragraph 1, the Specific Person shall be deemed to have given the consent provided for in such paragraph.

Article 4　(Transitional Measure about Notification)

With respect to any matters that the Entity handling Personal Information is required to notify the Specific Person, or to put in a state that the Specific Person can easily know such matters, according to the provision of Article 23 Paragraph 2, if such notification has been made to the Specific Person before enforcement of this Law, such notification shall be deemed to have been made under such paragraph.

Article 5

With respect to any matters that the Entity handling Personal Information is required to notify the Specific Person, or to put in a state that the Specific Person can easily know such matters, according to the provision of Article 23 Paragraph 4 Item 3, if such notification has been made to the Specific Person before enforcement of this Law, such notification shall be deemed to have been made under such paragraph.

Article 6　(Transitional Measure about Restriction on Use of the Name)

If any person was using the name of “Authorized Personal Information Protection Organization”, or any other name confusingly similar to such name, as of the date of enforcement of this Law, the provision of Article 45 shall not apply to such person for a period of six months from the enforcement of the provision of the same article.

Article 7　(Partial Revision of the Cabinet Office Establishment Law)

The Cabinet Office Establishment Law shall be partially revised as follows:

The following supplemental item shall be added after Article 4 Paragraph 3 Item 38.

“Item 38 (2)　Concerning the preparation and promotion of basic policy on the protection of Personal Information (such basic policy shall be the one provided for in Article 7 Paragraph 1 of the Law for the Protection of Personal Information (Law of 2003, No. 57).”

In Article 38 Paragraph 1 Item 1, “and promotion of civil activities” shall be revised to “promotion of civil activities and securing of proper handling of Personal Information”, and in Item 3 of the same paragraph, the wording of “and the Law for the Protection of Personal Information” shall be added to the end of “Law of 1973, No. 121”.

Computer-Processed Personal Data Protection Law (1995.08.11 Announced)(Chinese Taiepei)

Chapter I General Provisions

Article 1

This Law is enacted to govern the processing of personal data by computers so as to prevent infringement upon personal rights, and to facilitate the proper utilization of personal data.

Article 2

The protection of personal data shall be governed by the provisions of this Law, or governed by other laws if so provided in such other laws.

Article 3

The terms used herein denote the following meanings:

1.Personal data: the name, date of birth, I.D. Card number, characteristic, fingerprints, marital, family, educational, occupational, and health status, medical history, financial conditions, social activities of a natural person and other data which can serve to identify said specific person;

2.Personal data file: gathering of personal data through storage at magnetic storage or at other similar media for certain specific purpose;

3.Computer processing: to use computers or automatic machinery to key in, store, compile, correct, search, delete, output, or transmit data or process otherwise;

4.Collection: to collect personal data for the establishment of personal data file;

5.Utilization: refers to use of personal data file by government agency or non-government agency kept by it for internal use or for use by a third party other than the principal;

6.Government agency: refers to a government agency at the central government or local government level which is empowered to exercise sovereign power;

7.Non-government agency: refers to the following enterprises or groups or individuals other than those mentioned above:

(1) credit search businesses and groups or individuals whose major line of business is to collect or process personal data by computers;

(2) hospitals, schools, telecommunication, financial, securities, insurance, and mass communications industries; and

(3) other businesses, groups or individuals designated by the Ministry of Justice in conjunction with the government authority in charge of such industry at the central government level.

8.Principal: the individual to which the personal data belongs; and

9.Specific purpose: refers to those purposes prescribed by the Ministry of Justice in conjunction with the government authority in charge of the industry at the central government level.

Article 4

The following rights exercisable by the principal with regard to his personal data shall not be waived in advance nor limited by specific agreement:

1.any inquiry and request for review of the personal data thereof;

2.any request to make copies of the personal data thereof;

3.any request to supplement or correct the personal data thereto;

4.any request to discontinue processing of personal data by computers or utilization of personal data thereof; and

5.any request for deletion of personal data therefrom.

Article 5

Where a group or an individual is designated by a government agency or non-government agency to process data, the group or individual so designated to process data shall be considered part of the staff of said designating agency within the meaning of this Law.

Article 6

The collection or utilization of personal data shall respect the rights and interests of the principal and such personal data shall be handled in accordance with the principles of honesty and credibility so as not to exceed the scope of the specific purpose.

