

Regulatory Issues with Certification Authorities

Dr. Nassar Ikram* & Athar Mahboob‡

* National University of Sciences & Technology, Rawalpindi, Pakistan
nassar@pnec.edu.pk

‡ National University of Sciences & Technology, Rawalpindi, Pakistan
athar@pnec.edu.pk

Synopsis

With the recent promulgation of the Electronic Transactions Ordinance, 2002 finally the way has been cleared to include Digital Signatures and Electronic Transactions in the legal framework of the country. As a result Pakistan has taken a giant leap into the emerging global electronic economy. However, digital signatures are meaningful only within the existence of a reliable certification authority (CA) infrastructure also known as Public Key Infrastructure (PKI). Such a PKI has to be established based on internationally accepted norms and standard practices. The Certification Council formed under the ordinance has an uphill task of developing the standards related to various aspects of the certification authorities, including, but not limited to: (1) criteria for Certification Service Providers or CSP's (2) operational policies and procedures for CSP's (3) approved products for CSP's (4) standards on hardware and software configuration (5) standards for facility configuration and operations management (6) standards on encryption algorithms and key sizes (7) standards for key recovery/key escrow. The task is mammoth. However, a lot of guidelines and documented experiences are available from the relevant international agencies such as UNCITRAL, ITU and IETF. At the same time a lot can also be learnt from the experiences of other digitally developed countries. This paper elaborates on these very important regulatory issues and provides a comprehensive set of references for further information on the subject of regulatory issues for certification authorities.

1. Introduction

The world over countries have been making amendments in their laws to allow for digital signatures as valid legal instruments. One of the first governments to do so was the State of Utah in the United States, which passed the Utah Digital Signatures Act in 1995 [1]. Singapore passed the Electronic Transactions Act (ETA) in 1998 [2]. Malaysia's Digital Signature Act 1997 was also enforced in 1998 when the first certification authority was made operational in that country [3]. Finally the Government of Pakistan, realizing the urgency and importance of the issue, enacted the Electronic Transactions Ordinance 2002 [4], which is a step in the right direction. The Electronic Transactions Ordinance 2002 provides for amendments to existing laws in order to bring media-neutrality of statutes with special reference to electronic information and also sets forth the evidence rules for electronic records. However, the recognition of electronic signatures in the legal system has to be combined with a reliable certification authority system in the country. The Electronic Transactions Ordinance has created the Certification Council, which is charged with that responsibility. In performing its duties the Certification Council will confront the multidimensional issues in regulating the Certification Service Providers, which are highlighted in this paper. An outline of this paper is now given. In §2 we briefly discuss the concepts of digital signatures, digital certificates and certification authorities. In §3 we explain the importance of the system of digital certificates and certification authorities, known as the Public Key Infrastructure or PKI, to E-commerce. In §4 we justify the need for the regulation of the certification authority system by government. In §5 we present the important issues that arise in the regulation of certification authorities. Finally, we conclude in §6 by providing a list of important steps the Certification Council will need to take in order to fulfill its obligations under the Electronic Transactions Ordinance 2002. At the end we provide a comprehensive set of references for further information on the subject.

2. Digital Signatures, Digital Certificates and Certification Authorities

It is essential to understand the concepts of digital signatures, digital certificates and certification authorities. These are described below.

Digital Signatures

A digital signature is a unique bit-pattern that depends on:

- The message/information which is being signed and
- The author/sender/signer of the message

Although it is conceptually possible to base the digital signature on symmetric encryption but that type of a digital signature cannot be widely used because between each pair of communicating parties a separate key is required and also because either of the parties could forge a signature with that key and blame the other party. Public Key Cryptography which was proposed in 1976 by Whitfield Diffie and Martin Hellman [5] provides for a much more widely usable form of digital signature that is generated using a person's private key and verified using his/her public key. Since the public key is not secret, any one may easily verify the signature and because the private key is not known to anyone except the sender only he/she may generate a valid signature. Digital signatures are very important mechanisms of information

security. In particular by associating the identity of the author/sender/signer with the message they provide following security services:

- **Non-repudiation:** the sender of the message cannot later deny having sent the message.
- **Proof of Origin:** the source of the message is verified to the receiver.
- **Message Integrity Check:** if the digital signature verifies then the receiver also has the assurance that the contents of the message are original and have not been modified by any malicious entity.

