Asia-Pacific
Economic Cooperation

2009/TEL40/SPSG/003
Agenda Item: 3a

PKI/e-Authentication Advancement: Evaluation Report

Purpose: Information
Submitted by: Chinese Taipei

APEC 2009 Singapore

Security and Prosperity Steering Group Meeting
Cancun, Mexico
26-29 September 2009

Foreword

In October 2006, the project ”APEC TEL PKI/e-Authentication Training Program” was approved by APEC TEL 34, which is to encourage PKI/e-Authentication training activities and strategic promotion to accelerate PKI/e-Authentication prevalence and information security in e-Commerce. The project contains two parts: “APEC TEL PKI/e-Authentication Training Centre” and “Annual PKI/e-Authentication Advancement Survey”.

This report prepared by Chinese Taipei is based on input from member economies of APEC TEL and applicants of “2009 APEC TEL PKI/e-Authentication Training Program”. PKI/e-Authentication Advancement Evaluation Report can help identify the PKI/e-Authentication status of member economies and also be an essential reference for the better future planning of APEC TEL PKI/e-Authentication Training Centre.

PKI/E-AUTHENTICAITON Advancement Evaluation Report

Purpose and objectives

The purposes of this survey were to ：

- Understand level of PKI/e-Authentication development and PKI/e-Authentication implementer cultivation, and the on-going actions or effective approaches to PKI/e- Authentication advancement in the respective APEC economy.
- Encourage PKI/e-Authentication know-how and capability built-up via comprehensive training investment and strategic promotion

Annual PKI/e-Authentication Advancement Survey is designed to offer the respective economy a self-assessment and a broad view of the whole, and draw the attention to strengthen PKI/E-Authentication promotion and training fundamentally.

The survey is part of the ongoing project of APEC TEL PKI/e-Authentication Training Program that is aimed at：

- Assessing the need to strengthen PKI/e-Authentication training and implementer cultivation.
- Promoting the application of PKI/e-Authentication as an integral element of the trusted e-commerce world.
- Developing linkages so as to share experiences and achievements of PKI/e-Authentication applications.

Scope

The scope of this survey is：

- Inclusive of both survey information providers from APEC economies and applicants of 2008 APEC TEL PKI/e-Authentication Training Program.
- Inclusive of current PKI/e-Authentication environments in CA(Certificate Authority), PKI/e-Authentication applications, the barrier of PKI implementation, and opinions of the international cooperation.

Questionnaire structure and content

The questionnaires were mainly designed to collect the general PKI/e-Authentication advancement status in CA (Certificate Authority), PKI/e-Authentication applications, the barrier of PKI implementation, and opinions of the international cooperation.

The questionnaire is attached to the report as **Annex II**.

Survey responses

2008 survey collected responses from 11 APEC member economies, including Australia, Chile, Chinese Taipei, Japan, Malaysia, Mexico, Peru, Philippines, Russia, Thailand, Vietnam, and 11 non-APEC economies, including Austria, Brazil, Bulgaria, Burkina Faso, Czech Republic, Dominica, El Salvador, Guatemala, India, Jordan and Panama. The result of "2008 PKI/e-Authentication Advancement Survey" has confirmed that the applications of PKI/e-Authentication are growing. The official authority of organization in the respective economy administers the development of PKI or e-Authentication. There are lots of PKI applications in varied areas from G2G, G2B, G2C, B2B, B2C, including e-tax filing, e-payment, e-billing, e-invoice, e-passport, e-procurement, e-Customs, e-insurance, e-mail security, etc. It is generally acknowledged that PKI/e-

Authentication awareness, implementation and deployment experiences, best practice and lessons learnt can be interactively conveyed through APEC TEL PKI/e-Authentication Training Program, and the further cooperation opportunities are expected.

2009 survey has generally done a self-assessment for PKI advancement for the economy. For those economies that have not yet completed the survey, the questionnaires from Section One to Six are required to answer. For those economies have already provided information, the questionnaires can be updated if needed.

For the survey from applicants of 2009 APEC TEL PKI/e-Authentication Training Program, responses were received from 10 APEC member economies：Chile, Chinese Taipei, Indonesia, Malaysia, Mexico, Peru, Philippines, Russia, Thailand, Vietnam and from 9 non-APEC economies: Brazil, Bulgaria, Cambodia, Czech Republic, Dominica Republic, Guatemala, India, Jordan, Panama. The attached table as **Annex I** shows the interpretation of the summary information provided by the respective survey writer for each question, based on 2008 & 2009 survey.

Note:

For 2008 survey through HOD, APEC TEL were responded from 5 APEC member economies：Australia, Chile, Japan, Hong Kong, and Philippines. For the survey from applicants of 2008 APEC TEL PKI/e-Authentication Training Program, responses were received from 10 APEC member economies：Australia, Chile, Thailand, Vietnam, Philippines, Malaysia, Mexico, Peru , Russia, Chinese Taipei, and from 11 non-APEC economies：Austria, Brazil, Bulgaria, Burkina Faso, Czech Republic, Dominica, El Salvador, Guatemala, India, Jordan and Panama. For 2009 survey, there are no responses from HOD, APEC TEL, but only responses received from the applicants of 2009 APEC TEL PKI/e-Authentication Training Program.

General observations and conclusions

The 2008 & 2009 survey responses from 12 APEC member economies and 12 non-APEC economies (12 APEC member economies, including Australia, Chile, Chinese Taipei, Indonesia、Japan, Malaysia, Mexico, Peru, Philippines, Russia, Thailand, Vietnam, and 12 non-APEC economies, including Austria, Brazil, Bulgaria, Burkina Faso, Cambodia, Czech Republic, Dominica Republic, El Salvador, Guatemala, India, Jordan and Panama.) shows that the majority have established government CA, PKI/e-Authentication applications and recognized foreign CAs, while few economies are on-going government CA, or foreign CAs can not be recognized because of the regulation, and there are only very few without PKI-enabled applications.

The survey result confirms that the applications of PKI/e-Authentication are growing. The official authority of organization in the respective economy administers the development of PKI or e-Authentication. There are lots of PKI applications in varied areas from G2G, G2B, G2C, B2B, B2C, including e-tax filing, e-payment, e-billing, e-invoice, e-passport, e-procurement, e-Customs, e-insurance, e-mail security, etc. It is generally acknowledged that PKI/e-Authentication awareness, implementation and deployment experiences, best practices and lessons learnt can be interactively conveyed through APEC TEL PKI/e-Authentication Training Program, and the further cooperation opportunities are expected.

