The Benefits of PKI Application and Competitive Advantage

CHI-I HSU*

Department of Information Management
Kainan University,
No. 1 Kainan Road, Luchu, Taoyuan County 33857
Taiwan
imchsu@mail.knu.edu.tw

YU-CHING TUNG

Department of Information Management
Yuan Ze University,
No. 135 Yuantung Road, Chungli, Taoyuan 32003
Taiwan
s937732@mail.yzu.edu.tw

Abstract: - To understand the implementation advantages of Public Key Infrastructure (PKI) applications, this study identified PKI benefits and examined the effect of PKI benefits on competitive advantage. Four aspects of benefits are identified including cost benefits, time benefits, security benefits, and profit benefits. The CFA and regression analysis are used to check the factor structure and test the hypothetical relationships. The results suggest that the PKI benefits on saving cost, increasing security, and making profit have significant effect on obtaining the competitive advantage of corporate. A market survey is also reported to reveal the status of PKI applications in Taiwan.

Key-Words: - Public Key Infrastructure, PKI Benefits, Security, Competitive Advantage

1 Introduction

While EC (Electronic Commerce) has been changing the economic systems and business models, the security issue of the Internet becomes one big concern. PKI is the fundamental structure of electronic certificate which is exactly an essential factor for expanding global EC market and E-government services. Basically PKI can assure the data exchange security over public network such as the Internet. This mechanism uses a public and a private cryptographic key pair that is obtained and shared through a trusted authority. Because of the importance of the security of information systems, some industrialized countries have been actively devoted to the research on security technology.

Network security problems are discussed. To increase the security level, Alvarez, Martinez, Vicent, & Zamora [1] propose a public key cryptosystem using block upper triangular matrices. The cryptosystem allows an ElGamal based digital signature scheme. To solve the security problems of classical PKI methods, Sun & Cao [2] present a mechanism called UCCSSM, a simple PKI-based ubiquitous computing system used in context-aware service supply environments. Skinner [3] addresses a number of authentication issues, proposed an authentication framework that combines both traditional and biometric methods of authentication. Additionally, an intuitive privacy protecting visual representation of a member entity's authentication methods is also presented.

PKI has been widely applied in global. To embrace the global e-Trend and head on with all the challenges that are overclouding the future of Taiwan's IT industry, the Taiwan's government authorities have begun to put more emphasis on the development and application of PKI. The PKI was initiated at Taiwan since 2002. At that time few industries adopted PKI due to that the companioned legal environment and government regulation were not yet matured. The Ministry of Economic Affairs (MOE) of Taiwan started to endeavor the promotion of PKI usage with the aid of Industrial Technology Research Institute (ITRI) and Institute of Information Industry (III). During 2003~2005, more resources and efforts were poured into a large scale of promotion activities to accelerate the secure e-commerce deployments using PKI. Major promotion activities include [4]:

- Promote the adoption of PKI via series of training and awareness workshops.
- Provide consultation and subsidization program to encourage the enterprise to setup novel PKI applications.
- Survey and analysis on the status and obstacles of PKI usage, and publish PKI year book to summarize each year's new technology and service trend, fundamental policy and regulation, and example of application services.

Under the promotion from MOE in Taiwan for the adoption of PKI, totally 37 companies with 44 PKI projects received the funding support and project guidance during year 2003 to 2005. In order to more understand the overall application status and benefit effects of PKI in Taiwan, this research investigates the follow-up situations of the projects and companies through conducting a market survey and interviews. The market survey includes the current situation of the corporate, PKI budget amount, the motive for PKI adoption, the source of the certificate used, reasons to be considered for using the certificate, purposes of using the certificate, and the principal difficulties of developing and introducing PKI, etc. The findings can be used not only as a reference for PKI service providers to offer more appropriate services, but also as an guide for the evaluation of PKI implementation for businesses.

2 Benefits and Competitive Advantage

In this research, PKI refers to the mechanism based on the e-system; e-transactions and transmissions are performed under Public Key and certificates to increase the degree of security by confirming user identities; identity confirmation applied on the internet. To identify the benefits and competitive advantage of PKI application, this research adopts the approach of multi-case study by reviewing the PKI project reports from companies which received the funding support of MOE mentioned above [5, 6, 7, 8]. As shown in Table 1, four aspects of benefits and competitive advantage are identified [9].