Chapter II Data Processing by The Government Agency

Article 7

The government agency shall not collect or process personal data unless it has a certain specific purpose which complies with at least one of the followings:

1.it is within the scope of job functions provided by laws and regulations;

2.a written consent has been obtained from the principal; and

3.there is no possibility that it shall infringe upon the rights and interests of the principal.

Article 8

The government agency shall utilize the personal data in accordance with the scope of its job functions provided by laws and regulations, and in compliance with the specific purpose of collection, provided, however, that it may utilize the personal data other than for the specific purpose upon occurrence of any of the following conditions:

1.such utilization is provided for in the laws and regulations;

2.such utilization is justifiable and for internal purpose only;

3.such utilization shall safeguard the national security;

4.such utilization shall improve public interests;

5.such utilization shall eliminate any emergency danger which could endanger the principal's life, body, freedom or property;

6.such utilization shall prevent the rights and interests of another from being seriously damaged, and there is a need to utilize the same;

7.such utilization shall serve academic study purposes and the material interests of the principal will not be adversely affected;

making, correction or review. The classification of personal date referred to in Item 5 above shall be prescribed by the Ministry of Justice with the government authority in 8.such utilization shall benefit the rights and interests of the principal; and

9.such utilization has the written consent of the principal.

Article 9

The international transmission and utilization of personal data by the government agency shall be handled in accordance with relevant laws and regulations.

Article 10

A government agency which keeps personal data file shall announce the following in a government gazette or by other proper means; the above provisions apply to any amendment thereof:

1.name of personal data file;

2.name of the government agency keeping the personal data file;

3.name of the government agency utilizing the personal data file;

4.basis on which the personal data file is kept and the specific purpose for keeping the file;

5.classification of personal data;

6.scope of personal data;

7.means of collecting personal data;

8.places where personal data are normally transmitted and recipient of said data; and

9.the direct recipient of personal data transmitted through international channel; and

10. name and address of government agency accepting applications for inquiries charge of the industry at the central government level.

Article 11

The provisions of the preceding article have no application to utilization of the following personal data file:

1.where national security, foreign affairs and military secrets, overall economic interests or other major national interests are involved;

2.where cases are being reviewed by the grand justice of the Judicial Yuan, or cases are being reviewed by the Government Official Disciplinary Committee, and matters under investigation, trial, judgment, enforcement or handling of non-litigious matters by court;

3.where matters relevant to precautionary measures against criminal offenses, criminal investigation, enforcement, correction or protective measures or rehabilitation affairs are involved;

4.where matters relevant to administrative punishment and compulsory enforcement thereof are involved;

5.where matters relevant to administration of entry/exit of the country, security check or investigation and verification of refugees are involved;

6.where matters relevant to collection of taxes and dues are involved;

7.where matters relevant to personnel, job duties, salary payment, sanitation, welfare or other relevant issues of a government agency are involved;

8.where the personal data file is used for computer processing for experimental purpose;

9.where deletion will be made prior to announcement in the government gazette;

10. where the name, address, exchange of money and articles of the principal is recorded for the purpose of official contacts;

11. where a personal data file is specifically produced by the government official for performance of duties for internal use in said government agency; and

12. where laws and regulations specify otherwise.

Article 12

With regard to the personal data files kept by the government agency, the said government agency shall, at the request of the principal, reply to his inquiry, provide files for his review, or make copies of the files for him, provided, however, that the above provisions do not apply to any of the following:

1.where the file shall not be made public pursuant to the provisions of the preceding article;

2.where the performance of official duties may be interfered with; and

3.where the material interests of a third party may be adversely affected.

Article 13

The government agency shall maintain the accuracy of personal data, and shall make corrections or supplements thereto in accordance with its duty or at the request of the principal.

In the event there is a dispute about the accuracy of personal data, the government agency shall, pursuant to its duty or at the request of the principal, discontinue the computer processing or utilization thereof, provided, however, that the above provisions do not apply to a situation where the processing or utilization is necessary for performance of an official duty, and the dispute is specifically identified or a written consent is obtained from the principal.

In the event the specific purpose for processing the personal data no longer exists or the period for processing has expired, the government agency shall, pursuant to its duty or at the request of the principal, delete or discontinue the processing or utilization of said personal data, provided, however, that the above provisions do not apply to a situation where the processing or utilization thereof is necessary for performance of an official duty, or the use purpose is changed pursuant to the provisions of this Law or a written consent is obtained from the principal.

