# MULTI-LATERAL RECOGNITION OF PKI CERTIFICATION AUTHORITIES IN THE ASIAN REGION: TRANSBORDER DATA FLOW AND INFORMATION PRIVACY ISSUES

*Alana Maurushat**

*This article examines the feasibility of multi-lateral recognition of PKI certification authorities in the Asia region. It begins with a review of PKI technologies and the role of certification authorities. In the following sections, the notion of legal harmonisation of PKI certification authorities and issues in transborder data flow are explored by way of comparative analysis of Hong Kong, the PRC and Singapore. This examination compares and contrasts the legal recognition of PKI certification authorities in the relevant legislation as well as legislation relating to privacy, that is, the protection of personal data. It is argued throughout that any notion of multi-lateral legal recognition of PKI certification authorities should only be considered where a certain threshold has been met to harmonise the legal principles of PKI legislation, and where there is sufficient protection of personal data (privacy).*

## Introduction

There has been much debate over the centuries as to the legitimacy of Emperor Yongzheng's claim to the imperial throne.[1] It is said that Emperor Kangxi of the Qing Dynasty vacillated between his 24 sons as to which prince would inherit the throne. During Kangxi's last years the competition was narrowed to the fourth, eighth, and fourteenth sons with the favourite apparently being the fourteenth prince, Yintai. In 1722 it is noted that Kangxi assembled seven of his sons to his bedside where the box containing the Emperor's will was opened stating who would be the next successor to the throne. Yintai, the fourteenth son, was in Beijing at the time and was, therefore, not present.

* Formerly Assisant Lecturer and Deputy Director of the LLM in Information Technology and Intellectual Property Programme in the Faculty of Law, University of Hong Kong. She is indebted to student reasearcher, Eddy So, for his usual reliable, expedient and excellent research assistance. She is further indebted to the LLM students at HKU for their insights and opinions on many of the matters discussed in this article. Lastly, she is indebted for the quirkiness and creative aptitude of student researcher, Billy Poon.

1 The historical debate of Emperor Yongzheng's accession to the throne is well documented. *See* for example the following online sources: http://www.hkpc.150m.com/filmreviews/yongzhengdynasty.htm; http://www.san.beck.org/3-8-QingEmpire1644-1799.html; and http://www.hceis.com/ChinaBasic/ History/Qing%20dynasty%20history.htm.

There is dispute over whether Kangxi intended the fourth or the fourteenth son to accede to the throne. It has been alleged that the fourth son, Yinzhen, added a single stroke to one of the characters to change the will to read "the throne goes to the fourth son" as opposed to "the fourteenth son". Kangxi was unable to affirm his true intentions as he had died prior to the reading of the will. Against this controversial background, Yinzhen acceded to the throne proclaiming himself Emperor Yongzheng.

If the same scenario were to occur today, Emperor Kangxi would have a variety of ways to better ensure the integrity and authenticity of both the information and the authorship of the will: use a code; encrypt the plain text into ciphertext (the longer the key stroke, the more difficult to break the code), use an electronic signature, PIN or digital signature; rely on public key infrastructure (PKI);[2] and so forth. Had the will contained in the box used an encryption technology such as PKI, historians would have had little if anything to dwell on over whether the fourth or fourteenth son was the true successor to the throne. Indeed, Chinese history in the Qing Dynasty may have turned out quite differently had the fourteenth son, Yintai, been his father's successor.[3]

In the Asia region today the development of PKI is no longer in a state of infancy. Asian nations have begun to regulate PKI and the correlating trusted Certification Authorities (CA) who issue digital certificates used in PKI. Likewise, the industry has cooperated to adopt standards to facilitate PKI development. Both governments and businesses in the region have begun to embrace this technology. PKI could now more aptly be described as having entered primary school. We see PKI used in the delivering of government services, as one of the functions attached to national Smart ID cards, in logistics, and in banking transactions. The development of PKI has, however, predominantly been utilised within national borders. As governments and

[2] Public key infrastructure is explained in greater detail in the first part of this paper following the introduction.

[3] The idea to use the Qing Dynasty as an illustration, suggested by student researcher Billy Poon, was inspired in part by Susanna Fischer's use of Hamlet. Shakespeare's famous play, *Hamlet*, has become a well-known metaphor in the world of electronic transactions and public key infrastructure (PKI). The King of Denmark sends Hamlet away to England to be accompanied by his fickle friends, Rosencrantz and Guildenstern. He gives a sealed envelope to Rosencrantz and Guildenstern to be given to the King of England. The message says to kill Hamlet. Meanwhile, Hamlet intercepts the sealed envelope and changes the message inside to read, "Kill Rosencrantz and Guildenstern." Of course, this example seems somewhat dubious considering the envelope would have likely been sealed with the King of Denmark's official seal, and furthermore, signed by the King. Hamlet would have had to recreate an identical seal, and forge the King's signature. Nonetheless, Hamlet secures his survival and inflicts a tragic fate of his friends with the switching of messages. *See* Susanna Frederick Fischer, "Saving Rosencrantz and Guildenstern in a Virtual World? A Comparative Look at Recent Global Electronic Signature Legislation," (2001) Association of American Law Schools 2001 Annual Meeting: Section on Law and Computers. Available at http://www.bu.edu/law/scitech/volume7/Fischer.pdf (last accessed 18 Apr 2005).

businesses embrace this technology both within national borders extending to cross-border usage, there is a growing need for legal recognition of CAs across borders in the wider Asia-Pacific region.

Harmonisation will play a key role in the multi-lateral recognition of PKI Certification Authorities. The issue of harmonisation has largely referred to ensuring technological uniformity, compatibility and interoperability so that the essential elements of PKI are preserved: authenticity, integrity and non-repudiation. The harmonisation of PKI technologies is a very complex issue and to date, issues of technological harmonisation have deservedly monopolised much of the focus in PKI discussion.[4] This paper will argue that the notion of harmonisation should be expanded so as to include legal recognition of Certification Authorities in other countries but only where there exists a high level of security of personal data coupled with effective privacy regulations extending to the use of PKI and to the Certification Authorities responsible with issuing digital signatures and certificates.

The following discussion of harmonisation of PKI Certification Authorities draws upon the examples of three Asian regions:[5] Hong Kong, the People's Republic of China (PRC), and Singapore. The experiences from these three regions will be drawn upon to illustrate both the need for multi-lateral recognition of PKI Certification Authorities in Asia as well as the need to ensure that adequate mechanisms for security of personal data are in place coupled with adequate privacy protection. This paper will first provide a description of PKI and some of its related cryptographic technology. The second part will discuss the importance of multi-lateral recognition of PKI Certification Authorities – its perceived advantages and potential drawbacks. The third part of this paper will be divided into three parts, one part for each of the regions analysed. The analysis of each region, in turn, will provide examples of PKI industry practice in the region, and look at the current state of regulations of PKI Certification Authorities, and security of personal data and privacy measures. The next section will provide an integrated discussion of potential security risks to personal data as well as related privacy concerns. The last part will conclude by offering a strategy on how regions can be most effective in harmonising legal recognition of PKI Certification Authorities in a man-

[4] For example, The Organization for the Advancement of Structured Information Standardss (OASIS) recognises seven models of PKI interoperability: cross-certification, cross-recognition, bridge CAs, certificate trust lists, accreditation certificates, strict hierarchy, and delegated path discovery and validation. These models are described in detail in Galexia Consulting, "PKI Interoperability Models Feb 2005" available at http://consult.galexia.com/public/research/articles/research_articles-art32.html (last visited 18 Oct 2005). For a detailed overlook at the complexities involved in PKI harmonisation see the OASIS PKI website available at http://www.pkiforum.org/resources/whitepapers/ (last visited 18 Oct 2005).

