



Global Business Dialogue on Electronic Commerce

## **Cyber Security** MRA Issue, Digital Signature & Cross Certification

**September 14, 2001**

Issue Chair	<i>Dr. Taher Elgamal</i> President & CEO Securify
Contact Point (Europe/Africa)	<i>Stefan Röver</i> CEO Brokat Technologies
Contact Point (Asia/Oceania)	<i>Dr. Shigehiko Suzuki</i> Senior Vice President & Member of the Board NTT Corporation

### **INTRODUCTION**

It is one of the most important issues of cyber security combating all kinds of threats and crimes in cyber space to protect end user confidence of electronic commerce. Legal frameworks related to digital signatures and corresponding certificate infrastructures, including certificate management, are already in place or being developed in many countries. The GBDe recognizes that such certificate infrastructures should be established and be available to all people and all nations in order to protect the security of electronic commerce globally. The generic security of networks and information systems can be considered to consist of authentication, non-repudiation, integrity, and confidentiality, all of which can be realized through certificate infrastructures.

There have many international discussions and recommendations on certification issues in the context of cyber-security. In the GBDe, the Authentication and Security Working Group has published a recommendation at the Paris Conference in 1999, and the Cyber Security Working Group has given recommendations at the Miami Conference in 2000. This paper builds upon these recommendations and covers specifically the topic of mutual recognition of certification authorities (CAs), the actors establishing certification policies.

Accompanied with innovation of information technology, many governments have enacted and enforced Digital Signature and Digital Certification Acts in order to make certification services available for many users, and to establish a framework of legal recognition of digital signatures. Certification services, for which public

key infrastructure (PKI) technology is used in many cases, are provided in two styles:

- Provided by governments: A public entity, sometimes a government itself, provides Certification Services as one of its administrative services, for example for tax payments and patent applications. It constitutes one of the major elements of e-Government. Examples are the United States' Federal PKI, and the Japanese Government PKI.
- Provided by business entities: A business entity provides Certification Services in accordance with certification policies that depend on the context of usage. The policy might differ between the Certification Service Providers (CSPs)<sup>3</sup> depending on types of industry and the context of the applications.

As electronic commerce develops rapidly, many kinds of CSPs have been established. Such a variety of CSPs means that consumers, end users of Certification Services, might have to deal with too many kinds of Certificates, which can bring operational difficulties into the market. The GBDe considers that there is a potential threat to hamper e-commerce if companies and consumers have to face too many certificates.

To prevent this inconvenience for consumers, CSPs can mutually recognize other CAs through Mutual Recognition Agreements. CSPs can implement Mutual Recognition by establishing Cross Certification with each other. Alternatively, it is also possible to declare the Root Certificate of another domain as "trusted" without issuing an actual certificate.

Such Mutual Recognitions and Cross Certifications are put into practice both globally and domestically.

- Between governments
- Government with business entities
- Between business entities

---

<sup>3</sup> There exist different kinds of actors as CSP, for example, Certification Authority, Registration Authority, and Certification Operator.

## RECOMMENDATIONS

Mutual recognition and cross certification enables consumers to enjoy the benefit of certification services without using too many certificates. Therefore, the GBDe recommends that CSPs mutually recognize CAs through Mutual Recognition Agreements (MRAs) wherever their policies permit.

### 1. Models of Cross Certification

The GBDe understands that there exist two major models of Cross Certification. Though there would exist many definitions for cross certification<sup>4</sup>, we define "cross certification" as just "reciprocal certification process of two CAs."<sup>5</sup>

- a. CSPs recognize another CA by mutually issuing Cross Certificates. Providers confirm that each security policy has a similar level of security.
- b. CSPs submit to a common Trusted Third Party acting as root CA, and they authenticate each other through such TTP. Alternatively, CAs may cross-certify each with a trusted Bridge CA or any other similar system. In contrast to the hierarchical model described above, a Bridge CA does not have any authority over the policies and operations of the participating CAs.

---

<sup>4</sup> This recommendation is drafted basically in accordance with "Cross Certification Guidelines (alpha version)" by Electronic Commerce promotion Council of Japan (ECOM) in June 1998. [http://www.ecom.or.jp/ecom\\_e/report/full/ccg.pdf](http://www.ecom.or.jp/ecom_e/report/full/ccg.pdf). On the other hand, in March 2001, PKI Forum has released a White Paper titled, "CA-CA Interoperability", which suggests seven styles of CA-CA interoperability; cross certification, bridge CA, cross-recognition, certificate trust lists, accreditation certificate, strict hierarchy, and delegated path discovery and validation. [http://www.pkiforum.org/pdfs/ca-ca\\_interop.pdf](http://www.pkiforum.org/pdfs/ca-ca_interop.pdf)

<sup>5</sup> "Cross Certification Guideline (alpha version)", ECOM, June 1998.

