Asia PKI Application Case Book

1st Edition

Nov 2005

BAWG, Asia PKI Forum

Acknowledgment

This Business case book is developed as one of deliverables of BAWG, Asia PKI Forum.

Special thank is dedicated to each of following members in BAWG who had contributed much time and resources on it.

Edited and arranged by

Korea PKI Forum Chris Min Jang, Secretariat of BAWG in FY2004

Chinese Taipei PKI Forum Emilie S. Tsai, Member of BAWG in FY2005

With contributions from:

Korea PKI Forum Mr. Chris Min Jang

Japan PKI Forum Mr. Kotaro Fujimoto

Chinese Taipei PKI Forum Ms. Emilie S. Tsai

Singapore PKI Forum Mr. Chee Young Tan

Table of contents

1. INTRODUCTION 1

1.1 GOAL OF THE STUDY 1

1.2 ABOUT BAWG, APKI FORUM 2

2. OVERVIEW OF PKI BUSINESS TREND IN ASIA REGIONS 3

2.1 JAPAN 3

2.1.1 Background 3

2.1.2 Business environment 3

2.1.3 Related issues 4

2.2 KOREA 5

2.2.1 Background 5

2.2.2 Business environment 5

2.2.3 Related issues 6

2.3 CHINESE TAIPEI 7

2.3.1 Background 7

2.3.2 Business environment 7

2.3.3 Related issues 8

3. BUSINESS CASE STUDIES 9

3.1 "SAFE MANAGEMENT ON EDUCATIONAL INFORMATION" (KOREA) 9

3.1.1 Business background 9

3.1.2 Structure of the case 10

3.1.3 Configuration of the system 11

3.1.4 Effects 12

3.1.5 Further development 12

3.1.6 Other issues 12

3.2 "PARENT APPROVAL VIA DIGITAL SIGNATURE" (KOREA) 13

3.2.1 Business background 13

3.2.2 Structure of the case 13

3.2.3 Configuration of the system 14

3.2.4 Effects 15

3.2.5 Further development 15

3.2.6 Other issues 15

3.3 "CONTENTS AUTHENTICATION" (KOREA) 16

3.3.1 Business background 16

3.3.2 Structure of the case 16

3.3.3 Configuration of the system 18

3.3.4 Effects *18*
3.3.5 Further development *19*
3.3.6 Other issues *19*
3.4 "MEDICAL AND HEALTHCARE NETWORK" (JAPAN) 20
3.4.1 Business background *20*
3.4.2 Structure of the case *20*
3.4.3 System configuration *22*
3.4.4 Effects *23*
3.4.5 Further developments *23*
3.4.6 Other issues *24*
3.5 "ELECTRONIC ACCOUNT RECEIVABLES FOR SMALL-MEDIUM ENTERPRISES" (JAPAN) 25
3.5.1 Business Background *25*
3.5.2 Structure of the case *25*
3.5.3 Configuration of the System *25*
3.5.4 Effects *26*
3.5.5 Further development *27*
3.6 PKI APPLICATIONS IN E-GOVERNMENT (CHINESE TAIPEI) *27*
3.6.1 Business Background *27*
3.6.2 Structure of the case *28*
3.6.3 Configuration of the System *29*
3.6.4 Effects *31*
3.6.5 Further development *31*
3.6.6 Other issues *32*
3.7 "EXPANDING FINANCE CERTIFICATE APPLICATION RANGE" (CHINESE TAIPEI) 33
3.7.1 Business Background *33*
3.7.2 Structure of the case *34*
3.7.3 Configuration of the System *35*
3.7.4 Effects *38*
3.7.5 Further development *39*
3.8 "BAROC FXML UCA & I-SECURITY INTEGRATED TRADING SECURITY SYSTEM" (CHINESE TAIPEI) ... 40
3.8.1 Business case background *40*
3.8.2 Structure of the case *42*
3.8.3 Configurations of the system *44*
3.8.4 Effects *44*
3.9 "CORENET E-SUBMISSION" (SINGAPORE) 45
3.9.1 Business background *45*
3.9.2 Structure of the case *45*
3.9.3 System configuration *46*

3.9.4 Effects.....*47*
3.9.5 Further developments.....*47*
3.9.6 Other issues.....*48*
4. FUTURE APPROACH.....**49**
4.1 CONSIDERATION & FURTHER WORK.....49
4.2 CLOSING.....49

1. Introduction

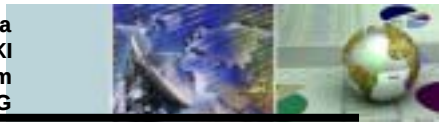
1.1 Goal of the Study

This book reports business models in Asia region using PKI technology. Based on the technology, which is mainly for online security and identification in remote location, the usage of PKI is expanding itself to various areas from Internet banking to online bidding.

During 5 year period from year 2000, there has been remarkable development in PKI areas in Asian region. Most of banks deployed or considered to deploy PKI for Internet banking and most governing bodies of each country/region also deployed or concern about deploying PKI technology for e-Government. Nowadays, PKI technology is no more difficult technology and is very familiar one to be faced with the public in real life.

BAWG has processed sharing business ideas for three years. Many ideas and business models were reported from our members and helped each member's understanding in other regions and for him to consider deploying them to its own region.

Among BAWG members, we need active business idea sharing for the development of PKI and promotion for good potential project for inter-region. Apparently, there is gap of understanding among members because the recognition level of online security is different from each other. Hopefully this book could help reducing the gap of understanding and enhancing online security of each region.



1.2 About BAWG, APKI Forum

Business Case/Application Working Group of Asia PKI Forum is a working group of Asia PKI Forum. Its main role is to find a good business model using PKI technology and to set up inter-regional project with other workgroups in Asia PKI Forum. Upon the expansion of deployment of PKI, BAWG's concern about new business model in every industry is more demanding in these days. BAWG provides industry information about each region in Asia; shares business ideas, tries to find good models helpful in each region, and also put an effort on setting up common projects for all members.

The Leader co-chair of BAWG in FY2004 and FY2005 are Mr. Young Chul Kang from Korea while Dr. Chin Lien Yen from Chinese from Taipei. Mr. Kang is CEO & President of KICA and Vice president of Korea PKI Forum. Dr. Yen is President of National Information Enterprise Promotion Association in Chinese Taipei.