The information collected in 2008 & 2009 surveys has been useful in terms of identifying PKI advancement status, and that can be a helpful reference for the upcoming APEC TEL PKI/e-Authentication Training Program. We are expecting valuable experiences sharing from APEC economies, a clearer picture of global market demand through participant economies' feedbacks, and ultimately to meet the goal of PKI/e-Authentication prevalence in global e-Commerce. Moreover, other e-authentication applications including RFID, Biometric Identification, Passwords, Digital Certificates, Tokens, Out-of-band Authentication (SMS) will become prevalent in developed economies, and will be starting in some developing economies.

As for the barriers of PKI promotion, there include： 1) Application procedures are too complicated. 2) The cost of PKI implementation is too high. 3) The PKI market is still immature. 4) Civilian and enterprises still lack PKI knowledge. 5) Technical support issues are concerned. 6) Cultural acceptance of personal PKI and privacy concerns. 7) The PKI Promotion by the government is not enough. These indicate that even though PKI is recognized as a mature technology, its promotion is still not quite easy.

The way forward follows by the annual APEC TEL PKI/e-Authentication Training Program initiated by Chinese Taipei to enable the implementation and application of PKI/e-Authentication technologies and services to expand access to unserved and underserved areas, and as an exchange platform to improve access, awareness, mastery, and application of ICT for the people of the region.

Annex I

The summarized table of "2009 PKI/e-Authentication Advancement Survey" ：
(If there is no update information, mark "N/A".)

Economy	Self-assessment for PKI Advancement	Certificate Authority	PKI application	E-Authentication application	The barriers of PKI Promotion
Australia	N/A	1. Government CA : Australian Tax Office, Health eSignature Authority Pty Ltd, Department of Defense, Australia Post (operate by private sector) 2. Private sector : ANZ Banking Group Ltd 3. Foreign CA: VeriSign Australia Pty Ltd, Verizon Business (Formerly Cyber Trust) Recognizes foreign CAs, but the foreign CAs need to be approved by a formal recognition process under the Gatekeeper PKI Framework, Department of Finance and Deregulation to be used in government. Private sector firms can accept whatever CA they want based on their own business rules.	1. Australia has E-Service for business, E-Tax Filing, E-Customs, E-passport, General e-Government service, E-payment, Online security trading (B2B, B2C), Document management (G2G, G2B) and E-mail Security (G2B, B2B) services. 2. Users need to pay fees for E-Service for business (by transaction US$40-4000 / application fee included). Other applications are free to use. 3. The purposes to apply PKI are ID Authentication , Information Integrity, Information Confidential and Electronic Signature (for non-repudiation) 4. Software token is most used for these applications. USB token and smart card are also used in some applications.	1. RFID 2. Biometric Identification 3. Passwords 4. Digital Certificates 5. Tokens 6. Out-of-band authentication (SMS)	1. Application procedures are too complicated 2. The cost of PKI implementation is too high 3. The PKI market is still immature 4. Civilian and enterprises still lack PKI knowledge 5. Technical support issues are concerned 6. Cultural acceptance of personal PKI and privacy concerns

Austria	N/A	1. Top 5 CA (based on the size of the community they serve): Telekcom-Control-Commision (is often understood as a national root CA), a.sign, e-card Vertragspartnersignature, A-CERT and eSignature. 2. CAs issuing non-qualified certificates for advanced electronic signatures have been added to the table because such signatures are important for invoices submitted electronically 3. The type "government CA" is not entirely adequate for the Main Association of Austrian Social Security Institutions: Although this institution is established by law, it is managed by parties representing interests (like the Economic Chamber and the Chamber of Labour) Recognize foreign CAs based on § 24 of the Federal Electronic Signature Law	1. Austria has lots of PKI-enabled applications currently proving services, like E-Invoice, E-Tax Filing, E-Service for business, E-Passport(Data stored in the passport (G2C) are digitally signed by the Austrian State Printing House), PKI-based National ID card(G2C, not a photo ID in general, except service cards of government officials, notaries, attorneys, etc.), e-Government, E-Payment (based on the citizen card), E-Billing, E-Procurement, E-insurance service (B2B), Document management (G2G), E-mail security, Services provided to students at the Vienna University of Economics and Business Administration, ARA Altstoff Recycling Austria AG. 2. Most of these applications are free to use, some of them depending on the specific application users need to pay certain fees. 3. The purposes to apply PKI are ID Authentication , Information Integrity, Information Confidential and Electronic Signature (for non-repudiation) 4. smart card, Software token, USB token and citizen card are used for these applications 2	1. RFID: e.g. the Austrian passport, complying with Council Regulation (EC) No 2252/2004 and applicable ICAO documents 2. Biometric identification: apparently not widely used in enterprises because use of biometric identification methods by employers must be reported to the Austrian Data Protection Commission; also not very popular because of still insufficient reliability 3. Passwords: ubiquitous, still used as an authentication method in e-banking and in e-government applications for people who do not have a	1. PKI Application is not user-friendly: Maybe. The Austrian Regulatory for Broadcasting and Telecommunications has received several complaints regarding difficulties with installation and usage of client-side software components (including the Citizen Card Environment) 2. Technical support issues are concerned: Partially. Several providers of PKI-based applications have observed increasing helpdesk demand when laymen are directly involved with certificates, private keys, etc 3. The PKI market is still immature: 4. Partially. Regarding the

Bulgaria	1. Legal Framework (e.g. Digital Signature Law) 2. CA Accreditation or Licence Mechanism 3. Some PKI-enabled Applications for private sectors 4. Some PKI-enabled Applications for government sectors	1. Government CA: Information services(operate by private sector) 2. Private sector CA: BankService(Shareholder company, shareholders: Bulgarian National Bank and 28 commercial banks), INFONOTARY PLC, Spectar, SEP Bulgaria 3. circulation of qualified certificates: BankService(20,000), Information services (20,000)INFONOTARY PLC (3000), Spectar(2000), SEP Bulgaria(1000) Bulgaria doesn't recognize foreign CAs by the Law for Electronic Document and Electronic Signature	1. Bulgaria has E-Invoice, E-Tax Filing, E-Customs, E-Service for business, E-payment and E-Billing services. 2. Users no need to pay nay fee for using these applications. 3. The purposes to apply PKI are Electronic Signature (non-repudiation) and ID Authentication. 4. USB Token and Smart card are used for these applications.	1. Passwords	1. The cost of PKI implementation is too high 2. Civilian and enterprises still lack PKI knowledge

