GOVERNMENT PKI DEPLOYMENT AND USAGE IN TAIWAN

Chung-Ming OU, Hwai-Ling SHAN, and Chuan-Te HO

Abstract: The ongoing e-Government Program in Taiwan started in 1997. It is based on the Government Service Network, which is the backbone infrastructure of the network transaction environment. During the first phase of this program in 1998, Taiwan established its first Certification Authority, namely, the Government Certification Authority (GCA), and this launched the electronic certification services in Taiwan. From 2001 to 2004, the Government Public Key Infrastructure (GPKI) has been established according to the planning set forth in the e-Government Program with the aim of strengthening electronic government infrastructure and establishing electronic certification and security applications for executive administration. Besides GPKI applications, PKI interoperability has become a major issue in Taiwan recently. Several interoperability schemes, such as strict hierarchy and Bridge Certificate Authority (BCA), have been deployed in different PKI domains. To achieve global PKI interoperability in Taiwan, BCA is being adapted as a major CA-CA interoperability engine, which will ensure trusted relationships between the different PKI domains.

Keywords: GPKI, GRCA, GCA, MOICA, MOEACA, Digital Signature.

PKI and Secure e-Taiwan

Taiwan was successful in shifting industry policies to focus on high-technology products, which is a strategy successfully transforming Taiwan into one of the largest hardware-exporting nations worldwide. This strategy has a major impact on national strategy in harnessing information and communication technologies for economic development and global competitiveness. To accelerate the transformation of traditional industries to a knowledge-based economy, the Cabinet had approved the e-Taiwan project (2002-2007), which is composed of e-Government, e-Industry and e-Society projects. Among these projects, e-Government will be the major driving force. There are several important plans under the “e-Taiwan Project” aim to build a more secure infrastructure for the information and communication security environment, and they are listed below[1]:

Natural Person Certificate Project

Object	• Assist e-Government to promote internet personal identification. • Issue over 3 million Natural Person Certificates by 2005.
Current Status	• Natural person CA was established and 50 register counters have been setup in registration offices in districts and counties. • More than 50 applications in 7 systems exploiting personal IDs have been developed by government agencies.
Period	2002~2007
Note	Electronic Signature Law was enacted on 31 October 2001 and became effective on 1 April 2002.

Establish Certificate Interoperability Mechanism

Object	• Build certificate interoperability mechanism between domestic and international domain. • Enhance CA industry development.
Current Status	• A PKI infrastructure interoperability committee has been setup and a Bridge CA which completed interoperability testing between two CA. • 28 PKI applications have been developed by private sectors under grant support from this project.
Period	2003~2007

Establish National Security Operation Center

Object	• Provide 24 hours/day network system monitoring and incident handling for 500 monitor points of important government agencies.
Current Status	• The design of monitor functions, SLA, common format of data exchange is under way. • A POC prototype is being developed.
Period	2003~2006

Information Security Product Certification Scheme

Object	• Create the security product certification scheme in Taiwan and plans of the testing laboratory construction.
Current Status	• Increase Information Security products testing and certification skill to provide consulting service. • Seek for the framework and its associated specifications for a CC-conformity testing laboratory. • Provide training courses for evaluators and assessors.
Period	2003~2006

The e-Government Program of Taiwan was initiated in 1997. The Government Service Network (GSN) was one of the sub-programs put to work since June 1997.[2,3,4] GSN is the fundamental infrastructure of the electronic government, providing network framework on which e-services are rendered. To establish a secure and trusted network transaction environment based on the GSN, Taiwan has launched electronic certification services. This involved establishing the e-government digital certification system, promoting Government PKI, and facilitating the development of government online information and service applications (see Figure 1). To promote e-government services, the Research, Development, and Evaluation Commission (RDEC) of the Executive Yuan (commonly known as the Cabinet) has since then instituted Government Electronic Certification Steering Committee so that opinions and ideas from experts and citizens can be efficiently and objectively reflected through the process.