The GBDe recognizes that many business associations and governmental organizations have started discussions and trials for the implementation of cross certification, domestically and internationally, and that each model of MRA would be effective as far as it would bring the development of electronic commerce and the global user convenience.

Each CSP has its own certificate policy, which shows level of security provided by the CSP. The certificate policy is defined as a set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.<sup>6</sup> In executing MRA, CSPs should agree through private agreements not only a format of each certificate but also on similar certificate policies. If cross certification would lower the level of security, CSPs should limit, even reject, such a Cross Certification. As written above, the scope of MRA should be related to certificate policy and it would be necessary to establish an appropriate agreements as to risk-management practices and business terms and conditions between cross certification organizations.

Not only operational issues but also technical ones should be considered. Especially technical interoperability is necessary to make cross certification work. So the GBDe recommends that governments and industries should cooperate with each other to promote standardized solutions to achieve interoperability in terms of cross certification and to realize technological interoperability between PKI-based applications, for example secure e-mail.

Another standard issue is related to the ITU standard X.509 v3. First of all, while it gives the flexibility to support a wide variety of different extensions, it may be necessary to define a set of common policies if users registered under different

---

<sup>6</sup> Information Technology – Open System Interconnection – The Directory: Authentication Framework, Joint Recommendation | Standard ITU-T X.509 and ISO/IEC 9594-8, 2000.

CAs are to successfully communicate with each other. Secondly, efficient validation of the certification chain should be clearly identified.

### **1-a. Mesh Model**

For executing MRA, CSPs should confirm the similarity of both technical and operational policies of each other's certificates, for example, certificate formats, certificate validity, renewal and revocation of certificates, responsibilities of authorities. The GBDe recommends that CSPs should publish such cross-certification policies to end-users. Especially the level of trust is crucial for its subscribing end-users so that it should be stated clearly and publicly.

### **1-b. Centralized Model**

Bridge CAs are regarded in many cases as the simplest way to achieve MRA in a group of CAs. A bridge-CA architecture has a much lower complexity than a model where each pair of CAs enters a separate MRA, while not requiring the CAs to submit to a common root CA. Bridge CAs have to carefully check the policies and technical interoperability of the participating PKIs, such that all parties can be certain that only similar policies are mapped onto each other, and that the system remains interoperable.

## **2. Liability of Certification Authority – legal issue**

In PKIs with cross certification, end-users can experience damages and losses by unauthorized use of certificates and leak of private data because of unauthorized access and decryption. The GBDe recommends that CSPs should clarify the liability issues when entering into cross certification. If this issue is discussed internationally, the legal systems of each region, for example, license systems of CAs, Digital Signature Acts, regulations of encryption, and customs of commercial transaction should be considered. On the other hand, private commercial agreements between the parties should be allowed to define the liability of each one of them in case of a damage or loss by the end user.

### **3. No legal barriers to MRA**

Large-scale, international MRAs are a complex issue, the details of which are not yet entirely clarified. While Digital Signature Acts should be open to the recognition of foreign signatures, legislators should closely observe the ongoing cross certification projects and consult with the participants before details of mutual legal recognition are being defined. In order to simplify such mutual legal recognition, the GBDe recommends not defining national schemes that are likely to be not interoperable with international PKIs and recommends that a CSP accredited in one country should be able to cross-recognize a CSP of another country without administrative constraint.

### **4. Government Regulation**

The GBDe recommends to the Government Regulators to eliminate constraints in the deployment of PKI based solutions by clarifying the regulatory and legal framework<sup>7</sup>.

### **5. User Education**

When signing documents or relying on electronic signatures, users should have guidance on what to observe in order to get secure results. Especially with respect to an underlying combination of different PKIs, users should understand whom they trust and be able to make educated decisions. To achieve this goal, the GBDe recommends that providers of PKI services should provide users with easily understandable information about the trust relationships and the secure handling of the relevant functions.

---

<sup>7</sup> For example,

1. Impulse the adoption of global standards in order to allow the cross certification among the different Certification Authorities.

2. Promote the deployment of PKI based solutions by providing the appropriate legal structure and coverage framework in the transactions performed with digital certificates.

### **6. Public/private cooperation and future developments**

PKIs emerge both in the public and the private area. For truly global and cross-sector interoperability of PKIs, and as an important ingredient to e-government, the GBDe recommends that governments and industries should cooperate in mutual recognition of certification services, especially by promoting cross certification between government CAs and business CAs.

Market development will not be possible without strong cooperation between governmental and private initiatives. As customer relationships and legal/financial liability are key in electronic signature and related PKI processes, the GBDe considers a few key actors like banks, insurances and operators (fix, mobile, cable/satellite TV) will play a significant role and encourages international discussions between them and governments through dedicated fora mirrored at national level. In particular cross certification should be studied at projects' start or first implementations (e-government, banking, m-commerce,) and should consider any type of terminal (PC, mobile phones and TV sets).