2. Overview of PKI business trend in Asia regions

2.1 Japan[1]

2.1.1 Background

Ever since the first e-Japan Strategy was formulated in January of 2001, Japan has been engaged in improving its electronic network and developing the IT base needed for the promotion of e-commerce and e-government. As a result, the IT base, centered upon the Internet, has been greatly enhanced. At present, the population of Internet users has exceeded 60%, approximately 15 million households nationwide use broadband connections, and connection services are continually being provided at inexpensive rates. Moreover, about 90% of mobile phones in Japan have Internet access capabilities ("Survey on the Direction of Communications Use," 2003, Ministry of Internal Affairs and Communications).

The second national strategy, e-Japan Strategy II, formulated in July of 2004, builds upon this IT base and focuses on utilizing IT to actively revolutionize social and economic systems. The efforts of both strategies are being concentrated in the 7 frontier fields of *medical treatment, food, living, small-medium enterprise (SME) finance, information, employment, and government services.* In promoting the benefits of IT utilization, these strategies are not limited to just the private sector or just the public sector but aim to bring benefits to the nation as a whole.

2.1.2 Business environment

Currently in Japan, the construction of the basic infrastructure for GPKI and Individual Public Certification Services is almost complete. This is the result of the first stage of the e-Japan strategy.

Amongst the businesses that are utilizing PKI, the providers of government

[1] The following versions for 2.1, 3.4, and 3.5 were selected, with the permission of METI, from the report entitled "2004 Survey Research on the Mutual Operability of an EC Technology Base (survey on the direction of PKI utilization)" commissioned by METI. These versions was edited and translated by the PKI Forum in accordance with the appearance and structure of the original text.

services are the most advanced in their adoption of the technology. Not only have national and local government offices installed the basic infrastructure for systems like PKI and Basic Resident Registry Networks, but they have also constructed and begun operating large-scale systems – e.g. electronic applications, electronic bidding and procurement, and electronic tax filing – that utilize PKI in the B2G and C2G fields. The central government is already at the evaluation phase with its electronic application systems and has even submitted several evaluative reports. Looking ahead, plans are under way to upgrade the vehicle ownership registration process into a "one-stop service."

However, while the PKI utilization in the B2G field is moving forward, PKI utilization for e-commerce in the fields of B2B and B2C is not making as much progressing as initially expected. Though it is true that about 20 private businesses have adopted the designated certification services that are described by the Electronic Signature Law and have issued Public Key Certificates, the majority of these certificates are not used for e-commerce between private companies. Rather, they are mainly used in the B2G field for electronic government services on the local and national level.

The recent increase of Internet "phishing" scandals, in which banking cards are fraudulently used, has heightened the need for more secure personal authentication. Meanwhile, the implementation of the Personal Information Protection law in April of 2005 has increased the general awareness toward information security. Amidst these trends, PKI based businesses can be expected to emerge not just in the B2G and C2G sectors, but also within the e-commerce industries of the B2B and B2C sectors as well.

2.1.3 Related issues

Much legislation has been made in connection with PKI technology. Under the Electronic Signature Law passed in 2000, electronic signatures were permitted as substitutes for actual signatures or personal seals.

The Electronic Document Law, a legislation concerning the use of IT technology with respect to the storage of documents by businesses, was passed in April of 2003. Under this law, a private company can substitute the

documents and signatures that it is required to store under commercial law with electronic data or electronic signatures. These laws aim to both reduce the costs that go into the circulation and storage of documents and sales records and stimulate e-commerce between private sector companies.

2.2 Korea

2.2.1 Background

PKI is already well-known technology in Korea. Licensed certificates issued based on PKI technology are now treated as a part of infrastructure in IT sector. Currently 9 million licensed certificates were issued nationwide. The licensed certificates are issued through the process of identifying a person in face to face with required documents. It is inevitable condition if one wants to have a licensed certificate. This strict criterion of issuance of licensed certificate enables the substitute of seal in online sector.

Many industry areas deployed this infrastructure: Internet banking, stock trading, civil petition, etc. Internet banking, stock trading using licensed certificate is very common activities of people. Above 70% of total bank users are using Internet banking. Upon this situation, some banks lead customers to use Internet banking instead of nearest offline branch by providing good interest rate just to Internet banking account. They have direction to reduce offline branch gradually. On the basis of this symptom, there is trustworthy licensed certificate infrastructure.

With the benefit of easy access, swift processing, and trustworthy identification, licensed certificate is expanding the areas.

2.2.2 Business environment

Internet Banking

All banks deployed licensed certificate authentication system. If a customer has to transfer his money online, the customer must sign digital signature using his licensed certificate. Some banks enhance the level of control by blocking

to see the transaction of an account if they haven't a certificate.

Online Stock trading

All securities deployed licensed certificate authentication system. If a customer has to trade his stock or transfer money online, the customer has to log-in by submitting digital signature using his licensed certificate. A customer can submit digital signature for transaction each time.

E-Government

The government services web sites for civil petition, many types of certificate issuance, notification of internal work process, etc. With licensed certificate, people submit their digital signatures when it is needed and access related information, get certificates by printing, and request civil petition.

E-Commerce

When they use credit card on the Internet shopping mall site, they have to submit digital signature if the total price of the product exceed 300,000 Korean Won. It is now applied to major two credit card companies, but supposed to apply to every credit card company from October 2005. It is expected to block illegal usage of credit cards.

2.2.3 Related issues

Recently it is discussed that there should be category of licensed certificate. A s it is, it's very powerful tool when we consider it as a representative of each p ersonal online. It is being discussed and already adopted partially in some ind ustry area. Restricted-purpose licensed certificate is still in discussion.

2.3 Chinese Taipei

2.3.1 Background

Along with the progress and rapid developments of Internet technology and high penetration of Internet, more and more companies and consumers conduct information exchanges and business transactions over the Internet. Internet security becomes a key issue as there is always risk of unauthorized transmitted data theft in the Internet open environment.