The need of providing the GSN with an authentication/secure communication mechanism was the motive of building our GPKI. GPKI has been built according to the structure defined in the ITU-T X.509 standard, namely, there is a trust anchor for GPKI, a Government Root Certification Authority (GRCA), and underlying subordinate CAs for individual government sectors. The evolution of GPKI in Taiwan comprises two phases. In phase 1, RDEC has implemented a pilot certification authority (CA), namely, the “Government Certification Authority” (GCA), which served as a multi-purpose CA for issuing public key certificates to the government agencies, citizens, and application servers, as well as to corporations. In February 1998, RDEC commissioned Chunghwa Telecom, which is a major telecommunication company in Taiwan, to establish the GCA in phase 1, which provides electronic certification services so that users can be identified online. The GCA provides currently a variety of electronic certification services to government agencies, business organizations, and citizens. More than 536 000 electronic certificates of all classes have been issued

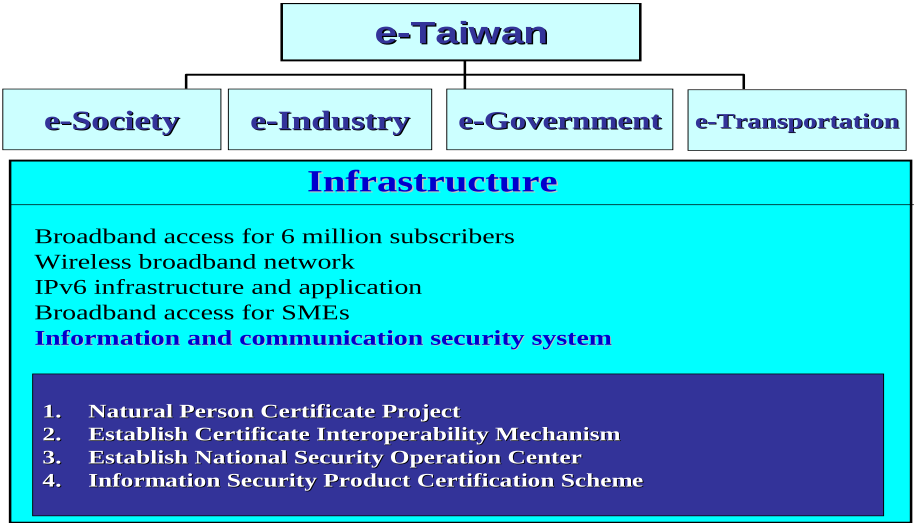
e-Taiwan
e-Society
e-Industry
e-Government
e-Transportation
Infrastructure
Broadband access for 6 million subscribers
Wireless broadband network
IPv6 infrastructure and application
Broadband access for SMEs
Information and communication security system
1. Natural Person Certificate Project
2. Establish Certificate Interoperability Mechanism
3. Establish National Security Operation Center
4. Information Security Product Certification Scheme

Figure 1: PKI and e-Taiwan Project.

since the establishment of GCA in 1998. The certificates have been used for such applications as online income tax filing, motor vehicle registration, electronic payment, electronic procurement, and official electronic document exchange.

In the mean time, as tremendous hands-on experience was gained, the acceptance of the PKI technology in Taiwan grew, and the relevant legislation such as the Electronic Signature Act was enacted, a clearer perspective appeared. RDEC recognized the need for "branching" the earlier multi-purpose GCA in response to more realistic and versatile applications. Hence, the objective of the *second phase* GPKI is to transform the earlier naive design into a full-fledged PKI based on the GPKI hierarchy and established GRCA, under which some government agencies acting as the proper authorities in corresponding fields will establish their CAs.

Framework and Services of GPKI

GPKI Framework

The GPKI in Taiwan is under the oversight of the Government Electronic Certification Steering Committee (GECSC). The responsibilities of the Steering Committee are as follows:

- To survey and review the Certificate Policy and Certification Practice Statements of CAs within the GPKI.
- To survey and review technical standards of digital certificates.

