Compliance of X.509 Certification Standard in the Implementation of Third Party Certification in Malaysian E-Commerce Websites

Syahida Hassan
Mohd Khairudin Kasiran
Graduate Department of Information Technology
Universiti Utara Malaysia, Sintok Kedah, Malaysia
syahida@uum.edu.my
mkasiran@uum.edu.my

Abstract
The concept of trusted services forms a key issue for any kind of electronic services. Third Party Certification (TPC) endorsement has been used as one of the methods to instill consumers' trust. Creating initial trust through implementation of TPC is very important because the consumer has a tendency to trust brand names.. This paper looked closely at the implementation of the TPC in Malaysia which reveals that there are many problems related to the implementation of these seals. Problems like the awareness of merchants on the important of third party seals to their business, unverifiable endorsement, misleading link, unauthorized use of logos and no endorsement at all are still there in Malaysian environment. Based on this fact, the paper will focus on how far the implementation of third TPC is complied with X.509 certification standard. The output of this study can give an important background on the current implementation of TPC and be used as a basis of initial evaluation for business opportunity as a service provider for this kind of certification in Malaysia

1. Motivation

E-Commerce is a business channel where the environment is created in the virtual world through connection of electronic devices. The setting of E-Commerce has open up the world of business into a single digital market where buyer and seller are no longer restricted to physical boundaries such as geographical or time differences [7]. E-Commerce is expected to have major influences in shaping the future of business to consumer segment [16].

E-Commerce had grown into a potential business in Malaysia. In 2003, Malaysian secretary of International Trade and Industry Ministry, Datuk Fu Ah Kiow announced that the E-Commerce grant scheme will be increased to US$ 5.26 million to enhance information and communications technology (ICT) usage among small and medium enterprises (SMEs) [17].

The fast rising number of broadband user also give significant changes in E-Commerce usage in Malaysia. According to [14], broadband will help make E-Commerce attractive to users. So, as more people connect to the Internet through faster connection, it is good news for those who venture online to sell their goods.

Despite the bright prospect of E-Commerce in Malaysia, however, according to the Taylor Nelson Sofres survey, only 3% of Malaysian Internet users shopped online in 2002, compared to 4% in 2001. Thirty-eight percent of Malaysians felt that it is safer buying goods or services in a store and 36% of them do not want to disclose their credit card details [8].

[14] said most people in Malaysia already used E-Commerce but the fact hasn't fully registered in their consciousness. This statement is proved by the number of people who bought airlines and cinema ticket via Internet. When Malaysian purchase stuffs like books, toys and gadgets, they end up buying from retailers located thousands miles away instead of local retailer. That's because Internet surfers have become familiar with overseas retailer. For example Amazon.com.

Security-related issues were cited as the main reason for not shopping online. The Malaysian consumer's lack of confidence and trust in E-Commerce transactions is further accentuated by the fact that the Consumer Protection Act specifically excludes protection in electronic transactions [8].

According to Giddens [5], trust is defined as confidence in the reliability of a person or a system, regarding a given set of outcomes or events, whereby that confidence expresses faith in the probity or love of another, in the correctness of abstract principles. The main condition that creates a need for trust is lack of full information. Therefore trust has to be created.

In the E-Commerce setting, establishing trust is difficult. It is because E-Commerce exists in a virtual marketplace, so different kind of trust environment is

required compared to traditional physical environment. Trust represents an evaluation of information. The difficulty to prove someone's physical presence and establish a direct relationship between two parties involved in the transaction caused this difference to exist. The inability of the participants to use physical gesture such as body language, eye contact and personal proximity to evaluate trustworthiness of each other make the problem of establishing trust between them in cyber world even more difficult compared to brick and mortar world [15].

A closer look at E-Commerce transaction cycle shows that consumers are in a disadvantaged position especially if the product is non-digital and non-service product. Consumers are expected to fulfill their obligation first by committing their financial and information resources in the transaction before the merchants are able to proceed with their obligation. Therefore the requirement for establishing merchant trust will be a very important factor in an E-Commerce market place setting [1],[6].