2.1 Cost benefits

The white paper of the OASIS Forum [10] suggests that the returns led by the implementation of PKI which can be assessed by constructs such as cost and revenue. In reports from companies A, B, and C, we found that PKI implementation could save costs in human resources and personnel. For example, five employees for telephone orders were reduced to one person with the adoption of the PKI application. Company D suggested in a report that PKI implementation would simplify the transaction process, thereby lowering monitoring costs. Companies C and E indicated that PKI would lower communication costs, such as mail, paper, fax, etc. as well as paper-accounting costs. Company F suggested that PKI implementation would reduce the costs of electronic accounting. Firms can transmit e-invoices by PKI encryption mechanism and decrypt received data, automatically complete overall invoicing processes. Finally, Company G suggested that the PKI application could accelerate goods delivery, thereby saving costs in customer services.

2.2 Time benefits

PKI benefits not only refer to money, but also include time. White paper of OASIS Forum also indicates that PKI can quickly active traders [10]. Many firms suggest that PKI applications can reduce process dealing time, such as time saving of account dealing (Company A), contacting time saving of confirming the users' identities (Company B), time saving of online transaction (Company C), etc.

2.3 Security benefits

Security benefits are the most significant issues in a firm since PKI is basically applied to increase the security of internet transaction. Basically, PKI include four security characteristics: authentication, integrity, confidentiality, and non-repudiation [11, 12, 2], which are described in the reports of many companies.

With regard to integrity, PKI is used to ensure safe and unchanged transmission of online data, including documents and e-mails, throughout the whole transmission process. As to authentication, PKI is able to identify, and verify online transactions or communication targets. With regard to non-repudiation, PKI can prevent senders from denying their transmission, and receivers cannot deny receipt of data. In other words, PKI confirms the results of certain transactions between two parties. With regard to confidentiality, PKI has identification and encryption through certificates, which require an RSA Public Key to decrypt the data. Thus, the confidentiality of data is effectively guaranteed. In addition, PKI can prevent users without authorization from accessing transaction content. The reports of D, F, and I companies suggested that PKI could clearly define a users' authorization for data acquisition.

Table 1. PKI Benefits and Competitive Advantage

	Company	A	B	C	D	E	F	G	H	I	J	K
Cost Benefits	Cost saving of personnel	∨	∨	∨								
	Cost saving of transaction monitoring				∨							
	Cost saving of communication			∨		∨						
	Cost saving of accounting services						∨					
	Cost saving of customer services							∨				
Time Benefits	Time saving for accounting service: e-invoices		∨									
	Time saving for contacting PKI users electronically				∨							
	Time saving for online transaction: price quotations								∨			
Security Benefits	Security for online data during the process of		∨	∨	∨	∨	∨	∨	∨	∨	∨	∨
	Efficient identification of online transactions and		∨	∨	∨	∨	∨	∨	∨	∨	∨	∨
	Confirming specific transaction results between two		∨	∨	∨	∨	∨	∨	∨	∨	∨	∨
	Encryption of transactions by certificates		∨	∨	∨	∨	∨	∨	∨	∨	∨	∨
	Clearly defining the users' authorization for data				∨		∨			∨		
Profit Benefits	Increasing new customer base										∨	
	Increasing the profits from original customers										∨	
	Increase the number of transactions performed										∨	
	Increasing total transaction amounts										∨	
Competitive Advantage	Provide better customer services											∨
	Improving corporate (brand) image						∨					
	Demonstrate effective and secure PKI application							∨				
	Increasing overall corporate competitiveness	∨					∨					

Thus, this research indicated that it is also an important benefit item of security.

2.4 Profit benefits

The report of J company suggested that PKI could increase transaction volumes, thereby, improving revenues. The reason might be that, the PKI application can quickly complete secure transactions, thereby increasing transaction instances from the original or new customers and the revenue generated.