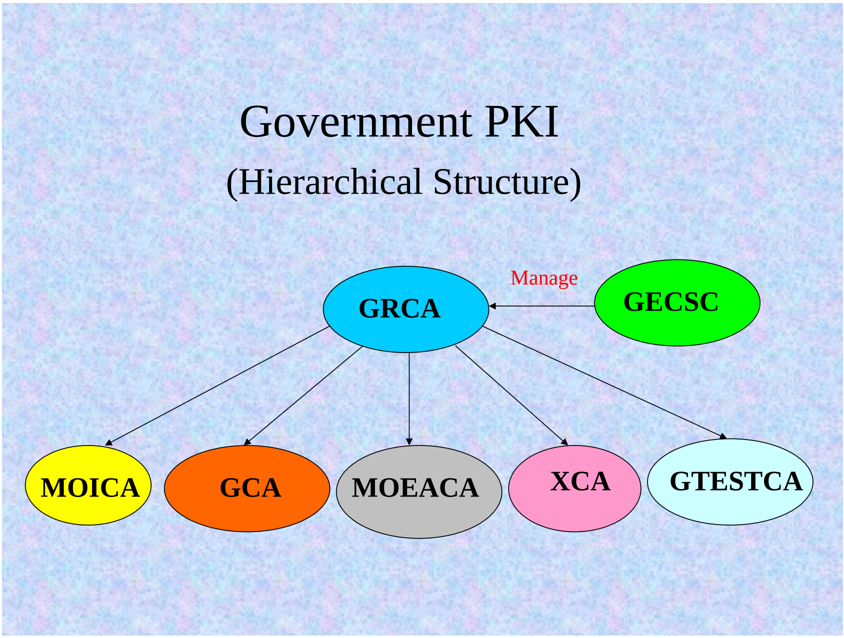

Figure 2: Framework of GPKI.

- To survey and review framework of digital certificates.
- To survey and review related administrative issues of digital certificates.

Following the hierarchical structure defined in the ITU-T X.509 standard,[5,6,7] GRCA is a trust anchor for GPKI. Other CAs within the GPKI are established by individual government sectors. They issue certificates to be used in applications of electronic government in order to provide more convenient Internet service for the citizens and business; this improves governmental administration efficiency and promotes applications development of electronic commerce. According to the e-Government Program (2001-2004), the designated organizations responsible for building corresponding CAs are illustrated in Figure 2; those CAs are responsible for providing certification services to government agencies, industry and business organizations, and citizens, which are named GCA, MOICA, MOEACA, XCA and GTestCA. The GRCA has issued certificates to these CAs since 2002. Table 1 lists the number of certificates issued by these CAs.

GCA (Phase 2)

Phase 2 of the GCA was initiated by RDEC in 2003, whose mission has switched from the phase 1 mission to issue certificates to all government sectors, which includes government organizations, government organizational units and server appli-

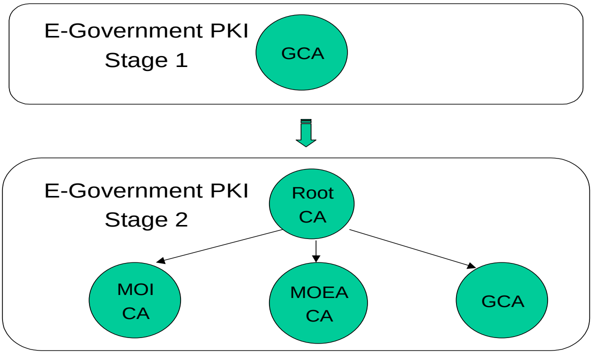

Figure 3: Evolution of E-Government PKI.

cations. It has issued more than 55 228 certificates so far.

MOEACA

The MOEACA was established by the Ministry of Economic Affairs (MOEA) in 2003. It issues certificates to all industry and business groups, which includes factories, companies and proprietors. So far there are around 3 493 certificates being issued. This MOEACA can be used for e-government applications such as industry and commerce registrations, bid getting and bid submitting, tax filing, and labor insurance updating.

MOICA

The MOICA was established by the Ministry of Interior in 2003. It issues certificates to all Taiwanese citizens and there are around 521 904 certificates being issued so far.

XCA

The XCA was established by RDEC in March 2004. It issues certificates to schools, juridical associations and consortiums. Total number of issued certificates is around 1 719.

GTestCA

The GTestCA was established by RDEC in 2003, which issues testing certificates to all GPKI applications. So far there are 4 056 certificates being issued.

Table 1: Certificates Issued by GPKI.