Article 14

The government agency shall maintain a book to record all the particulars required to be made public pursuant to the provisions of Paragraph 1 of Article 10 hereinabove for review.

Article 15

Where a request is made by the principal to the government agency pursuant to the provisions of this Law, it shall be handled

within thirty days. Where said request is not handled within the aforesaid time period, a written notice stating the reason said request was not handled shall be sent to the principal.

Article 16

The government agency may charge a fee to those who make an inquiry or request to review, or make a copy of the personal data.

The amount of the fee shall be prescribed by the said government agency.

Article 17

The government agency which keeps personal data files shall, pursuant to relevant laws and regulations, appoint a full time employee to handle matters relevant to the security and maintenance of said files to prevent personal data from being stolen, altered without authorization, damaged, lost or disclosed.

Chapter III Data Processing by Non-government Agency

Article 18

A non-government agency shall not collect or process by computer any personal data unless it has some specific purpose and it complies with any of the followings:

1.where a written consent is obtained from the principal;

2.where an agreement or similar contractual relationship is entered into with the principal whereby the rights and interests of the principal shall not be infringed upon;

3.where the information is already known to the public and no material adverse effect will be caused to the interests of the principal;

4.where there is a need for academic study, and no material adverse effect will be caused to the interests of the principal; and

5.the provisions of Article 3, Item 7 Sub-item 2 of this Law and other laws and regulations otherwise specify.

Article 19

Any non-government agency which is not registered with the government authority in charge of the industry and does not have a license issued thereto pursuant to the provisions of this Law shall not collect, process by computer, make international transmission or utilize personal data.

Credit search industry and groups or individuals whose major line of business is to collect or process by computer personal data shall obtain a special permit from and register with the government authority in charge of the industry for issuance of a license.

The registration procedures, qualifications required for applying issuance of a special permit and handling fee referred to in the two preceding paragraphs shall be prescribed by the government authority in charge of the industry at the central government level.

Article 20

Those applying for registration referred to in the preceding article shall submit an application stating thereon the followings:

1.name, domicile and residential address of the applicant; if the applicant is a juristic person or a group of non juristic persons, the name, address of the head office and branch office(s), and the name, domicile and residential address of the statutory representative or administrator;

2.name of personal data file;

3.the specific purpose for keeping the personal data file;

4.classification of personal data;

5.scope of personal data;

6.period for keeping the personal data file;

7.method used for collecting personal data;

8.scope of utilization of personal data file;

9.the recipient who directly receives personal data through international transmission;

10. name of the person responsible for maintaining personal data file; and

11. security and maintenance plan for personal data file.

In the event there is any change to the entries of registration, an application for amendment registration shall be filed within 15 days after said change. In the event of termination of business operations, an application for terminating business operations shall be filed within one month after the cause of business termination occurs.

Those applying for termination of business operations shall report their method of handling personal data to the government authority in charge of the industry for approval.

The specific purpose referred to in Item 3 of Paragraph 1 and the classification referred to in Item 4 above shall be prescribed by the Ministry of Justice in conjunction with the government authority in charge of the industry at the central government level.

Article 21

After applications for registration filed pursuant to the provisions of the preceding Article are approved, the non-government agency shall list all the particulars referred to in Items 1 to 10 of Paragraph 1 of the preceding Article in the government gazette or by public notice in a local newspaper.

Article 22

The non-government agency shall maintain a book to record all the particulars referred to in Items 1 to 10 of Paragraph 1 of Article 20 for review.

Article 23

The non-government agency shall utilize the personal data within the scope of the specific purpose, provided, however, that it may utilize the personal data otherwise upon occurrence of any of the following:

1.such utilization shall improve public interests;

2.such utilization shall protect the life, body, freedom or property of the principal from imminent danger;

3.such utilization shall prevent the rights and interests of another person from sustaining material adverse effect; and

4.such utilization has the written consent of the principal.

Article 24

Where the international transmission or utilization of personal data by a non-government agency meets any one of the following criteria, the government agency in charge of the industry may limit the transmission and utilization thereof:

1.where major national interests are involved;

2.where national treaty or agreement specifies otherwise;

3.where the nation receiving personal data lacks laws which fairly protect the rights and interests of the principal thereby causing injury to the principal; and

4.where international transmission and utilization of personal data are made through a circuitous means in order to evade the provisions of this Law.