[5] The term "region" is used in place of nation as Hong Kong is a Special Administrative Region of the People's Republic of China in spite of the fact that it has a separate legal system, as well as the constitutional power under the Basic Law to regulate in the area of technology.

ner which offers adequate protection to security of personal data and ensures that privacy is protected in a meaningful manner.

## What are Cryptography and Public Key Infrastructure?[6]

Public key infrastructure[7] is a system of technologies and authorities which authenticate the validity of parties involved in electronic transactions. Typically, PKI involves cryptography, digital signatures, digital certificates, and certification or registration authorities.

Cryptography is the science of encryption and decryption. Julius Caesar popularised the practice. Not trusting his messengers when communicating with his governors and officers, he encrypted his messages.[8] Encryption is the coding of plaintext into an unreadable form called ciphertext so that it cannot be understood by those who are not privy to the code. Caesar created a rather simple system in which each character in his messages was replaced by a character three positions ahead of it in the Roman alphabet. Authorised recipients of his messages were provided with the means of decrypting them. Decryption is the process of converting ciphertext back into its original form so that it can be understood and acted upon. Cryptography allows the communication of information in a manner that is disguised so as to keep its content hidden from unintended or unauthorised recipients.[9]

Caesar's system was premised on the creation and sharing of a private code, nowadays referred to as a private key (made up of characters or numbers). Private key cryptography, also known as symmetric cryptography, uses the same key for both the encryption and decryption processes.[10] The following is an explanation of how symmetric encryption works:

> "The encrypted messages and the key are sent separately to the intended recipient. If this were simply a case of two friends wanting to share secret information, it would be easy. Person A encrypts the message and sends the encrypted message and the key separately to Person B. Person B is

6 This section borrows from a previous paper co-written by the author: Dr Ian Kerr, Alana Maurushat and Christian Tacit, "Technical Protection Measures: Tilting at Copyright's Windmill," (2002–2003) Vol 34(1) *Ottawa Law Review* 9.

7 PKI is also referred to as trusted hierarchies and key escrow.

8 M. McInnes, I. Kerr, Carmody & J.A. Vanduzer, *Managing The Law: The Legal Aspects of Doing Business* (Toronto: Pearson Education, 2002), Ch 17.

9 C. Risher, "Technological protection measures (anti-circumvention devices) and their relation to exceptions to copyright in the Electronic environment", IPA Copyright Forum Frankfurt Book Fair 20 Oct 2000, pp 1–2. See also Network Associates and its Affiliated Companies, *Introduction to Cryptography* (1990–1999) available at http://www.pgpi.org/doc/pgpintro (date accessed: 8 Apr 2002).

10 L. Janczewski, *Internet and Intranet Security Management: Risks and Solutions* (Hershey: Idea Publishing, 2000), p 149.

> then able to decrypt the message [using the key]. If the key is left in clear format (decrypted) it could potentially be captured during transmission and readily used to decrypt the message leading to a compromise of security."[11]

For this reason public key (or asymmetric) cryptography (also referred to as key escrow or trusted party) is often the preferred approach. In public key cryptography, a twin pair of keys is created: one key is private, the other public. Their fundamental property is that, although one key cannot be derived from the other, a message encrypted by one key can only be decrypted by the other key. Because two keys are required – one to encrypt, the other to decrypt – no one has to share her private key with anyone. In fact, it is essential that the private key be kept secret and remain in the custody of the person to whom it belongs. The public key, on the other hand, is only useful if it is possessed by as many people as possible. Only by making the public key readily available is it possible to enable others to send encrypted data. Although not necessary, the keys are often interchangeable.[12] In other words, "if key A encrypts a message, then key B can decrypt it, and if key B encrypts a message, then key A can decrypt it."[13]

A similar procedure is used to create digital signatures, which can be used to authenticate the identity of an individual in order to determine whether he or she is authorised to gain access to a digital work. A digital signature is often confused with an electronic signature; the two are not interchangeable.

An electronic signature is broader; it refers to any letters, characters, numbers or symbols in digital form intentionally used for the purpose of authenticating or approving the electronic record.

A digital signature on the other hand is a type of electronic signature or more accurately, it is a computer software program. A simple digital signature is the ciphertext resulting from encrypting a message. This electronic signing process is one way to fulfil the functional equivalence requirement for electronic signatures in many jurisdictions' electronic commerce legislation. If one person signs his message and sends it to another along with an appended digital signature (signer), she can decrypt the appended digital signature with his public key and compare it to the message (verification). If they are identical, and assuming that the public key that was used to decrypt the signature really is his public key, she can reasonably infer that the message was in fact from him since it must have been signed with his private key.[14] To be more precise, the private key is used to generate a "hash" function which in turn, produces

[11] *See* Risher (n 9 above), p 2.
[12] *Ibid.*
[13] *See* n 9 above, p 2.
[14] R.E. Smith, *Internet Cryptography*, (Reading: Addison Wesley, 1997) p 280.

a hash result (a unique alphanumeric code). The private key encrypts the hash result and attaches it to the data. At the other end commences the verification process using a public key. The recipient uses the public key to decrypt the hash result. At this point, a new hash result is created. The resulting two hash results are compared. If they are identical the digital signature is authenticated. Thus, decrypting a digital signature using a public key is one way (and the method most commonly referred to in the literature) to verify a digital signature.[15]

The standard example that is given in the literature to explain public key cryptopgraphy is the use of Alice, Bob and Carol. Alice and Bob have a longstanding commercial relationship. They have exchanged public keys. Alice may send an encrypted message to Bob using her private key, while Bob will use Alice's public key to decrypt the message. This is one of the most secure ways of exchanging keys in public key cryptography: a face-to-face transaction between parties with prior acquaintance to exchange public keys.

Another form of authentication similar to a digital signature is a digital certificate. Digital certificates act as a form of identification for users in the digital world and are registered and distributed by trusted third parties known as certification authorities (CAs). A digital certificate normally contains the version number of the certificate, the serial number of the user, the algorithm used to sign the certificate, the CA that issued the certificate, the expiration date of the certificate, the user's name, the user's public key and the user's digital signature.[16] Certificates play an important role in security, since system administrators can configure servers to accept only certificates signed by certain CAs. Reputations and trust are of critical importance for this system to work well.