	GCA(old)	GCA(new)	XCA	MOEACA	MOICA	TOTAL
1998	33,901	0	0	0		33,901
1999	67,561	0	0	0		67,561
2000	104,854	0	0	0		104,854
2001	212,408	0	0	0		212,408
2002	418,178	0	0	0		418,178
2003	522,541	14,396	0	1,295	248,392	786,624
2004(Oct. 28)	530,490	55,228	1,719	3,493	521,904	1,112,834

GPKI Services

In RDEC's design of electronic certification applications (based on X.509 v3, year 2000 edition), the e-government electronic certification structure has the following components: Public Key Infrastructure (PKI) and Privilege Management Infrastructure (PMI). The former provides public certification services for authentication and non-repudiation with public key certificates stored in smart cards; the latter provides attribute certification service for authorization. PMI does not have a hierarchical structure in that, each Attribute Authority (AA) will issue attribute certificates within the scope of its authority independently and it is not subordinated to any other authority. Implementation of a functioning PMI which provides attribute certification services is expected to be completed in the near future. Therefore, we may conclude that the GPKI major services are as follows:

- To issue and manage certificate services;
- To manage certificate revocation and renewal;
- To publish certificates and certificate revocation list (CRL);
- To provide application programming interface (API) such as data encryption, digital signature, and digital envelope;
- To provide time stamp services;
- To provide testing certificates.

To support these services, the GPKI framework is designed to comprise the following components:

- A secure, trusted, and interoperable electronic certification mechanism. It supports secure and trusted government services;
- A variety of public key certification services. Their integrated and innovative functionalities will promote the widespread use of online applications;

- The PMI (Privilege Management Infrastructure), which will provide attribute certification services and satisfy various certification requirements for GPKI applications.

PKI-Enabled e-Services

According to Wang,[8] there are around 353 applications for GPKI and 45 companies are becoming solution providers for GPKI applications. Those applications can be divided into three categories, which are G2G, G2B, and G2C.

G2G Applications

e-Official Document Interchange

E-Official Document Interchange provides a portal for all governmental sectors to exchange electronic documents among them. GCA certificates are needed for those government sectors while adapting to this application. According to the future GPKI plan, each government official in charge of producing electronic documents will also need to append his/her digital signatures to those documents via his/her MOICA certificate. This so-called multi-signature document format will meet practical situations among government sectors in Taiwan.

e- Payment

E-Payment transforms the payment and fund-transferred information to non-reputable electronic forms, which are sent to the government payment center via GSN. This application requires the participating government sectors to apply their GCA certificates.

G2B Applications

e-Procurement

E-Procurement provides a portal to contractors and solution providers to get and submit governmental bids. This guarantees a fair bidding environment for every qualified contractor and service provider. All solution providers and contractors can purchase bid-offering documents and deliver bidding documents through Internet, after they have been issued MOEACA certificates. GPKI services guarantee that this application initiates a trusted and secure network transaction environment between government sectors and corporations.

e-Corporation

E-Corporation assists corporations in registering or updating their corporation information on-line. Corporations need to apply the MOEACA certificates first and this application can reduce lots of time-consuming paperwork.

e-Tax Refund

E-Tax Refund assists the Customs in returning taxes to foreign tourists while leaving Taiwan. This application provides a gateway for electronic information exchange between the tax bureau, corporations, the Customs, the Bank of Taiwan and the tax data center. Moreover, this application is a combination of a G2G and a G2B application, or we may refer it as a G2G2B application. GCA and MOEACA certificates are needed depending on the end-entities.

Customs e-Applying

An applicant for Customs e-Applying may be a person, a corporation, a Customs-applying company, or a special delivery company, among others. A Customs-application form is appended by a digital signature of a Customs-applicant. Depending on the entity, a Customs-applicant needs to provide either MOICA certificate or MOEACA certificate to this application.

Labor and Farmer Insurance On-Line System

The Labor and Farmer Insurance on-line system utilizes MOICA certificates to assist government officials in doing administrative work via Internet such as updating insurers' information. On the other hand, insurers can inquire about their insurance information using MOICA certificates.

G2C Applications

e- Household Registry

The e-Household Registry assists all residences in Taiwan in performing household services via Internet, such as completing general household information. The Ministry if Interior is planning to put most of the household registry services on-line.