Burkina Faso	N/A	1. Private sector CA : BCEAO, executive by CMTI(Regional Banking CA issuing certificates for banks in the Region Recognize foreign CAs, but the foreign CAs need to be approved by Telecom Regulatory Body (ARTEL)	1. Burkina Faso has E-invoice and E-payment services. 2. Users need to pay monthly fee for using E-payment service. 3. The purposes to apply PKI are ID Authentication , Information Integrity, Information Confidential and Electronic Signature (for non-repudiation) 4. Smart card is used for these applications.	1. Biometric Identification 2. Passwords	1. The cost of PKI implementation is too high 2. The PKI market is still immature 3. Civilian and enterprises still lack PKI knowledge 4. Lack of PKI implementation skills
Cambodia	1. Some PKI-enabled Applications for private sectors 2. Some PKI-enabled Applications for government sectors	Cambodia has Government CA (Operated by private sector) Recognizes foreign CAs, but the foreign CAs need to be approved by Cambodia government.	For Cambodia just arrange to do a law about E-Commerce by government so E-billing, E-insurance service, E-payment, E-voting… do not execute for private sector, International company in country	N/A	N/A

Chile	1. Legal Framework (e.g. Digital Signature Law) 2. CA Accreditation or Licence Mechanism 3. Certified CAs Interoperability 4. Major CAs Implementation 5. Some PKI-enabled Applications for private sectors 6. Some PKI-enabled Applications for government sectors	1. Government CA: CNC-ONCE (operate by private sector) 2. Private sector CA: E-Certchile, E-sign(VeriSign Inc), Acepta, Certinet 3. Research and Education CA: Reuna CA Recognizes foreign CAs, but the foreign CAs need to be approved by Economy Ministry	1. Chile has E-Invoice (B2G), E-Tax filing (B2G), E-Customs, E-service for business, General e-Government services to citizens (G2C), E-Payment (B2B, B2C), E-Billing (B2C), Online Security trading (G2B, B2B, B2C), E-procurement (G2B,G2C, B2B, B2C), Order management (G2B, G2C, B2B, B2C), E-insurance service (G2B, G2C, B2B, B2C), Document management (G2G, G2B, G2C, B2B, B2C), E-mail Security services. 2. Users need to pay fees for using these applications. (by annual fee or transaction) 3. The purposes to apply PKI are ID Authentication , Information Integrity, Information Confidential and Electronic Signature (for non-repudiation) 4. Software token, USB token and smart card are used for these applications	1. RFID 2. Biometric Identification 3. Passwords 4. Near Field Communication 5. SSL (secure communication channel)	1. The implementation of the policy for privacy protection in Chile is at a planning stage 2. Chile is at an early stage of development of a policy to foster a culture of security 3. Application procedures are too complicated 4. PKI Application are not user-friendly 5. Civilian and enterprises still lack PKI knowledge 6. The PKI market is still immature 7. The cost of PKI implementation is too high 8. Technical support issues are concerned

Chinese Taipei	1. Legal Framework (e.g. Digital Signature Law) 2. CA Accreditation or Licence Mechanism 3. Certified CAs Interoperability 4. Major CAs Implementation 5. Some PKI-enabled Applications for private sectors 6. Some PKI-enabled Applications for government sectors	1. Government CAs (1)GCA for government agencies (2) XCA for non-government organizations --Administering by RDEC, the Executive Yuan (3)Ministry of the Interior Certificate Authority, MOICA for citizen certificate services --Administering by Ministry of the Interior (4)Ministry of Economic Affairs Certificate Authority, MOEACA for business and company certificate services --Administering by Ministry of Economic Affair --operated by Chung-Hwa Telecom. (5)Health Certificate Authority, HCA for the certificate service for medical purpose Administering by Department of Health, the Executive Yuan 2. Private CA： (1) TWCA, TaiCA, for on-line financial service and electronic commercial trade (2) BankPro e-Service Technology Co., BankPro CA 3. Foreign CA：HiTrust, Verisign	1. e-Government applications include e-Tax filing, e-invoice, e-Trade Facilitation, e-document, e-labor insurance, e-cadastral etc. 2. e-Commerce applications include e-procurement, e-order, e-biddng, e-billing, e-invoice, e-payment, e-banking, e-stock, etc. 3. USB token, Smart card and Software authentication are used for these applications.	1. RFID 2. Biometric Identification 3. Passwords 4. Near Field Communication (NFC) 5. Tokens 6. Out-of-band authentication (SMS)	1. Application procedures are too complicated 2. PKI application are not user-friendly 3. Civilian and enterprises still lack PKI knowledge

Czech Republic	1. Legal Framework (e.g. Digital Signature Law) 2. CA Accreditation or Licence Mechanism 3. Some PKI-enabled Applications for private sectors 4. Some PKI-enabled Applications for government sectors	1. Government CA: except Country Signing CA(CSCA), I.CA, PostSignum QCA, and eIdentity are operated by private sectors. 2. Private CA: CA Czechia.cz Recognize foreign CAs, but the foreign CAs need to be approved by other EU member state	1. Czech Republic has E-Invoice (QCA), E-Tax filling (G2B,G2C), E-Customs, E-Passport (RFID, CSCA)E-payment, E-Billing(QCA), E-Procurement(G2B, G2C), E-Insurance (G2B, G2C) services. 2. Users has to pay monthly fee for using E-payment service, other services are fee to use. 3. The purposes to apply PKI are ID Authentication , Information Integrity and Electronic Signature (for non-repudiation) 4. Software token, USB token and smart card are used for these applications Next project is eID. From 1st July 2010 EID will enable electronic communication with authorities and eID cards will support utilization of PKI-services	1. RFID 2. Biometric Identification 3. Passwords	1. The cost of PKI implementation is too high 2. The PKI market is still immature