In addition, the low barrier level for both parties to enter and leave the digital market space has prompted the two parties to assess the level of risk involved before trusting each other in an E-Commerce transaction. Since consumers are the one who usually initiates E-Commerce transaction, trust creation from consumer to merchant or merchant trust will be very important [10].

In Malaysia, the same issue of trust seems to be the one of the reasons why Malaysian do not shop online. Even though the statistics shows that E-Commerce in Malaysia is growing faster, most Malaysian consumers are not confidence with E-Commerce transactions.

IBM (taken from [2]) in their survey in January 2006, stated that 70% Internet users only use Internet shopping sites that display a security protection seal. Harris Interactive stated that having a company's security verified by a third party would lead 9 in 10 consumers to do more business with such a firm (taken from [2]).

The concept of trusted services forms a key issue for any kind of electronic services. Based on the literature, third party certification (TPC) endorsement has been used as one of the methods to encourage consumers' trust. Creating initial trust through implementation of TPC is very important because the consumer has a tendency to trust brand names.

Several studies on TPC endorsement have been conducted in the past by several researchers such as [3], [4], [12] and [13] in United States and Europe. All of these researches conclude that TPC endorsement has some impact on influencing consumers to proceed with the digital transaction. The influences of TPC endorsement in creating trust toward merchant become more significant, especially to unknown merchants where the perceived risk is higher than well-known merchant like Amazon.com [11].

TPC endorsement providers may come from government or private base organizations and offer a wide range of assurances such as quality assurance, code of conduct, code of practice, rating service, privacy etc. Some of these providers require fee from merchants for using their assurance seals in the merchant's website but some of them provide the service without any charges.

Among major services that are being offered by the third party assurances are:

i. verifying the legitimacy of the company (existence).
ii. ensuring certain standard of network security has been put in place by the business organisation (performance).
iii. acting as protector to the consumer if something goes wrong in the transaction (policy/procedure).

A great number of researches had been carried out academically or professionally on the role and effect of third party endorsement on E-Commerce website but none of the research focused on Malaysian environment. Therefore, this research is intended to fill the gap. This research will investigate the implementation of TPC in Malaysian E-Commerce website. X.509 guideline on how to ensure secured transaction on the Internet is used as a based to measure the implementation of TPC in Malaysian environment

2. X.509 Certification Standard

There are a number of trust-models on the Internet providing authentication which attempt to achieve the maximum of trust with minimum of risks. These include X.509 standard Public Key Infrastructure (PKI), other PKI such as Pretty Good Privacy (PGP), the Simple Public Key Infrastructure (SPKI) and a Simple Distributed Secure Infrastructure (SDSI). These models use public key encryption techniques, certificates, and digital signatures. A certificate is used as a trust-token between different parties on the

Internet to tell others you are really who you say you are [19].

X.509 is published as ITU recommendation ITU-T X.509 (formerly CCITT X.509) and ISO/IEC/ITU 9594-8 which defines a standard certificate format for public key certificates and certification validation. X.509 (Version 1) was first issued in 1988 as a part of the ITU X.500 Directory Services standard. When X.509 was revised in 1993, two more fields were added resulting in the Version 2 format. These two additional fields support directory access control. X.509 Version 3 defines the format for certificate extensions used to store additional information regarding the certificate holder and to define certificate usage. Collectively, the term X.509 refers to the latest published version, unless the version number is stated [18].

To ensure transaction security in X.509, the following elements are necessary:

i. **Authentication-** securing the identities of the parties to a transaction
ii. **Integrity** - ensuring that that information or process has not been modified or corrupted without detection
iii. **Non-repudiation** - ensuring neither party can refute that the transaction occurred, i.e. ensures that the transaction is binding.
iv. **Confidentiality** - ensuring that the information is kept private

3. Objective

The overall objective of this research is to investigate the compliance of X.509 certification standard with the implementation of TPC in the Malaysian B2C E-Commerce web sites

To fulfill the objective of this research, a few questions must be. The following are the research questions:

i. How many of the sample websites have TPC in digital storefront?
ii. What type of TPC is used in this digital storefront?
iii. How far is their implementation complied with the X.509 certification standard guideline produced by International Telecommunication Union (ITU) (authenticity, integrity, non-repudiations and confidentially)

4. Scope

This research will focused on Malaysian B2C E-Commerce website with:

i. non digital and
ii. non service product.