Since PKI (Public Key Infrastructure) possess four major information security functions, including “authentication”, “integrity”, “confidentiality”, and “non-repudiation”, the technology has been generally acknowledged as the most effective way to achieve data protection goal. A lot of government sectors in many countries have adopted or promoted PKI as a way to create secure B2G or G2G e-transaction platform.

In Taiwan, the government has put forth efforts on PKI promotion since 8 years ago. A government PKI framework was designed in 1997 and in the consecutive year, Government Certificate Authority, GCA was established. The Electronic Signature Law was enacted in 2001. The Government PKI framework, including Government Root Certificate Authority, Certificate Authority of MOI as well as Certificate Authority of MOEA, is in full operation now.

2.3.2 Business environment

In addition to government PKI applications, PKI in the private sectors is growing enormously in Taiwan. For instance, the Bankers Association set up TFRCA (Taiwan Financial Root Certificate Authority), and TFPCA (Taiwan Financial Policy Certificate Authority), for the financial industry.

In Taiwan, the PKI applications in the private sector can be categorized as (1)e-commerce, and (2) industrial supply chain. The e-commerce category includes online transaction, e-invoice, electronic Certificate of Origin, customs clearance and etc. As for the industrial supply chain category, many PKI

enabled services are taken into practices in logistic, automobiles, electronics, irons and steels, petrochemicals, and printings industries.

2.3.3 Related issues

Ministry of Economic Affairs formally lunched Chinese Taipei PKI Forum in 2001, and participated in Asia PKI Forum. To encourage corporations to adopt PKI, MOEA started PKI subsidization program in 2003. Since then, MOEA has accomplished 42 major PKI application projects and helped more then 4,000 local companies to introduce PKI in their e-business operations.

3. Business case studies

3.1 “Safe management on Educational Information” (Korea)

3.1.1 Business background

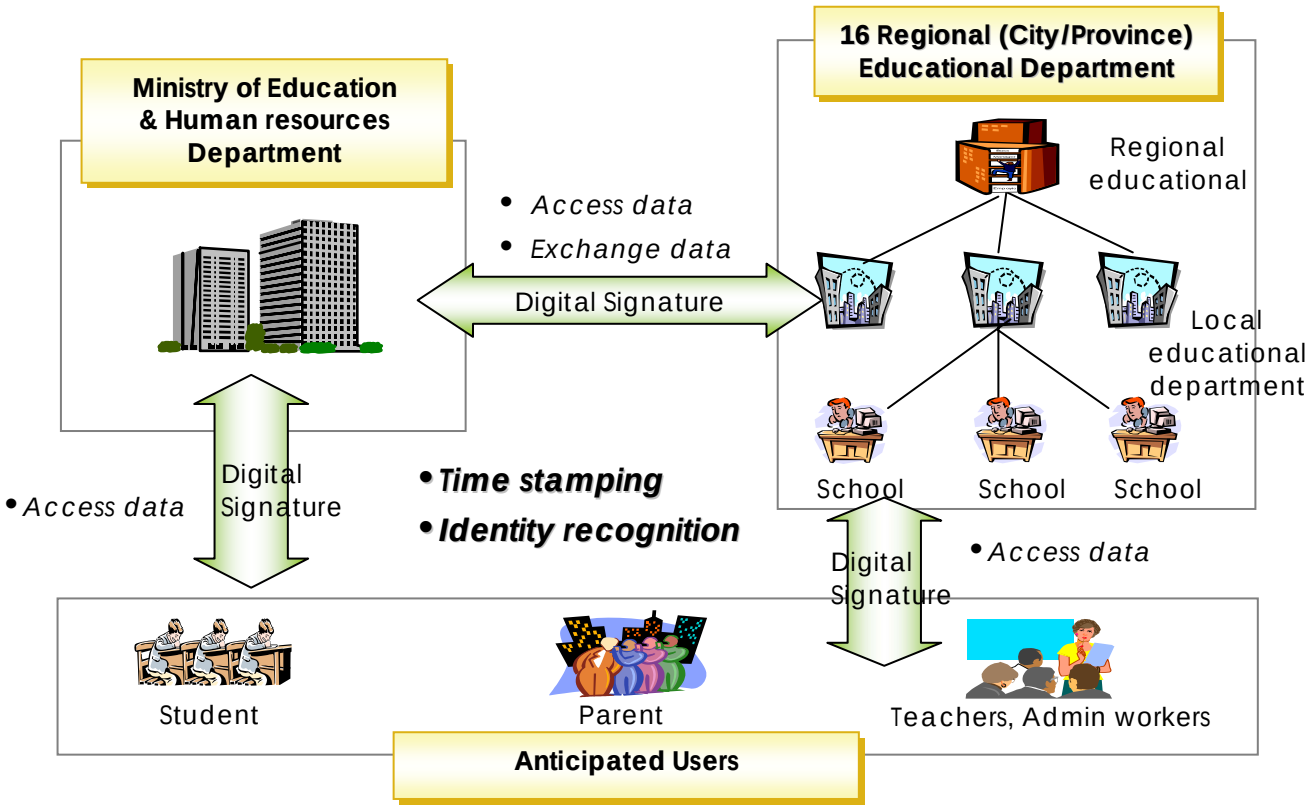
There has been discussed safe educational information management for elementary schools, middle schools, and high schools for a long time. From late eighties, each middle and high school started to consider a system for student-related information in digital format. During the nineties, each school can manage the administrative information using a small-size computer like desktop size computer. Though a closed group or selected person can access the information at that time and it had a risk to be hacked by unauthorized person after breaking physical protection or neglecting management in security. An introduction of web caused security matter severely when they deployed the need of access in any time anywhere to the system by expanding the access to students and parents. Because student-related information is very critical information, it needs higher level security.

Thus, NEIS (National Education Information System), a nationwide scale system for educational information was introduced in 2004. Now it handles petition, issuance of every certificate online and has capability of covering requests from parents, students, and teachers.