Dominica Republic	1. Legal Framework (e.g. Digital Signature Law) 2. CA Accreditation or Licence Mechanism 3. Certified CAs Interoperability	1. Government CA: CÁMARA DE COMERCIO Y PRODUCCIÓN DE SANTO DOMINGO (operate by private sector) 2. Private sector CA: Avansi Recognizes foreign CAs, but the foreign CAs need to be approved by another CA or by Cross Certification Agreements	1. There are 3 projects are now being developed, including E-Tax Filing, E-Customs and PKI-based National ID Card in Dominica Republic. 2. Dominica Republic also has E-Payment services (for online banking services, banks are using foreign certificates issued by Verisign, mostly for ID Authentication) The PKI National ID card has been stipulated in the draft of the E-Government Law, but according to said text the Junta Central Electoral (organism which issues National ID cards) has a period of ten years to issue the PKI National ID cards to the whole population.	1. RFID 2. Biometric Identification 3. Passwords 4. Near Field Communication (NFC)	1. The cost of PKI implementation is too high 2. The PKI market is still immature 3. Civilian and enterprises still lack PKI knowledge 4. Not enough applications use PKI
El Salvador	N/A	VeriSign is the most known foreign CA in El Salvador. Recognize foreign CAs, but no legislation. It's expected to approve legislation in the next governmental period.	El Salvador has E-Tax filling service. There is no other information regarding the fees for using or what kind of token is used for this application	1. Passwords.	1. Technical support issues are concerned 2. The cost of PKI implementation is too high 3. The PKI market is still immature 4. Civilian and enterprises still lack PKI knowledge 5. Lack of legislation

Guatemala	1. Legal Framework (e.g. Digital Signature Law) 2. CA Accreditation or Licence Mechanism 3. Some PKI-enabled Applications for private sectors 4. Some PKI-enabled Applications for government sectors	There is only one Foreign CA Chunghwa Telecomin Guatemala. Recognize foreign CAs, but the foreign CAs need to be approved by Ministry of Economy. The law that enables digital signature (simple and advanced) was issued on late 2008 and Ministry of Economy has just created the national registry in charge of authorizing RA/CA based on PKI model, so far there are 3 companies in this process that have to comply with ISO-9000 for local office and have the backup of a security certified CA. Some applications are cooking but it is more likely the will get noticed when first CA is approved	1. The only one PKI-enabled application is E-Customs (DUA-GT). Smart card is used for this application. 2. The purposes to apply PKI are ID Authentication , Information Integrity, Information Confidential and Electronic Signature (for non-repudiation)	1. RFID 2. Biometric identification 3. Passwords 4. Near Field Communication 5. Tokens	1. The PKI market is still immature 2. The cost of PKI implementation is too high 3. Civilian and enterprises still lack PKI knowledge 4. PKI is a new technology that has been not developed all in Latin American and Central America

India	1. Legal Framework (e.g. Digital Signature Law) 2. CA Accreditation or Licence Mechanism 3. Major CAs Implementation 4. Some PKI-enabled Applications for private sectors 5. Some PKI-enabled Applications for government sectors	1. Government CA : Root CA, National Informatics Centre, IDRBT, Icert 2. Public sector CA: (n)Code Solutions, MTNL 3. Private sector CA: TCS, Safe scrypt, E mudra Recognizes foreign CAs, but the foreign CAs need to be approved by Central Government	1. India has E-Tax Filing (G2C), E-Customs (G2B),E-Invoice (B2C) , E-Billing (G2G, IDRBT CA), E-service for Business(G2B), E-procurement (G2B,B2B) and E-mail Security services. 2. Users no need to pay any fees to use these applications. 3. The purposes to apply PKI are ID Authentication, Information Integrity, and Electronic Signature (for non-repudiation) 4. USB token and smart token are used for these applications Current project: Filing of company returns , E-Tender, E-Procurement , filing of Cooperate Income Tax Future project:filing of indvidual's Income tax return, E-Banking	1. RFID 2. Biometric identification 3. Passwords 4. Near Field Communication(NFC)	1. The PKI market is still immature. 2. Civilian and enterprises still lack PKI knowledge awareness 3. Application procedures are too complicated 4. The cost of PKI implementation is too high 5. Technical support issues are concerned 6. Interoperability of certificates, costs, technical issues like certificates being supported by various browsers , awareness

Indonesia	1. Legal Framework (e.g. Digital Signature Law) 2. CA Accreditation or Licence Mechanism 3. Certified CAs Interoperability 4. Some PKI-enabled Applications for government sectors	1. Government CA : Supervisory Board – CA (Badan Pengawas CA or BP CA), InaSign (operated by private sector) 2. Private sector CA: Indosign 3. Foreign CA: VeriSign Recognizes foreign CAs, but the foreign CAs need to be approved by Ministry of Information and Technology	1. Indonesia has E-Invoice (using BP CA, InaSign CA) , E-Tax Filing (G2B, G2C), E-procurement, E-service for Business(G2B) 2. Users no need to pay any fees to use these applications, except E-invoice services. 3. The purposes to apply PKI are ID Authentication, Information Integrity, Information Confidentia and Electronic Signature (for non-repudiation) 4. Smart card and software token are used for these applications PKI-based National ID Card is in the design stand and development (Ministry of Home Affair and Ministry of ICT)	1. RFID 2. Biometric identification 3. Passwords	1. Application procedures are too complicated 2. The cost of PKI implementation is too high 3. PKI Applications are not user-friendly 4. Civilian and enterprises still lack PKI knowledge

Japan	N/A	1. Official Status Certificate Authority, Application Certificate Authority and Bridge Certificate Authority these 3 Government CAs has issued about 20,000 certificates. 2. CA for Public Certification Service for Individuals has issued 600,000 certifications 3. There are 17 CAs accredited as Accredited Certificate Authorities in Japan. These CAs had issued 314,000 certificates by March 2007. (Each circulation of the certificates is not disclosed.) Japan doesn't recognize foreign CA , because Japan have not received any application form foreign CA yet.	1. Japan has E-Tax filling, E-passport and Document management (G2G) services. 2. Users no need to pay any fee for using these applications. 3. The purposes to apply PKI are ID Authentication , Information Integrity, Information Confidential and Electronic Signature (for non-repudiation) 4. Smart card is used for these applications.	1. RFID 2. Biometric Identification 3. Passwords 4. Near Field Communication (NFC)	1. PKI Application are not user-friendly 2. The PKI market is still immature 3. Civilian and enterprises still lack PKI knowledge