2.5 Competitive advantage

PKI can simplify transaction processes and increase transaction accuracy, which results in improved customer service, and reduced transaction disputes. The report of Company K indicated that PKI could accelerate the speed of products sales or services. In addition, Lancastera, Yena & Huang [13] pointed out that companies devoted to the promotion of PKI are excellent representations of the PKI application in their various industries. Company G also indicated that the PKI application could generate the demonstration effect within an industry. There will be more companies which are attracted and

participate in the safe transaction system of PKI. According to an interview to Company F, this research found that, one of the reasons for the firm's willingness to promote PKI was that affiliation may upgrade the firm's professional image. In conclusion, as indicated by the report of Company A and F, the varied benefits available in the PKI application can upgrade the overall competitiveness of a firm.

3 Research Model and Method

3.1 Hypothesis

This research is to examine the effects of PKI benefits on competitive advantage. The research model is shown in Figure 1. It includes five constructs: (1) cost benefits (COS), (2) time benefits (TIM), (3) security benefits (SEC), (4) profit benefits (PRO), and (5) competitive advantage (COM).

This research suggests that the greater the cost savings, time efficiency, and security degree, the more pronounced is the profit for a company to implement PKI applications. Therefore, H1, H2 and H3 are established as follows:

H1: The cost benefits of PKI positively influence the profit benefits of a company.
H2: The time benefits of PKI positively influence the profit benefits of a company.
H3: The security benefits of PKI positively influence the profit benefits of a company.

This study also suggests that the greater the degree to which the four aspects of benefit items are perceived, the more pronounced is the competitive advantage of a company to implement PKI applications. Therefore, H4~H7 are established as follows:

H4: The cost benefits of PKI positively influence the competitive advantage of a company.
H5: The time benefits of PKI positively influence the competitive advantage of a company.
H6: The security benefits of PKI positively influence the competitive advantage of a company.
H7: The profit benefits of PKI positively influence the competitive advantage of a company.

3.2 Survey method

A questionnaire is developed to ask responders to rate on a scale of 1 to 5 his or her degree of agreement with each benefit or advantage item. The survey also includes questions regarding the motives for PKI adoption and purposes of using the certificate, etc. Totally 660 questionnaires were distributed to PKI project managers, systems facilitators and users. 142 valid samples were collected with a valid return rate of 21.52%.

4 Data Analysis and Results

Initial reliability analysis and confirmatory factor analysis (CFA) are conducted to check the appropriateness of the factor structure. The multiple regression analysis is then used to test the hypothetical relationships. The software LISREL 8.71 and SPSS for Windows 13.0 are used to conduct the CFA and regression analysis.

4.1 CFA analysis

The measurement model is shown in Figure 2. In CFA analysis, this study basically examines (1)

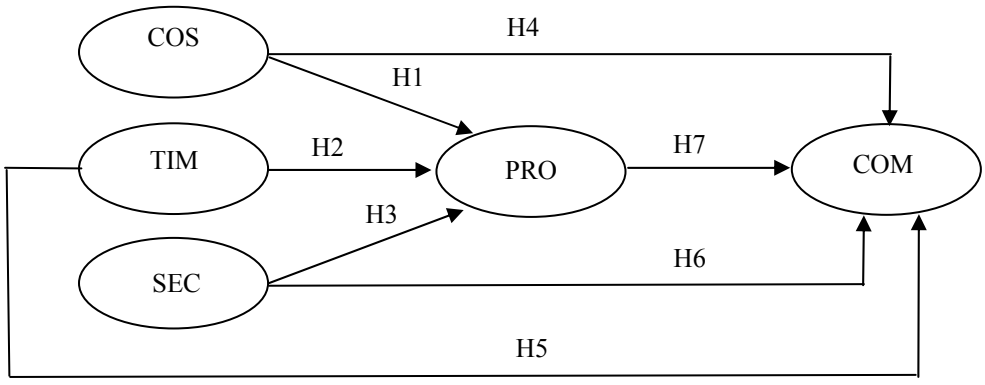

Fig.1 Research Model

whether the factor loading are significant, that is, the t-values should be greater than 1.96 at the significant level of 0.05; and (2) whether the measurement model are good of fit. The CFA results are shown in Table 2. All t-values for loading estimates are greater than 1.96. The goodness-of-fit indexes indicate that the measurement model is acceptable. We also examined Cronbach's alpha (α) and the composite reliability (CR). An α greater than .70 [14] and a CR greater than .60 is preferred [15]. As shown in Table 2, the values of α and CR satisfy the requirement.