These 2 types of E-Commerce website are chosen because of the following reasons:

i. For digital and service product, customers will instantly get their product once they transmitted their credit cards number
ii. For non digital and non service product, customers have to wait for the product a few days (week) after transmitting their credit cards details.

In this case, the risk for non digital and non service product are higher than the digital and service product and the trust issues are relatively higher for this type of E-Commerce website.

5. Methodology

Based on the objectives and scopes of the research, content analysis is adopted to be the suitable methodology for this research.The content analysis methodology used in this research is divided into the phases:

i. Sampling
ii. Data Collection
iii. Descriptive Statistic.

Sampling

The first step to complete this research is choosing the sample of potential Malaysian B2C E-Commerce website. The overall method of choosing the potential respondent of websites is done through convenience sampling. This is due to the unavailability of a list for all Malaysian websites.

The sampling list is created by using two major search engines. Several keywords that might hit on the Malaysian based websites are chosen for the searching purpose.

The two major search engines are Yahoo and Google. Meanwhile, the phrase that being used to search the potential websites are:

i. “online shopping in Malaysia”,
ii. “online shopping”,
iii. “halaman dari Malaysia”,
iv. “buy online Malaysia” and
v. “online flourist + halaman dari Malaysia”.

The first 40 potential Malaysian B2C E-Commerce website were selected from the list of potential website that appears during the searching process. The URL of the websites is recorded for data gathering purpose.

Data Collection

The next phase of the research is the data collection phases. There are two types of data collection techniques in this research which were observation & interview

i. Observation

The data set were collected at three different point of time:

a. April 2006
b. July 2006
c. October 2006

The reason why the data set were collected at three different times is to see whether or not the same number of TPC seals was used by the e-commerce merchant. From the three data sets, we can compare the pattern of the usage of TPC seals whether there are changes in six months time.

Out of the 40 websites, which were chosen as a sample for this research, 7 of them were no longer available during the course of the research. The reason why they were no longer available was beyond the research scope. Therefore, the total website that had been used in this research was 33. However during the third data gathering (October 2006), the number reduces to 31 website due to the same reason. Refer Table 1 for the details.

Table 1: The data set

First Data Set	Second Data Set	Third Data Set
n = 33	n = 33	n = 31

For every data set, all of the selected websites were closely monitored to determine it there was any presence of TPC on their websites. If there is any TPC endorser link available on the website, the link of the TPC providers were followed to collect the data.

In other words, every website was monitored thoroughly and any TPC seals on the website were recorded by the following category:

a. Does the website have TPC seals?
b. How many TPC seals they have on the website?
c. Where did the merchants put the TPC seals?
d. Validity of the TPC seals.

Then the data were analyzed in order to answer the research questions as mentioned before.

ii. Interview

a. An interview was made with founder of a company that specializes in providing Ecommerce solutions to their clients in order to get a better understanding of the implementation of TPC in Malaysia.
b. Technology used in TPC application

After completing both observation and interview session, Draft ISO/IEC 9594-8 or X.509 Certification document is reviewed to get better understanding on the recommendation.

All of the data gathered in the previous phase was analyzed based on the research questions. Upon analyzing the data, the information obtained from the data gathering process is presented using a descriptive statistic method

6. Finding

Based on the first and second data set, out of 33 websites (n=33), only 13 websites (39.4%) had placed third party seals on their websites. Out of these 13 websites, 9 websites (69.2%) used the seals illegally or used unverified seals. Only 4 websites (30.8%) had a legal and verified seals.