## Endorsing Public Key Infrastructure and Multi-lateral Recognition of PKI Certification Authorities: its Perceived Advantages and Potential Drawbacks

The greatest advantage of promoting and using public key infrastructure is the amount of control exuded over the trusted third party, ie the certification authority (also referred to as certification bodies and certification service providers). CAs maintain records (certificates) containing important information relating to identity, as well as they have a record of both private keys and public keys. It has been argued that such a system benefits both e-commerce as well as law enforcement.

[15] *See* n 8 above.

[16] See n 10 above, p 12. The author analogises digital certificates with a driver's license or a passport.

From an e-commerce perspective, PKI is able to offer a high level of authenticity, integrity and non-repudiation of data. The technology operates in conjunction with the trusted third party, the CA, in order to achieve a high level of authentication of the parties involved in a transaction, a well as integrity and non-repudiation of data during the transaction. PKI has been heralded as one of the most secure methods of transacting on the Internet.[17] However, the security level and reliability of PKI is highly dependent on the trustworthiness of the CA who issues and maintains lists of the digital certificates used in a transaction. Recognising the important role of the CA, many states have begun to regulate the industry.

PKI also offers advantages to law enforcement agencies wishing to identify parties involved in suspicious transactions. Examples include, but are not limited to, criminal investigations, national security, and international terrorism. The ability to identify parties effectively, however, is contingent (or at least more efficient) when state's regulate (and to a certain extent perhaps even control) certification authorities. Certification Authorities are often government entities or corporations.[18]

There is a growing call for multi-lateral legal recognition of CAs both in Asia and in the world. This is often referred to as the need for harmonisation. Harmonisation efforts have predominantly focused on standardisation and interoperability between the technologies involved in PKI.[19] There is an increasing awareness that the promotion of PKI in e-commerce will also require harmonisation of the legal framework.[20] The use of digital certificates in e-commerce between parties (whether in the same nation or in different countries) is facilitated through what can best be described as a web of trust ratings. Yee Fen Lim describes this system aptly:

> "Public key infrastructure ... produces authenticity by assuming that each authority wishes to protect and enhance its reputation. This assumption is then tested as each authority checks the security of another authority's system. In this way, one authority can often carry the seal of numerous others, as a testimony to its own reliability. In return, that authority will test and seal numerous others."[21]

[17] Stephen Blythe, "Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce with Enhanced Security," (2005) 11 *Richmond Journal of Law & Technology* 6.

[18] For example, the Postmaster General is a recognised certification authority in Hong Kong SAR.

[19] See, for example, Report of the First Asia PKI Form, available at http://www.japanpkiforum.jp/E/1st_forum/program-E.htm (last accessed 18 Apr 2005) as well as industry efforts in the Asia region available at http://asia-pkiforum.org/NEW/01_aboutus/sub06.php (last accessed 18 Apr 2005). See also, ISO standards in the area of PKI available at http:///iso.org (last accessed 21 Apr 2005).

[20] See keynote speech by Mr Michiro Naruto, "Key issue for global deployment of electronic commerce," found in the Report of the First Asia PKI Form, *ibid.*

[21] Yee Fen Lim, "Digital Signatures, Certification Authorities: Certainty in the Allocation of Liability," (2003) 7 *Singapore Journal of International & Comparative Law* 183, 190.

The above comments were written in the context of transactions between "non-government certification bodies" with the assumption that non-government refers to those certification bodies which are not licensed by a government body. At this juncture, it is important to note that PKI regulations apply to both licensed and non-licensed certification authorities in certain jurisdictions (most notably Singapore), while PKI regulations only apply to licensed certification authorities in other jurisdictions (eg Hong Kong). This may have important implications in the context of level of security measures, protection of personal data, presumption of legal validity, and a CA's ability to limit liability. It is thought that a harmonisation of legal regimes would promote confidence and trust in the use of PKI in e-commerce by providing a high level of system security (authentication, integrity and non-repudiation) as well as *potentially* a high level of security of personal data. Such harmonisation would further provide more legal certainty to CAs; this is especially true in the context of setting valid reliance limits for liability.[22] There is *potentially* a major drawback to multi-lateral legal recognition of CAs. Where regulation of CAs is similar between jurisdictions, personal data and privacy protection is not. The notion of privacy may be divided into two concepts. The first is protection of personal data which is often protected with Personal Data legislative instruments. The second is protection from invasion of privacy which is often protected by interception of communications or surveillance legislation, and other legislative instruments such as the tort of invasion of privacy or protection afforded in civil codes or other human rights instruments. The second point falls outside of the scope of this paper; it is the notion of personal privacy of data which will be considered.

The use of PKI prompts a competing tension. On the one hand, there is the desire to provide secured transactions which offer high levels of authentication, integrity and non-repudiation, while on the other hand, it is of vital importance that the use and collection of a person's data by CAs is carefully limited so as to afford a high degree of privacy protection to individuals.

There are two paramount concerns in relation to privacy protection with multi-lateral recognition of CAs offering PKI services.[23] The first concern is

[22] *Ibid.*, p 194.

[23] A third concern is the inability to transact anonymously using PKI. The author will not, however, address this issue. For a better look at the issue of anonymity see Deborah Morgan, "Digital Signatures: Will Government Registration of Users Mean That Anonymity in Transactions on the Internet is Forever Lost?" (2004) *University of Illinois Law Review* 1003. Another potential concern is of a more general nature – PKI itself is inherently privacy invasive by design. See generally Roger Clarke, "Conventional Public Key Infrastructure: An Artefact Ill-Fitted to the Needs of the Information Society" (2000) available at http://www.anu.edu.au/people/Roger.Clarke/II/PKIMisFit.html. Clarke additionally refers to the work of Stefan Brand who advocates for PKI to adopt technology which is less privacy invasive.

that many jurisdictions have weak laws or no law at all directly relating to the limit of the government's collection of personal data of its citizens. This has ramifications where governments request information from private or non-government CAs. The potential for abuse is even greater where the administering CA is itself a government entity. And even where privacy and surveillance laws are present, the practice may indicate a different reality. The second concern is that in many jurisdictions, privacy laws are only binding on government agencies; private corporations are free to use and abuse personal data. While the aforementioned concerns may be present in a variety of jurisdictions worldwide, they are particularly acute concerns in the Asia region.

## Regional Analysis

The following section outlines the use of PKI in the Asia region (Hong Kong, China and Singapore), as well as provides an analysis of the regulation of CAs and applicable privacy (personal data) protection law.

### *Hong Kong SAR*

#### A) Use and endorsement of PKI

The Hong Kong SAR readily endorses the use of PKI. The new Hong Kong Smart ID card has the option of embedding a digital certificate into the card. This certificate is designed for transactions and dealings in general with the government (e-government).

In the logistics industry, the use of a system known as BOLERO.[24] BOLERO is a non-recognised certification authority which provides digital signature services in the logistics field.[25]

Many universities in Hong Kong have likewise embraced PKI issuing digital signatures through the University CA.[26] Students and staff can order and pay for a variety of services online with their digital signature including printing credits.