4.2 Regression analysis

The results of regression analysis are shown in Table 3 and 4. The variables COS and SEC are statistically significant to dependent variable PRO with Sig. < 0.05. The variables COS, SEC, and PRO are statistically significant to dependent variable COM with Sig. < 0.05. The results provide partial support for the hypotheses proposed in the research model. Table 5 outlines the summary of the results.

5 Survey Result

According to the survey, the industries of corporate responded to the questionnaire including information technology and service (37%), manufacturing (15%), banking (12%), mass communication (9%), health service (6%), travel (6%) , insurance (6%), and others (9%) ◦ The pie chart is shown in Figure 3.

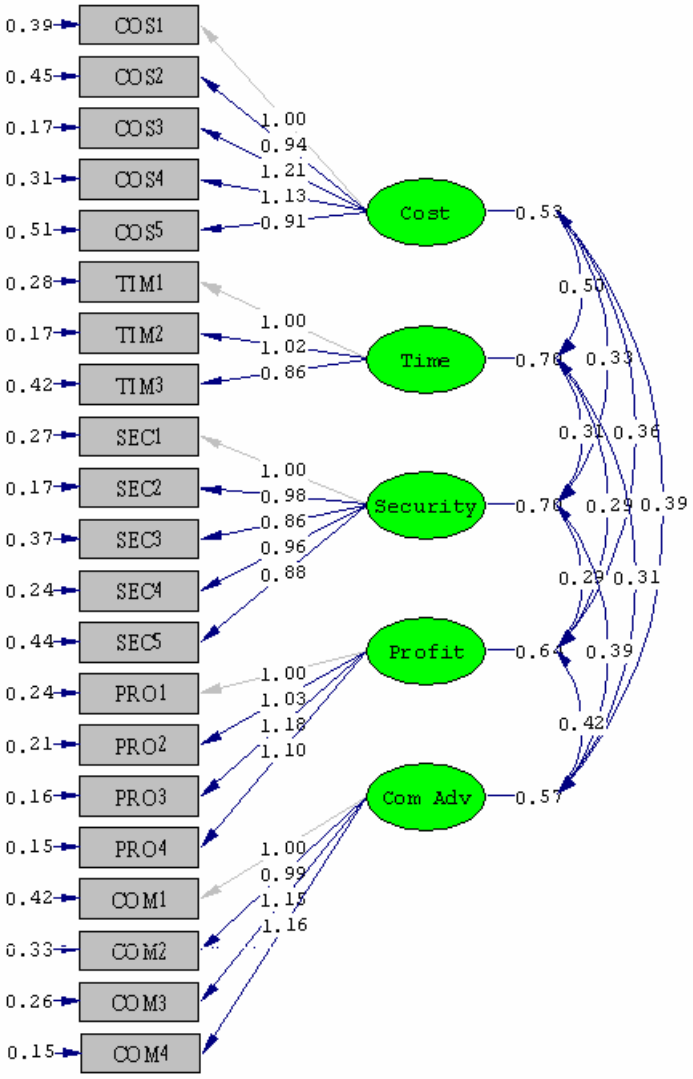

Fig.2 Measurement Model

Table 2 CFA Results

Variable	Items	Std. solution	Completely Std. solution	Std. error	t-value
Cost (α = 0.880) (CR = 0.885)	COS1	0.73	0.76	-	-
	COS2	0.68	0.71	0.11	8.71
	COS3	0.89	0.90	0.11	11.42
	COS4	0.82	0.83	0.11	10.31
	COS5	0.67	0.68	0.11	8.24
Time (α = 0.861) (CR = 0.871)	TIM1	0.84	0.85	-	-
	TIM2	0.85	0.90	0.08	12.82
	TIM3	0.72	0.74	0.08	9.99
Security (α = 0.909) (CR = 0.911)	SEC1	0.83	0.85	-	-
	SEC2	0.81	0.89	0.07	13.57
	SEC3	0.72	0.76	0.08	10.65
	SEC4	0.80	0.85	0.08	12.61
	SEC5	0.74	0.74	0.09	10.27
Profit (α = 0.939) (CR = 0.939)	PRO1	0.80	0.85	-	-
	PRO2	0.82	0.87	0.07	13.67
	PRO3	0.94	0.92	0.08	15.10
	PRO4	0.88	0.92	0.07	15.00
Competitive Advantage (α = 0.900) (CR = 0.901)	COM1	0.76	0.76	-	-
	COM2	0.75	0.79	0.10	9.90
	COM3	0.88	0.87	0.11	10.94
	COM4	0.88	0.91	0.10	11.62