Land Administration Electronic Gateway Information System

This is an on-line service for citizens who may file applications such as land price reporting, land registers' basic information update and land information update. A land register can also inquire about the rate of processing of his/her case on-line.

e-Motor-Vehicle Service

The e-Motor-Vehicle service assists all car owners who have MOICA certificates in requesting and renewing automobile registration licenses; it also assists car owners in requesting and paying traffic tickets.

e-Taxation Service

The e-Taxation service—the first G2C application of GPKI started in 1998—assists

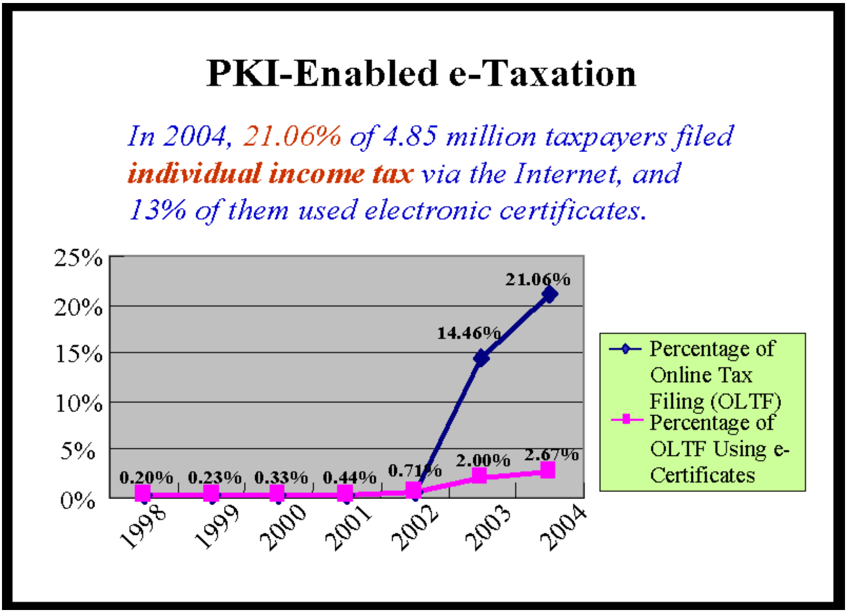

Figure 4: PKI-Enabled E-Taxation.

citizens and corporations filing income taxes and business taxes, respectively. This application has become one of the major achievements of Taiwanese GPKI for the past several years.

PKI Interoperability

PKI interoperability is identified as one of the most important obstacles to PKI deployment and usage. A survey conducted by OASIS in June 2003 highlights that the most serious interoperability problems are path validation, smart cards, unusual certificate content, cross-certification, certificate issuance, certificate revocation, and protocols. The most common problems[9] identified were standards: too many in some areas, too few in others, too ambiguous, poor implementations, no conformance testing, etc. Incompatible certificate policies were another concern. Due to the fact that PKI interoperability is especially complex, RDEC has allocated more resources and put a lot of effort in dealing with this issue.

Cross Certification with GRCA

There are three interoperability technologies deployed in Taiwan: cross certification, Bridge CA, and strict hierarchy. Basically, GRCA is in charge with the interoperability of GPKI with other PKI (including foreign PKI).

A CA that interoperates with GRCA through cross-certification is referred to as an interoperating CA. To get GRCA's approval for cross-certification, the applicant CA must comply with the requirements of the assurance level defined in the cited Certificate Policy. Additionally, the applicant CA must have the capabilities to establish and manage the following aspects: Public Key Infrastructure; Digital signatures and certificate issuing technology; the corresponding responsibilities and obligations among CA, RA, and the relying party.

GRCA issues the certificate to the applicant CA if instructed by RDEC. After issuance, RDEC shall notify the applicant CA with formal official document, attached with the issued certificate. If RDEC decides not to issue the cross-certificate, the applicant CA shall also be notified by a formal official document along with the reason(s) for the rejection.

GRCA has its self-signed certificate (verified by RDEC) delivered to the applicant CA in accordance with the procedures of GRCA's Certificate Policy Statement (CPS). Upon receiving the notification of the approval delivered via formal official document, the applicant CA shall examine the attached certificate to ensure the correctness of its content. After the applicant CA verifies the correctness, it must sign a confirmation document, which shall be sent back to GRCA and RDEC by a formal official document. When GRCA receives a confirmation document, it shall post the newly issued certificates to the repository. If the applicant CA fails to respond within 30 days (upon receiving the approval notification), it is viewed as a refusal to accept the certificate. RDEC shall then authorize GRCA to revoke that certificate after verification. No additional announcement shall be made concerning the application.