The result is slightly different on the third data set whereby only 31 websites are available during the data collection. Out of 31 websites (n=31), only 12 websites (38.7%) had placed third party seals on their websites. 8 from the 12 websites used an illegal or unverified seals. It contributes 66.7% of the sample. The total websites that had a legal and verified seals are 4 or 33.3%

Table 2: Percentage of website with TPC seals

	First Data Set	Second Data Set	Third Data Set
Sample website (n)	33	33	31
Website with TPC Seals	13 (39.4%)	13 (39.4%)	12 (38.7%)

Table 3: Comparison between website with legal/verified seals and website with illegal/ unverified seals

	First Data Set	Second Data Set	Third Data Set
Website with TPC seals	13	13	12
Website	9 (69.2%)	9 (69.2%)	8 (66.7%)

with illegal/unverified seals			
Website with legal/verified seals	4 (30.8%)	4 (30.8%)	4 (33.3%)

Table 4: Percentage of website with legal/verified TPC compared to percentage of website with no seals or illegal/unverified seals.

	First Data Set	Second Data Set	Third Data Set
Website with legal TPC seals	4 (12.12%)	4 (12.12%)	4 (12.8%)
Website with illegal/unverified seals and website with no seals	29 (88.9%)	29 (88.9%)	27 (88.2%)

From the finding, it can be said that during the data gathering process, the usage of TPC in Malaysian B2C E-Commerce websites range between 30.8% and 33.3%. The percentage shows that Malaysian E-Commerce merchant is not utilizing the potential of the TPC seals on their website in order to attract their customer as 66.7% to 69.2% of the sample shows that they placed an unverified and illegal seals.

However, the data shows that merchants realize the potential of using the TPC seals on their website but did not use the legal and verified seals due to certain reason. Some of the reasons are:

i. The price of TPC seals may be not affordable for certain merchants, and
ii. The seal has been expired and not renewed by the merchant.

The standard addresses some of the security requirements in the areas of authentication, and other security services through the provision of a set of frameworks upon which full services can be base (ITU, 2001).

X.509 certification defines a framework for obtaining and trusting a public key f an entity in order to encrypt information to be decrypted by that entity, or in order to verify the digital signature of that entity.

Based on the Draft ISO/IEC 9594, it also defines a framework for obtaining and trusting privilege attributes of an entity in order to determine whether or not they are authorized to access a particular resource. The framework includes the issuance of a certificate by an Attribute Authority (AA) and the validation of that certificate by a privilege verifier.
In X.509, the directory uses public-key certificates in its provision of security services including:

i. strong authentication between and among directory components;
ii. authentication, integrity and confidentiality of directory operations; as well as
iii. integrity and authentication of stored data.

In other word, the following elements are necessary to ensure transaction security in X.509:

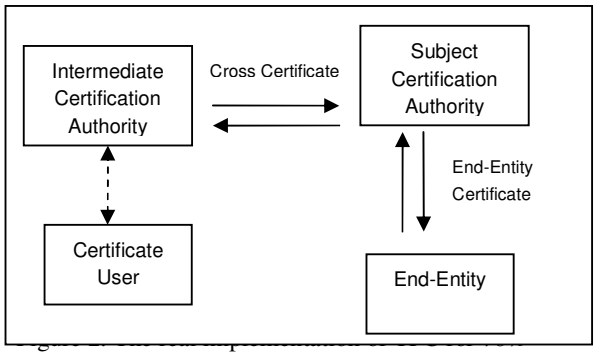
i. Authentication
ii. Integrity
iii. Non-repudiation
iv. Confidentiality

Based on the investigation done during the data gathering process, the implementation of TPC in Malaysian E-Commerce environment is not up to the X.509 certification standard guideline produced by ITU. This is supported by the following facts:

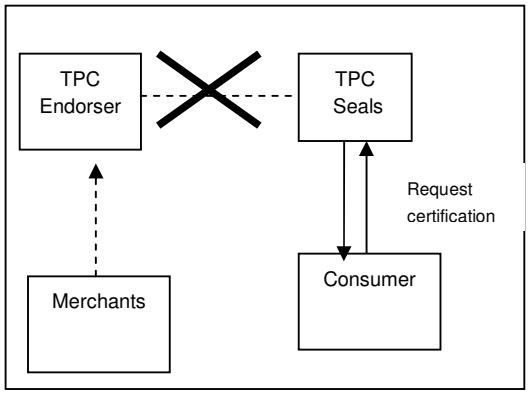
Certificate policy
Certification policy of X.509 requires some reason to believe that other parties operate a reliable implementation of its policy. A certificate may be issued in accordance with one or more than one policy. Definition of policy is performed by a policy authority. In this case, the authority is TPC endorser. It means that any TPC seals must have their own policy. And one TPC endorser can come out with more than one policy through their seals. However, in Malaysian environment, more than 60% merchants used the seals illegally. It shows that the merchants did not operate a reliable implementation of TPC endorser's policy

