E-Government Electronic Certification Services in Taiwan

Chii-Wen Wu[1], Hwai-Ling Shan[2], Wen-Cheng Wang, Dung-Ming Shieh, and Ming-Hsin Chang
[1] Research, Development, and Evaluation Commission, Executive Yuan, Taiwan
E-mail: larry@rdec.gov.tw
[2] Chunghwa Telecommunication Laboratory, Taiwan
E-mail: shanhl@cht.com.tw, wcwangl@cht.com.tw, dmshiehl@cht.com.tw, ucc@cht.com.tw

ABSTRACT
The ongoing E-Government Program in Taiwan has been started in 1997. It is based on the Government Service Network, which is a backbone infrastructure of the network transaction environment. During the first phase of this program in 1998, Taiwan established its first Certification Authority, namely, Government Certification Authority (GCA), and this launched the electronic certification services in Taiwan. From year 2001 to 2004, Government Public Key Infrastructure (GPKI) is being established according to the planning set forth in E-Government Program with the aim of strengthening electronic government infrastructure and establishing electronic certification and security applications for executive administration.

1. Introduction

The "E-Government Program" of Taiwan was initiated at the beginning of 1997. Government Service Network (GSN) [1][2][3] is one of the sub-programs put to work since June 1997. 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. Electronic certification services are essential for e-government, as they make it possible to provide secure and trusted online application services, to prevent the forgery of transaction information by identifying and/or authenticating users on-line, to protect confidentiality and to prevent the parties in online communications and transactions from repudiating the transmission or receipt of critical data.

To promote e-government services, the Research, Development, and Evaluation Commission (RDEC) of Executive Yuan 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. In 1998, Taiwan established Government Certification Authority (GCA). This facility provides online identity authentication services to government agencies and the public. GCA has laid the foundation for e-government electronic certification services. From year 2001 to 2004, Government Public Key Infrastructure (GPKI) is being established according to the planning set forth in E-Government Program [4] with the aim of strengthening electronic government infrastructure and establishing electronic certification and security applications for executive administration. In this paper, we describe E-Government Electronic

Certification Services in Taiwan. In Section 2, various services in Government PKI are first illustrated. In Section 3, we introduce the Government PKI Framework in Taiwan. In Section 4, the building of Government PKI is depicted. Future Work and conclusion are cited in Section 5 and Section 6, respectively.

2. Services of Government PKI

According to E-Government Program (from 2001 to 2004), the scope of the e-government electronic certification services should cover at least the following tasks:

- To draft a GPKI Certificate Policy (CP) and technical specifications, enabling the CAs to draw up their own Certification Practice Statement (CPS), and thereby achieve a just certification system, secure network service, and CA interoperability.
- To deploy a Government PKI (GPKI) and provide a secure and trusted information and communications environment, and thereby facilitate the government information processing and protect users' rights.
- To establish a secure and trusted electronic certification system, and thereby accelerate the development and widespread application of e-government.

In our design of electronic certification applications (based on X509 v3 2000 edition), we have decided to divide the e-government electronic certification structure into the following components: one is Public Key Infrastructure (PKI) and the other is Privilege Management Infrastructure (PMI). The former provides public certification services and the latter provides

- 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, e-government electronic certification 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 e-government applications.