Jordan	1. Legal Framework (e.g. Digital Signature Law) 2. Some PKI-enabled Applications for private sectors	1. Government CA: Govdco01 (https://mail.gov.jo), Jopay. Recognizes foreign CAs, but the foreign CAs need to be approved by (Telecommunications Regulatory Commission).The current laws do not address this issue, however there is a legislation under processing that will allow such scenario and foreign CAs have to be approved by the government	There has no PKI-enabled application currently providing service in Jordan. Currently the plan is to design and build a PKI owned by the government of Jordan to enable different security ervices such as Authentication, Authorization, Non-Repudiation (Digital Signature), and data integrity. There will be many projects in Jordan that will utilize the PKI to provide the previous security services.	1. Passwords 2. We are currently working on a national smartcard project that will enable PKI and Biometric based identification	1. The cost of PKI implementation is too high 2. Application procedures are too complicated 3. Technical support issues are concerned 4. Civilian and enterprises still lack PKI knowledge

Malaysia	1. CA Accreditation or Licence Mechanism 2. Major CAs Implementation 3. Some PKI-enabled Applications for private sectors 4. Some PKI-enabled Applications for government sectors	1. Government CA : DIGICERT SDN BHD(1.5 million active users), operate by private sector a. Certification Authority license (by Malaysian Communications and Multimedia Commission (MCMC) b. Certification of Recognition for Repository (by MCMC) 2. Private sector CA: MSC Trustgate.com. Sdn. Bhd. a. Certification Authority license (by Malaysian Communications and Multimedia Commission (MCMC) b. Certification of Recognition for Repository (by MCMC) Recognize foreign CAs, but the foreign CAs need to be approved by Malaysia Communications and Multimedia Commission, and has to sign an for International Treaty, agreement or convention in which Malaysia is a party	1. Malaysia has E-invoice, E-tax filling, E-customs, E-service for business, General e-Government services, E-payment, E-procurement (G2B, G2C), E-insureance service, E-mail Security services. 2. Except E-tax filling and E-service for business is free to use, Users need to pay annual fee or by transaction for using these applications. 3. The purposes to apply PKI are ID Authentication , Information Integrity, Information Confidential and Electronic Signature (for non-repudiation) 4. Software token, USB token and smart card are used for these applications It is vision of the government as well as Certification Authority in Malaysia to enable government related e-services whether it concerns intra-government or government to public applications. With that in mind, applications such as e-tanah, HRMIS, GoE will be PKI enabled in the near future	1. RFID 2. Biometric identification 3. Passwords 4. Other Two Factor Authentication such as OTP	1. The PKI market is still immature 2. The presence of other competitive products / services such as 2 FA via mobile phone

Mexico	1. Legal Framework 2. CA Accreditation or Licence Mechanism 3. Certified CAs In teroperability 4. Some PKI-enabled Applications for private sectors 5. Some PKI-enabled Applications for government sectors	1. Government CA: CA-SE Root, DGNM/Siger, FIEL, CompraNET, DeclaraNET and IDSE 2 Firma Digital (operate by private sector) 2. Private sector CA: Advantage Security, PSC World, IES-CA CECOBAN, PSC-CA CACOBAN, BancaNET, IES 3. Autonomous academic sector CA: Identity Unit and Electronic Signature, UNAMGrid 4. FIEL has 1,600,000 qualified certificates. The other CAs has 10 - 22,847 certificates. Mexico doesn't recognize foreign CAs now, but the Direction of Regulation and Supervision of Certification Service Providers is working on that.	1. Mexico has E-Invoice (G2B,G2C, B2B), E-Tax filling (G2B,G2C), E-Service for business, E-Voting (Academic 2 Academic), General e-Government, E-payment, E-Billing, E-mail Security (B2B, C2C, B2C, C2B), Electronic signature in Commerce Public Register activities and Financiers guarantees. 2. User need to pay by annul fee or transaction for some of these applications. 3. The purposes to apply PKI are ID Authentication , Information Integrity, Information Confidential and Electronic Signature (for non-repudiation) 4. Software token is most used for these applications. USB token and smart card are used as well. Aligning strategies and issue digital certificates using advanced electronic signature Federal Government and use of technological infrastructure currently operating in the E-Tax Filing, E-Billing (Ministry Of The Economy) and General e-Government services to citizens. Simplification of the use and application of FEA in the processes of the Federal Government.	1. RFID 2. Biometric Identification 3. Passwords 4. Near Field Communication (NFC)	1. The cost of PKI implementation is too high 2. The PKI market is still immature 3. Civilian and enterprises still lack PKI knowledge

Panama	1. Legal Framework 2. CA Accreditation or Licence Mechanism	1. Government CA: Centro de Firma Digital, Tribunal Electoral de Panamá, Procuraduria de la Administración, Universidad Technologica de Panama, Autoridad del Canal de Panama, AMP and Secretary for Government Innovation (not yet operate) 2. Private sector CA: Procuraduria de la Administración 3. These CAs have issued 100-1000 qualified certificates. Recognize foreign CAs, but the foreign CAs need to be approved by General Director of Electronic Commerce - Ministry of Commerce and Industries	1. Panama now has e-Government services and E-Tax Filing. But both of them do not use Digital IDs. 2. There are several projects are planed to provide in the future, including E-invoice, E-Tax Filing, E-Customs, PKI-based National ID Card, E-procurement (G2B), Document management and E-Mail Security Currently Panama is implementing a National Certification, to set the Root CA countries like the Government Certification Authority	1. RFID 2. Biometric Identification 3. Passwords	1. Application procedures are too complicated 2. The cost of PKI implementation is too high 3. Civilian and enterprises still lack PKI knowledge 4. Technical support issues are concerned

Peru	1. Legal Framework 2. CA Accreditation or Licence Mechanism 3. Some PKI-enabled Applications for private sectors	1. Government CA: National Institute for the Defense of Competition and Intellectual Property(INDECOPI),National Registry for Identification and Civil Status(RENIEC) and Electronic System of Acquisitions and Hiring of the State(SEACE). These three CAs are still in implementation stage. Recognize foreign CAs, but the foreign CAs need to be approved by INDECOPI	There is no PKI-enabled application currently providing services in Peru now. But many projects are in evolving stage. The peruvian legal framework as support of the paper less capacity building has been established.Through Indecopi, Peru will become one of the Andean Member State to implement the national adminstrative authority responsible of the official Infrastructure of Electronic Signatures PKI Perú It is the starting point for building a PKI enabled economy. The accreditación procedures are already developed and available The National Registry for Identification and Civil Status (RENIEC), actually developing de PKI infrastructure for the public domain.	1. RFID 2. Biometric Identification 3. Passwords 4. Near Field Communication (NFC)	1. The cost of PKI implementation is too high 2. Technical support issues are concerned 3. The PKI market is still immature 4. Civilian and enterprises still lack PKI knowledge