Cross Certification
The following diagram (Figure 1) shows the cross-certification authority suggested by ITU X.509 recommendation. However, Malaysian E-Commerce website environment seems did not apply the recommendation by ITU whereby the cross certificate is not fully implemented by almost 70% of the website (Figure 2).

Figure 1: Cross - Certification frameworks recommended by ITU



of Malaysian E-Commerce Website.



Authentication rules

The entire 4 website that use a legal and verified seals conform to the authentication rules because user knows that the site is authenticated by the TPC and its secure the identities of the parties to a transaction. However, the number is still small compare to the sample website used in this research. It ranges between 30.8% and 33.3%.

Integrity rules

The Malaysian E-Commerce Website is not conforming to the integrity rules since about 87.8% of the sample website don't have a verified or legal seals, and don't have any seals at all on their website. That's mean, nobody can ensure that the information or process has not been modified or corrupted without detection

Confidentiality

Looking closely on the data collection, the implementation also does not ensuring that neither party can refute that the transaction occurred as the customer want it to be. It also shows that most of the website is not ensuring that the information given by the customer is kept private because it cannot be proven by the merchants or supported by the third party.

Validity

A public key certificate-using system needs to validate a certificate prior to using that certificate for an application. The public-key certificate framework defined here is for use by applications with requirements for authentication, integrity, confidentiality and non-repudiation. X.509 also defines the procedures for performing that validation, including verifying the integrity of the certificate itself, its revocation status, and its validity with respect to the intended use.

In Malaysian environment, up to 70% of the merchant seems to revoke the validity policy for the following reason

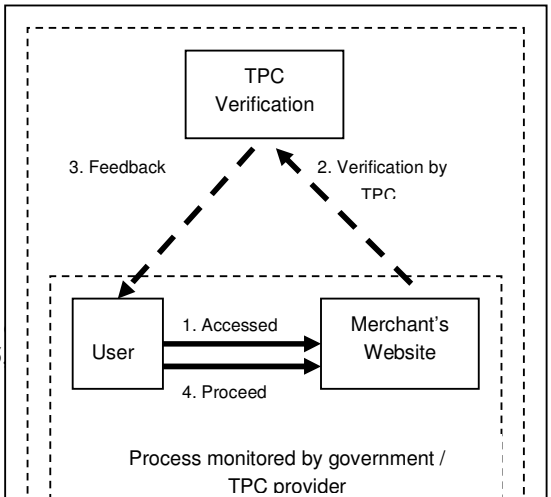
a. The privileges in the certificate are not sufficient when compared against the privilege policy;
b. Not establishing a trusted delegation path of certificates if necessary
c. Unverified digital signature are used because of the illegal/unverified used of certificate in the path
d. Merchants was not authorized to delegate privileges
e. The usage of TPC show that the certificates have expired or been revoked by their issuers.

All of the criteria are chosen to be the benchmarks because they are related to the scopes of this research. And based on the criteria, it shows that the implementation of TPC in Malaysian E-Commerce website are not conforming the X.509 certification standard.

7. Discussions and Conclusion

Based on the finding, we knew that the implementation of the TPC in Malaysia is not significant to what have been suggested by X.509 certification standard and most of the researches as mentioned in earlier part.

Figure 3: Suggested framework to implement TPC for Malaysian E-commerce Website



Based on the problem, it is suggested that a new framework for the implementation of TPC in Malaysian E-commerce Website is needed. The idea of this framework is to suggest the ideal ways for merchants to utilize the usage of TPC seals of their website.

The government of Malaysia under Ministry of Energy, Water and Communications should monitor the process of having the TPC on merchant's website so that the TPC seals will not be misused by the businesses and it will upgrade the usage of TPC as tools to confirm the security of the website. Government, as well as TPC providers should try to educate the user so that the user will aware of the function of TPC seals on the E-Commerce website.