Hong Kong is also an active member of the Asia PKI Forum[27] as well as a contributing member of Asia Pacific Economic Corporation's (APEC) e-Security Task Force. The Asia PKI Forum is an organisation consisting of representatives from Hong Kong, Singapore, China, Macau, Korea, Japan,

[24] Bill of Lading Electronic Registry Organisation.
[25] Felix Chan, "China's Electronic Signature Act 2005: A Great Leap Forward or Backward," (2005) *Computer & Telecommunications Law Review* 1.
[26] For example, the University of Hong Kong Certification Authority. *See* http://www.hkuca.hku.hk.
[27] *See* http://www.asia-pkiforum.org/.

Taiwan and Malaysia mandated to promote and facilitate the use and interoperability of PKI in the Asia region. As a member of the APEC e-Security Task Force, Hong Kong is committed to the Draft Guidelines for Schemes to Issue Certificates Capable of Being Used in Cross Border Jurisdiction e-Commerce.[28] Both groups focus on the technological harmonization of PKI technologies.

### B) PKI and certification authorities

PKI is regulated under the Electronic Transactions Ordinance (ETO) and Code of Practice for Recognized Certification Authorities (Codes of Practice).[29] These two legislative instruments form the basis for PKI regulation. The ETO was amended in 2004. Previously, the ETO was technology-specific in that a rule of law requiring a signature could only be satisfied by the use of a digital signature generated by a recognised certification authority. The ETO no longer plays favouritism to a certain type of electronic signature, namely that of the digital signature. Recall that the former is broad, while the latter refers to a specific software program. The ETO had been heavily criticised for technological preferences as opposed to technological neutrality. As such, section 6 was amended to better reflect a neutral approach to technology. An electronic signature will satisfy legal requirements if it is used to identify and authenticate; is reliable and appropriate for the purpose of communication of the document; and the recipient has consented to its use. The ETO is now best considered a mixed-model – when transacting with a government or governmental agency only a digital signature will satisfy a rule of law, whereas the ETO recognises electronic signatures as a whole when contracting parties are non-government agencies.[30]

Digital signatures (digital certificates) are issued by Certification Authorities (CA). The ETO distinguishes between Recognized Certification Authorities (RCA) and CAs.

Certification Authorities are not necessarily regulated by the ETO. Only RCAs are directly affected by the ETO. Certification Authorities who are not recognised are governed under the Common Law.

To become a RCA, one may apply to the Government Chief Information Officer (CIO) under section 20 of the ETO. The CIO may, in turn, determine eligibility for certification under section 21 of the ETO.

[28] The Guidelines are available at http://www.apectel29.gov.hk/download/estg_20.doc.

[29] Government Chief Information Officer Hong Kong SAR, *Code of Practice for Recognized Certification Authorities* (2004) available at http://www.ogcio.gov.hk/eng/caro/cop_pdf/cop.pdf.

[30] *See* ETO, s 6.

The eligibility criteria for a RCA is relevantly stringent. Under section 21 applicants must have an appropriate financial status, liability insurance, security arrangements, only "fit and proper person" may apply (no liquidation, bankruptcy, or criminal record), while there are a number of annual reports which must be complied with. The specific elements to be addressed for each of these requirements is laid out in detail in the Code of Practice.[31]

Most RCAs issue more than one type of digital certificate. RCAs are required under the law (section 22) to obtain approval from the CIO for each type of recognised certificate issued (non-recognised certificates do not require approval from the CIO). In other words, the process is two-fold: application to become an RCA and another application to obtain certificate approval.

There are currently three RCAs in Hong Kong: 1) Postmaster General, 2) Digi-Sign, 3) Hi TRUST.COM. Many benefits are afforded to RCAs under the ETO:

1) Presumption of validity under the law (section 6).
2) Ability to limit liability (section 42).
3) Formal publication on the HK SAR government website (indicates trust as well as provides free publicity).

Liability limits are still subject to the standard of reasonableness as set out in the Exemption Clauses Ordinance. The "reasonableness" standard will likely, in turn, look to a RCAs compliance with the ETO as well as the Code of Practice. Recognized Certification Authorities will also be liable for intentional misrepresentation, and negligent or reckless misrepresentation.

### C) Security of personal data and privacy protection

Provisions on the security of personal data and privacy protection are found predominantly in two legislative instruments: Code of Practice and the Personal Data (Privacy) Ordinance (PDPO). The ETO itself simply mandates by way of section 37 that a trustworthy system must be in place when issuing, revoking or renewing digital certificates. A "trustworthy system" is defined in section 2 as:

[31] These specifications will be looked at in detail the following section of the paper.

"computer hardware, software and procedures that–
(a) are reasonably secure from intrusion and misuse;
(b) are at a reasonable level in respect of availability, reliability and ensuring a correct mode of operations for a reasonable period of time;
(c) are reasonably suitable for performing their intended function; and
(d) adhere to generally accepted security principles."

The ETO does not directly refer to security of personal data and privacy protection; this is found in the Code of Practice.

The Code of Practice is a comprehensive instrument. It occupies a unique position in that it is neither subsidiary legislation (ETO section 33(4)) nor is it legislation in a sense that it is legally binding. However, failure to comply with the Code of Practice may lead to suspension or revocation of a RCA (ETO sections 23 and 24) or the inability to rely of liability limitation as set out in section 42.

The Code of Practice provides detailed guidance on trustworthy systems. In general, a secure or trustworthy system needs to meet widely-accepted technical standards. This is an evolving concept so that the level of required security is commensurate with the advancement of security technology (sections 5.6 and 14.1). In addition to technological security, RCAs are required to adhere to generally accepted security principles found in section 5 of the Code of Practice:

- asset classification and management
- personnel security
- physical and environmental security
- management over systems access
- operational management
- development and maintenance of computer systems
- continuity of business operations
- maintenance of appropriate event journals
- compliance monitoring and assurance
- disclosure of business practice statements
- key management ("maintain effective procedures and controls over the generation, storage, backup, recovery, distribution, use, destruction, and archiving of the recognised DA's own keys")
- management of key generating devices ("maintain effective procedures and controls over the procurement, receipt, installation, acceptance tests, commissioning, usage, repair, maintenance, and retirement of key generating devices")
- lifecycle management of tokens
- management of certificates

- management of publication of certificate revocation
- accurate record retention for at least seven years, and
- maintain and security and risk management policy

One of the most onerous tasks for a RCA is the requirement to submit an assessment of compliance with the ETO and the Code of Practice (report) every 12 months, for the renewal of recognition and when any major changes are made to an RCA (Code of Practice, section 12). RCAs are required to obtain a *qualified and independent* assessment of the certification service. Assessment is based on trustworthiness of the service, system security, procedural safeguards, and financial viability. The independent assessor, however, does not have to comment on the level of protection of privacy of personal data.