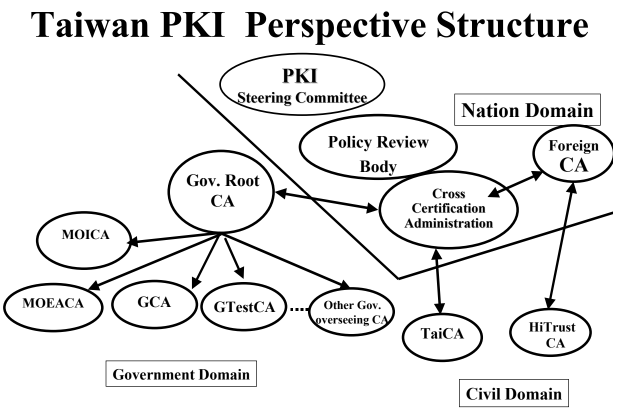
3. Building Government PKI

When GSN was first proposed, the goal was to connect connect all our government agencies to the Internet so that the communications among them would be speeded up and thus their efficiency would be greatly increased. In addition, it would enable the government agencies to provide convenient services to our citizens and enterprises through the Internet. The need of providing the GSN an authentication/secure communication mechanism was thereupon the motive of building our Government Public Key Infrastructure (GPKI). GPKI will be built according to the structure defined in ITU-T X.509 standard. In the structure, there is a trust anchor for this PKI, Government Root Certification Authority (GRCA), and underlying subordinate CAs for individual government sectors. The evolution of our Government PKI comprises three phases. In phase 1, provide convenient services to our citizens and (CA), namely, the ¡§Government Certification for issuing public key certificates to the government mechanism was thereupon the motive of building our agencies, to the citizens, to the application servers, as well as to corporations. In the mean time, as tremendous hands-on experiences were gained, as acceptance of PKI technology in the society of Taiwan grew, and as relevant legislation was enacted, a more clear perspective appeared. We recognize the need for branching the earlier multi-purpose GCA in response to more realistic and versatile applications. Hence, the objective of the second phase will be to transform the earlier naive design into a full-fledged PKI based on the GPKI hierarchy. In the forthcoming phase   , the Government Root CA (GRCA) will be established, under which some government agencies acting as the proper authorities in corresponding fields will establish their CA¡ s, such as M   ICA (Ministry of Interior CA) for issuing public key certificates to the citizens and M   EACA (Ministry of Economic Affairs CA) for issuing public key certificates to the commercial and industrial organizations. Since growing international cooperation is envisioned in the greater picture of PKI application, cross certification will be addressed next. In phase   , a   ridge CA will be established as the connector for cross certification among the Government PKI and commercial PKIs in Taiwan.   or a perspective structure of Taiwan PKI, see fig.   .1.

In February 1998, the RDEC commissioned the Chunghwa Telecom to establish the GCA as we mentioned earlier. The GCA provides electronic certification services so that users can be identified online. The GCA currently provides a variety of electronic certification services to government agencies, business organizations, and citizens. More than 400,000 electronic certificates of all classes have been issued since the GCA was established in 1998 (Fig 3.2). The certificates have been used for such applications as online income tax filing, motor vehicle registration, electronic payment, electronic procurement, and electronic official document exchange, etc.

For a better-organized and policy-consistent GPKI framework, a handful important documents are developed and produced as guidelines for parties joining or intending to join this PKI. Among them are the Certificate Policy and Technical Specification of GPKI. By the definition given in ITU-T X509, Certificate Policy “indicates the applicability of a certificate to a particular community and/or class of application with common security requirement”. For the users of the certificates, CP gives good indication of the degree to which they can trust the binding embodied in a certificate as well as the proper range of usage of a specific certificate. Technical Specification details the suggested relevant standard to be employed in the vital operations of CAs, such as CP, CPS, cryptographic modules, key management, information security management, and audit, etc.

As mentioned in the framework earlier, the Government’s hierarchical PKI framework rolled out in 2001 included the establishment of a Root Certification Authority (RCA) with several CAs under it. The CAs are responsible for providing certification services to government agencies, industry and business organizations, and citizens. The GRCA is beginning to issue certificates to government CAs in 2002. The MOEACA is planning to issue corporate certificates to industry and business organizations (including factories, companies, and proprietorship) in Oct. 2002. The MOICA is planning to issue natural person certificates to citizens in Jan. 2003. It should be noted the GCA has been issuing a great deal of certificates that are supposed to be issued by MOICA and MOEACA respectively only because the latter two CAs are still under development.