Article 25

Where the government authority in charge of the industry deems it necessary, it may send officials with identification certificates to any non-government agency which is subject to its jurisdiction and granting of a special permit or approval of registration and order such non-government agency to present relevant information with regard to matters provided by this Law or to take other necessary measures to comply with this Law, or to enter the premises of the non-government agency to conduct an investigation. In the event the investigations show the relevant information is in violation of the provisions of this Law, it may be confiscated.

With regard to the above order, investigation, or confiscation by the government authorities, the non-government agency shall not evade, obstruct or refuse.

Article 26

The provisions of Articles 12, 13, 15, 16 Paragraph 1 and 17 shall be applied mutatis mutandis to all non-government agencies.

The criteria for the charging of a fee by a non-government agency pursuant to the provisions of Paragraph 1 of Article 16 hereinabove shall be prescribed by the government authority in charge of the industry at the central government level.

Chapter IV Damages and Other Remedy

Article 27

A government agency which infringes upon the rights and interests of the principal and violates any provision of this Law shall be liable for the damages arising therefrom, provided, however, that the above provisions do not apply to damages arising from natural disaster, incident or other force majeure.

With regard to damages caused to non-property, the injured party may also request proper monetary compensation. With regard to damages of reputation, the injured party may also request the rehabilitation of his reputation.

The total amount of compensation for the damages referred to in the two preceding paragraphs shall not be less than NT$20,000 but not more than NT$100,000 for each case of damages per person, provided, however, that the above provisions do not apply to the situation where the injured party can prove that the damages sustained by it are more than the aforesaid prescribed amount.

With regard to damages caused to the principal by the same cause and fact, the total amount of compensation shall not be more than NT$20 million.

The right of claim referred to in the second Paragraph above shall not be transferred or inherited, provided, however, that these provisions do not apply to the situation where the monetary compensation is undertaken in an agreement or is claimed in a legal action.

Article 28

A non-government agency which infringes upon the rights and interests of a principal as a result of its violation of this Law shall be liable for the damages arising therefrom, provided, however, that these provisions do not apply to the situation where the non-government agency can prove that the damages are not caused by its willful conduct or negligence.

The provisions of Paragraphs 2 to 5 of the preceding Article are applicable to claims for damages made in accordance with the provisions of the preceding Paragraph.

Article 29

The right to claim damages is subject to a statute of limitation of two years calculated from the time the claimant has knowledge of the damages and the identity of the party liable for the damage arising therefrom or five years calculated from the date the damaged actually occurs.

Article 30

With regard to compensation for damages, apart from complying with the provisions of this Law, the government agency shall comply with the provisions of the State Compensation Law, while the non-government agency shall comply with the provisions of the Civil Code.

Article 31

Where a principal exercises his right prescribed in Article 4 hereinabove against a government agency, but the government agency refuses or fails to handle his case within the time period specified in Article 15 hereinabove, the principal may, within twenty days after refusal or upon expiry of the specified time period, file a written application with the supervising government agency requesting proper handling.

The supervising government agency shall, within two months after accepting said application, notify the principal in writing of the results of his application.

Article 32

Where a principal exercises his right prescribed in Article 4 hereinabove against a non-government agency, but the non-government agency refuses to handle his case, the principal may, within twenty days after refusal or upon expiry of the specified time period, file a written application with the government authority in charge of the industry requesting proper handling of his case.

The said government authority in charge of the industry shall, within two months after accepting said application, notify the principal of the results of his application. If the application is considered reasonable, the government authority in charge of the industry shall order the non-government agency to make corrections within the specified time period.

Chapter V Penalties

Article 33

A person who intends to make profits for himself by violating the provisions of Articles 7, 8, 18, 19 Paragraphs 1 & 2, and 23 hereinabove or the injunction order make in accordance with Article 24 hereinabove and cause injury to another shall be punished with an imprisonment of less than two years, detention or, in lieu thereof or in additional thereto, a criminal fine of less than NT$40,000.

Article 34

A person who intends to make unlawful gains for himself or for a third party or intends to infringe upon the interests of another by illegally outputting, interfering, changing, deleting personal data file or by other illegal means to impede the accuracy of personal data file thus causing damages to another shall be punished with an imprisonment for less than three years, or detention, or a fine of less than NT$50,000.