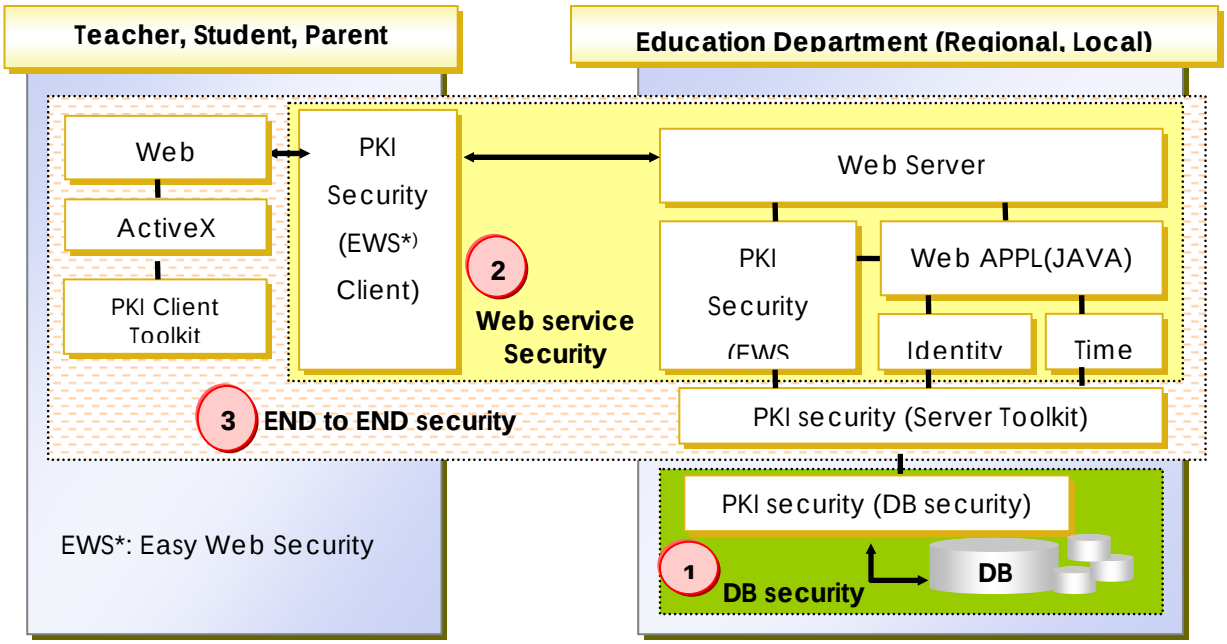
- Before
  - Each school has its own computer system
  - Administrate itself in a school and need a personnel to admin and operate
  - Weak to protect hacking attempts

- Needs
  - Establish centralized system for administration
  - Access allowance to each teacher and related workers effectively

3.1.2 Structure of the case



Above picture shows the logical role playing model of the service. Following diagram shows the security concern about the system: server side, client side, end-to-end issues.

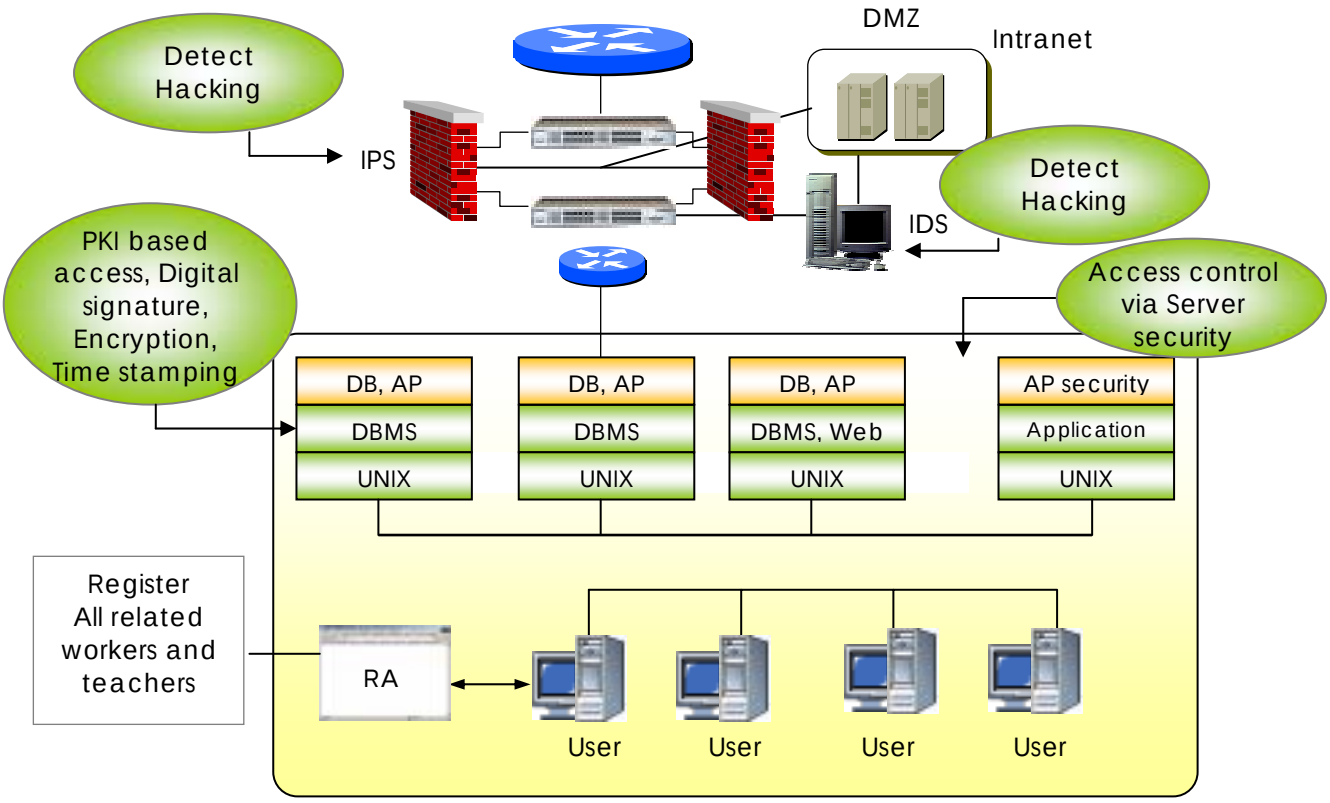


When the system was designed, there were three points of security concern. See following points.