There are several mathematical algorithms that can be used to create a digital signature such as those given in [7], [8] and [14]. For the purpose simplicity and understanding following general steps are involved in creating a digital signature:

1. The sender generates a digest of the message (M) using a one-way hash function H (e.g., SHA-1 [13], MD5 [10], etc.)
2. Sender encrypts the digest of the message, $H(M)$, produced in step 1 with his/her Private Key and appends that value to the message and transmits the resulting value
3. The receiver decrypts signature value using sender's Public Key and compares with the digest of the message computed at receiving end
4. A match verifies the signature and vice versa

Figure 1 shows this process diagrammatically.

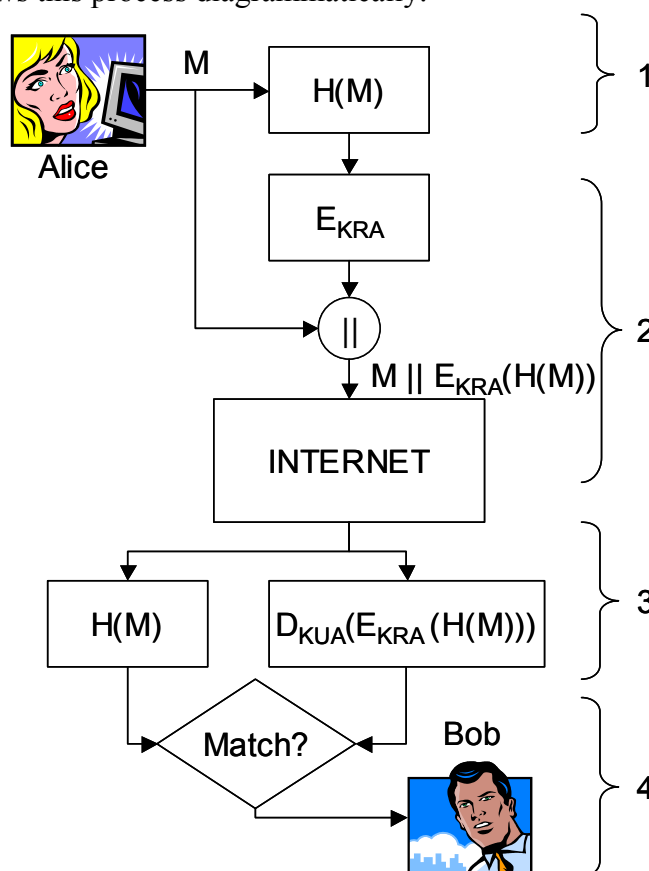


Figure 1. Steps involved in making a digital signature

Digital Certificates

There is one important aspect of the digital signature scheme as described above that has been overlooked. That is, how does the receiver know that the public key which verifies the signature is indeed the sender's public key? As far as the receiver is concerned it needs a bulletproof assurance that the public key that it uses to verify the signature belongs to the entity it thinks it belongs to. There are two possible solutions to this problem:

- **Face-to-Face Meeting:** The sender gives the public key to the receiver in person prior to the exchange of any electronic messages and the receiver stores it securely. This is not very practical, at least for most entities in the world that would like to exchange information over the network and engage in any transactions electronically.
- **Digital Certificates:** The receiver uses a digital certificate issued by a party which both the sender and receiver trust to verify the authenticity and integrity of the public key of the sender.

A digital certificate is an electronic document that is issued by a Certification Authority (CA) and certifies/authenticates a Public Key. In a nutshell the digital certificate becomes one's digital identity. Digital certificates are based on the X.509 standard [9]. A person may have more than one digital certificate, each based on a particular role/use. Digital certificates can be used in a large number of applications, for example:

- Secure email
- Authenticated access to a network service
- Conducting secure purchases on the Internet
- Signing official documents
- ...

Figure 2 shows the structure of an X.509 based digital certificate. The digital certificate contains the public key and the identity of the entity to which the certificate is issued. The receiver of a digital certificate verifies the authenticity and integrity of the certificate by checking the digital signature on the certificate.