Reference：Taiwan NICI

Fig 3.1 Taiwan PKI Perspective Structure

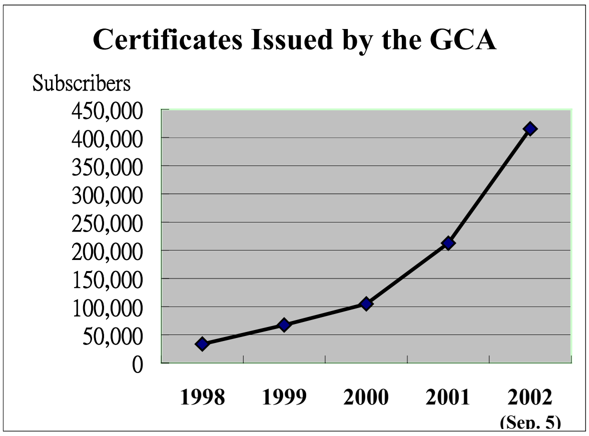


Fig 3.2 Certificates Issued by GCA from 1998 to 2002(Sep. 5)

4. Government PKI Framework

As mentioned earlier, the e-government electronic certification framework consists of a PKI and PMI. Currently Government PKI in Taiwan is under the oversight of Government Electronic Certification Steering Committee (GECSC). In the following we describe briefly the role each party in the GPKI community plays.

4.1 Government Electronic Certification Steering Committee

The PKI has a hierarchical structure that includes a Government Electronic Certification Steering Committee (GECSC) responsible for reviewing the GPKI CP, technical specifications, and the CA's CPS to ensure compliance with the CP. The Convener (concurrent post) of this Committee is designated by the Chair of RDEC. The numbers of 15 to 17 Committee members are composed of experts and representatives from industry, academia, and public offices. The responsibilities for 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.
- To survey and review framework of digital certificates.
- To survey and review related administrative issues of digital certificates.

4.2 Government PKI Framework

Government Public Key Infrastructure (in Fig 4.1, GPKI) is established according to the planning set forth in E-Government Program (from 2001 to 2004). Following the hierarchical structure defined in ITU-T X.509 standard [5][6][7], GPKI has a trust anchor, in this case, Government Root Certification Authority (GRCA), and subordinate CAs for individual government sectors. Other CAs within the GPKI are established by individual government sectors. They issue the certificates to be used in applications for electronic government in order to provide more convenient Internet service for the citizens and business, to improve governmental administration efficiency and to promote applications development of electronic commerce.

According to E-Government Program (from 2001 to 2004), the designated organizations responsible for building corresponding CAs are listed below:

- Research, Development and Evaluation Commission (RDEC) of Executive Yuan: establish the GRCA, Government Certification Authority (GCA) and GtestCA.
- Ministry Of Economic Affairs（MOEA）: establish the CA of Ministry of Economic Affairs (MOEACA).
- Ministry Of Interior（MOI）: establish the CA for citizens.

4.3 Class of the End-Entities

In the framework of Government PKI, end-entities are classified into several classes so that the CA policy will be able to operate more smoothly. The following table describes the meaning of each kind of the end-entities and Fig 4.2 shows the structure of end-entity certificates.

- **End-Entity:** An end-entity can be a natural person (i.e., an individual), an organization or a property.
- **Natural Person:** A natural person can be a citizen, member, employee, customer, etc.
- **Citizen:** A citizen is a natural person with the nationality of the country. In Taiwan, MOI is in charge of the administration of the nationality registration with the implementation of local governments.

