

# 5

## **PKI Solutions for Trusted E-Commerce: Survey upon the De Facto Standard Competition in PKI Industries**

*Atsuhō Maeda*

### **1. INTRODUCTION**

In this section, we focus on a new field of technology called 'Electronic Certification,' which is expected to be an effective tool for ensuring the safety of commercial transactions (including international trade) in the midst of the increase in e-commerce on the open networks through the Internet. We will discuss the activities of the new enterprises related to the de facto standard at the industry level, and analyze their strategies for making inroads into Asian markets and their impact.

We have been shifting our transaction basis from a norm of 'Face-to-face commercial transactions,' which involved only the trusted participants, into a business (including trade) format of 'Open electronic commerce (EC)' conducted via the Internet. The question of how to ensure the mutual trust between those involved in the transaction has become an important issue. Along with the growth of the Internet as the basis of business affairs, 'the positive impact' is that conventional business practices of exclusive associations have been shaken off, and business opportunities have expanded. On the other hand, 'the negative impact' is that it

is also necessary to be aware of the unlimited increase in the danger of illegal access to the data for transactions conducted on the Internet, including 'Wiretapping,' 'Tampering' and 'Impersonation.' Transactions that are made on an open network are between multiple, unspecified users (individuals, corporations, government agencies), unlike the dealings within a business hierarchy upon guaranteed mutual trust. For these open network transactions, the issue of the reliability of the other party is an extremely difficult one to find the best solutions for.

The mutual trust system for business transactions is divided into the following 2 areas;

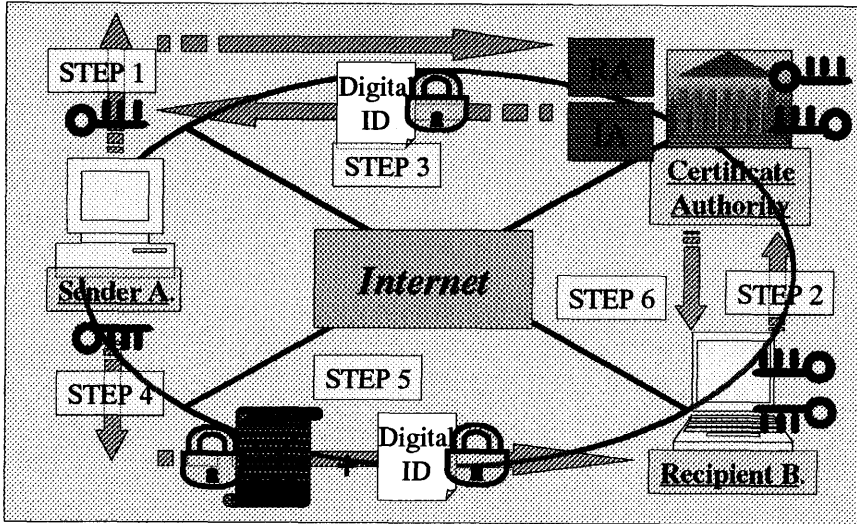
- (i) Credit Rating (evaluation of the quality as a business partner and its solvency).
- (ii) Authentication (verification that the communicating party is actually who they claim to be, as well as the integrity of the transferred contents).





The first of these, (i) Credit Rating, has been commonly used by businesses and financial institutions, and is the important point that requires the most attention for a commercial transaction. It will remain difficult to handle electronically, even in the future. For item (ii) Authentication, as there has been a shift to the Internet as the basis for commerce, this has been an emerging issue, particularly since the latter half of the 1990s. There continues to be lively development by the rising system solution enterprises aiming to offer a trusted communication technology platform. Some of the systems established so far are a Digital Signature (verification using an appended digital ID) as a means of verifying the true identity of another party, and a Certificate Authority (CA) to verify registration of the communication partner. These are both based on technologies of encrypted data transfer by the Public Key method. For this, these are generally called PKI (Public Key Infrastructure), as the following Figure shows.

The purpose of this section is to clarify the characteristics of the de facto standard strategies of the main vendors associated with PKI (hereafter, called PKI vendors). Hence, with regard to the Credit Rating, it will not be discussed here.

The PKI forming the basis for (i) Authentication originally developed from technology that was used by the military. In order to ensure the security of top-secret and highly-sensitive information, state-of-the-art element techniques were adopted. Among these, encryption technology has been known since the period of the ancient Roman Empire as an

Figure 5.1: Image of Public Key Infrastructure



 : Public Key for Sender A.  : Public Key for Recipient B.  
 : Private Key for Sender A.  : Private Key for Recipient B.

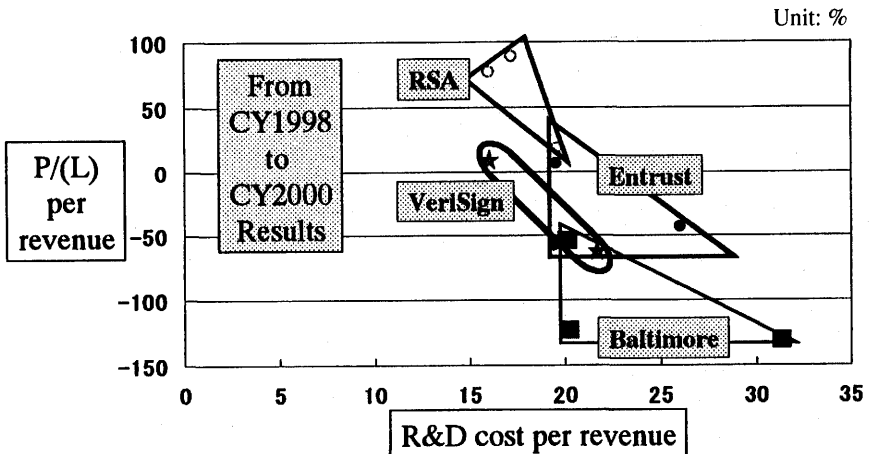
effective and convenient tool. Since the late 1980s, international society has been facing the rapid demise of the Cold War structure. The increasing military competition between superpowers based on nuclear weapons has abated. As a result, the security menace has shifted from being certain nations that possessed special weapons to being anonymous individuals with an excellent understanding of advanced Internet technology. In a sense, nowadays, the authentication infrastructure has the same significance as the national security systems during the Cold War.