Privacy concerns are addressed in section 3.6 of the Code of Practice. It reads as follows:

> "3.6 A recognized CA shall comply with all applicable ordinances and regulations regarding the privacy of personal data. In particular, a recognised CA shall:
> (a) set out its privacy policy in respect of the collection, holding and use of personal data of data subjects (eg applicants of its certificates and subscribers);
> (b) give a written Personal Information Collection Statement to data subjects before or upon the collection of personal data from the data subjects;
> (c) include a purpose statement (eg in its repository or certification practice statement as appropriate) defining the purpose(s) of keeping its repository and the permitted use of personal data contained therein; and
> (d) as a minimum requirement to ensure compliance with all applicable ordinances and regulations regarding the privacy of personal data, conduct a self-assessment in accordance with the "Privacy Compliance Self-Assessment Kit" or any document of a similar nature published by the Office of the Privacy Commissioner for Personal Data. Such a self-assessment shall be conducted by the recognized CA regularly or whenever there is major changes in its operation affecting its handling of personal data of data subjects."

It is interesting to note that the protection of personal data (privacy) is a self-assessment exercise; the independent assessor is not required to review personal data protection policy. All that is required is that the RCA have a privacy policy available to the user (data subject), and the user is shown a

written copy of how personal data will be collected. Consent is not required under the Code of Practice. The user will of course have no bargaining power to alter personal data collection or disallow data collection by means other than choosing not to contract with the particular RCA. The last requirement is that the RCA must comply with relevant privacy legislation, namely the PDPO.

The PDPO entered into force on 20 December 1996 prior to the handover of Hong Kong to the PRC. It is derived from the Hong Kong Bill of Rights Ordinance (section 14) which gives effect to Article 17 of the International Covenant on Civil and Political Rights (ICCPR) – providing against arbitrary or unlawful interference with privacy. It is concerned with protecting information privacy (personal data). Except in a limited number of cases, parties cannot contract out of the Ordinance by obtaining consent of the individual.

The PDPO was not designed to capture electronic transactions. In fact, it is altogether ill-suited to privacy issues in cyberspace.[32] Nonetheless, it does have specific applications to PKI technology. The 1999 Court of Appeal case of *Eastweek Publisher v Privacy Commissioner*, casts serious doubt as to the broad scope of PDPA. Eastweek Publisher published a photograph of a young woman taken from the populated and busy area of Hong Kong known as Causeway Bay. Although the photographer was unable to obtain consent from the young woman, the photograph was published. The photograph was labeled, "Japanese Mushroom Head" followed with a scathing article describing this young woman's utter lack of fashion sense. On the issue of whether the PDPO had been violated, the court ruled, in a 2 to 1 ruling, that there was a lack of intent to identify the young woman or to compile personal data about her. When this ruling is applied to cyberspace, it is likely that most companies using cookies to trace and record user information would likewise lack the requisite "intent" to identify and profile their users. The same, however, may not be said of PKI technology as one of its chief features is its high degree of authentication of its users.

The following section considers the most relevant provisions in the context of PKI.

The PDPO espouses several key definitions which are briefly listed below:

> "data" (資料) means any representation of information (including an expression of opinion) in any document, and includes a personal identifier;
> "data subject" (資料當事人), in relation to personal data, means the individual who is the subject of the data;

[32] *Eastweek Publisher Ltd & Another v Privacy Commissioner of Personal Data* [2000] 1 HKC 691.

"data user" (資料使用者), in relation to personal data, means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data;
"personal data" (個人資料) means any data–
(a) relating directly or indirectly to a living individual; [Attribution]
(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; [Identification] and
(c) in a form in which access to or processing of the data is practicable [Retrievability]

Under section 4 of the PDPO, data users must follow the six Data Protection Principles espoused in Schedule 1. The principles can be summarised using the following headings:

Principle 1: Purpose and manner of collection of personal data
Principle 2: Accuracy and duration of retention of personal data
Principle 3: Use of personal data
Principle 4: Security of personal data
Principle 5: Information to be generally available
Principle 6: Access to personal data

It is important to note that principle 1 requires consent, either explicit or implicit, to collect personal data from the data subject on or before collection. Thus, where section 3.6 of the Code of Practice fails to include consent, it is covered by virtue of principle 1 of the PDPO.

Section 33 of the PDPO, "Prohibition against transfer of personal data to place outside Hong Kong except in specified circumstances," is of particular relevance to PKI regulation. Although section 33 is not yet in operation, it can best be described as a basic ban on trans-border data flow to a place outside of Hong Kong. There is, however, a list of exceptions:

- specified place as officially published in the Gazette[33]
- law in foreign place offers same level of protection[34]
- consent of data subject[35]
- data subject *would have* given consent[36]
- exempted from data protection principle 3 (use of personal data)[37]

[33] Section 33(2)(a) of the PDPO.
[34] *Ibid.*, s 33(2)(b).
[35] *Ibid.*, s 33(2)(c).
[36] *Ibid.*, s 33(2)(d).
[37] *Ibid.*, s 33(2)(e).

- user has taken reasonable precautions and exercised due diligence to ensure that information is used and collected in a manner in the foreign place which would not contravene the PDPO.[38]

There are currently no designated places for the recognition of foreign CAs as allowed under section 33(3) of the PDPO. The Post Master General has, however, signed a MOU with Korea and Shanghai.[39] It is difficult to see how Korea, given its reputation for lax privacy law (especially as it pertains to private corporations), offers privacy protection similar to the PDPO. Meanwhile, China does not have any law relating to personal data privacy. It is easy to infer that the Hong Kong position is one of facilitating e-commerce and perhaps at the expense of privacy concerns.

The legal protection of trans-border data flow remains an empty concept. Section 33 is not yet in operation in spite of the fact that the legislation is now in its ninth year of operation! The point is perhaps best made in the following excerpt from the Electronic Privacy Information Center (EPIC):

> "The recent economic downturn has led to some companies outsourcing data processing functions to jurisdictions that have weaker privacy protections for personal data, particularly mainland China and India. To date this development has largely gone unchecked by the Privacy Commissioner because §33 of the Ordinance, governing transborder data flows, has yet to be enacted."[40]

One may only assume that at some point section 33 will be enacted. At this point, multi-later recognition of CAs will only be possible with CAs who either: (1) are located in places with the same level of privacy protection to Hong Kong, or (2) maintain privacy policies similar to the level of protection afforded in the PDPO. In any event, where a provision of the PDPO is violated, a data subject may lodge a complaint with the Privacy Commissioner

[38] *Ibid.*, s 33(2)(f).

