PKI Interoperability in Taiwan

Chung-Ming Ou Chun-I Fan Hwai-Ling Shan
Telecommunication Laboratories
Chunghwa Telecom Co., Ltd.
12, Lane 551, Min-Tsu Road Sec. 5
Yang-Mei, Taoyuan, Taiwan 326, R.O.C.
E-mails: {cou, chuni, shanhl}@cht.com.tw

ABSTRACT
PKI interoperability becomes a major issue in Taiwan. Several Interoperability methods, such as strict hierarchy and bridge certificate authority (BCA), have been deployed in different PKI domains. Global PKI interoperability in Taiwan is adapting BCA as a major CA-CA interoperability engine, which will bridge trust relationship between different PKI domains.

KEY WORDS
PKI, CA, Interoperability, Bridge CA

1. Introduction

The purpose of PKI interoperability is to reduce the number of certificates being issued. Today an end-entity often needs to apply new certificates in different PKI domains; unfortunately, this situation seriously hinders the PKI development. The PKI interoperability can extend the usability of certificates, which is similar to what VISA and MasterCard have achieved. Since most public key certificates can be used in different PKIs for authentication or non-repudiation, PKI interoperability can reduce the number of issued certificates for each end-user.

A certificate user means an end-entity who receives a certificate from some certificate holder. From a certificate user ‘s point of view, PKI interoperability will extend certificate trust to other PKI domains. While a certificate user receives a public key certificate and documents attached sender’s digital signature from other PKI domains, this user is facing the problem whether he should trust that certificate or not, otherwise he cannot use such certificate to verify the attached signature.

For PKI interoperability, the interoperability between certificate authorities (CA-CA interoperability) is the major issue, which faces both policy and technical challenges. PKI Forum [4] has listed 7 different CA-CA interoperability methods, which includes cross certificate, strict hierarch, Bridge certificate authority, etc. Some countries have decided to adapt Bridge CA as the nation-level Cross Certification engine. In Taiwan, the Executive Yuan’s National Information and Communication Initiative (NICI) has also made the same decision. In this paper, we describe the necessary process for PKI interoperability.

2. CA-CA interoperability in Taiwan

We introduce some CA-CA interoperability methods, which are being deployed in Taiwan now. The government and non-government have different PKI schemes. However, BCA will be a proper way to bridge these two PKI domains.

2.1. CA-CA Interoperability Methods in Taiwan

In this subsection, we introduce the interoperability technology deployed in Taiwan. They include cross certification, Bridge CA, and strict hierarchy.

- **Cross Certification:** Cross certificate is the certificate that a CA can issue to another CA. According to what ITU-T X.509 standard has stated: a CA can be the subject of a certificate issued by another CA; such certificate is called cross certificate. If every CA issue cross certificate to another CA, then it will produce complicated PKI trust relationship.
- **Bridge CA:** Bridge CA (BCA), sometimes called “hub and spoke” model. The purpose of BCA is to reduce the number of cross certification between different CAs. Each PKI domain selects its principal CA, which is connecting to BCA. Therefore two different PKI can bridge together via principal CAs and BCA. The advantage is each PKI domain still follows their trust path. Bridge CA also adapt cross-certification as the basis for CA-CA interoperability. Every CA will receive a cross certificate issued by BCA once it become a member of BCA. The

bridging procedure is the result of Certificate Policy mapping between PKI domains.

- **Strict Hierarchy:** This PKI domain has the root CA, which plays the major role for the trust relationship. Relying party will not trust any subordinate CA, only when a certificate path can be traced to the root CA ◦ Each subordinate CA has a unique superior CA; a subordinate CA does not allow having its self-signed certificate. Only this root CA can issue self-signed certificates.