However, it is not necessarily required to prevent society from using the electronic certification systems based on strong encryption technology. Society's awareness of issues such as (1) Expansion of the use of the Internet, (2) Spread of e-commerce (B2B, B2C, etc.), (3) Legal framework to deal with the digitalization of business transactions, and (4) Security problems related to e-commerce has progressed rapidly. As a result, as the 20th century draws to a close, the following major changes have begun in the environment surrounding encryption technology.

- Relaxation of encryption technology export control regulations by US Dept. of Commerce (January, 2000): The DOC announced that, in accordance with President Clinton's policy on regulation relaxation, the export of any cryptographic commodity to an individual or commercial enterprise outside the US would be allowed without a government approval, except for some special cases.
- Expiration of the RSA method encryption technology patent (basic PKI patent) (September, 2000): The exclusive right of use within US held by RSA Security Inc. for 17 years regarding the patent on the RSA method of public key encryption expired on 20th September, 2000, and the algorithm entered into the public domain.

As this shows, 'the year 2000' was a significant turning point for the commercial application of encryption technology, particularly in the US, with rapid progress in openness and liberalization. It is impossible to measure the significance of relaxation of the technological entry barriers and the expansion of the possibility of international deployment of authentication technology (cf: huge R&D cost in PKI industry, irrespective of profit level, in the following Figure). Especially significant is the lapsing of the RSA patent, which will eliminate the licensing fees that PKI vendors have been required to pay in order to use the PKI basic patent (encryption technology). Reduction in licensing fees → Drop in PKI-related costs → Increase in the number of PKI users. In line with the

**Figure 5.2: Profit/Loss, R&D per Revenue of Major PKI**



Source: US SEC.

economic effect of network externalities, it is expected that there will be global expansion of PKI.

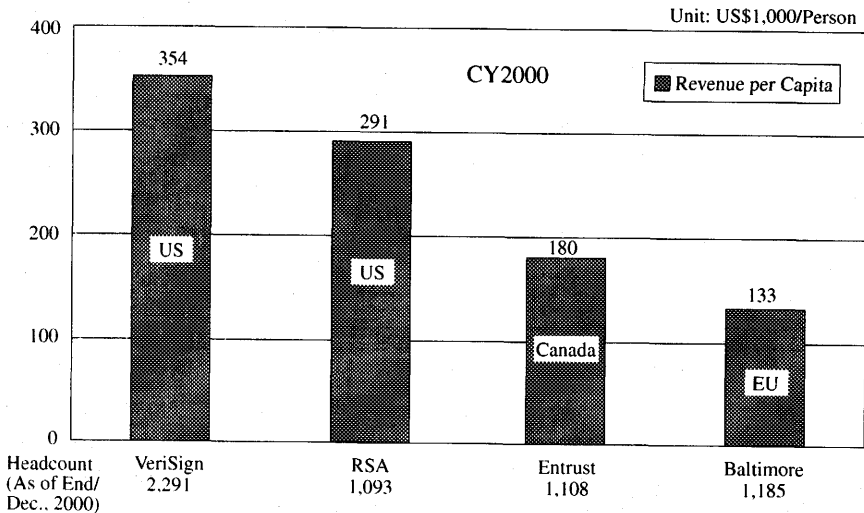
On the other hand, from the perspective of PKI business, in response to PKI market expansion, various kit products will be offered, and product differentiation will progress (for example, development of products for mobile communications, etc.). As a result intense competition among businesses to become the de facto standard in the system solution field has begun. The analysis described below primarily focuses on the main PKI vendors.

## 2. ANALYSIS OF MAJOR PKI VENDORS

At present, the major enterprises known throughout the world, and expected to develop internationally in the field of electronic authentication (including Certificate Authority supporting systems) are;

- A. RSA Security Inc. (US); the licensor of the RSA patent described above,
- B. VeriSign Inc. (US); the largest company, spun off from RSA,
- C. Entrust Inc. (Canada); an off-shoot of Nortel Networks Ltd.,
- D. Baltimore Technologies plc. (Ireland); EU standard.

**Figure 5.3: Revenue per Capita by Major PKI Vendor**



Source: US SEC.

Each of these companies has their own strategy. However, what is common is that they all have strategies for government, industry and business, pursuing aggressive sales with the aim of establishing the de facto standard. 'The division of the world' in PKI business has begun by these 4 players. A., B. and C. are struggling for supremacy in North America, while D. commands the largest share of the European market. The question of Asia will be discussed in detail in a later section. This section deals with the specifics of the strategies to become the de facto standard by studying the global strategies of each of these companies.

### **A. RSA Security Inc.**

#### ● *Corporate Strategy*

The strategic theme for the company is 'Shaking off from its patent dependency and establishment of supremacy through its technical advances other than patent.'

Since September of 1983, when the patent for 'Public Key Encryption and Decoding Algorithm'<sup>1</sup> was granted, the company has taken advantage of its patent, which continues to be the effective standard in the huge US market. Most of the rival PKI vendors sold PKI systems that use the RSA method, and a portion of their profits have been paid as licensing fees to RSA. RSA has aggressively defended these patent rights, including suits claiming patent infringement.