[39] The MOU was reported in the People's Daily, "Hong Kong Signed MOU with Korea," available online at http://english.people.com.cn/english/200103/16/eng20010316_65232.html (last accessed 20 Apr 2005). The MOU with Shanghai was reported on the Hong Kong SAR government's website, "Cooperation Arrangement between HK Post and Shanghai Electronic Certificate Authority," available at http://www.info.gov.hk/gia/general/200105/24/0523310.htm. Criticism of Korea's lax privacy laws may be found on the following websites: Caslon Analytics Privacy Guide at http://www.caslon.com.au/privacyguide6.htm#skorea and the Electronic Privacy Information Center's (EPIC) international survey of privacy laws and developments titled, "Privacy & Human Rights 2003," available at http://www.privacyinternational.org/survey/phr2003/countries/southkorea.htm (last accessed 20 Apr 2005). Criticisms of China's privacy laws may be found on the same website at http://www.privacyinternational.org/survey/phr2003/countries/china.htm (last accessed 24 Apr 2005).

[40] EPIC website, *ibid.* The specific passage is found at http://www.privacyinternational.org/survey/phr2003/countries/hongkong.htm (last accessed 26 Apr 2005).

(section 37). After the investigation of a complaint and the issuance of an official report by the Privacy Commissioner, if it is determined that an offence has been committed pursuant to section 64, the Commissioner has the power to impose fines and even sentence the data user to imprisonment. The Commissioner may further award compensation to the data subject pursuant to section 66.

*Peoples Republic of China (PRC)*

A) Use and endorsement of PKI

PKI is used in a number of ways in the PRC. Some of applications are used in banking, government services, health and insurance, and logistics operations.[41] One application that is particularly noteworthy is the "Electronic Signature Safety Seal" system. The safety seal system is designed to authenticate the special red seal required in a number of commercial operations. Each enterprise has its own special seal. In the past, there was a problem with forged seals. The use of PKI is expected to enhance credibility and authentication of such seals.[42]

China is also a member of the Asia PKI Forum and APEC, and readily participates in technological interoperability PKI initiatives.

B) PKI and certification authorities

Certification Authorities are now required as of 1 April 2005 under the new PRC Electronic Signatures Law (2005) to be licensed (Article 16). Prior to this legislation, many regions of China had enacted electronic signatures law (eg Shanghai) along with regulations pertaining to CAs. The new PRC E-Signatures Law is a national law binding all CAs operating or wishing to operate in the PRC.

To provide digital signature services issued by a third party, a CA must meet five criteria under Article 17 (paraphrased):

1) have appropriate technicians and management personnel
2) have appropriate funds and business premises
3) technologies that comply with state security standards
4) maintain documentary evidence from relevant authority for the use of encrypted technology
5) comply with any other relevant laws and regulations where appropriate.

41 See Ning Jin-Ju, "The Application of PKI in E-Business in PRC," available at http://www.symposium.pki.or.kr/ 08%20PKI%20Status%20-%20Jiajun%20Ning.pdf (last accessed 24 Apr 2005).

42 For a more detailed explanation, *see* n 25 above.

In order to become licensed, CAs must submit an application to the relevant State Council department in charge of the information industry pursuant to Article 18 (entity is assumed to be the State Council Information Office (SCITO)). Foreign CAs may not become licensed in the PRC; they are, however, recognised and enjoy legal validity in the PRC (Article 26).

Licensed CAs have a number of legal obligations. The CA must ensure that information on a certificate is true, complete and accurate (Articles 20 and 21). CAs must ensure that parties using electronic signatures can verify the contents of the certificate and other relevant matters (Article 22).

CAs must formulate and publish their certification rules and submit them to the SCITO.

The certification rules must comply with state provisions (Article 19). State provisions refer to the requirements under the Act as well as regulations to be promulgated in the future.

The certification rules must state, "the scope of liability, operational standards, the measures for their preservation of information security, etc." (Article 19). The above ambiguous wording is not likely to inspire confidence in CAs ("etc") nor consumers with such vague qualifications. Consumers will take comfort in the fact that the Law imposes strict liabilities on CAs. Article 28 provides that where a signatory or relying party suffered losses when acting in its civil activities based on electronic signature services provided by a CA, the CA will be responsible damages if it fails to prove it is not at fault.

The E-Signatures Law is rather a basic document which focuses on foundational elements for e-commerce. It will likely be supplemented with more detailed rules and regulations. These rules and regulations will be pivotal in inspiring both consumer and business confidence in the PRC.

### C) Security of personal data and privacy protection

Although the PRC does not have any legislation which directly deals the personal data, they are currently drafting a bill on Personal Data Privacy Protection In China. In an effort to promote e-commerce and e-government, The State Council Information Office (SCITO) was left in charge of promulgating electronic signature legislation as well as to draft China's first personal privacy protection law. A copy of the draft is not available to the public but it has been reported that the bill will "appl[y] to both public sector records at all levels of government, and all personal records of enterprises and other institutions in China ... Some exclusions can be expected for information with state security implications."[43] Little is currently known about the

[43] Russel Pipe, "China Launches Privacy Protection Law Project," on the Privacy and American Business website available at http://www.pandab.org (last accessed 24 Apr 2005).

drafting of this bill as it is in the earliest stage of drafting. Members of the working group are currently researching various elements of data protection. A seminar on Data Protection in the Information Society is being organised for the fall of 2005 with participants from local governments, academic organisations, industry players, as well as foreign experts.[44] It is, therefore, too early to speculate on the scope of protection of this bill.

The PRC E-Signatures Law, unlike its Hong Kong and Singapore counterparts, does not contain any provisions directly related to data protection or confidentiality of subscriber information. The only potentially applicable article refers to securing the integrity of the information. Article 15 reads:

> "Article 15: An electronic signatory shall duly safeguard his electronic signature creation data. If an electronic signatory learns that his electronic signature creation data has been descrambled or may have been descrambled, he shall promptly notify the relevant parties thereof and cease to use such electronic signature creation data."

One would expect, however, that the SCITO will write regulations which relate more specifically to security requirements of CAs as well as data protection measures. For now, there are no personal data protection measures in the PRC.

*Singapore*

A) Use and endorsement of PKI

Singapore is involved in a number of projects to promote and test PKI. Certification functions have been embedded into civil servants ID cards (in particular the Central Welfare Annuity Fund Board and Government Procurement Portal).[45] PKI is additionally used in many e-government functions such as CORENET e-Submission System, Epatents, Government Electronic Business (GeBIZ), iBook, Integrated Land Information System (INLIS), and MINDEF Internet Procurement System (MIPS).[46]

More formal industry collaboration is seen in the projects e-ASEAN and PKI Forum Singapore. e-ASEAN brings together over twenty community pilot projects in the countries of Singapore, Malaysia and Philippines. Participating members must maintain PKI regulations.[47]

[44] *Ibid.*
[45] *See* Report of the First Asia PKI Forum, n 19 above.
[46] Asia PKI Forum 2004 available at http://www.pkiforumsingapore.org.sg/casestudies.asp (last accessed 21 Apr 2005).
[47] *See* Report of the First Asia PKI Forum, n 19 above.

e-ASEAN predominantly works as a community advisory organisations actively working to solve PKI issues.

PKI Forum Singapore brings together key companies whose mandate is to educate the industry and public, propose policy recommendations pertaining to PKI and e-commerce, promote interoperability, and to work to harmonise cross-border laws.[48]

As in Hong Kong and China, Singapore has played an active role in Asia PKI Forum and those working groups of APEC which deal with e-commerce and PKI.