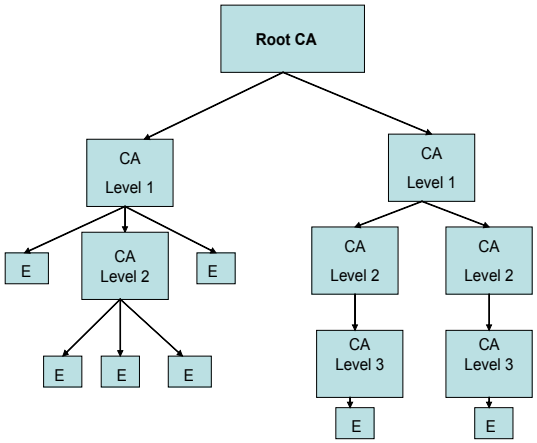

Fig.1. Strict Hierarchy

2.2. Government PKI Interoperability

Taiwan Government PKI (GPKI) is adapting the strict hierarchy scheme, the root CA (GRCA) will be the highest- level CA. Basically the interoperability of GPKI with other PKI (including foreign PKI) is in charge by GRCA. GRCA can interoperate with Taiwan BCA if necessary. GRCA supposed to operate in this year (2002).

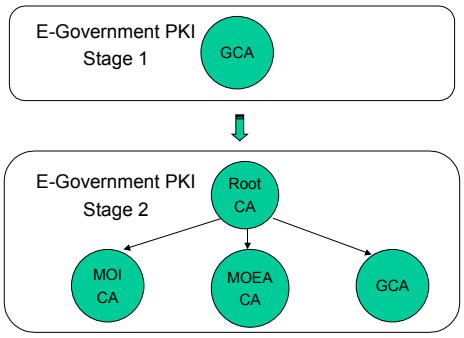

Fig.2. Evolution of Taiwan Government PKI (with GRCA as its root CA)

2.3. The Interoperability for Non-Government PKIs

Ministry of Economic Affair (MOEA), which is the official sector in charge of PKI, has decided to deploy Taiwan BCA in near future as the major PKI interoperability platform. This BCA will only issue cross certificate to the CA becoming its member; BCA will not issue any certificates to end-users. Taiwan BCA won't play the trust point for any PKI in order to respect the autonomy for each PKI.
Taiwan BCA major goal is to provide peer-to-peer trust relationship with different PKI domains and hence reduce the complexity due to the mutual cross certification by each PKI. Since there are distributive PKIs throughout different domains, such as government, finance and healthcare systems, BCA is regards as a proper solution for Taiwan PKI interoperability, see Fig.3. Furthermore, many foreign countries have been either deploy or being planned for BCA interoperability, for example, US federal government is conducting Federal BCA (FBCA) testing plan, which is in the second phase now. Japan, Germany, Mainland China and Canada are also planning using as future BCA international interoperability.

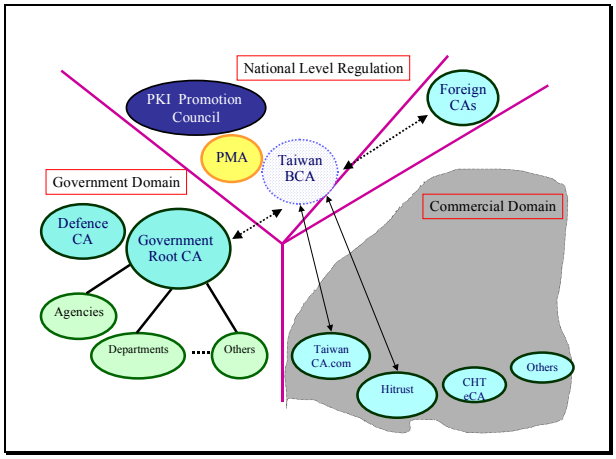

Fig.3. BCA in Taiwan and its functionality

2.4. Global PKI Interoperability in Taiwan

Global PKI interoperability in Taiwan means we are considering all PKI domains in Taiwan, and the interoperability issues with foreign CAs. From 2.2 and 2.3, we realize that government Root CA and Taiwan BCA will play the central role, in particular Taiwan BCA; which can be a bridge of different PKIs.