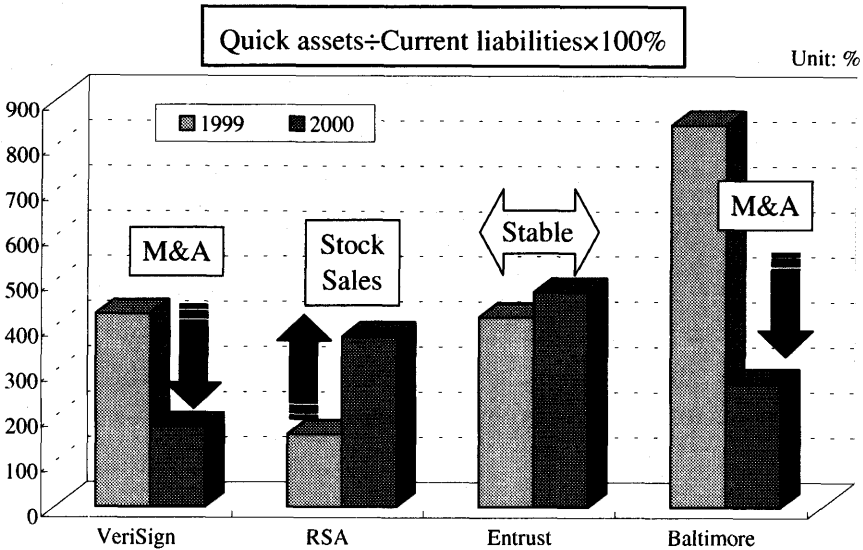
However, as explained in an earlier section, this patent lapsed on 20th September, 2000, hence the situation has changed. During the time that the patent was in effect, PKI peripheral technology, such as access authorization systems etc., that the company established, was predominant. In order to continue this dominance, these products and PKI products are being integrated as a market expansion strategy.

#### ● *Business Model*

Unlike other companies, the certification system is not set according to a specific business model; instead, RSA emphasizes the interoperability with systems from other PKI vendors. The global standards Secur ID<sup>TM</sup> (a two-factor access authorization system, with an 80 percent share in the US market) and BSAFE<sup>TM</sup> (an encryption generation tool kit, 800 million licenses sold worldwide as of the end of 2000), and the highly-compatible certificate authority supporting system KEON<sup>TM</sup> were developed for corporations performing their own PKI structure, and sales expanded rapidly (Worldwide 1999: US\$5M. → 2000: US\$20M.). However, they do not issue certificates as a certificate authority.

The sales operation of RSA is based on direct sales. Particularly for developing new markets outside the US, there is a great deal of importance on the sales channels, like resellers and distributors, and they are more cautious than other companies about establishing branch offices. For this reason, entry to the market outside the US has been delayed.

**Figure 5.4: Quick Ratio Comparison by Major PKI Vendor**



Source: US SEC.

**B. VeriSign Inc.**

● *Corporate Strategy*

The objective of this company, as stated by the company President & CEO, Stratton Sclavos, is “From a security services company into the Internet’s most trusted utility.” In keeping with this, company strategies are to establish a solid business foundation as a pillar of the US and to embrace customers and powerful industries through M&A, as a result, VeriSign’s Quick Ratio<sup>2</sup> shows its weakened financial balance as above.

Customers include public agencies like the US Internal Revenue Service (IRS) as well as major businesses like Bank of America, Hewlett-Packard, Kodak, and Texas Instruments. It is known as the ‘World’s largest electronic certificate (digital ID) issuing organization,’

with more than 500,000 (total as of March 2001) electronic certificates for 'Websites' issued. The company is succeeding in getting a network of multinational businesses based in the US using its company's certification networks.

VeriSign's strong domain is that it also supports companies in issuing electronic certificates on their own. Customers are not required to build the difficult-to-manage certificate authority infrastructure; they are able to completely outsource all the work prior to the actual issue of electronic certificate, to VeriSign.

● *Business Model*

This company's PKI product is a certificate authority supporting system called VeriSign OnSite™. The features, as mentioned above, are the high-level certificate processing functions that allow total outsourcing to meet the customer requirements. It has passed the system audit by the American Institute of Certified Public Accountants (AICPA), known for strict on-site audits, and VeriSign also issues electronic certificates as a certificate authority.

With regard to the composition of the authentication systems, this company has adopted its own unique strategy. A worldwide certification service network, called VTN (VeriSign Trust Network) has been established, and the company is succeeding in promoting the VeriSign brand as a certificate authority through associated companies and affiliates throughout the world. In other words, the strategy is to build systems connecting global sales networks based on the certificate structure, centered at the US headquarters. Structurally, it is a 'hierarchical authentication structure,' but a defining difference is that the highest level in the authentication hierarchy is not a public root CA (that is, an authority that is recognized by a public sector, etc.), but a private business, i.e. VeriSign. The advantage is that it is possible to expand the communication network to any entity or individual in the world, based on the assumption of 'trust in the closed community of VTN.' As a result, the company's clients include government agencies with strict security requirements, including the FBI (Federal Bureau of Investigation) and IRS (Internal Revenue Service), as well as the NRC (Nuclear Regulatory Commission). One of the problems that can be pointed out is the risk of all authentication functions being in the private sector. There is likely to be particular resistance to this among users outside the US, since the highest authority in the system is in a US company. It is not possible to get away from this trade-off in this case. In this regard, there is a great deal



of attention being paid to public safety assurance, and VeriSign obtained a certification of qualification of Common Criteria EAL4 (Evaluation Assurance Level 4) in December 1999, recognized as an international standard of the ISO (International Organization for Standardization) (ISO/IEC 15408).

The sales system of VeriSign is primarily Website transactions bolstered by its strong brand identity. As mentioned earlier, in the overseas markets its subsidiaries are the private sales network called VTN.

### ***C. Entrust Inc.***

#### **● *Corporate Strategy***

Started as the electronic certification business department of Nortel Networks Inc., the Canadian communication equipment manufacturer (as of the end of December 2000, Nortel holds 26 percent of the Entrust shares). This company's strategy is to build an authentication network focused on large clients in North America, and to enhance the direct sales system aimed at powerful customers. Among its strategic customers, in addition to the Ontario provincial government and the Canadian federal government, are many relatively large government agencies and companies, such as the US Department of Defense, NASA, NSA (National Security Agency), SWIFT (Society for Worldwide Interbank Financial Telecommunication S.C.), J.P. Morgan Chase & Co. and Canon. This company has increased clients on the basis of certificate compatibility with major certification systems for specific government and industry users. There is a striking tendency to form blocks of the same type of customers, such as the federal government and securities industry. In July 2001, the company successfully closed a deal for the largest order since its founding (value US\$18 million) for 'the Secure Channel Project (part of a digital government plan being conducted by the Canadian government).'