Bridging GPKI and Commercial PKIs

The Ministry of Economic Affairs (MOEA), which is the authority in charge with PKI, has deployed Taiwanese BCA in 2004 as the major PKI interoperability platform. BCA will only issue cross certificate to a CA that becomes its member; BCA will not issue any certificates to end-users. Taiwanese BCA will not play a trust point for any PKI in order to respect the autonomy of each PKI.

Since there are distributed PKIs throughout different domains, such as government, finance and healthcare systems, BCA is regarded as a proper solution for Taiwanese PKI interoperability (see Figure 5) Furthermore, many foreign countries such as United States, Japan, Germany, China and Canada, have been either deployed or being planned for BCA interoperability.

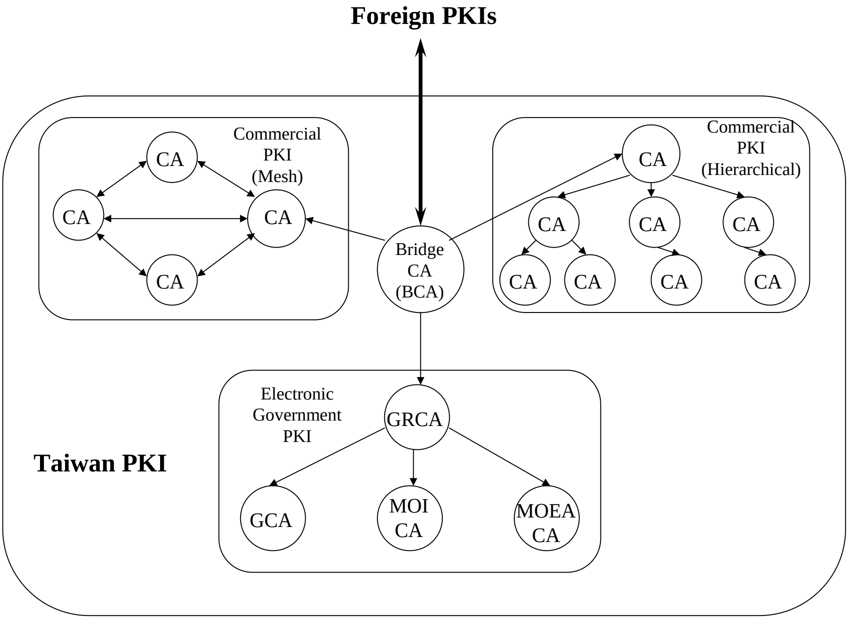

Figure 5: The Role of the Bridge CA in Taiwan PKI.

Currently, there are several companies acting as certification service providers for issuance of public-key certificates for commercial use. There are some end-entities the jurisdiction of which is out of the GPKI domain. Thus, the appearance of commercial PKI is a complement to a complete Taiwanese PKI. It is anticipated that there will be a need for cross certification between CAs in the GPKI and CAs in a commercial PKI. The rough draft, as shown in Figure 5, is to establish a Bridge CA (BCA)[10] as a bridge of trust that provides trust paths between the various PKIs in Taiwan. In addition, the BCA will also act as a bridge of trust that provides trust paths between Taiwanese PKI and foreign PKIs.

Each PKI has one principal CA that cross-certifies with the BCA. In the case of a PKI with hierarchical certification paths, it will be the root CA of the domain. In a mesh-organized PKI, the principal CA may be any CA in the domain. However, it will normally be one operated by, or associated with, the domain policy management authority. It is also anticipated that there will be a need for constituting a Policy Management Authority because cross certification will involve policy approval and policy mapping among different PKIs and the overall policies of the BCA. Thus, the main subject of phase 3 will comprise policy management, policy approval, policy map-

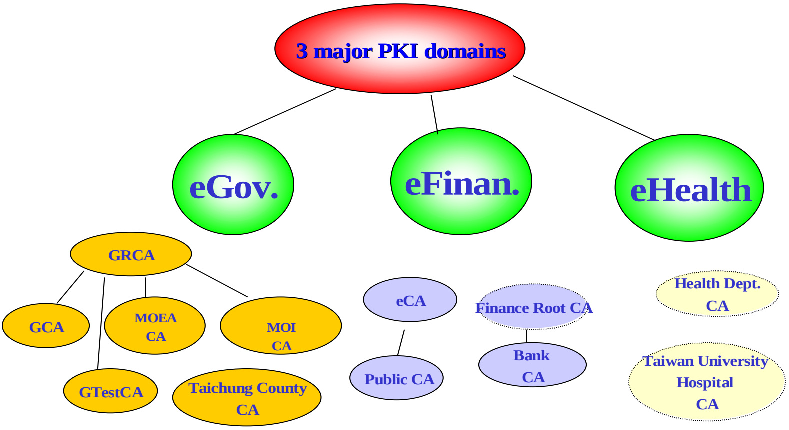

Figure 6: Three Major PKI Domains in Taiwan.

ping, and cross certification.