Due to different organizational policies between cooperation and government, the key for global PKI interoperability is to keep original certificate path within each PKI domain. For example, GRCA is the trust source for GPKI. We think it is a better approach as such BCA establishes a peer-to-peer relationship and it is not superior to RGCA or

principal CA in each PKI domain. BCA will not influence any certificate path of each PKI domain. Those CAs don't need to connect to Taiwan BCA unless they need to interoperate with other CAs in different PKI domain.

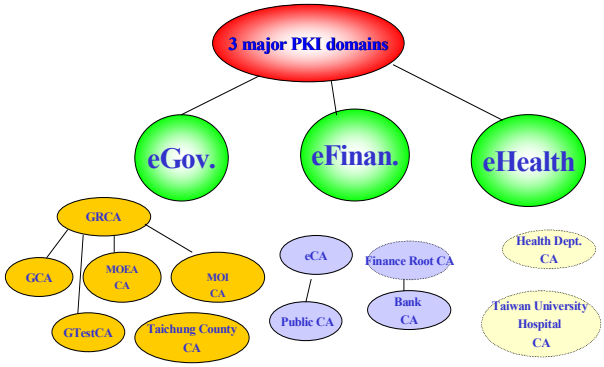

Fig.4. Three major PKI Domains in Taiwan

Both from policy and technology point of view, the following 4 issues arise while considering adapting BCA as Global Taiwan PKI Interoperability.

- **Establish the Policy Management Authority (PMA):** PMA provides the operational guideline for BCA. PMA members may be elected from PKI Promotion Committee, which includes experts from industry, government and academy. PMA members may include those CAs which have joined the BCA. The responsibility of BCA includes:
  - **Verify BCA Certificate Policy**
  - **Audit CA Assurance Level**
  - **Performing Policy Mapping**
  - **Technical consultancy**
  - **Information exchange format for this BCA and other BCA**
  - **Certificate usage for BCA member**
  - **Maintenance and update for BCA member List**
- **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). Furthermore, the assurance level of this CA's certificate has to be determined via BCA CP. Therefore, following this procedure, every CA has establish the assurance level by BCA, that is, trust relationship between CA 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 major issue. According to the NIST FBCA Test for interoperability, technical details can be categorized into different areas.
  - **The Cryptographic algorithms specification, such as symmetric and public key algorithm**
  - **Certificate formats**
  - **Certificate extension fields and interoperability**
  - **CA Directory access**
  - **Certificate Path Validation**
- **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 Certificate Practice Statement (CPS). According to the international routine for CA auditing, the auditing execution can be achieved by both paper works and via third parties. The international standard includes
  - **ABA PAG v0.30 [1]**
  - **CICA/AICPA WebTrust Program for Certification Authorities [2]**
  - **ANSI X9.79 [3]**
  - **BSI BS7799**
  - **IETF RFC 2527**
  - **NIST FIPS 140-2**

  Our suggestion is that a better auditing system for information system may refer to the auditing scheme from US, Canada and Australia. On the other hand, we may also adapt the existing Badge Issuing and Management System in Taiwan, such as medicine GMP and food CAS. Therefore, such CA auditing system can meet both domestic and international requirements.

3. Conclusion

We have concluded that BCA is not only a feasible but also a practical solution for Global PKI Interoperability in Taiwan. There are challenges for BCA from both policies and technology sides. Our survey is that they can be solved via systematic ways and testing procedures. US FBCA is a good example. On the other hand, security auditing system will provide CA the security auditing to

make sure that security service provided by CA is consistent of its assurance level. This is a key issue whether a CA can be a decent Internet service which gains the general public confidence. If the answer is positive, with the successful implementation of BCA interoperability, which improves the usage of certificate, PKI will be a major Internet security tool.

References

[1]. ABA, ”PKI Assessment Guidelines,” Jun. 2001.

[2]. AICPA/CICA, ”WebTrust Program for Certificate Authorities,” Aug. 2000.

[3].ANSI X9.79-1: 2001,”Part 1: PKI Practices and Policy Framework,” Jan. 2001.

[4].CA-CA Interoperability, white paper, March 2001, PKI Forum.

[5]. X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), June 14, 2001