Since May 1999, Entrust began operating an electronic certificate issuing business with the platform 'Entrust. net.' However, the operation is fundamentally different from the outsourced certificate authority offered by VeriSign. Entrust.net assumes the function of the certificate authority is operated by the enterprise itself (in-house). As a result, Entrust's customers are mainly large enterprises that are capable of operating as a certificate authority on their own.

#### **● *Business Model***

The company's main PKI product is the certificate authority supporting

system Entrust/PKI™. As mentioned above, the presumed customers are enterprises running their own certificate authority, and this defines the business model. In other words, it inevitably adopts an operation style that is adapted to big business, since its customers are large enterprises who can run a certificate authority themselves within their own organization. For example, compatible certification is built into the authentication system for each client enterprise, forming an enormous certificate network. There is an assumption of a distributed certification system that has a 'cross-certification structure.' The remarkable differences from B. VeriSign is that the network is expanded on the basis of the certification systems of the client enterprises, not by absorbing the customers into the company's own network. In order to implement this original business model, Entrust has a strong tendency to enhance the direct sales system focusing on large institutional customers.

#### ***D. Baltimore Technologies plc.***

##### **● *Corporate Strategy***

This company is headquartered in the EU. As clearly seen from the shipments in 1999 (80 percent to European countries), its primary markets are the EU, including Great Britain and Ireland. The main customers include the EU government, the British Ministry of Defense, and Deutsche Telecom. However, since keen international competition has started in the electronic certificate market, it has become necessary to develop bases of operation abroad, as the following Figure indicates. To accomplish this, the company began a thorough M&A strategy in 2000, moving into markets outside of Europe, such as the US, Canada and Japan. The company's acquisition of Security Domain Pty. Ltd. in March 1998 marked the start of its entry into Australia. Later, it began accessing markets in areas with different cultural backgrounds, like the US and Asia. Excluding Japan and Korea, it has conducted business through wholly-owned subsidiary companies.

Furthermore, the company has become a major PKI vendor, forming a global network and establishing a cooperative relationship with Identrus LLC, which performs Root CA for financial institutions. Identrus is affiliated with 47 financial institutions worldwide (as of July 2001), including ABN AMRO Bank, N.V., ING Group, Citi Group, and the HSBC Group.

This company has been designated the SET certificate authority by VISA and MasterCard International, starting with Asia and the Pacific

region. It is characteristic of the company to focus on certificates for the financial sector.

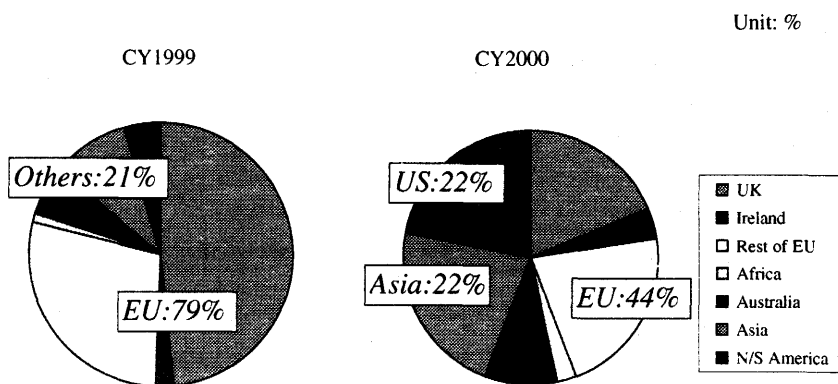
● *Business Model*

First, this company's product strategy is to provide certificate authority supporting systems as well as certificate authority hosting services. It does not conduct any electronic certificate issuing business (except in Australia).

From the perspective of certificate system structure, this company adopts a hierarchical structure. This means the Root CA (supreme level certificate authority) is at the top of a pyramid format authentication system. The upper level CA issues the electronic certificates to the lower-level CA. The Root CA is typically established for each field of industry, ensuring industry-wide PKI. Naturally, if the secret key of the Root CA is compromised, the entire PKI as a whole collapses, so there is an extremely high demand for security.

Specifically, Identrus (this company's main customer) is a typical Root CA, issuing electronic certificates for financial institutions. Identrus has introduced the Baltimore Technologies CA supporting system, and issues an electronic certificate meeting global shared specifications for the member financial institutions. For the businesses with which these financial institutions have dealings, electronic certificates with the Identrus electronic signature (digital ID) form an impressive credit guarantee system for e-commerce, including accounts settlement. Identrus is

**Figure 5.5: Consolidated Revenue by Region of Baltimore**



Source: US SEC.

not merely in the certificate business, it is a comprehensive credit rating business too.

In the past, direct sales were the main format of the operations, but there is a tendency to focus on indirect sales through its partners for advancing into markets.

### **3. STRATEGY FOR ASIAN MARKET**

In this section, we will review how these PKI vendors enter into the Asian PKI market, especially, from the strategic point of view by country.

#### **3.1. Republic of Singapore**

##### ***B. VeriSign Inc.***

In the past, VeriSign supported the Singapore market from MSC Trustgate.com (Malaysian related company). In response to the expansion of the electronic certificate market, in August 2001 a strategic alliance, including capital investment (less than 50 percent), was started with a private Singapore certificate authority, TrustAsia Inc. (established : April 2001). The company also received investment funding from the US, Singapore, and Japan (Nippon Venture Capital Corp.), and the range of operations is expanding through ASEAN and into China. For this reason, the center of operations for Southern Asia is in Singapore, and a base for Northern Asia operations is being established in Shanghai, China.

Unlike the VTN member companies so far, TrustAsia has its own R&D facilities (encryption technology research in Shanghai). In addition, there is a unique business strategy, such as moving into regions where there are already VTN affiliated companies, like Malaysia and China.