An extension of work will be covering the same issues but focusing more on the merchant and why does merchant do not exploit the benefits of using TPC seals on their website. Since the third party certificate is related to security issues, the future works will also study on the awareness of the usage of TPC seals on E-Commerce website by the customer.

8. References

[1]American Institute of Certified Public Accountants (AICPA). *Electronic commerce assurance: attitudes toward CPA Webtrust*. Retrieved December, 30 2006. From http://www.aicpa.org/webtrust/yankel.htm

[2]American Institute of Certified Public Accountants (AICPA). *Privacy On and Off the Internet:What Consumers Want.* Retrieved April, 26 2007. From http://www.aicpa.org/download/webtrust/priv_rpt_21mar02.pdf

[3]Cheskin Research. *Trust in the wired Americas.* Retrieved April, 12 2006. From http://cheskin.com/p/ar.asp?mlid=7&arid=12&art=0

[4]Cheskin Research and Studio Archtype/Sapient. *E-Commerce Trust Study (1999)*. Retrieved April, 12 2006. From http://www.studioarchetype.com/cheskin/assets/images/etrust.pdf

[5]Hameed, S. *Consumer Trust and Confidence in Internet Commerce in Internet Commerce and Software Agents: Cases, Technologies and Opportunities*, Idea Group Publishing : USA, 2001.

[6]Hoffman, D. L., Thomas P. N. and Marcos P. "Building Consumer Trust in Online *Communications of the ACM*, 42 (4), 1999, p 50-56.

[7]Guo J., Sun C. and Chen D. "Articulating Autonomously Distributed Electronic Product Catalogues for Constructing Dynamic Conex Net", *IEEE Conference on E-Commerce Technology for Dynamic Business* (CEC'04-East), Beijing China, September 13-15, 2004, p 118-121

[8]Kaur, K. Consumer Protection in E-Commerce in Malaysia : An Overview in *UNEAC Asia Papers* No 10. 2005.

[9]Kasiran, M.K. and Meziane F. The Usage of Third Party Seals in e-Commerce websites: Current Implementation in *Work with Computing System*, 2004, p 794-798.

[10]Kasiran, M.K. and Meziane F. An Information Model for a Merchant Trust Agent in Electronic Commerce. IDEAL 2002, 2002, p. 243-248

[11]MscTrustGate. Retrieved 28 December 2006. From www.msctrustgate.com

[12]Noteberg, A.,Christiaanse, E. and Wallage, P. *Consumer trust in electronic commerce: the impact of electronic commerce assurance on consumers' purchasing likelihood and EC risk perception*. Retrieved November, 10 2005. From http:/imwww.fee.uva.nl/~anna/pub.htm

[13]Noteberg, A.,Christiaanse, E., & Wallage, P. *The role of trust and assurance services in electronic channels: an exploratory study*. In

proceeding of the International Conference on Information Systems, Charlotte, North Carolina, 1999

[14]Oh, A. *Two cents worth of E-Commerce Opinion.* Retrieved December 31, 2006. From www.neowave.com.my/sellmore/index.php

[15]Ratnasingam. P. "The Importance of Trust in Electronic Commerce," *Internet Research: Electronic Networking Applications and Policy,* v. 8, no. 4, 1998, p. 313-321

[16]Schmitz M., and Michael Latzer: Competition in B2C eCommerce: Analytical Issues and Empirical Evidence. Electronic Markets (12).
Retrieved November 22, 2006. From http://www.electronicmarkets.org/modules /pub /view.php/electronicmarkets-226

[17]WorldIT. Malaysian Government Increases E-Commerce Grant. Retrieved November 22, 2006 From http://findarticles.com /p/articles/mi_qn4175/is_20030409/ai_n129 23801#continue

[18]Webopedia. X.509. Retrieved August 11, 2006 From http://www.webopedia.com/TERM/ X/X_509. html

[17]Yang Y. Security Mechanism in Electronic Commerce. Retrieved June 12, 2006 **F**rom http://www.cs.adfa.edu.au/~yany97/secure-payment.html