Certification Authority

A Trusted Third Party (TTP) or Certification Authority (CA) generates the digital signature on the certificate using its private key. The certification authority's public key can be used to verify the signature on the certificates issued by it. The public key of the certification authority is already supposed to be installed in a secure and trusted manner on the computer of the party wishing to use the certificates issued by that certification authority. There are many issues involved with the technical design of digital certificates and the relationships of various certification authorities with each other. Some good references on the subject of digital certificates and the Public Key Infrastructure are [6], [11] and [12].

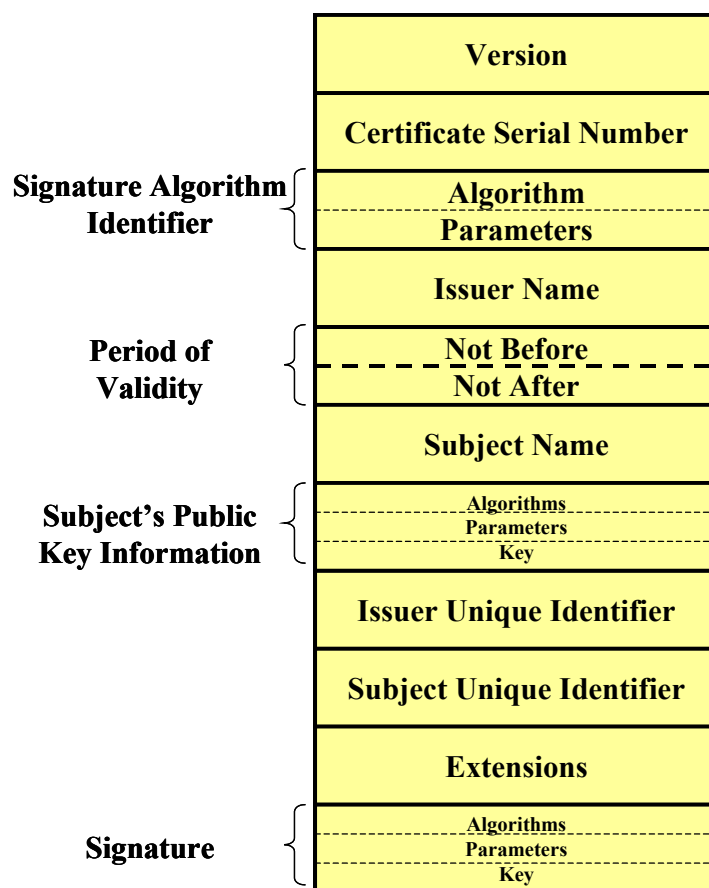


Figure 2. The structure of an X.509 Digital Certificate

3. E-commerce and PKI

E-commerce requires the existence of a system of certification authorities which is called a Public Key Infrastructure. In the PKI, certification authorities act as the Trusted Third Parties (TTP). A certification authority may also be called a Certification Service Provider (CSP). This name is less objectionable and has been used in the Ordinance. The reason is that some people object to the use of the term “Authority” [15]. Authority implies a governmental power and many of the certification authorities established in the initial years operated as businesses outside any control of the government. Furthermore, most certification authorities in the future, it is foreseen, will be operating in the private sector. Hence it is better to use the term Certification Service Provider (CSP) for the business entities that issue and verify digital certificates. On the other hand a government has to create a Registration Authority (RA) that licenses and regulates the entities that are involved in providing certification services. Because CSP’s/CA’s make up the PKI and are necessary for secure national and international E-commerce and Electronic commerce is to going proliferate further with the passage of time, this implies that CSP’s role will become more important with the passage of time. The situation will be exacerbated by the exponential growth being forecast for the M-commerce. Since all E-commerce will depend on the trust provided by the CSP’s they themselves would need to be monitored and regulated very carefully to ensure public’s continued confidence in that trust. Figure 3, adapted from [22], shows the role of certification authorities in the overall scheme of E-commerce.