Philippines	1. Legal Framework 2. Some PKI-enabled Applications for private sectors 3. Some PKI-enabled Applications for government sectors	1. Private sector CA: (also Foreign CA) mysecuresign owned by ePLDT has more than 2000 qualified certificates.(www.mysecuresign.com) Recognizes foreign CAs, but the foreign CAs need to be approved by the Dept. of Trade and Industry	1. Philippines has E-Tax Filing (G2B), E-service for Business(G2B), General E-Government (G2B, G2C), E-payment (B2C,B2B,G2C) , E-procurement (G2B,G2C,B2B,B2C), Order management (B2B, B2C) and E-mail Security services. 2. Users no need to pay any fees to use these applications, except E-payment services (by transaction) 3. The purposes to apply PKI are Information Integrity and Confidential 4. Software token is used for these applications	1. RFID 2. Biometric identification 3. Passwords	1. Application procedures are too complicated (for civilian) 2. The cost of PKI implementation is too high 3. Civilian and enterprises still lack PKI knowledge 4. Technical support issues are concerned 5. The PKI market is still immature

Russia	N/A	1. Government CA: Central Bank of Russian Federation for all commercial banks 2. Private sector CA: Most of Commercial Banks for their customers and bank-to-bank transactions , Russian Stock Exchange 3. Foreign CA: S.W.I.F.T 4. Theses CAs have issued hundreds to thousands qualified certificates. Recognize foreign CAs, but the foreign CAs need to be approved by Federal Agency of information technology of the RF	1. Russia has E-Invoice, E-Tax Filing, E-Customs, E-Service for business, E-Passport, PKI-based National ID card, E-Voting, General e-Government, E-Payment, E-Billing, Online security trading, E-Procurement, Order management, E-insurance service (B2B), Document management (G2B, B2B,B2C), and E-mail security services. 2. Most of these applications are free to use, few of them users need to pay by month or transaction. 3. The purposes to apply PKI are ID Authentication , Information Integrity, Information Confidential and Electronic Signature (for non-repudiation) 4. Software token, USB token and smart card are used for these applications	1. Biometric Identification	1. Application procedures are too complicated 2. The cost of PKI implementation is too high 3. The PKI market is still immature 4. Civilian and enterprises still lack PKI knowledge 5. Legal environment is not quite mature yet, especially for e-Government services. Basic authentication laws has been adopted (Russian Federal Laws “About Digital Electronic Signature’’, "About the information, information technologies and protection of the information"), but the laws requirements are somewhat vague yet.

Thailand	N/A	1. Government CA : G-CA 2. Private sector CA: TOT CA, CAT CA, Thai Digital ID, PCC Digital ID CA 3. Foreign CA: Verisign SSL Recognize foreign CAs, but the foreign CAs need to be approved by authorized organization (according to the law)	1. Thailand has E-Customs, E-Passport, PKI-based National ID Card, General e-Government service to citizens, E-payment, E-Procurement (G2B), Order management(G2B), E-mail Security systems. 2. Users no need to pay for using most of these applications. But to use General e-Government service, E-payment and Order management services, users need to pay annul fee. 3. The purposes to apply PKI are ID Authentication , Information Integrity, Information Confidential and Electronic Signature (for non-repudiation) 4. USB token, Smart card and Software token are used for these applications	1. RFID 2. Passwords 3. Near Field Communication (NFC) 4. OPT Token	1. Application procedures are too complicated 2. PKI application are not user-friendly 3. The PKI market is still immature. 4. Civilian and enterprises still lack PKI knowledge 5. The cost of PKI implementation is too high 6. Technical support issues are concerned 7. The PKI Promotion by the government is not enough

Vietnam	1. Legal Framework (e.g. Digital Signature Law) 2. CA Accreditation or Licence Mechanism 3. Certified CAs Interoperability 4. Major CAs Implementation 5. Some PKI-enabled Applications for private sectors 6. Some PKI-enabled Applications for government sectors	7. Government CA : National Root CA Center(Executive by Ministry of Information and Communication), Government Root CA(Executive by Committee for Government Encryption), CA for Ministry of Public Security and CA for Businesses(Executive by Ministry of Industry and Trade) Recognizes foreign CAs, but the foreign CAs need to be approved by National Root CA	1. Vietnam has scarce implement in E-Customs, E-Invoice, E-Tax Filing, E-Service for business, General e-Government service, E-payment, E-Billing , Online security trading(B2B, B2C), E-Procurement (G2B、B2B), and Document management (G2G) 2. Users need to pay fees for using E-invoice (by annual fee), E-Payment, E-Payment, Online security trading and E-Procurement (all by transaction). 3. The purposes to apply PKI are ID Authentication , Information Integrity, Information Confidential and Electronic Signature (for non-repudiation) 4. Software token is most used for these applications, second is smart card.	1. RFID 2. Biometric Identification 3. Passwords 4. Near field Communication	1. Application procedures are too complicated 2. The cost of PKI implementation is too high 3. The PKI market is still immature. 4. Civilian and enterprises still lack PKI knowledge 5. Technical support issues are concerned

Annex II

Asia-Pacific
Economic Cooperation

2009 PKI/e-Authentication Advancement Survey for "APEC TEL PKI/e-Authentication Training Program" Project

Submitted by: Chinese Taipei

39th APEC Telecommunications and Information
Working Group Meeting – SPSG

Singapore
13-18 April 2009

A SURVEY FOR APEC TEL SELF-FUNDED PROJECT TO OFFER THE RESPECTIVE ECONOMY A SELF-ASSESSMENT AND DRAW THE ATTENTATION TO STRNGTHEN PKI/E-AUTHENTICATION PROMOTION AND TRAINING FUNDAMENTALLY

2008 survey collected responses from 11 APEC member economies, including Australia, Chile, Chinese Taipei, Japan, Malaysia, Mexico, Peru, Philippines, Russia, Thailand, Vietnam, and 11 non-APEC economies, including Austria, Brazil, Bulgaria, Burkina Faso, Czech Republic, Dominica, El Salvador, Guatemala, India, Jordan and Panama. The result of "2008 PKI/e-Authentication Advancement Survey" has confirmed that the applications of PKI/e-Authentication are growing. The official authority of organization in the respective economy administers the development of PKI or e-Authentication. There are lots of PKI applications in varied areas from G2G, G2B, G2C, B2B, B2C, including e-tax filing, e-payment, e-billing, e-invoice, e-passport, e-procurement, e-Customs, e-insurance, e-mail security, etc. It is generally acknowledged that PKI/e-Authentication awareness, implementation and deployment experiences, best practice and lessons learnt can be interactively conveyed through APEC TEL PKI/e-Authentication Training Program, and the further cooperation opportunities are expected. Please find "PKI/E-Authentication Advancement Evaluation Report" Doc. No. SPSG/004 published at APEC TEL 38, http://www.apectelwg.org/, or you may contact Cindy Tseng at hsuyingtseng@itri.org.tw.