### B) PKI and certification authorities

Singaporean PKI and CA legislation consists of the Electronic Transactions Act 1998 (ETA) coupled with regulations: Electronic Transactions (Certification Regulations) 1999, Security Guidelines for Certification Authorities, and Guidelines for Preparing Certification Practice Statements. As one scholar writes, "the Singapore regime is undoubtedly the most effective regime for attaining the elements of authenticity, integrity and non-repudiation at the legal infrastructure level."[49]

The ETA is somewhat unique in that many of its provisions apply to both licensed and non-licensed certification authorities. The ETA allows for voluntary licensing of CAs. A non-licensed CA, however, must still comply with certain requirements under the Act including general duties relating to digital signatures (Part VII), duties of certification authorities (Part VII), and general duties (Part XII). Key duties include the issuance of Certification Practice Statements, meeting requirements as to issuance, revocation and suspension of certificates, as well as having the obligation of confidentiality.[50]

There is one licensed PKI in Singapore, NETRUST. As a licensed CA, NETRUST enjoys several advantages: evidentiary presumption for its issued digital certificates (signatures), specified liability limits, publication on the government's website, and the assumption that because it is a licensed CA, it is afforded a high degree of trust and meets stringent standards. In meeting stringent standards, licensed CAs take on additional obligations under both the ETA as well as the regulations of the Security Guidelines and Electronic Transactions (CA) Regulations.

In general, both licensed and unlicensed CAs must use a trustworthy system under section 27 of the ETA. Licensed CAs, as well as those CAs that

[48] For more information about the PKI Forum Singapore visit their website at http://www.pkiforumsingapore.org.sg/aboutus.asp (last accessed 21 Apr 2005).

[49] See n 21 above.

[50] Obligation of confidentiality is found in ETA, s 48.

eventually intend to be licensed,[51] must comply with the stringent security measures set out in the Security Guidelines. Some of the salient areas dealt with:

- certification management
- key management
- system and operations management
- application integration
- personnel control
- maintenance of subscriber's data.

While neither the ETA or the Security Guidelines offer any consequences if the provisions in the Security Guidelines are not meant, one assumes that the ability to become a licensed CA and thereafter have one's license renewed would be tied with meetings the requirements in the Security Guidelines.

The Electronic Transactions (CA) Regulations provide the continuing operational requirements to maintain a license. The Regulations provide the "nuts and bolts" of obtaining and maintaining a license. The criteria set out in the Regulations considers the financial position of the CA (including posting a performance bond or banker's guarantee), level of technical security of the digital signatures issued, record keeping requirement, confidentiality of subscriber information, and requires a CA to seek approval for each of the types of digital certificates issued. Licensed CAs must also undergo and pass an audit based on meeting a high level of operational criteria (to be determined by compliance with the ETA and Regulations and its own Certificate Practice Statement) and compliance with the Security Guidelines. Audits are performed at the time a CA seeks to become licensed as well as when a CA seeks renewal of a license.

### C) Security of personal data and privacy protection

The state of privacy law and data protection in Singapore might best be described as minimal.[52] There is no general data protection or privacy protection similar to the PDOP in Hong Kong, or even that of the draft bill of personal data protection as proposed in the PRC. Moreover, the Singaporean government has been readily criticised for its surveillance of its citizens and, in particular, of political opponents to the current leadership.[53] There are,

[51] It is unclear by what is meant by this concept.

[52] As an anecdote, when describing the content of this paper to a friend from Singapore, the individual let out an audible laugh claiming, "that ought to be a short section on privacy law. There is none!"

[53] See EPIC website available at http://www.privacyinternational.org/survey/phr2003/countries/singapore.htm.

however, provisions found in various legislative instruments which regulate certain aspects of personal data use, in particular the ETA, its accompanying Regulations, the Computer Misuse (Amendment) Act, and legislative instruments related to banking.

Both licensed and non-licensed CAs have the obligation to keep subscriber-specific information confidential.

Section 48 of the ETA sets forth the general obligation of confidentiality. It reads:

> **"Obligation of confidentiality**
>
> **48.** — (1) Except for the purposes of this Act or for any prosecution for an offence under any written law or pursuant to an order of court, no person who has, pursuant to any powers conferred under this Part, obtained access to any electronic record, book, register, correspondence, information, document or other material shall disclose such electronic record, book, register, correspondence, information, document or other material to any other person.
>
> (2) Any person who contravenes subsection (1) 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 12 months or to both."

Section 28 of the Regulations reads:

> **"28. Confidentiality**
>
> 1. Except for the purposes of Part XII of the Act, or for any prosecution under any written law or pursuant to an order of court, every licensed certification authority and its authorised agent must keep all subscriber-specific information confidential.
> 2. Any disclosure of subscriber-specific information by the licensed certification authority or its agent must be authorised by the subscriber.
> 3. This regulation shall not apply to subscriber-specific information which–
>    a. is contained in the certificate for public disclosure;
>    b. is otherwise provided by the subscriber to the licensed certification authority for this purpose; or
>    c. relates to the fact that the certificate has been revoked or suspended."

Section 2.7.1 of the Security Guidelines mandates:

> "2.7.1 Procedures and security controls to protect the privacy and confidentiality of the subscribers' data under the CA's custody shall be implemented. Confidential information provided by the subscriber must not be disclosed to a third party without the subscriber's consent, unless the information is required to be disclosed under the law of the Republic of Singapore or a court order."

The general proposition is that disclosure of information is banned pursuant to the ETA unless an exception would apply (this is binding on both non-licensed and licensed CAs). The Regulations and the Security Guidelines mandate that subscriber data must be kept confidential unless otherwise mandated by law, or if consent has been obtained by the subscriber. The Regulations and Security Guidelines, however, are only binding on licensed CAs. Furthermore, there is no mention as to whether consent must be express or may be implied.

The last point relates to recognition of foreign certification authorities. Section 43 of the ETA allows the Controller (of CAs) allows the legal recognition of foreign certification authorities for the purpose of a recommended reliance limit, and evidentiary presumption for digital signatures. Thus the emphasis is placed on facilitation of e-commerce by affording the advantages of the ETA to foreign CAs. There is no requirement that a foreign CA meet security standards or privacy protection of personal data according to the legislation. It may, however, be the case where the practice is more stringent than the actual law.

Another measure which would apply to non-government bodies is the National Internet Advisory Committee (NIAC)'s Model Data Protection Code for the Private Sector (Data Code). This is an option, self-regulatory measure with, "the softest privacy options: weak principles and no enforcement."[54] In the Legal Subcommittee's discussion of whether to adopt a self-regulatory approach, one advantage listed was that it "allows seamless transfer of data between different sectors within Singapore."[55] Some of the principles included in the Data Code are: accountability, identifying purposes, consent, limiting collection and use, and transborder data flows. Again, as the Data Code is non-binding, the only measures which may protect personal data are found in specific provisions of relevant legislation.