##### ***D. Baltimore Technologies plc.***

This company concluded a procurement agreement for its PKI supporting system (UniCERT) with ID.Safe in December 1999. ID.Safe has been the official electronic certificate provider for the e-ASEAN working group since November 2000, using Baltimore's technology.

It also has a business tie-in with Singapore Network Services (SNS) Pte. Ltd., a trading system enterprise in Singapore. Since January 1989,

it has also been performing certificate services for TradeNet, a trading system that is being constructed.

### **3.2. Malaysia**

The first licensed certificate authority in Malaysia was DIGICERT Sdn. Bhd. In 1998, POS Malaysia Bhd. was established with funding from MIMOS Berhad, a government science and technology research organization, and the network business GITN Sdn. Bhd. iD2 Technologies (Swedish company, funded by CISCO, Ericsson Reuters, etc.) is a PKI vendor for DIGICERT.

After DIGICERT, the second licensed certificate authority MSC Cybersign International Sdn. Bhd. (renamed MSC Trustgate.com Sdn. Bhd.) was established as an agency of the Multimedia Development Corporation (MDC) which holds an 80 percent share. In June 2000, MSC Trustgate.com concluded a strategic alliance (including capitalization) with VeriSign and the Malaysian communications business, Lityan Holdings Berhad. In July 2000, it was licensed as a certificate authority by the CCA (Controller of CA). MSC Trustgate.com participated in the e-ASEAN Task Force conference held in Kuala Lumpur in August 2000, advocating the establishment of an international electronic certificate system making use of the ASEAN framework (integration of cross-certification and the legal framework) and the establishment of a 'Central e-ASEAN Certificate Authority.'

### **3.3. Hong Kong Special Administrative Region**

#### ***B. VeriSign Inc.***

In order to conform to the system of regulations and launch an aggressive offense on the rapidly growing Hong Kong market, VeriSign established HiTRUST.COM (HK), a Hong Kong subsidiary of HiTRUST.COM Inc. (Taiwanese company) as part of the VTN (December 2000). At that time, in addition to Hong Kong, major cities in China were added to the area of operation for HiTRUST.COM (HK), including Hebei, Jiangsu, Guangdong, Beijing, Shanghai, and Guangzhou.

#### ***D. Baltimore Technologies plc.***

In October 1999, this company established a base of operations into the Asian market in Hong Kong, opening a branch office. It was the first

large PKI vendor to move into Hong Kong. In the Asian market, this company is a strong PKI builder for the trading sector, successfully marketing to the trading and financial EDI system operations groups in various Asian countries, including Hong Kong's Tradelink, SNS in Singapore, and Trade-Van in Taiwan. The business organizations headed by these system operation entities conform to this company's PKI system concept of a hierarchical structure. Since January 1997, Tradelink has been issuing electronic certificates for trading-related businesses as a voluntary certificate authority.

Baltimore announced a business alliance with Hong Kong Post in January 2001. The purpose of the alliance is to offer this company's WTLS (Wireless Transport Layer Security) technology. As a result, the Hong Kong Post has decided to adopt Baltimore as the electronic certificate system for mobile communications devices, allowing Baltimore's product to become the de facto standard in Hong Kong.

### **3.4. Japan**

#### **A. RSA Security Inc.**

In November 1996, a wholly-owned subsidiary (Japan RSA Ltd. K.K.) was established. In May 1998, Security Dynamics Ltd. K.K. was established as a wholly-owned subsidiary of Security Dynamics Technologies, Inc. In November 1999, these two subsidiaries merged to form the current RSA Security Japan Ltd. In order to strengthen its operations organization in Japan, an agreement was reached with Fujitsu in August 1999 to form a sales alliance.

The company is well-known for the interoperability of its systems with the systems of other vendors, and it is expected to participate in Japan that is likely to become crowded with multiple system vendors at national and regional government levels.

#### **B. VeriSign Inc.**

VeriSign Japan K.K. was established in February 1996, and has come to lead the market as a private certificate authority. In March 1997, the PKI Processing Center was opened and operations for Japan's first certificate authority started. As a result of a business strategy of sales alliances, this company's electronic certificate system is incorporated in system products, like SCM and VPN, sold by system integrators such as NTT Data, NEC, Toshiba and Japan Unisys. VeriSign Japan K.K. is the first over-

seas corporation of the VeriSign Group.

With regard to capitalization, in addition to the 51 percent from VeriSign headquarters, investors include Sumitomo Mitsui Banking Corporation, Toshiba, NEC, SONY, etc. In December 2000, there was a capital increase through a third-party allocation of shares, adding investors like Tokio Marine and Nomura Securities, bringing the total number of investor companies to 33. When the capital increase through a third-party allocation of shares was conducted, VeriSign headquarters increased its stake to 69 percent.

### ***C. Entrust Inc.***

This company's entry into the Japan market was in June 1998 with SECOM Co., Ltd. as its sales distributor in Japan. In December 1998, Entrust Japan Co., Ltd. was established. However, Entrust Inc. provided only a little more than 10 percent of the funding, with SECOM, the largest stockholder at 46 percent, making Entrust Japan Co., Ltd. a joint venture between 16 companies, including NTT Data, SONY, Bank of Tokyo-Mitsubishi, Sumitomo-Mitsui Banking Corporation, Sanwa Bank, Nomura Securities, and Sumitomo Electric. As Entrust, the business operations focus mainly on supplying PKI products and consulting, with the bulk of the operations handled by NTT Data and SECOM TrustNet. In recognition of its penetration into the Japanese market, a capital increase through a third-party allocation of shares was held in April 2002, at which time Entrust Inc. announced its intention to increase its share to 37 percent (SECOM 38 percent).

In order to support digital government in Japan, which assumes certificate compatibility through Bridge CA, this company released the electronic certificate system 'Entrust PKI E-Government Edition' in April 2001.