Fit Indexes	$\chi 2$=320.28, df=179, $\chi 2$/df=1.7893, p=0.00, CFI=0.97, NFI=0.95, NNFI=0.97, IFI=0.97, GFI=0.82, AGFI=0.77, RMSEA=0.075, SRMR=0.053				

Table 3 Regression Results[a] (Dependent Variable: PRO)

Model	Unstandardized Coefficients		Std. Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	.459	.328		1.402	.163
COS	.593	.119	.536	5.004	.000
TIM	-.069	.106	-.067	-.655	.514
SEC	.196	.086	.180	2.275	.024

[a]R=0.597, F=25.517, Sig. 0.000

Table 4. Regression Results[a] (Dependent Variable: COM)

Model	Unstandardized Coefficients		Std. Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	1.859	.225		8.248	.000
COS	.240	.088	.311	2.725	.007
TIM	-.122	.073	-.169	-1.684	.094
SEC	.257	.060	.340	4.298	.000
PRO	.158	.058	.227	2.718	.007

[a]R=0.621, F=21.513, Sig. 0.000

Table 5 Hypothesis Tests

Hypothesis	Coefficient	t-value	Support
H1	.536	5.004***	YES
H2	-.067	-.655	NO
H3	.180	2.275*	YES
H4	.311	2.725**	YES
H5	-.169	-1.684	NO
H6	.340	4.298***	YES
H7	.227	2.718**	YES

* Sig. <0.05; ** Sig. <0.01; *** Sig. <0.001

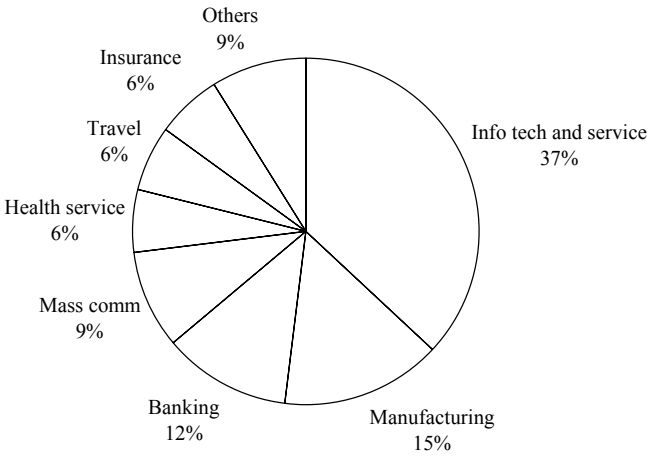

Fig.3 Industries of Corporate

The employee numbers of corporate responded to the questionnaire including below 100 (39%), 100~500 (23%), and above 500 (38%). The IS personnel numbers of corporate responded include below 20 (15%), 20~50 (62%), and above 50 (23%). The bar charts are shown in Figure 4 and 5.

The PKI budget amounts of corporate responded to the questionnaire including NT$1~3 million (39%), NT$3~5 million (38%), NT$5~7 million (8%), and NT$7~9 million (15%). The bar chart is shown in Figure 6.