- **Member:** A member is a natural person affiliated to an organization. A stockholder or a director of a company is an example of a member of the company. A partner of a proprietorship is also an example of a member of the proprietorship.
- **Employee:** An employee is a natural person employed by an organization (e.g., a company or a proprietorship). Note that an employee of an organization is not considered as a member of an organization in our taxonomy.
- **Customer:** A customer is a client of an organization (e.g., a company or a proprietorship).
- **Organization:** An organization can be a government organization, a corporation, or an unincorporated organization.
- **Government:** A government organization can be a government agency or a government unit.
- . **Central Government Agency:** A central government agency is an agency of the central government. R EC, M I, and M EA are examples of central government agencies.
- **Local Government Agency:** A local government agency is an agency of a local government. In Taiwan, local governments mean county, municipal governments or townships.
- **Government-Operated Enterprise:** A government-operated enterprise is an enterprise operated by the central government or a local government. Chunghwa Telecom Co., Ltd. is an example of a government-operated enterprise.
- **Public Educational Institution:** A public education institution is an educational institution established by the central government or a local government. In Taiwan, all public primary schools are public education institutions. A national university is also an example of a public education institution.
- **Government Unit:** A government unit is an organizational unit within a government agency.
- **Corporation:** A corporation (a.k.a. a legal person, a juridical person or a corporate body) can be a profit corporation or nonprofit corporation.
- **Profit Corporation:** A profit corporation is a corporation for making profit for the member of the corporation. In Taiwan, profit corporations include companies and cooperation.
- **Company:** A company is a corporation formed and operated according to the Company Law. In Taiwan, MOEA is the administration of the company registration.
- **Cooperation:** Cooperation is a cooperative society formed and operated according to the Cooperation Law. A consumer's cooperative society is an example of cooperation. In Taiwan, MOEA is the administration of the company registration.
- **Nonprofit Corporation:** A nonprofit corporation is a society for makes public interests. In Taiwan, MOI is the administration of the registration of nonprofit corporations.
- **Unincorporated Organization:** An unincorporated organization is a registered society without corporate rights. A proprietorship is an example of an unincorporated organization. In addition, an organizational unit subsidiary to a corporation or unincorporated organization is an unincorporated organization.
- **Proprietorship:** A proprietorship is a small-scale business (a shop). A proprietorship is a profit organization without corporate rights. In Taiwan, MOEA is the administration of the registration of proprietorships.
- **Organizational Unit:** Here, an organizational unit means an unit subsidiary to a corporation or unincorporated organization. Subsidiary companies and factories are two important categories of organizational units. In Taiwan, MOEA is the administration of the registration of subsidiary companies and factories.
- **Property:** A property is an estate (including physical estates or virtual estates) owned by a natural person or organization. In the information world, a property can be a application process or a hardware device.
- **Application Process:** An application process is an element within a system which performs the information processing for a particular application. A web server process is an example of an application process.
- **Device:** A device is a physical hardware unit. A virtual private network (VPN) service unit is an example of a device. A smart card reader is also an example of a device.

Government PKI Framework

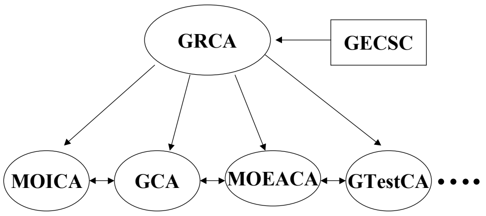


Fig 4.1 Government PKI Framework

5. Future Work

In the process of developing the e-government services, Taiwan focuses on the GPKI establishment pointed out in E-Government Program (from 2001 to 2004). In the future Taiwan will invest more resources in building GPKI. The follow sections describe what we plan to do in the near future.

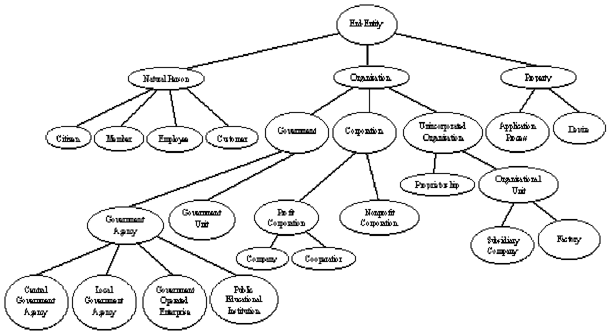


Fig 4.2 The Taxonomy of End-Entities in Taiwan

5.1 Bridging Government and Commercial PKIs

As the Government PKI evolves and develops, the business of commercial PKIs in Taiwan is growing, too. Currently, there are several companies acting as certification service providers to issue public key certificates for commercial use. There are some end-entities of which the jurisdiction is out of the Government PKI domain. Thus, the appearance of commercial PKI is a complement to a complete Taiwan PKI. It is anticipated that there will be a need for cross certification between CAs in the Government PKI and CA s in a commercial PKI. The rough draft, as shown in Fig 5.1, is to established a Bridge CA (BCA) [7] 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 Taiwan 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 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 theme of phase 3 will comprise policy management, policy approval, policy mapping, and cross certification