### ***D. Baltimore Technologies plc.***

The earliest progress in Japan by the four major PKI vendors was the recognition of NSJ Corp. (Est: August 1995) as a sales distributor by Baltimore in June 1998. In March 2000, Baltimore acquired 73 percent of NSJ Corp., and in May 2000 changed the name to Baltimore Technologies Japan Co., Ltd (buy-out completed in July 2000). As a result, Baltimore has come to have a 45 percent share<sup>3</sup> of the Asian PKI market, including the rapidly developing Japanese market. Baltimore Japan has funding from 14 companies, including NTT DoCoMo, Sanwa

Bank, Nomura Securities, Tokyo Electricity, and the Japan Research Institute.

In May 2001, an alliance was announced with SOK, a company that had started operations as a voluntary certificate authority, and Japan Baltimore decided to build a PKI structure to issue SOK brand electronic certificates. Through this, it began its pursuit of SECOM which had already begun operating in the network security business as a voluntary CA through its alliance with Entrust. In addition, Teikoku Databank, which is affiliated with this company, in September 2001, was recognized as the accredited certificate operator for the electronic bidding system for the Ministry of Land, Infrastructure and Transport (MLIT), and the vendor of this system is Baltimore Technologies. Teikoku Databank has amassed results for 100 years performing business credit checks, and can combine electronic certification and credit rating administration.

A. VeriSign, C. Entrust, and D. Baltimore have formed an electronic application promotion consortium targeting the digital government infrastructure for Japan; and, in cooperation with companies like Netmarks Inc., are realizing the world's first certificate compatibility for systems from different PKI vendors. As a result, when PKI users perform electronic applications or electronic bidding, it will be possible to generally support each vendor's certificate authority supporting system.

### **3.5. Republic of Korea**

#### ***B. VeriSign Inc.***

This company is developing its certificate business by agreeing to cooperate in a strategic alliance (announced September 1999) with Korea Electronic Certification Authority, Inc. (KECA, est: March 1999, Korea's first certificate authority), operating as a certificate authority under the umbrella of KECA, and establishing CrossCert Inc. (est: March 1999 as a separate company from the Korean PKI vendor Syntech) as the base of VTN for Korea. In addition, in August 2001, an application was submitted to the MIC for designation as a licensed CA. Customers include large businesses such as POSCO, Samsung Electronics, Dongbu Insurance, and Hanhwa Securities. In June 2001, investments were also made in iTrusChina Co., Ltd., a VTN member certificate authority in China.



**C. Entrust Inc.**

This company established Entrust.net Korea Ltd. in December 1998 as a CA for Korea. In August 2000, a business tie-up with Nattrak, a Korean Internet security company was made for electronic certificate business operations supporting Wireless Application Protocol (WAP), beginning the first certification business for mobile communications in the Korean market.

**D. Baltimore Technologies plc.**

The SET (Secure Electronic Transactions) solutions vendor BARA e-Business and Communications Co., Ltd. (established in April 1997) changed its name to BARA Baltimore Technologies Korea Co., Ltd. and was designated as the sales agency for Korea (September 2000).

**3.6. People's Republic of China****B. VeriSign Inc.**

Through HiTRUST.COM(HK), a member of VTN in Hong Kong, VeriSign is aiming to expand the network into China. In December 2000, the CA Processing Center was established in Hong Kong and began offering certificate services for users in Hebei, Jiangsu, Guangdong, Beijing, Shanghai, and Guangzhou, as well as Hong Kong. In April 2001, HiTRUST Inc. was established as a Chinese subsidiary of HiTRUST.COM Inc.

Furthermore, in September 2000, iTruschina Co., Ltd. was established, and began operations as a VTN affiliate following approval from the government in April 2001.

**C. Entrust Inc.**

In May 2000, this company opened a branch office in Beijing, and has been proposing independent CA construction systems for the People's Bank of China (PBOC). The China Financial Certification Authority (CFCA) established as a joint venture of 13 commercial banks under the auspices of the PBOC, adopted the Entrust system in August 2001, and is conducting certificate services for bank users and those making security transactions.

**D. Baltimore Technologies plc.**

In March 2000, this company and its business partner in Korea, BARA

e-Business and Communications Co., Ltd., established a PKI service company called Beijing Ether Electronics Group Co., Ltd., as a joint venture with the Engineering Research Center for Information Security Technology (ERCIST), an agency of the Chinese Academy of Science and Technology (CAS). In September 2000, the company formed a cooperation and business alliance with the largest software developer in China, Neusoft Corporation, reaching an agreement on PKI educational support for China.

#### **4. FUTURE PROSPECTS**

So far, we have looked at the business strategies of the major European and North American vendors that are proceeding to divide up world PKI markets, and analyzed the most recent circumstances of their progress into Asian PKI markets. As indicated by the statement<sup>4</sup> "Strategic globalization of a business accelerates the new hegemony of competitiveness through the creation of new operation strategies to respond to global markets, such as international transfers of business know-how, and optimization of operation resources for the new region," it should not be surprising that the PKI vendors from advanced countries in Europe and North America are aiming at geographic expansion in Asia, including Japan.

So what are the developments we can expect in the future, in the PKI market (including Asian markets)? The following is a case study of the likely major trends in the PKI industry.

##### **4.1. Scenario 1: Establishment of the Open Global Standard for PKI**

As mentioned in the previous section, since the dawning of the PKI market in 2000, the Asian market has been aggressively pursued by major European and North American vendors. Many of the public sector CA in Asia rely on solutions provided by these Western vendors. In the private sector as well, the main attitude from the Internet society, seems to be 'Introduce a world-class level electronic certificate foundation from a leading PKI vendor, and participate in a global certification network,' minimizing the power of nations or governments.

VeriSign's VTN and Entrust's 'Cross-recognition type' network of CA and Baltimore's 'Hierarchical type' network of CA are probably designed for this kind of international society. This tendency is especial-

ly notable in areas with a strong dependence on trade with Europe and North America, and relatively smaller domestic markets, such as Singapore, Malaysia, Hong Kong, and the Philippines. In such areas, the authentication and certificate technology of the Western PKI vendors is actively introduced, with the priority on achieving smooth trade transactions with 'certification tools' that conform to Western standards.