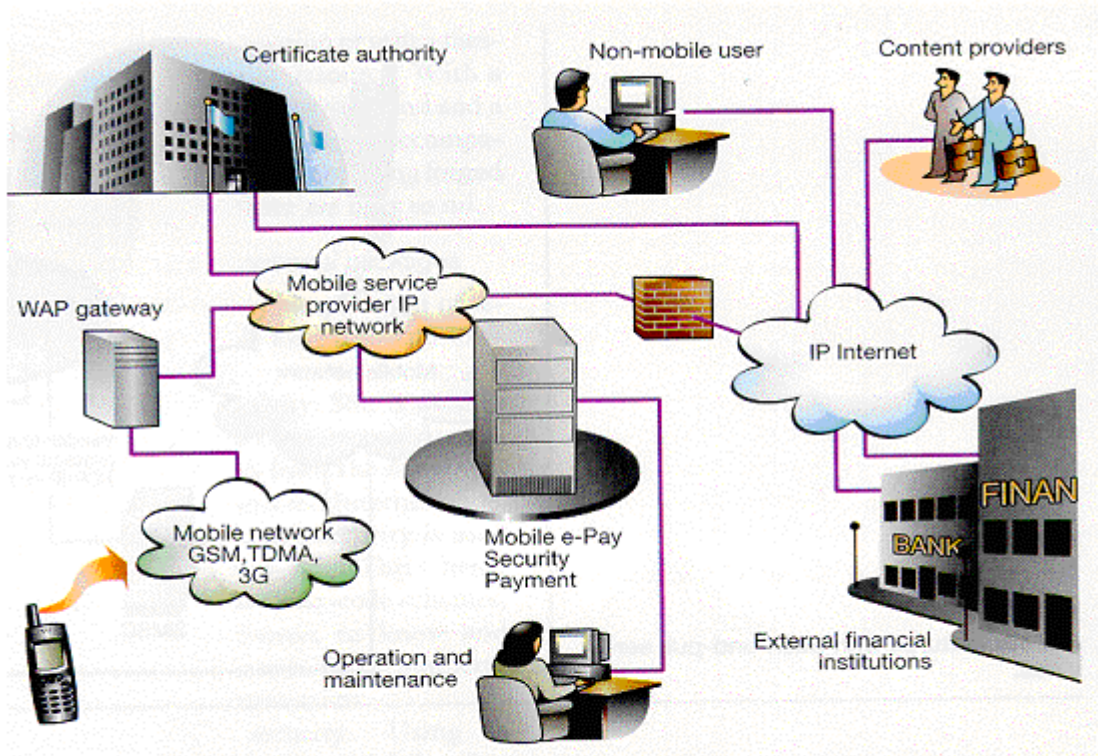


Figure 3. Role of Certification Authorities in E-commerce

Since a single certification authority is undesirable due to performance and reliability reasons, not to mention the geographic and political compulsions, a system of CA's has evolved globally. Figure 4 shows this phenomenon.