Global PKI Interoperability in Taiwan

The key for global PKI interoperability is to adapt the original certificate paths within each PKI domain. BCA will not influence any certificate path of each PKI domain. It is a better approach BCA to establish a peer-to-peer relationship; this means it is not superior to GRCA or the principal CA in each PKI domain. CAs do not need to connect to Taiwanese BCA unless they need to interoperate with CAs in different PKI domains.

Both from policy and technology point of view, the following four issues arise while considering adapting BCA as Global Taiwanese PKI Interoperability.

- *Establish the Policy Management Authority (PMA)*: PMA provides the operational guideline for BCA. PMA members should be those CAs which intend to interoperate with each other.
- *Establish the BCA Certificate Policy (CP)*: Before BCA issues a cross certificate to its member CA, this CA has to be audited by the BCA (actually, BCA can outsource this auditing task to some proper third-party organization). Furthermore, the assurance level of an issued certificate has to be mapped to that of BCA CP. Therefore, trust relationship between CAs can be built. The standard of the BCA CP may be referred to ANSI X9.79 and IETF RFC 2527.

- *BCA Technical Template*: After the CA-CA trusted relationship has been established, the technical details for interoperability will be a major issue.
- *Establish CA Auditing System*: CA has to be ensured that its operational and management security engine has passed the third–party inspection. One of the major auditing procedures is that CA must operate according to the assurance level acclaimed by its CPS.

Conclusions

GPKI is used in many e-services in Taiwan. As of October 2004, government agencies have promoted more than 900 online services. However, GPKI has not reached its full potentials in Taiwan. A number of barriers, including lack of applications, high cost, poor understanding of PKI, and interoperability issues have contributed to the limited use of Government PKI.

According to the survey conducted by OASIS in June 2003, respondents identified that the most important obstacles to PKI deployment and usage are (1) Software applications do not support IT; (2) Costs are too high; (3) PKI is poorly understood; (4) Too much focus on technology, not enough on need; and (5) Poor interoperability. The survey also indicated that the most important applications for PKI are document signing, secure e-mail, electronic commerce, and single sign-on. Document signing was further broken down into singing forms, signing contracts, and signing documents before dissemination. GPKI deployment and usage in Taiwan is facing the similar obstacles. In order to increase take-up of PKI, RDEC identified electronic document exchange and e-taxation as the most important applications. RDEC also adopts a free digital certificate policy, which means that every citizen, company and government agency can apply a digital certificate for free. This policy helps the users to set up a test PKI with little or no cost. It is useful for testing and as a way to encourage people to get started with PKI.

PKI was invented more than 20 years ago. Today, it is used in many important online services. But a number of barriers limit usage of PKI. Increasing take-up of GPKI was directly related to the value gained from a secure e-government program in terms of improved service, greater efficiency, costs saving, and trusted online services. Clearly, the full potential of GPKI will be realized only if citizens and business use it, but most governments still find themselves confronted with the challenge of low usage and the need for innovative methods to drive take-up. In Taiwan, promoting take-up of GPKI is taking hold, but the challenge remains. PKI involves many parties: customers and users, operators, software developers (for applications, auditors, and security experts). GPKI take-up needs support from all these parties.

Notes:

[1] National Information and Communication Security Taskforce (NICST), *Information and Communication Security Services for e-Government* (October 2003), <http://www.nicst.nat.gov.tw> (12 November 2004).

[2] The Executive Yuan of the Republic of China, *Note of the Executive Yuan Council No. 2557 Meeting* (1997), <http://www.ey.gov.tw> (12 November 2004).

[3] Research Development and Evaluation Commission of the Executive Yuan, *Introductory to the Electronic/Networked Government Program* (1998), <http://www.rdec.gov.tw>.