Firstly, please do a self-assessment for PKI advancement in your economy. We sincerely request those economies that have not yet completed the survey (i.e. the economy is not listed in the above paragraph) to help with answering the questionnaires Section One to Six. For those economies have already provided information, please simply update the questionnaires. The result of this survey will not only provide an essential reference for planning of APEC TEL PKI/e-Authentication Training Program, but also be expected to find a feasible scope for application interoperability and international collaborations.

☐ Self-assessment for PKI Advancement

Please mark the stage(s) of PKI advancement that your economy has completed. (Multiple selections are accepted)

☐ Legal Framework (e.g. Digital Signature Law)
☐ CA Accreditation or Licence Mechanism
☐ Certified CAs Interoperability
☐ Major CAs Implementation
☐ Some PKI-enabled Applications for private sectors
☐ Some PKI-enabled Applications for government sectors

☐ New **(For the economy is not listed in the first paragraph)** ☐ Update

Section One: Certificate Authority

1. Please fill in the table below for the current status of Certificate Authority (CA) in your economy. (Please add or delete the rows if necessary)

No.	Name of CA	Name of CA Owner/Executive	Type of CA	Circulation of qualified certificates (Approximate number is accepted)	Website
A			□ Government CA Operated by private sector ☐ Yes ☐ No □ Private sector CA □ Foreign CA		
B			□ Government CA Operated by private sector ☐ Yes ☐ No □ Private sector CA □ Foreign CA		
C			□ Government CA Operated by private sector ☐ Yes ☐ No □ Private sector CA □ Foreign CA		
D			□ Government CA Operated by private sector CA ☐ Yes ☐ No □ Private sector CA □ Foreign CA		

E			□ Government CA Operated by private sector ☐ Yes ☐ No □ Private sector CA □ Foreign CA		

2. Does your economy recognize foreign CAs?

   □ Yes

   □ Yes, but the foreign CAs need to be approved by _____(organization)

   □ No, the reason is _____

Session Two: PKI Application

No.	Please mark the PKI-enabled application(s) currently providing services in your economy. Please also identify the type of usage (i.e.G2B, G2C, B2B and/or B2C)	Please identify the name of CA which issue the certificate	Does the user need to pay any fee for the application?	What are the purposes to apply PKI in the application? (Multiple selections are accepted)	What kind of token is used for the application?
1.	E-Government Services				
1.1	□ E-Invoice		□ Yes ☐ By transaction US$_____ ☐ By monthly fee US$_____ ☐ By annual fee US$_____ □ No	□ ID Authentication □ Information Integrity □ Information Confidential □ Electronic Signature (for non-repudiation)	□ USB token □ Smart card □ Software token
1.2	□ E-Tax Filing		□ Yes ☐ By transaction US$_____ ☐ By monthly fee US$_____ ☐ By annual fee US$_____ □ No	□ ID Authentication □ Information Integrity □ Information Confidential □ Electronic Signature (for non-repudiation)	□ USB token □ Smart card □ Software token

No.	Please mark the PKI-enabled application(s) currently providing services in your economy. Please also identify the type of usage (i.e.G2B, G2C, B2B and/or B2C)	Please identify the name of CA which issue the certificate	Does the user need to pay any fee for the application?	What are the purposes to apply PKI in the application? (Multiple selections are accepted)	What kind of token is used for the application?
1.3	□ E-Customs		□ Yes ☐ By transaction US$_____ ☐ By monthly fee US$_____ ☐ By annual fee US$_____ □ No	□ ID Authentication □ Information Integrity □ Information Confidential □ Electronic Signature (for non-repudiation)	□ USB token □ Smart card □ Software token
1.4	□ E-Service for business (e.g. applications of registration, business closure, and company information inquiry)		□ Yes ☐ By transaction US$_____ ☐ By monthly fee US$_____ ☐ By annual fee US$_____ □ No	□ ID Authentication □ Information Integrity □ Information Confidential □ Electronic Signature (for non-repudiation)	□ USB token □ Smart card □ Software token
1.5	□ E-Passport		□ Yes ☐ By transaction US$_____ ☐ By monthly fee US$_____ ☐ By annual fee US$_____ □ No	□ ID Authentication □ Information Integrity □ Information Confidential □ Electronic Signature (for non-repudiation)	□ USB token □ Smart card □ Software token

No.	Please mark the PKI-enabled application(s) currently providing services in your economy. Please also identify the type of usage (i.e.G2B, G2C, B2B and/or B2C)	Please identify the name of CA which issue the certificate	Does the user need to pay any fee for the application?	What are the purposes to apply PKI in the application? (Multiple selections are accepted)	What kind of token is used for the application?
1.6	□ PKI-based National ID Card		□ Yes ☐ By transaction US$_____ ☐ By monthly fee US$_____ ☐ By annual fee US$_____ □ No	□ ID Authentication □ Information Integrity □ Information Confidential □ Electronic Signature (for non-repudiation)	□ USB token □ Smart card □ Software token
1.7	□ E-Voting		□ Yes ☐ By transaction US$_____ ☐ By monthly fee US$_____ ☐ By annual fee US$_____ □ No	□ ID Authentication □ Information Integrity □ Information Confidential □ Electronic Signature (fro non-repudiation)	□ USB token □ Smart card □ Software token
1.8	□ General e-Government services to citizens (e.g. ID applications, household or cadastral information inquiry, Medicare service, etc.)		□ Yes ☐ By transaction US$_____ ☐ By monthly fee US$_____ ☐ By annual fee US$_____ □ No	□ ID Authentication □ Information Integrity □ Information Confidential □ Electronic Signature (for non-repudiation)	□ USB token □ Smart card □ Software token