Below are some concrete examples for the above 'Scenario 1.'

### ***A. Establishment of an Asian PKI Forum***

PKI vendors are not only competing to establish themselves as a de facto standard. They are also beginning to build cooperative relationships in order to develop interoperability and compatibility of PKI. In the US, with the most developed e-commerce industry, a 'PKI Forum' was established in December 1999. Major PKI vendors, including RSA, Entrust, Baltimore, IBM, and Microsoft, as original founders, participate with the intent to expand the number of users through an open strategy of technology standards. Later, VeriSign also joined.

In Asia and the Pacific regions too, there has been a spurt of international activity to promote and spread PKI. Japan Promotional Association for Asia PKI Forum (APKI-J) was set up in Japan in December 2000, mainly by Hitachi, NEC, Fujitsu, Mitsui and Toyota. In June 2001, the first joint meeting was held in Tokyo with attendance from the following 8 regions, Australia, China, Hong Kong, Japan, Korea, Malaysia, Singapore and Taiwan. And it was agreed to establish an 'Asia PKI Forum' for building interoperable PKI in Asia.

In Korea as well, activities have begun, such as the Korea PKI Forum (established: March 2001). However, when the Korea PKI Forum sponsored a conference in Seoul on building a shared Root CA for Asia in April 2001, in addition it laid an emphasis on "the threat to the Asian Market from multinational PKI vendors based in the US and Canada."<sup>5</sup>

### ***B. International 'Cross-Recognition' of PKI in Asia***

Some examples of bilateral cross-recognition in Asia have been started already. At the specific industry level, some international schemes for inter-connection of PKI have been launched. At the 5th Conference (held in Beijing, August 2001) of the Pan-Asian e-commerce Alliance (PAA), which is a private-sector group on trade EDI in Asia, formed by representatives from Hong Kong, Singapore, Taiwan, China and Korea (Japan joined later), it was announced that the outlook of commencement of

field testing for PKI interoperability between Asia nations by early 2002. As mentioned above, the trade sector is a very important area for Singapore and Hong Kong, etc., and internationalization is a higher priority than regional individuality in this field. Even to establish an effective trade system, it is urgent to establish a shared certification and authentication infrastructure. It is believed that the motivation for integration of the individual electronic certificate systems is from those fields in which there is a high priority on interaction. For reference, Tradelink of Hong Kong, a leader in PAA, as well as SNS in Singapore, and Trade-Van in Taiwan are all Baltimore users.

For the financial sector, the importance of interoperable PKI is high too. Hence the similar industry based PKI project called 'Identrus' is in progress as stated in section 2. From Asia, participants include Bank of Tokyo-Mitsubishi, Sumitomo Mitsui Banking Corporation, Sanwa Bank, the Industrial Bank of Japan, the Korea Exchange Bank, and ChoHung Bank. Identrus could take the initiative to integrate PKI of member banks including their worldwide client networks. Identrus is also a Baltimore user.

### ***C. Reorganization of PKI under One Vendor***

As mentioned above, the global electronic certificate market is divided by four major PKI vendors. However, this framework is not at all stable. As stated by Alex Van Someren, the CEO of NCipher Corporation Ltd., "It is difficult to participate in a PKI market controlled by VeriSign," in extreme cases, the market can be looked at in terms of the opposition between VeriSign's network and the alliance of other PKI vendors. Along with such movements, a simple structure will arise under a strong 'hierarchy.'

## **4.2. Scenario 2: Revival of Regionalism in PKI**

However, it cannot be denied that there is a risk regarding certification and authentication as mere tools. At the beginning of this chapter, authentication was defined as "verification that the communicating party is actually who it claims to be, as well as verification of registration and the integrity of the transferred content," but it is not possible to simply determine whether electronic certification can be handled by this kind of telecommunications technology, even in the future. As indicated,<sup>6</sup> a CA could expand its business to include services which accumulate informa-

tion such as financial status, ability to settle accounts, and transaction history of those involved in the transaction. If it is possible to clearly demonstrate appropriate evaluation criteria for the trade partner to the e-commerce user on demand, this should make an enormous contribution to the growth of e-commerce.

From this point of view, the question becomes the risk of European and North American businesses taking over specific technology areas. There is a deep-seated wariness, particularly toward US companies, in many Asian countries and it is considered entirely natural for government policy to eliminate monopolies of a business sector controlled by foreign capital. In fact, for the electronic certificate industry, in Korea solutions from the PKI vendors in the country are offered for the certificate authorities under the close scrutiny of the government. As discussed later, there is research underway on Chinese character-based electronic certificate services for China, Hong Kong, and Taiwan. In Japan as well, large Japanese electronics companies device makers, like NEC, Hitachi, and Fujitsu are setting up a joint venture as the 1st accredited CA in Japan (JCSI).

These examples show the strong tendency to pay careful attention to the trust and credit structure that reflects national cultural backgrounds. Some concrete examples for the above 'Scenario 2' are shown below.

#### ***A. Regionalism in the US (After the 9-11 Terrorist Attacks on the Security Leader)***

We have no doubt about the position of the US as the leader in the security field including the PKI industry. However, after the terrorist attacks on the US on 11th September, 2001, there have been large tremors in previous ideas about security. There is a sudden shift in public opinion in the US toward strengthening the government's ability to monitor activities and perform criminal investigations beyond the security of businesses and individuals. There has been a reversal on the point of security, from 'protecting individual privacy (information)' to 'ensuring safety at the national level.' The anti-terrorism act, the 'Uniting and Strengthening America (USA) Act' enacted on 26th October 2001, was proposed by Republicans John Kyl (senator from Arizona) and Orrin Hatch (senator from Utah). This act legalizes investigative techniques, such as interception of communications on the Internet by the relevant government authorities for the purpose of countering terrorist activity. Furthermore, the Republican senator from New Hampshire, Judd Gregg, stated that

there should be an international system of cooperation between national governments and PKI vendors, and that there should be cooperation to break encryption when necessary. There is a high possibility that terrorists use encryption technology to communicate with each other, and it has been pointed out that 'online terrorism' is another danger, following the attacks and the anthrax mailings. In such circumstances, there is probably no choice but to impose some degree of limitation on privacy rights on the Internet. However, measures which rock the foundation of PKI, such as worldwide prohibition of the use of encryption technology and the private key public registration (deposit) system, are beyond the authority of countries. There is a limit to the public control of private keys, and the government's risk of information control is excessively high. Incidentally, Senator J. Gregg also insists that "PKI vendors have 'influence strong enough to determine the fate of nations,' so they, as corporate citizens, should cooperate in the development of decryption technology by the US government."