Article 35

A government official who takes advantage of his position, or opportunity or means available to him to commit the offenses prescribed in the two preceding articles shall be subject to punishments half as severe as those enumerated above.

Article 36

The offenses referred to in this Chapter may be instituted only upon complaint.

Article 37

In the event a more severe punishment is provided for in other laws with respect to the offenses outlined in this Chapter, the more severe punishment shall apply.

Article 38

Upon occurrence of any of the following, the government authority in charge of the industry shall impose an administrative fine of not less than NT$20,000 but not more than NT$100,000 on the responsible person, and order the said responsible person to take corrective measures within a specified time period. In the event the responsible person fails to take corrective measures within the specified time period after having been ordered to do so, the government authority in charge of the industry may continue to impose a fine each time a violation of any of the following occurs:

1.a violation of the provisions of Article 18 hereinabove;

2.a violation of the provisions of Article 19 Paragraph 1 or Paragraph 2 hereinabove;

3.a violation of the provisions of Article 23 hereinabove; and

4.a violation of the injunction order imposed in accordance with the provisions of Article 24 hereinabove.

In the event the degree of violations referred to in Item 1, 3 or 4 above is serious, an order to revoke the special permit or registration granted in accordance with this Law may be issued.

Article 39

Upon occurrence of any of the following, the government authority in charge of the industry may order the responsible person to take corrective measures within a specified time period. If corrective measures are not taken within the specified time period, an administrative fine of not less than NT$10,000 but not more than NT$50,000 may be imposed upon the responsible person each time a violation of any of the following occurs:

1. a violation of the provisions of Article 20 Paragraph 2 hereinabove;

2.a failure to place an announcement in the local newspaper which would cause a violation of the provisions of Article 21 hereinabove;

3.a violation of the provisions of Article 22 hereinabove;

4.a violation of the provisions of Article 12, 13, 15 and 17 in accordance with the provisions of Article 26 Paragraph 1 hereinabove; and

5.a violation of the criteria for fee charge provided for under Article 26 Paragraph 2 hereinabove.

In case the degree of violations referred to in Items 1, 2, 3, or 4 of the preceding Paragraph is serious, an order to revoke the special permit or registration granted in accordance with this Law may be issued.

Article 40

Upon occurrence of any of the following, the government authority in charge of the industry may impose an administrative fine of not less than NT$10,000 but not more than NT$50,000 on the responsible person each time a violation of any of the following occurs:

1.a failure to handle personal data pursuant to the means approved by the government authority in charge of the industry in accordance with Article 20 Paragraph 3 hereinabove;

2.a violation of the provisions of Article 25 Paragraph 2 hereinabove; and

3.a failure to comply with an order to take corrective measures issued in accordance with Article 32 Paragraph 2 hereinabove.

In the case the degree of violation referred to in Item 2 or 3 of the preceding Paragraph is serious, an order to revoke the special permit or registration granted in accordance with this Law may be issued.

Article 41

Failure to pay administrative fines imposed according to this Law shall cause the case to be referred to court for compulsory execution if fines are still not paid within the specified time period even upon due notice.

Chapter VI Supplementary Provisions

Article 42

The Ministry of Justice shall be responsible for coordinating and contacting matters relevant to the enforcement of this Law. Rules governing said coordination and contact shall be prescribed by the Ministry of Justice.

With regard to matters which are prescribed to be handled by the government authority in charge of the industry, if there is no such government authority in charge of the industry to handled the same, they shall be handled by the Ministry of Justice.

The administration governing the collection, computer processing, utilization of personal data, and registration, public announcement or other matters by non-government agency may be handled by public interests group designated by the Ministry of Justice or the government authority in charge of the industry when deemed necessary.

Article 43

Those who are already engaged in the collection or computer processing of personal data before promulgation and enforcement of this Law and are required to process registration or special permit pursuant to the provisions of this Law shall process the same within one year after enforcement of this Law.

Enterprises, groups or individuals designated by the Ministry of Justice in conjunction with the government authority in charge of the industry pursuant to the provisions of Article 3 Item 7 Sub-item 3 shall process registration or special permit within six months after designation.

Those who fail to process registration prescribed in the two preceding paragraphs or those whose applications are disapproved shall be considered as un-registered or without a special permit and shall be punished accordingly.

Article 44

The enforcement rules of this Law shall be prescribed by the Ministry of Justice.

Article 45

This Law shall become effective upon promulgation.

(This is the end of the Request Form)