[4] Data Communication Group of Chunghwa Telecom Co. Ltd., *Proposal for Government Service Network (GSN) of the Electronic/Networked Government Program* (1998), <http://www.rdec.gov.tw> (12 November 2004).

[5] Russell Housley, Warwick Ford, W. Polk, and David Solo, "Internet X.509 Public Key Infrastructure, Certificate and CRL Profile," Internet Draft, The Internet Engineering Task Force (IETF), PKIX Working Group, RFC 2459, January 1999, <http://www.faqs.org/rfcs/rfc2459.html> (12 November 2004).

[6] Stefan Santesson, Tim Polk, Petra Barzin, and Magnus Nystrom, "Internet X.509 Public Key Infrastructure Qualified Certificates Profile", The Internet Engineering Task Force (IETF), RFC 3039, January 2001, <http://www.faqs.org/rfcs/rfc3039.html> (12 November 2004).

[7] William E. Burr, "Public Key Infrastructure (PKI) Technical Specifications: Part A - Technical Concept of Operations," NIST FPKI, Working Draft TWG-98-59, September 1998, < http://csrc.nist.gov/pki/twg/baseline/pkicon20b.PDF> (12 November 2004>.

[8] Wen-San Wang, "Current Status & Future Perspective of PKI Development in Taiwan," (paper presented at the International Conference of Collaboration of e-Commerce Applications and Security, Taipei, Taiwan, 14-15 September 2004).

[9] The OASIS PKI Technical Committee, *PKI Action Plan* (22 February 2004), <http://www.oasis-open.org/committees/pki/pkiactionplan.pdf> (12 November 2004).

[10] Burr, "Public Key Infrastructure (PKI) Technical Specifications."

CHUNG-MING OU received BS degree in Applied Mathematics in 1987 from Chung-Yuan Christian University, Taiwan, and MS and Ph.D. degrees in Applied Mathematics from Iowa State University, Ames, IA in 1994 and 1996 respectively. Dr. Ou was a MATLAB consultant and software engineer before he joined Chunghwa Telecommunications Lab as a researcher in 1997. His research focuses on cryptography, wireless security and PKI. Dr. Ou also assists in Government PKI e-Government project in Taiwan and PKI Interoperability within Asia PKI Forum. His area of specialty includes Cryptography, Information Security, Numerical Simulation, Computational Sciences and Applied Mathematics. *E-mail:* cou@cht.com.tw.

HWAI-LING SHAN received BS degree in Applied Mathematics in 1986 from Chung-Yuan Christian University, Taiwan, Ph.D. degree in Mathematics and MS degree in Computer Science from Pennsylvania State University, University Park, PA in 1995. She was a Post-doctoral Research Fellow within the Department of Computer Engineering, National Central University, Taiwan until 1998, when she joined Chunghwa Telecommunications Lab as a researcher. She focuses on cryptography, analyzing cryptographic algorithms and standards (including FIPS140, Common Criteria, etc). She also participates in the certification process of Hardware security module against FIPS140-2 and the development and establishment of Government PKI e-Government project in Taiwan. Her area of specialty includes Number Theory, Cryptographic Standards & Protocols, Applications & Services based on Public-Key Infrastructure and Telecommunication Products & Services. *E-mail:* shanhl@cht.com.tw.

CHUAN-TE HO received his master’s degree from the Institute of Public Administration, National Chengchi University (Taiwan). Before assuming his present position as a Director of Department of Information Management, Research, Development, and Evaluation Commission of Executive Yuan in July 2004, he had served in the field of Information Management for over 20 years, during which he had participated in the planning or/and management of a number of IT-related projects, such as Electronic Government programs planning and promoting, Public Key Infrastructure policy planning, Government IT outsourcing policy planning, and Electronic Signature Law (as a drafter). He has also written a number of papers on information-related subjects and he has presented them at international workshops and conferences, including: A Study on Government Information Business Overall Outsourcing Systems, A Study on Government Information Security Management Systems, Secure and Trusted Infrastructure for e-Government, How to Establish an e-Government Information Security Mechanism, Electronic Signature and Electronic Authentication Mechanism, and Encryption Technology and Trust Mechanism in Digital Society. *E-mail:* chuan-te@rdec.gov.tw.