No.	Please mark the PKI-enabled application(s) currently providing services in your economy. Please also identify the type of usage (i.e.G2B, G2C, B2B and/or B2C)	Please identify the name of CA which issue the certificate	Does the user need to pay any fee for the application?	What are the purposes to apply PKI in the application? (Multiple selections are accepted)	What kind of token is used for the application?
2	Online Banking				
2.1	□ E-Payment		□ Yes ☐ By transaction US$_____ ☐ By monthly fee US$_____ ☐ By annual fee US$_____ □ No	□ ID Authentication □ Information Integrity □ Information Confidential □ Electronic Signature (for non-repudiation)	□ USB token □ Smart card □ Software token
2.2	□ E-Billing (i.e. the electronic delivery and presentation of financial statement, bills, invoices, and related information sent by a company to its customers)		□ Yes ☐ By transaction US$_____ ☐ By monthly fee US$_____ ☐ By annual fee US$_____ □ No	□ ID Authentication □ Information Integrity □ Information Confidential □ Electronic Signature (for non-repudiation)	□ USB token □ Smart card □ Software token
3	□ Online security trading (e.g. stock, bonds or fund) □ G2B □ B2B □ B2C		□ Yes ☐ By transaction US$_____ ☐ By monthly fee US$_____ ☐ By annual fee US$_____ □ No	□ ID Authentication □ Information Integrity □ Information Confidential □ Electronic Signature (for non-repudiation)	□ USB token □ Smart card □ Software token

No.	Please mark the PKI-enabled application(s) currently providing services in your economy. Please also identify the type of usage (i.e.G2B, G2C, B2B and/or B2C)	Please identify the name of CA which issue the certificate	Does the user need to pay any fee for the application?	What are the purposes to apply PKI in the application? (Multiple selections are accepted)	What kind of token is used for the application?
4	□ E-Procurement □ G2B □ G2C □ B2B □ B2C		□ Yes ☐ By transaction US$_____ ☐ By monthly fee US$_____ ☐ By annual fee US$_____ □ No	□ ID Authentication □ Information Integrity □ Information Confidential □ Electronic Signature (for non-repudiation)	□ USB token □ Smart card □ Software token
5	□ Order management (i.e. trading order entry and processing over electronic mechanisms) □ G2B □ G2C □ B2B □ B2C		□ Yes ☐ By transaction US$_____ ☐ By monthly fee US$_____ ☐ By annual fee US$_____ □ No	□ ID Authentication □ Information Integrity □ Information Confidential □ Electronic Signature (for non-repudiation)	□ USB token □ Smart card □ Software token
6	□ E-insurance service (i.e. web based insurance services, including applications, indemnification, information inquiry) □ G2B □ G2C □ B2B □ B2C		□ Yes ☐ By transaction US$_____ ☐ By monthly fee US$_____ ☐ By annual fee US$_____ □ No	□ ID Authentication □ Information Integrity □ Information Confidential □ Electronic Signature (for non-repudiation)	□ USB token □ Smart card □ Software token

No.	Please mark the PKI-enabled application(s) currently providing services in your economy. Please also identify the type of usage (i.e.G2B, G2C, B2B and/or B2C)	Please identify the name of CA which issue the certificate	Does the user need to pay any fee for the application?	What are the purposes to apply PKI in the application? (Multiple selections are accepted)	What kind of token is used for the application?
7	□ Document management (i.e. managing documents over electronic systems or networks, including filing, retrieval, archiving and exchange) □ G2G □ G2C □ G2B □ B2B □ B2C		□ Yes ☐ By transaction US$_____ ☐ By monthly fee US$_____ ☐ By annual fee US$_____ □ No	□ ID Authentication □ Information Integrity □ Information Confidential □ Electronic Signature (for non-repudiation)	□ USB token □ Smart card □ Software token
8	□ E-mail Security		□ Yes ☐ By transaction US$_____ ☐ By monthly fee US$_____ ☐ By annual fee US$_____ □ No	□ ID Authentication □ Information Integrity □ Information Confidential □ Electronic Signature (for non-repudiation)	□ USB token □ Smart card □ Software token

No.	Please mark the PKI-enabled application(s) currently providing services in your economy. Please also identify the type of usage (i.e.G2B, G2C, B2B and/or B2C)	Please identify the name of CA which issue the certificate	Does the user need to pay any fee for the application?	What are the purposes to apply PKI in the application? (Multiple selections are accepted)	What kind of token is used for the application?
9	□ Others - Please identify the application: _____		□ Yes ☐ By transaction US$_____ ☐ By monthly fee US$_____ ☐ By annual fee US$_____ □ No	□ ID Authentication □ Information Integrity □ Information Confidential □ Electronic Signature (for non-repudiation)	□ USB token □ Smart card □ Software token
10	□ Others,-Please identify the application: _____		□ Yes ☐ By transaction US$_____ ☐ By monthly fee US$_____ ☐ By annual fee US$_____ □ No	□ ID Authentication □ Information Integrity □ Information Confidential □ Electronic Signature (for non-repudiation)	□ USB token □ Smart card □ Software token

※ Please add or delete the rows if necessary.

Session Three: E-Authentication Application

Please identify the authentication technologies other than PKI have been applied in your economy? (Multiple selections are accepted)

- □ RFID
- □ Biometric identification
- □ Passwords
- □ Near Field Communication (NFC)
- □ Others- Please identify:

_____

_____

Session Four: The barriers of PKI promotion

What are the barriers of PKI promotion in your economy? (Multiple selections are accepted)

- □ Application procedures are too complicated
- □ The cost of PKI implementation is too high
- □ PKI Applications are not user-friendly
- □ Technical support issues are concerned
- □ The PKI market is still immature. (i.e. The industry has not yet found PKI necessary)
- □ Civilian and enterprises still lack PKI knowledge
- □ Others, please identify:

_____

_____

Session Five: International Cooperation

How do you think about enhancing PKI/e-Authentication or the internet security in the respective economy to enable collaboration among economies?

_____

_____

_____

_____

_____

_____

_____

_____

_____

Session Six: Survey Information Provider

1. Name：_Ms./Mr./Mrs./Dr._____
2. Organization：_____
3. Position/Job Title：_____
4. Economy：_____
5. Contact Information:

   Phone：_____

   E-mail：_____

═══ Thank you very much for the valuable contribution ═══

Chinese Taipei sincerely requests that all APEC economies can complete this survey. Please send your completed survey to Cindy Tseng at hsuyingtseng@itri.org.tw before ***18, May 2009***. For more information, please feel free to contact Cindy by e-mail or phone +886-2-23925090 ext.108.