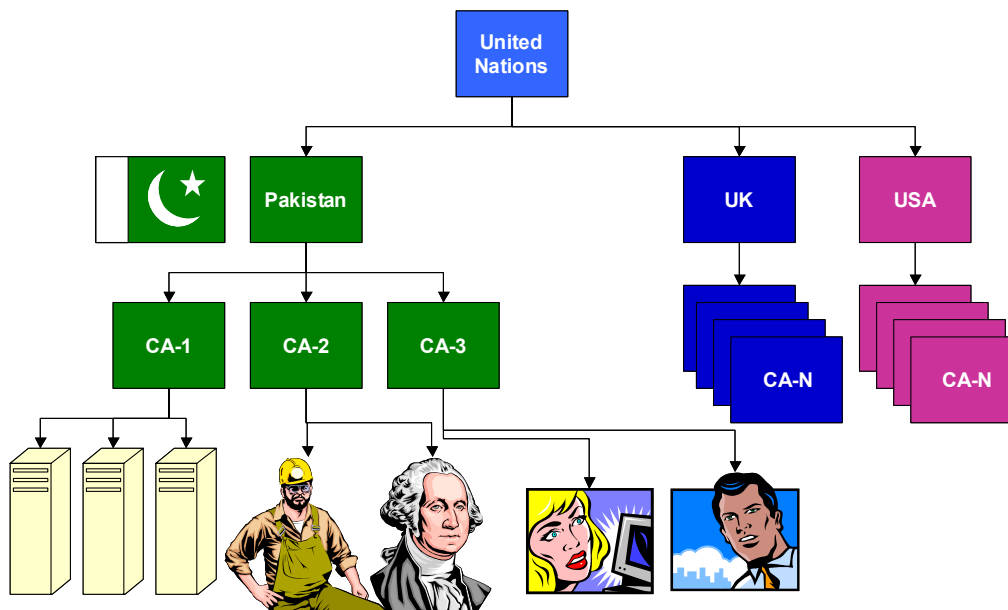


Figure 4. A system of certification authorities

4. Role of the Government in Regulating Certification Authorities

Having established that certification of public keys is a service extremely vital for the E-economy, it is prudent to ensure the non-stop and reliable availability of this service. It is clear that the government does not and cannot run the economy so it should allow Certification Service Providers in the private sector to operate as businesses. As a result there will be many certification authorities and the resulting competition will benefit the consumers in terms of quality of service and cost of service. However, the government needs to ensure interoperability between the CSP's. Having said that the government will still need to have its own CA's for governmental use.

If the CSPs are left unregulated then one can forecast the following disadvantages:

- Rouge CSP's can cause harm to public locally
- May be used internationally for criminal activities
- Pakistan might become excluded from global E-economy

In view of the seriousness of the harmful effects of not doing so, the government must regulate CSP's in public interest. In doing so the government must make rules so that only genuine entities can set up CSP's. The monitoring function must ensure that everyone follows the rules of the game – since public trust in CSP's depends on integrity and security of CSP's practices and procedures. The regulatory function of the government will also ensure interoperability where required. The importance of regulating certification authorities is borne out from the fact that many of the digital signature legislations of individual countries and states spelled out those regulations along with their digital signature laws. As an example, in the case of Malaysia, the digital signature law became effective only when a certification authority was created.

The Electronic Transactions Ordinance 2002 provides for a Registration Authority for CSP's in the form of a five member Certification Council, which would make the regulations for certification service providers and enforce them. The Certification Council should ensure that national CSP regulations conform to international norms and standards such as:

- United Nations Commission On International Trade Law (UNCITRAL) Working Group on Electronic Commerce [16]
- International Telecommunications Union (ITU) [19]
- Internet Law and Policy Forum (ILPF) [17] and Internet Engineering task Force (IETF) [18]
- Other digitally developed countries – USA, UK, Malaysia, Singapore [20], Australia [21], etc.

A word of caution is also in order. The government should not over-regulate. Intelligent/smart regulation is needed, not more regulation.

4. Important Regulatory Issues

The regulations related to Certification Service Providers (CSP's) have to be comprehensive in terms of covering regulations on:

- Who is allowed to become a CSP?

- The procedure for application for CSP and its evaluation
- Time duration of the license issued to a CSP
- Rules of operation for a CSP
- Rules on assurance of service availability
- Procedures for audit of a CSP
- Penalties in case of non-compliance of a CSP with the regulations

Table 1 lists the several important items for consideration in forming the regulations for CSP's and provides a description of each item. In coming up with this list, CSP regulations of Utah [1], Singapore [20] and Australia [21] have been considered as guidelines.

Table 1. Important Items for Certification Service Provider Regulation

S. No.	Regulation Item	Description
1.	Financial Viability	Only financially very strong entities should be allowed to establish a CSP. In addition the CSP should be insured against liability of loss for claims arising out of errors or omission by the CSP, its officers or employees.
2.	Service Assurance Guarantee	The CSP is to be bound by very stringent service assurance guarantees. For example, this could include a value of sub 1% aggregate down time over a 30-day period and a maximum single down time whether scheduled or unscheduled of less than 30 minutes.
3.	Compliance with government requirements for communications security	The CSP regulation must specify the communication security requirements for a CSP. These requirements are intended to ensure that the mechanisms supporting the confidentiality of communications between a CSP and Certification Council are appropriate for the sensitivity of the data being communicated. Important items would include physical security of keys and key generation equipment, accounting and distribution of keys, key initialization keys, and key generation equipment and violation reporting mechanisms.
4.	Legal Issues such as: <ul style="list-style-type: none"> • Privacy • Data protection • Liabilities of Service Providers • Intellectual property rights, copyright • Digital signatures • Electronic contracts • Consumer protection • Jurisdiction for Cross-border transactions 	The CSP regulations must address these legal issues. Some of these have been partially addressed in the Ordinance.
5.	Technology issues such as: <ul style="list-style-type: none"> • Digital Signature schemes to be supported • Encryption algorithms • Key sizes for various algorithms 	Algorithms and Key Sizes, both for Public Key and Symmetric encryption, also for Digital Signatures. These must keep US export restrictions in mind. An important issue to be addressed is Key recovery/key escrow – when and how?