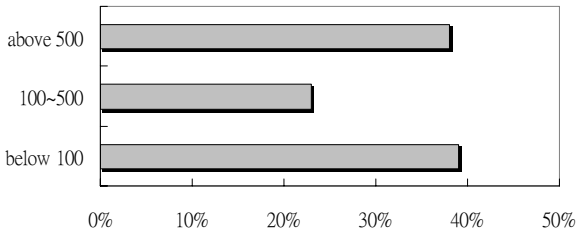

Fig.4 Employee Numbers

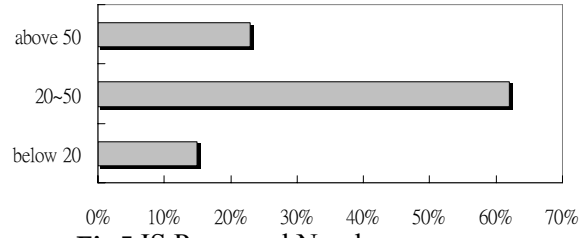

Fig.5 IS Personnel Numbers

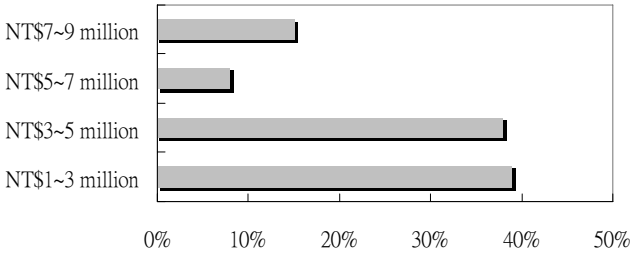

Fig.6 PKI Budget Amounts

The purposes of PKI applications are shown in Table 6.

Table 6 Purposes of PKI Application

Purposes	Percentage
Online data inquiring	27%
Online orders	18%
Online price quotations	17%
E-invoices	17%
E-documents	4%
Ease of administration	4%
Convenience of e-finance	4%
Others	9%

According to the survey, the motives for companies to adopt PKI applications are shown in Table 7.

Table 7 Motives for Adopting PKI

Motives	Percentage
Obtaining competitive advantage	46%
Security consideration	42%
Requirement of governmental regulations	8%
Requirement from the customers	4%

The percentage of corporate adopting external certificates (MOEACA, MOICA and other financial certificates in Taiwan) is 61%; internal certificates 31%; and both 8%.

The reasons of corporate use of external certificates are shown in Table 8.

Table 8 Reasons for Adopting External Certificates

Reasons	Percentage
Reducing development and maintaining the costs	38%
Promotion of the government	31%
Users do not always trust internal certificates and their legal effectiveness	23%
Others	8%

The reasons of corporate use of internal certificates are shown in Table 9.

Table 9 Reasons for Adopting Internal Certificates

Reasons	Percentage
Control of the PKI application system	33%
The unique corporate environment and information demand issues are addressed by customized certificates	28%
Having PKI technical capacities and resources	22%
Integrating partners in the supply chain	11%
Others	6%

Major difficulties of PKI development and introduction are shown in Table 10.

Table 10 Difficulties of PKI Development and Introduction

Difficulties	Percentage
The lack of interoperability in PKI	17%
PKI is too complicated	12%
Technical respect is over emphasized, neglecting actual business demands	12%
High costs involved	11%
Firm's current software does not support PKI	9%
Unclear benefits of costs	9%
PKI is difficult to use	9%
Application process for certificates is complicated	9%
Lack of total understanding PKI	6%
Legal application of the disputes caused in the transactions	3%
Partners/users are not willing adopt PKI and it is difficult to promote	3%

6 Conclusion

This research identified PKI benefits and examined the effect of PKI benefits on competitive advantage which means providing better customer services, increasing corporate (brand) image, demonstration effect of PKI application in the industry, and increasing overall corporate competitiveness. According to the results of CFA analysis, PKI benefits are confirmed as follows.

- Cost benefits:
  - Saving the cost of personnel matters
  - Saving the cost of transaction monitoring
  - Saving the communication costs such as mails, paper and fax
  - Saving the cost of account dealing such as e-invoices
  - Saving the cost of customer services
- Time benefits:
  - Saving account (such as e-invoices) dealing time
  - Saving the times of contacting the partners by data dealing and exchange
  - Saving the time of dealing with online transaction such as price quotation and orders
- Security benefits:
  - Remaining the security of online data (such as documents and e-mails) during the process of transmission.
  - Identifying the identities of the targets of online transaction or communication
  - Confirming certain transaction result between two parties
  - Encryption of transaction by certificates
  - Clearly defining the users' authorization of data acquisition
- Profit benefits:
  - Increasing new customers
  - Increasing the profits from the original customers
  - Increasing transaction times
  - Increasing total transaction amount

The results of regression analysis indicate that cost benefits and security benefits have influence over profit benefits. The cost benefits, security benefits together with profit benefits have influence over competitive advantage. The results suggest that the PKI benefits on saving cost, increasing security, and making profit have significant effect on obtaining the competitive advantage of companies adopting PKI applications.