(1) In DB security: Access management
(2) Web security: Protect unauthorized person, Protect internal data
(3) End-to-end security: Data exchange between only designated users

3.1.3 Configuration of the system

Following picture shows that network and system configuration.



3.1.4 Effects

It is a big project and PKI itself is a module of the project. So it is difficult to calculate separate ROI related on PKI stuffs. However, the ministry of education and human resources reported the effect of the system in pubic as following. Up to now, the investment of building the system is 52.1 billion won (52.1 million US$). The expected money-saving effect on the investment by 2008 is calculated 1,400 billion won (1.4 million US$) and it is 25 times compared to the investment.

3.1.5 Further development

In early 2005, this system serves to issue 6 types of certificates online as a web service. The system was designed to have functions of showing important personal information like credits, marks, comment of teacher, etc. But the service of showing the items online is postponed and the system for this service will be built as a separated system because of public opinion that it might be a disaster if one's marks or comment of teacher is disclosed as a result of hacking attempt. Currently the item is accessed to restricted person who has authority. Even though it takes some time to design database and related information for a secured web service, it will be accomplished in near future.

3.1.6 Other issues

To adopt this system, there had been a quarrel between the education depar tment and some teachers who joined in the nationwide teacher labor union. T he labor union issued that concentrated information might be a dangerous if t here was, even though not intentionally, slight opening to hacking attempts or if they abused it both internally and externally. They urged that critical inform ation should be not opened to web site or separated system was needed for t he service. It is concluded to separate systems for each service. Though discus sion was focused on the system and network security, not on certificate or PKI related part, this quarrel delayed the project so long.

3.2 “Parent approval via digital signature” (Korea)

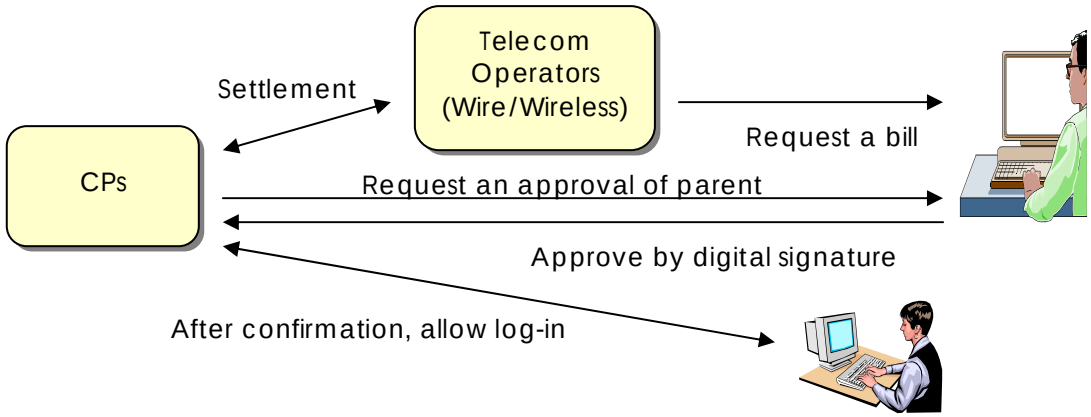
3.2.1 Business background

Many children and youngsters are spending quite lot of money to play online & download games, to decorate their mobile phones with their own bell sound, avatar, etc. It is easy for youngsters to pay by mobile payment or ARS charge of telephone lines provided by tele-communications operators. It is usually called value-added charge and is added in a bill when telecommunications operator issues a bill. But this convenient way of payment cause quarrel between parents and content providers because of the approval of payment.

Based on “The Act on Promotion of Information & Communication Network Utilization and Information Protection, etc”, every CP has to have an approval of parents to charge the money to young children and youngsters. The telecommunications committee (MIC) put penalties for contents providers who didn’t keep the law. In April 26, 2004, total 13 Internet portals and online game sites got penalty of 82 million won (about 68,000 US$).

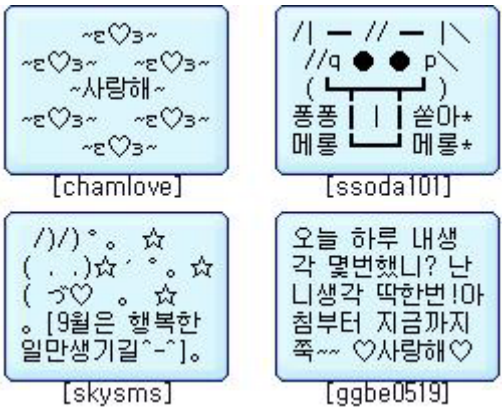
According to the law, when a CP sell online items (game, avatar, and cartoon) to youngsters age under 20 or even let youngsters join their site age under 14, they have to get the approval of parent. From April 2005, CPs has to receive digital signature as one of methods with two other ways: receiving a fax or a phone call of a parent for an approval.