5.2 Cross Certification with GRCA

CAs, including principal CAs within Government PKI and any CAs without, that interoperate with GRCA through cross-certification are referred as interoperating CAs. To get approval from GRCA 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 shall issue the certificate to the applicant CA if instructed by RDEC as such. 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 shall have its self-signed certificate (verified by RDEC) delivered to the applicant CA in accordance with the procedures of GRCA's 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 receive the 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 refusing to accept the certificate. RDEC shall then authorize GRCA to revoke that certificate after verifying. No additional announcement shall be made concerning the application.

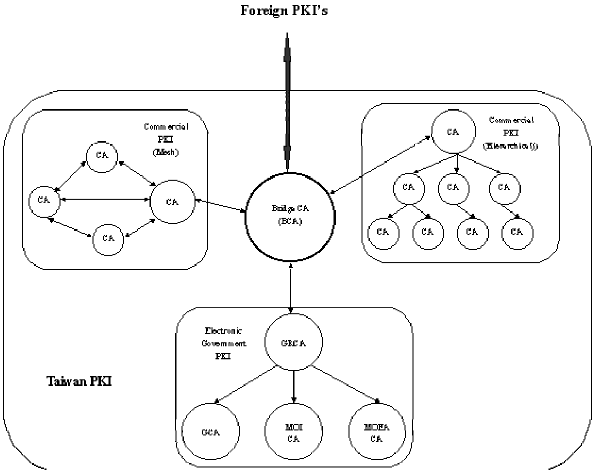


Fig 5.1 The Role of the Bridge CA in Taiwan PKI

6. Conclusions

E-government is an excellent opportunity to take advantage of the increased productivity and reduced costs that can be achieved using Internet-based technology. Even better, e- government can enhance the citizen's access to government information and services, and can provide new ways to increase citizen participation in the democratic process. Globally, it has therefore become a recognized form for providing efficient government services.

According to Electronic Government Promotion Act (from year 2001 to 2004), Taiwan is going to provide 1,500 Internet-based online services in 3 years. In order to achieve this goal, e-government electronic certification service is one of the key successful factors to success. Through electronic certification services, e-government would be able to strengthen trustworthiness of online services, and enhance online safeguards.

In conjunction with the enactment and implementation of the Digital Signature Act (enacted in Oct. 2001, put into effect in Apr. 2002), more efforts will be made to publicize and promote relevant e-government electronic certification applications. In the future, electronic certificates will be widely used between government and the general public, between government and businesses, and between different government agencies. The availability of a broad range of trusted online services will dramatically enhance the efficiency and quality of government services.

References

[1]. Executive Yuan, “Note of the Executive Yuan Council No. 2557 Meeting”, http://www.ey.gov.tw, 1997.

[2]. RDEC of the Executive Yuan, “Introductory to the Electronic/Networked Government Program”, http://www.rdec.gov.tw, 1998.

[3]. Data Communication Group of Chunghwa Telecom Co., Ltd., “Proposal for Government Service Network (GSN) of the Electronic/Networked Government Program”, http://www.rdec.gov.tw, 1998.

[4]. RDEC of the Executive Yuan, “Electronic Government Program: 2001-2004”, http://www.rdec.gov.tw, 2001.

[5]. Housley, R., Ford, W., Polk, W. and D. Solo, “Internet X.509 Public Key Infrastructure Certificate and CRL Profile”, *IETF RFC 2459*, January 1999.

[6]. Santesson, S., Polk, W., Barzin, P. and M. Nystrom, “Internet X.509 Public Key Infrastructure Qualified Certificates Profile”, *IETF RFC 3039*, January 2001.

[7]. Burr, W. E., “Public Key Infrastructure (PKI) Technical Specifications: Part A - Technical Concept of Operations”, *NIST FPKI TWG-98-59*, September 1998.