6.	Standards for Operational Policy and Procedures	There are several aspects of the CSP operation that need to be tightly regulated. These include issues ranging from hiring of employees by CSP to the use of hardware and software products by the CSP. Some of these are discussed in following items.
7.	Approved Products	All CSP products will have to be approved by Certification Council against recognized information security criteria. This includes products that will be used in the creation and handling of certificates and/or digital signatures which may be used to protect any information including classified information or information that has a high value.
8.	Hardware and Software Configuration	These regulations will ensure that the approved hardware and software products utilized by the CSP have been installed and configured in their most secure state - this shall be called the security baseline. The CSP systems are to be protected by appropriate physical safeguards, have no connections except through an accredited gateway, have been 'hardened' in terms of the removal of unwanted facilities/services and have only acceptable technical vulnerabilities.
9.	Configuration and Operations Management	Configuration and operations management is a process that aims to ensure that the security baseline established at start-up does not erode over time. This requires the existence of mechanisms to ensure that change is managed properly; that appropriate activity monitoring and logging capabilities are established and utilized; that mechanisms are in place to ensure that appropriate levels of operator skills are maintained; and that all operations staff are aware of their tasks and responsibilities.

Table 2 lists and describes some of the important documents that have to be prepared by a CSP along with its application for the CSP license [21].

Table 2. Important Document for Certification Service Providers

S. No.	Document Name	Description
1.	Certificate Service Provider concept of operations	This document will describe, at a high level, the PKI services offered by the CSP, a functional description of the services offered and the management and security arrangements supporting the functions performed by the CSP.
2.	Certification Policy Statement	These statements will describe the PKI certification framework, mechanisms supporting the application, issuance, acceptance, usage, suspension/revocation and expiration of certificates signed by the CSP, and the CSP's legal obligations, limitations and miscellaneous provisions. The Certificate Policy Statement describes the policy for each certificate issued by the CSP in terms of its approved usage and validity.
3.	Agreements with Certification Council	These documents define the relationship between the CSP (certificate issuer) and the Certification

		Council (certificate provider) in terms of their respective responsibilities for the secure operation of the national PKI. Areas of concern will be subscriber identification and verification, subscriber revocation, operational requirements and representations made by the parties.
4.	Subscriber agreement	This Subscriber agreement document will define the undertakings that subscribers will make in order to obtain and use certificates confirming their digital identities. It is expected that this will be part of the terms and conditions used to encourage user participation in the electronic service delivery. The agreement should make it clear that the user accepts all liability where the keys are generated by means other than a Certification Council accredited product.
5.	System Security Plan (SSP) and Standard Operating Procedures (SOP)	These documents describe the security safeguards that will be put in place to protect the operable products utilized by the CSP.
6.	Disaster Response Plan (DRP)	<p>This DRP will describe the emergency response procedures to be followed in the event of:</p> <ul style="list-style-type: none"> • A natural calamity affecting the function of the CSP operable product; • A security incident or suspected security incident affecting the operation of the operable product; • A compromise of the CSP's private key; or • The failure of the CSP audit trail mechanisms. <p>The DRP will include mechanisms for the preservation of evidence of system misuse, the purpose of which could be evidence admissible in a court of law at some later date.</p>
7.	Certificate Key Management Plan	This purpose of this document is to describe in detail those procedures that are required to ensure that CSP clients can have the highest possible level of assurance that critical functions have been identified and have been provided at appropriate levels of trust. Areas of concern will be CSP private key security, subscriber key recovery, certificate publication and integrity, privileged user management, key generation and transfer mechanisms.