[54] Graham Greenleaf, "Singapore takes the softest privacy options," (2002) 8 *Privacy Law & Policy Reporter*, pp 169–173.

[55] *Ibid.*

## Key Issues in Harmonisation: Transborder Data Flow and Information Privacy

The issue of multi-lateral legal recognition of certifications authorities may be seen as similar to the notion of cross-fertilisation. Cross-Fertilisation is defined as:

1. Fertilisation by the union of gametes from different individuals, sometimes of different varieties or species. Also called *allogamy*.
2. Mutual exchange, as between dissimilar concepts, cultures, or classifications, that enhances understanding or produces something beneficial.[56]

This paper has argued that the facilitation and growth of e-commerce requires harmonisation. Traditionally, harmonisation has referred making the technologies of PKI interoperable between certification authorities. The notion of harmonisation needs to be expanded to the legal forum to allow for the multi-lateral legal recognition of certification authorities.

Multi-lateral recognition of certification authorities involves three key components:

1) harmonisation / interoperability of technologies (which is not considered in this paper),[57]
2) harmonisation of legal regulations in the PKI framework, and
3) harmonisation / sufficient threshold of personal data privacy protection

The harmonisation of legal regulations in the PKI framework would ideally encompass several key elements. It is not the objective to ensure that legal frameworks are identical or even substantially similar. The key objective is to ensure that CAs receive the same legal treatment in foreign jurisdictions. This would ideally apply to both licensed and unlicensed certification bodies. Similar legal treatment would include the ability to reasonably limit liability and presumption of evidentiary matters where digital signatures are used. In order to allow for multi-lateral legal recognition of certification authorities, certain thresholds must be met:

- secure technology,
- secure personnel and management policies,

[56] Definition found at http://www.answers.com/topic/cross-fertilization (last accessed 24 Apr 2005).
[57] The technological harmonization of PKI technology is no small feat. For a comprehensive look at many of the issues involved refer to previous references (n 3 above).

- secure certification and private/public key management, and
- the security of the maintenance, collection and use of personal data both within the jurisdiction as well as in the case of transborder data flow.

Licensed certification authorities in Hong Kong and Singapore squarely meet these thresholds with the potential exception of security of personal data. The PRC currently does meet these criteria though this may not be the case once supplemental rules and regulations are enacted – one must remember that the *E-Signature Law* only came into effect on 1 April 2005. In this respect, the cross-fertilisation of PKI laws and regulations of Hong Kong, PRC and Singapore will *likely* provide a, "mutual exchange, as between dissimilar concepts, cultures, or classifications, that enhances understanding or produces something beneficial."

Unlicensed certification authorities do not, on the surface, meet the aforementioned thresholds. In Hong Kong, unlicensed CAs are governed by the Common Law and are free to do as they please within the confines of the law. In Singapore, many principles of the ETA apply to non-licensed CAs but the important Security Guidelines and CA Regulations do not. This is not an issue in the PRC as CAs must be licensed.

It has been argued that a high level of security of personal data coupled with effective privacy laws must be met in order to for multi-later legal recognition of certification authorities in the Asia region.

The issue of security of personal data and privacy are particularly acute in the Asia region where many jurisdictions have either weak or no legislation at all in the area; Singapore and the PRC fall within these respective classifications. Where some jurisdictions do have relevant legislation, often it does not apply to private corporations as in the case of Singapore (though arguably Singapore does not have adequate legislation applicable to government either). A further problem emerges where privacy legislation binds the government. Most privacy laws, especially in the Asia region (though this is the case in many parts of the world after 11 September), contain a carve-out section which provides a list of exemptions. Common exemptions are criminal investigation and national security. National security ideology has been used by authorities in Asia as a means to purportedly justify human rights infringement. This has led to a pervasive climate of surveillance under the rubric of national security. While this paper has not wish to dwell on the issue of human rights infringement, it would be negligent not to at least mention the problem (admittedly, this problem is more readily associated with state interception of communications and surveillance as opposed to protection of personal data). Even where privacy laws appear to be strong, as in the case of Hong Kong, in practice, the reality may prove otherwise.

Sufficient personal data protection and privacy law are important not only within the domestic scene, but are important with the transborder flow of data. Transborder flow in data refers to information found on the certificates as well as the content of the transaction between parties in different jurisdictions. This may take place in the form of a transaction. It may also take place where a CA has outsourced its functions to a place outside of its place of business (most often China and India – two countries with questionable privacy records and a high level of corruption).[58] Transborder data flow may also occur where governments request access to data – both the identity of the data senders as well as the actual data coming in and out of its jurisdiction through the use of PKI.

Issues of personal data protection and privacy law should not be viewed as an area of incompatible norms and social policy, but rather, should be viewed as an evolving area of law. There is room for cross-fertilisation. That is a, "mutual exchange, as between dissimilar concepts, cultures, or classifications, that enhances understanding or produces something beneficial." There is room for education, and continued cooperation between countries in the Asia region. In fact, much of the groundwork has been laid with the writing of the APEC privacy principles.[59] Furthermore, China is looking to adopt its first privacy law and more importantly, it looks as though this will be an open and debated process within the writing of the legislation. As Asians themselves begin to incorporate the concept of privacy into their culture, privacy is increasingly seen as an important value. For these reasons, the notion of cross-fertilisation remains a possibility in the Asia region.

The author recommends that when regulatory bodies negotiate recognition of foreign CAs, that attention is paid to the protection of personal data and privacy laws in the region. While it may not be possible for a government body in one jurisdiction to persuade another to enact personal data legislation, it is possible to insist that only CAs whose Certification Practice Statements and User Contracts provide for personal data protection will be legally recognised in a foreign jurisdiction. Though not an ideal solution, it offers a workable and practical means of ensuring that there is a minimum level of privacy of personal data.

The facilitation e-commerce in the Asia region remains an important goal. E-commerce will undoubtedly benefit from the promotion of secure methods of transacting over the Internet. PKI provides a secure environment for

[58] *See* for example a report by Rediff Corporation on outsourcing initiatives available at http://in.rediff.com/money/2005/mar/24bpo1.htm. For information relating to bribery and corruption reports see Transparency International Bribe Payer's Index available at http://www.transparency.org/cpi/2002/bpi_faq.en.html (last accessed 18 Oct 2005).

[59] *See* privacy principles espoused at APEC at http://www.export.gov/apececommerce/privacy/consultation-draft.pdf (last accessed 18 Oct 2005).

electronic transactions. Certification authorities who act as trusted third parties in the issuance of digital signatures and certificates used in PKI, must meet many criteria in order to ensure that PKI is a secure method of transacting. As such, Hong Kong, Singapore and the PRC have enacted legislation to regulate CAs. It has been argued that there should be a multi-lateral legal recognition of certification authorities in the Asia region but only where there exists a high level of security of personal data coupled with effective privacy regulations extending to the use of PKI and to the Certification Authorities responsible with issuing digital signatures and certificates.