Finally, even though companies implementing PKI have domain knowledge, most people do not know PKI. The users do not understand what the PKI application is, in addition, their low recognition and approval of certificates. Thus, the related administration units can start from the public's knowledge of the advantages of PKI. With the reinforcement of PKI applications to B2C EC, the public will find increased advantages to the PKI application. For instance, a Citizen Digital Certificate is a good example of a PKI application by performing secure identification confirmation of internet transactions, which increases both the degree of security and convenience.

Acknowledgemens:
This research was supported by the Commerce Development Promotion Program (CCL9301-P204-016), the Ministry of Economic Affairs of Taiwan. The author would like to give thanks to Professor C. Chiu for his assistance in the development of benefit items and the collection of survey data.

References:

[1] R. Alvarez, F. M. Martinez, J. F. Vicent, and A. Zamora, "A Matricial Public Key Cryptosystem with Digital Signature," *WSEAS Transactions on Mathematics*, Issue 4, Volume 7, pp.195-204, April 2008.

[2] Daoqing Sun and Qiying Cao, "UCCSSM: Ubiquitous Computing Context-aware Service Supply Mechanism," *7th WSEAS Int. Conf. on Applied Computer & Applied Computational Science (ACACOS '08)*, Hangzhou, China, April 6-8, 2008.

[3] Geoff Skinner, "Making A CASE for PACE: Components of the Combined Authentication Scheme Encapsulation for a Privacy Augmented Collaborative Environment," *WSEAS Transactions on Computers*, Issue 6, Volume 7, pp.630-639, June 2008.

[4] MOE, Available from: *http://gcis.nat.gov.tw/English/index.jsp*, Accessed 15 June 2007.

[5] MOE, *Midterm Report of PKI Interoperability Management and Promotion Program*, Taipei, Taiwan, 2003a.

[6] MOE, *Final Report of PKI Interoperability Management and Promotion Program*, Taipei, Taiwan, 2003b.

[7] MOE, *Midterm Report of PKI Interoperability Management and Promotion Program*, Taipei, Taiwan, 2004a.

[8] MOE, *Final Report of PKI Interoperability Management and Promotion Program*, Taipei, Taiwan, 2004b.

[9] C. Chiu, C. Hsu, and Eldon Li, Yu-Ching Tung, A Study of Performance Evaluation Indicators of PKI Applications and Market Survey in Taiwan, *Final Report of the Commerce Development Promotion Program*, Taipei, Taiwan, 2005.

[10] Derek Brink, PKI and Financial Return on Investment, *OASIS White Paper*, Aug 2002, http://www.oasis-pki.org/resources/whitepapers/, Data accessed 2008/7/8.
[11] David Henry, Who's Got the Key?, *Proceedings of the 27th Annual ACM SIGUCCS Conference on User Services: Mile High Expectations*, Denver, Colorado, USA, Nov 1999.
[12] Chen-Chi Lin and Chi-Sung Laih, The GPKI Developing Status of Taiwan and Some Major Asia Countries, *Computer Communications*, Vol.26, Issue16, Oct. 2003, pp. 1884 – 1892.
[13] Sean Lancastera, David C. Yena, and Shi-Ming Huang, Public key Infrastructure: A Micro and Macro Analysis, *Computer Standards & Interfaces*, Vol.25, 2003, pp. 437 – 446.
[14] J. Nunnally, *Psychometric Theory*, 2nd Ed., New York: McGraw-Hill, 1978.
[15] C. Fornell and D. F. Larcker, Evaluating Structural Equation Models with Unobervables and Measurement Error, *Journal of Marketing Research*, Vol.18, No.1, 1981, pp. 39-50.