A very important point related to the CSP regulations is their proper enforcement. Any set of regulations is only as good as its enforcement. This requires that the Certification Council obtain services of professional experts in the area. No doubt that the composition of the Certification Council, as given in the ETO itself, is indicative of the recognition of the very high-tech nature of the business of certification. The team at the disposal of the Certification Council needs to be of high quality and of a good enough size to be able to do the job properly. For this purpose the Certification Council would need to decide on rational amounts of fees for processing CSP license applications and issuing CSP licenses so that it also covers its costs.

5. Conclusion

To make the Electronic Transactions Ordinance effective, the Certification Council needs to:

- Quickly develop national standards and regulations for CSP's
- Grant CSP license to at least two parties who fulfill the CSP's license criteria
- Accelerate the establishment of model CSP in public sector, e.g. State Bank of Pakistan ...

Due to the complex nature of its assignment, the Certification Council needs experts:

- To help in developing the national standards and regulations relating to CSP's
- To evaluate new technology and products for approval for use by CSP's
- To evaluate CSP's compliance with regulation

While making full use of the readily available international documentation and experience on the subject, it would be prudent of the Certification Council to also utilize the services of the experts available locally to achieve its important mission.

References

- [1] The State of Utah Digital Signatures Act, available at <http://www.jmls.edu/cyber/statutes/udsa.html>.
- [2] Singapore Electronic Transactions Act (ETA) 1998, available at <http://www.cca.gov.sg/>
- [3] Malaysia Digital Signature Act 1997, available at <http://www.geocities.com/Tokyo/9239/digisign.html>.
- [4] Electronic Transactions Ordinance 2002, Government of Pakistan, available at <http://www.most.gov.pk/Final%20Draft%20of%20Electronic%20Transactions%20Ordinance%>
- [5] Diffie W., Hellman, M. E.: New Directions in Cryptography, IEEE Transactions on Information Theory, v. IT-22, n. 6, Nov. 1976, pp. 644-654
- [6] Branchaud, M.: A Survey of Public key Infrastructures, MS Thesis, McGill University, Canada, 1997
- [7] ElGamal, T.: A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory 31 (1985), 469-472
- [8] Rivest, R. L., Shamir, A., Adleman, L.M.: A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM (2) 21 (1978), 120-126
- [9] Housley, R., Ford, W., Polk, W., Solo, D.: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC 3280, April 2002
- [10] Rivest, R. L.: The MD5 Message-Digest Algorithm, RFC 1321, 1992
- [11] Kuhn, D. R., Hu, V. C., Polk, W. T., Chang, S.: Introduction to Public Key Technology and the Federal PKI Infrastructure, NIST Publication, February 26, 2001
- [12] NIST Special Publication 800-21: Guideline for Implementing Cryptography in the Federal Government, November 1999
- [13] National Institute of Standards and Technology: Secure Hash Standard, Federal Information Processing Standards Publication 180-1, April 17, 1995

- [14] National Institute of Standards and Technology: Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186, May 19, 1994
- [15] Ellison, C., Schneier, B.: Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure, available at <http://www.counterpane.com/pki-risks-ft.txt>
- [16] Background documents regarding the UNCITRAL Model Law on Electronic Commerce, available at http://www.uncitral.org/english/sessions/wg_ec/ml-ec-bckdocs/index.htm
- [17] An Analysis of International Electronic and Digital Signature Implementation Initiatives, available at http://www.ilpf.org/groups/analysis_IEDSII.htm
- [18] <http://www.ietf.org/html.charters/pkix-charter.html>
- [19] <http://www.itu.int/osg/sec/spu/ni/esca/>
- [20] Singapore Electronic Transactions (Certification Authority) Regulations 1999, available at <http://www.ida.gov.sg/>
- [21] Australia GATEKEEPER - A strategy for public key technology use in the Government, available at <http://www.ogit.gov.au/>
- [22] Ntoko, Alexander: E-Commerce Issues for Policy Makers, Regional Seminar on E-Commerce, E-Commerce Centres, Bucharest, Romania, 14-17 May 2002, available at <http://www.itu.int/ITU-D/e-strategy/Seminars/Romania/presentations.html>