3.2.2 Structure of the case



Star image character screen

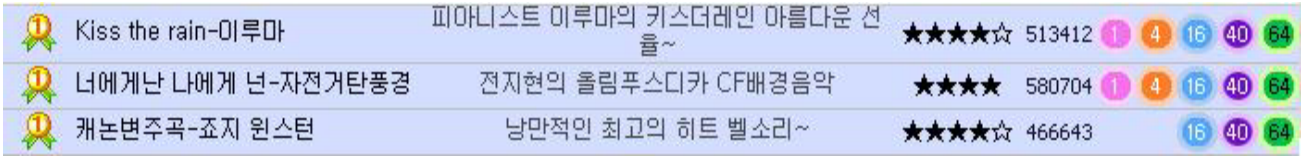
Colorful character screen



Special Text message via SMS

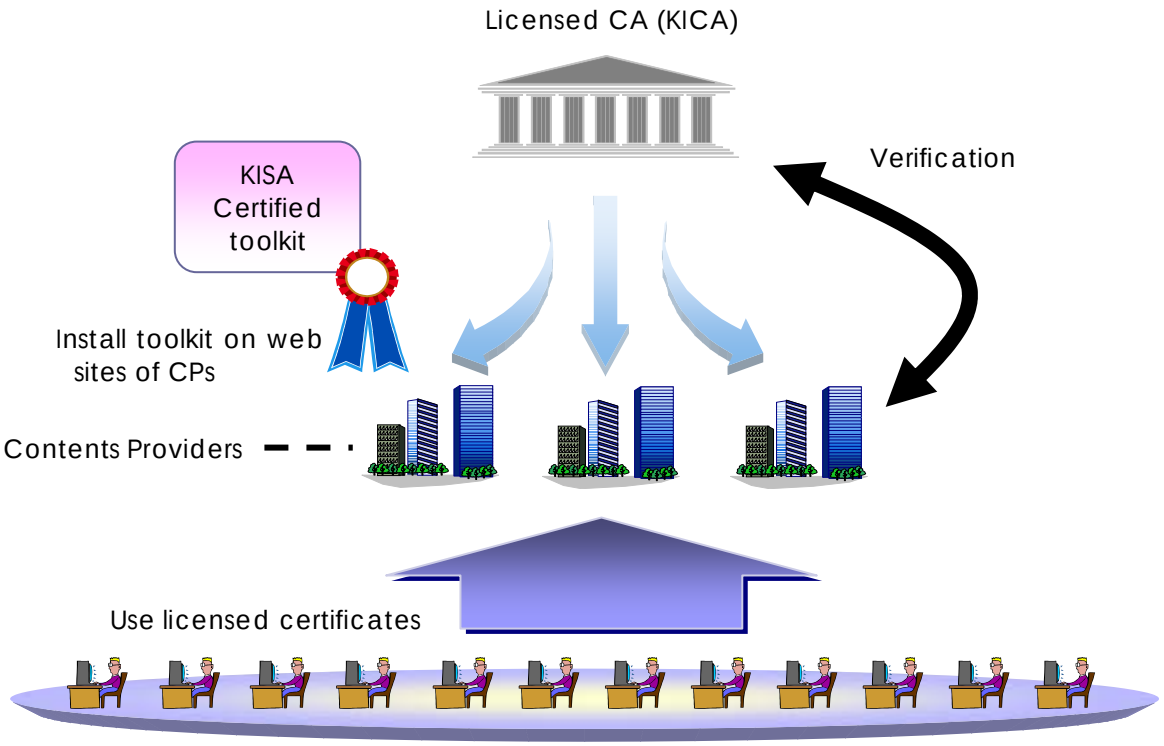
Avatar

Bell sound download



3.2.3 Configuration of the system

Each CP has to deploy an authenticated system (server toolkit) or use a service to authenticate digital signatures that submitted by parents.



3.2.4 Effects

This approach will significantly reduce the civil petition of disputes between parents and CPs. It also protects children from the excessive usage of contents & games and wrong activity-driven web sites.

3.2.5 Further development

It will be combined to adult verification in a while. The module of youngster verification is also considered.

3.2.6 Other issues

There has been issued a need of deploying restricted licensed certificate for just online identification. Its main usage is for identifying oneself online and it needs to be classified for this purpose. It will be issued online only based on the strictly verified personal information.

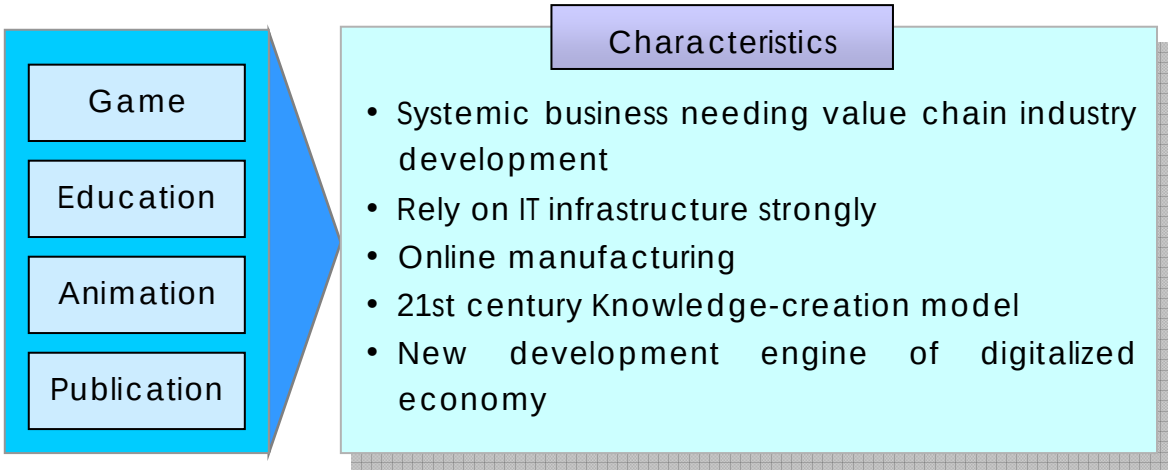
3.3 “Contents Authentication” (Korea)

3.3.1 Business background

There has been discussed about an issue of illegal copies of digital contents after the digital era is opened. As a solution for illegal copy and untraceable contents, it is propelled to deploy contents authentication.

- Meaning of Digital Contents?
  - Created, processed, transferred data or information in digital format covering signal, text, voice, sound, image, etc on wired/wireless networks

Following picture is showing characteristics of digital contents industry. Game, Education, Animation, Publication sectors are in this category.