The US government is destined to work toward restoring confidence in the security system even if it means disregarding the protection of personal information. In a state of emergency US regionalism may destroy a security network that has been built at the worldwide level.

### ***B. Regionalism in China***

As mentioned in section 2 on VeriSign's business strategy, there is a risk in having all authentication functions in the private sector. It is likely that the Chinese government will be among those with the strongest aversion to this situation. Moreover, for an American company, the Chinese government will certainly want to eliminate such influence as much as possible. The Shanghai Electronic Certificate Authority Center Co., Ltd. (SHECA) mentioned in section 3 on Hong Kong PKI, is working with Hong Kong on a project to build a Chinese character-based electronic certificate system. There is a strong tendency for China to erect hurdles for foreign PKI vendors based on some sense of sovereignty. In addition, for the future the goal seems to be to build an authentication and certification mechanism that is optimized for the business customs and regulatory system within China.

Furthermore, in China, regionalism is definite even at the level of domestic CA; and the construction of a certificate infrastructure has been initiated at the local city administration level, such as Beijing, Shanghai, Sichuan, etc., under its strong 'hierarchy.'

Both above scenarios offer a completely different perspective. But these are the realities to be confronted in the first year of 21st century. What is important for PKI will be how the balance of power between government and business enterprises (major vendors) is kept. Especially, how to prevent egoism of leading nations is significant to the development of an open security standard for global networking.

## 5. CLOSING REMARKS

For social efficiency and convenience, apparently, we shall see 'Network globalization,' apart from the conventional hierarchy, in setting up the new information infrastructure. However, it will take an enormous time to establish an infrastructure agreeable to anyone. Particularly, it will be difficult to build up an international infrastructure related to social credibility.

So far, we have reviewed PKI as a business tool for authentication in Internet communication. With each vendor struggling to be the global standard, pushing each business model to the market as the best solution.

On the way to the establishment of the best infrastructure as a final solution, it will be required to test more business tools through de facto standard competition in the private sectors. For a more sophisticated standard business enterprises will continue to invent new technologies, such as PKI in combination with biometrics using unique characteristics (fingerprints, iris, etc.). In this regard, the construction of original business models will be important as the great social contrivance. Whatever it may be, the technical effect will be proven in the future.

On the other hand, for the public sector, much wider perspectives are necessary. Especially, with respect to a trust system, such as PKI, that could be said to be a national issue. The trust framework of each society will be determined in accordance with the status of each society respectively. It is not a simple matter of business tools, but of complicated political issues. Before selecting the trust system of society, we have to determine the national policy. Should the government have a decentralized or centralized structure? Should the society accept the international standard or not? If the trust system is set before the social consensus is reached on these points, such a society shall be 'distrustful.'

## Notes

- <sup>1</sup> US Patent No.4,405,829: Generally, called 'RSA Algorithm Patent' on Cryptographic Communications System and Method. This patent is used for creating a set of Public Key and Private Key which are important factors for encryption under PKI. Effective from 20th September, 1983 with the duration of 17 years.
- <sup>2</sup> Quick Ratio: A (financial) stringent test that indicates if a firm has enough short-term assets to cover its current liabilities, also called 'Acid test ratio.' Calculated at  $(\text{Cash} + \text{Marketable securities} + \text{Accounts receivable} + \text{Other short-term investments, without Inventory}) \div \text{Current liabilities} \times 100$  percent. From the view-point of business administration theory, a company with a ratio more than 100 percent can pay its current liabilities immediately, then should be regarded as favorable.
- <sup>3</sup> Asian PKI Market Share: Comment by Patrick Hugh Holahan, Executive Vice President Marketing, Baltimore Technologies plc. in PKI Seminar on 7th July, 2000 in London, England.
- <sup>4</sup> Advantage of Strategic Globalization: W.J. Keegan [1999] *Global Marketing Management*, Prentice-Hall.
- <sup>5</sup> US and Canadian initiatives in Asian markets: Conference presentation by Korea PKI Forum on 17th April, 2001 in Seoul, Korea.
- <sup>6</sup> Business expansion of certificate authority: K. Miyawaki, K. Kato [2001] *Electronic Certification will Change Japan*, Japan Productivity Center for Socio-Economic Development, June.

## References

- Carlisle Adams, Steve Lloyd [2001] *Understanding Public-Key Infrastructure: Concepts, Standards, and Development Considerations*, McMillan Technical Publishing, July.
- Discussion Paper [2000] "Current Issues on E-Commerce Legal Framework," *Jurist*, No.1183, Yuhikaku Publishing Co., Ltd., 15th August.
- Miyagawa, Shoko and Yamazaki, Juichiro [1998] "'Trust' and 'Reputation' in the Internet Society," *Hitotsubashi University Business Review*, Vol.46, No.2, Toyo Keizai, Inc., November.
- Ross Davies and Yahagi, Toshiyuki, Toshiyuki Yahagi [2001] *Retail Investment in Asia Pacific: Local Responses and Public Policy Issues*, Oxford Institute of Retail Management, Templeton College, University of Oxford, January.
- UNIZON Corp. [2001] *Framework of the Network Security — Chart Guidance* — D.Art Corp., April.