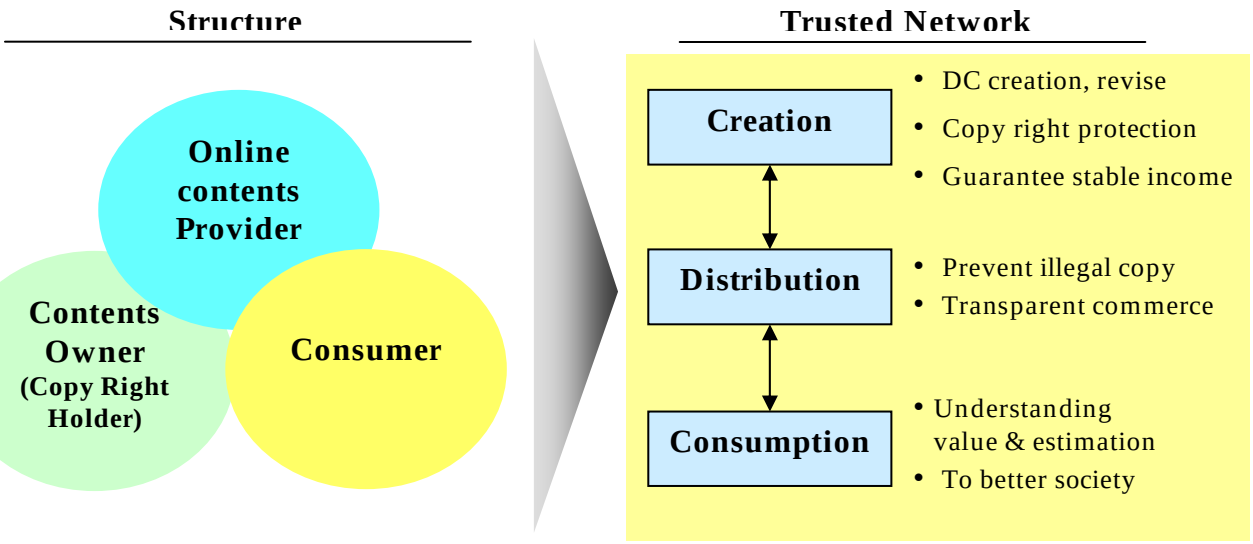


To protect digital rights of authors, and to set-up reasonable trading custom among author, distributor, and retailer, they deploy a concept of DC (Digital Contents) authentication for it.

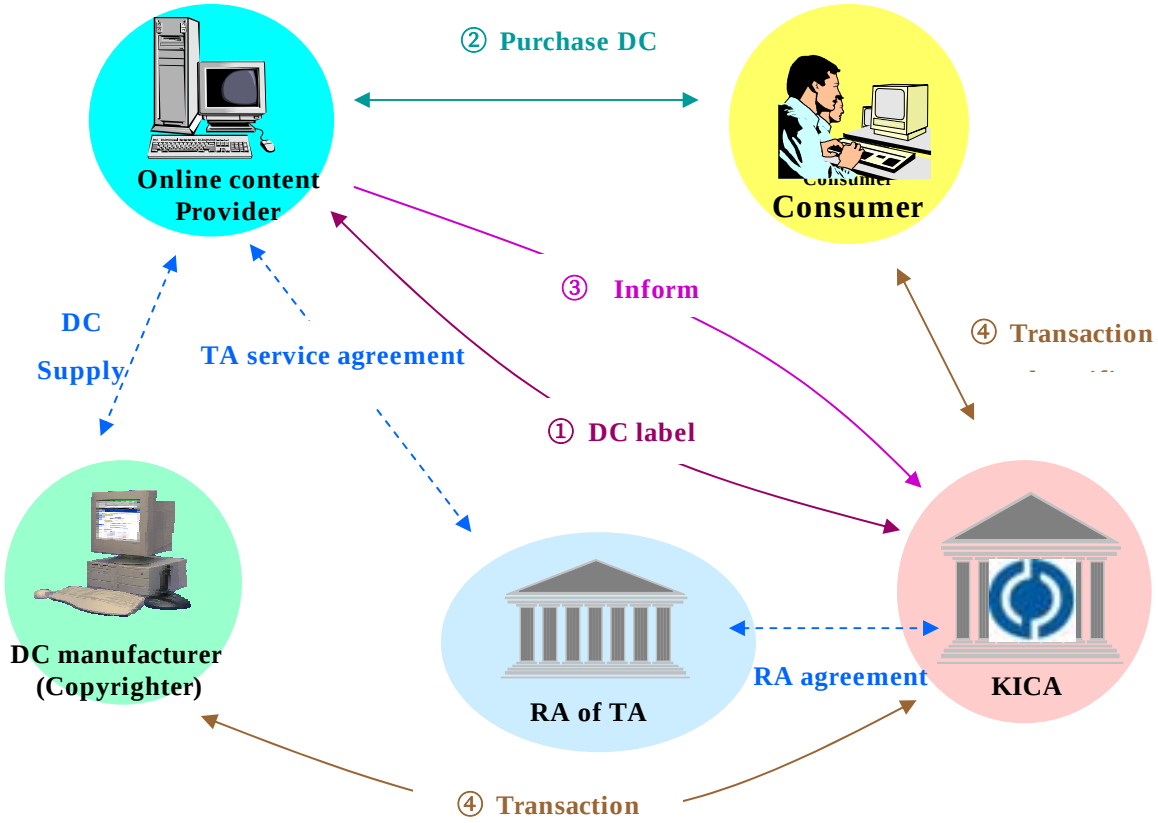
3.3.2 Structure of the case

Definition of DC authentication

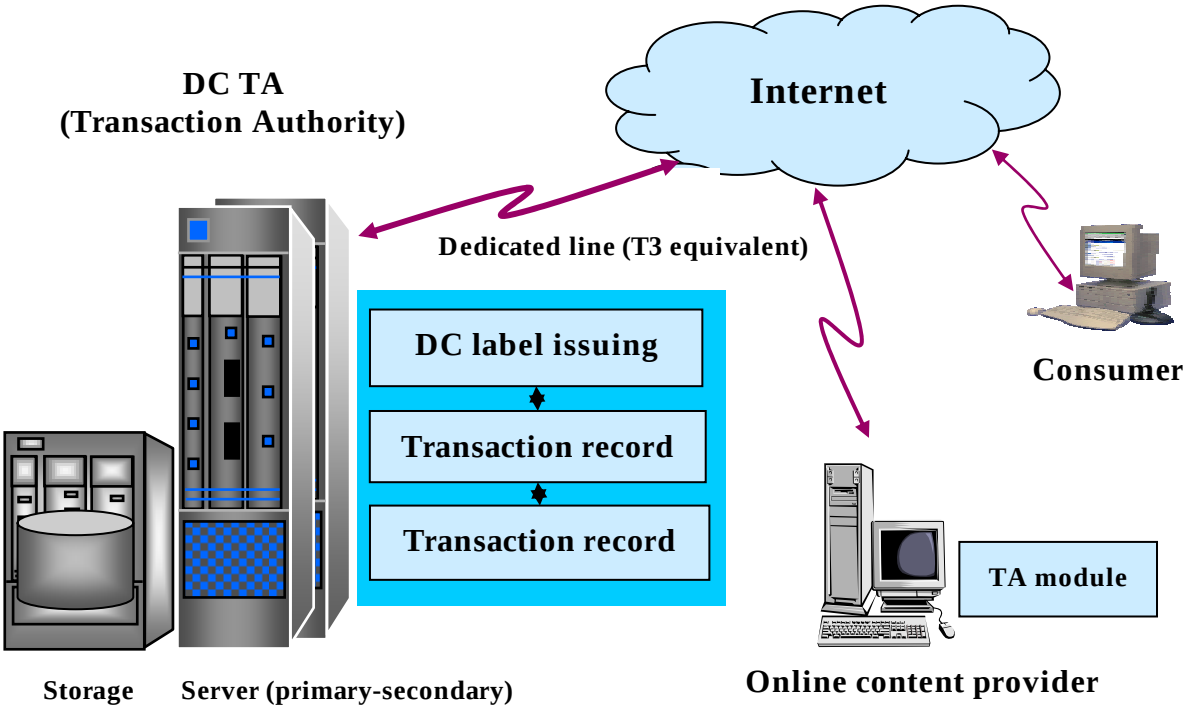
Authentication/Verification Activity of transaction record & facts between parties exchanging contents by DC Transaction Authority



For trusted network of circulation, there needs transparent route among contents owner, consumer, and online content provider. Above picture shows the structure after DC Authentication is deployed.



3.3.3 Configuration of the system



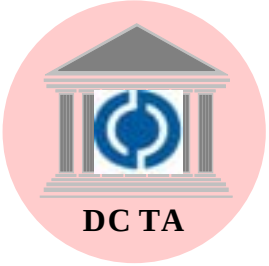
3.3.4 Effects

DC manufacturer
(Copyrighter)

- Boost DC manufacturing
- Protect copyright
- Guarantee stable income

Consumer

- Pay the amount of DC
- Able to use High-quality DC
- Contribution to industry



DC TA

- With reasonable transaction fee
- Build safe transaction environment
- Protect copyright

Online content
Provider

- Transparent transactions
- Convenient environment to us
- Safe transactions

Government

- Tax reduction to company using the service
- Rearrange law/regulations
- Prevent illegal contents

3.3.5 Further development

This model is not commercialized yet. Its commercial approach will be started in the fourth quarter, 2005. Up to now, it is focused to establish a structure of trusted circulation network of digital contents. As next step in 2006, DRM function and related function for more security will be added to current structure.

3.3.6 Other issues

DC authentication is initial stage to be implemented. It is also researched for customers to use this structure more easily and for contents provider to have security preventing illegal copies.

3.4 “Medical and Healthcare Network” (Japan)

3.4.1 Business background

Reforms are being planned in the healthcare industry that will better ensure that patients will able to receive long-term medical treatment. This will involve building a medical information database that, with the protection of many security measures that are currently under consideration, can be jointly accessed by multiple medical and healthcare institutions. Also being planned is the construction of a network that will facilitate distance medical treatment.

3.4.2 Structure of the case

In the vision for this system, institutions, e.g. hospitals, healthcare centers, and inspection agencies, and licensed professionals, e.g. medical doctors, nurses, and pharmacists, will cooperate in electronically recording the examination and treatment history of the patients as well as the patients’ personal health information. It goes without saying that a high level of security will be required. High levels of security will also be required for electronic bills, electronic bill payments, and electronic purchasing of drugs and medical equipment. Figure 1 demonstrates how the business base for PKI in the healthcare industry will be realized through the cooperation of industry stakeholders.

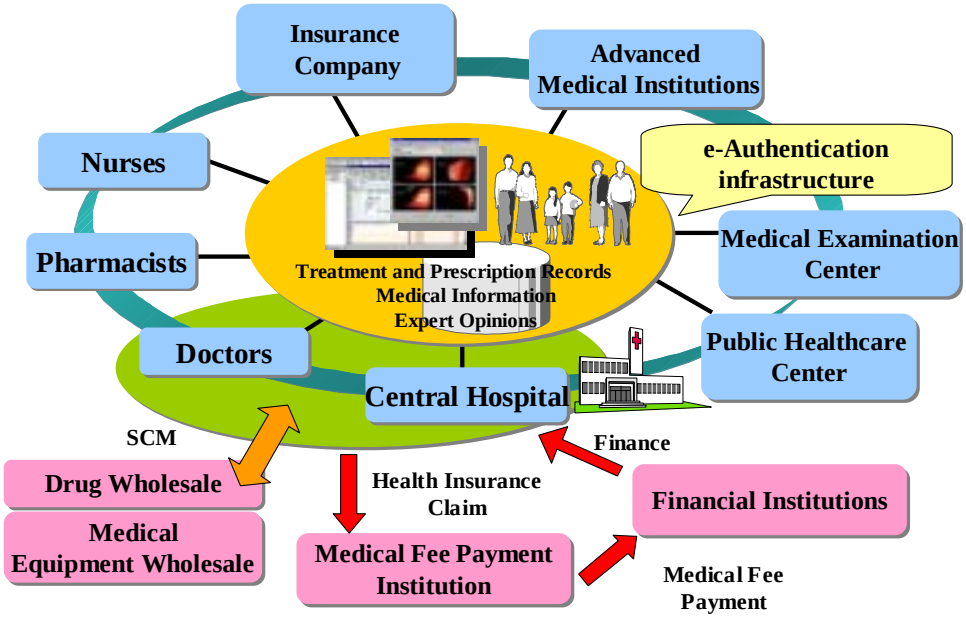


Figure 3.4.1 Application of PKI to the Medical Field

What the people want today is a more comprehensive healthcare service that will aid in maintaining and promoting their health for the duration of their life. Spurring on this call for a better healthcare system is the sharp appreciation of prices caused by the aging of society and the current stringency of health insurance plans due to the stagnation of the economy. In response to this, the industry is trying to hold down prices and generate a new healthcare service industry. The following figure presents a model of the new services created to answer the need for enhanced healthcare.

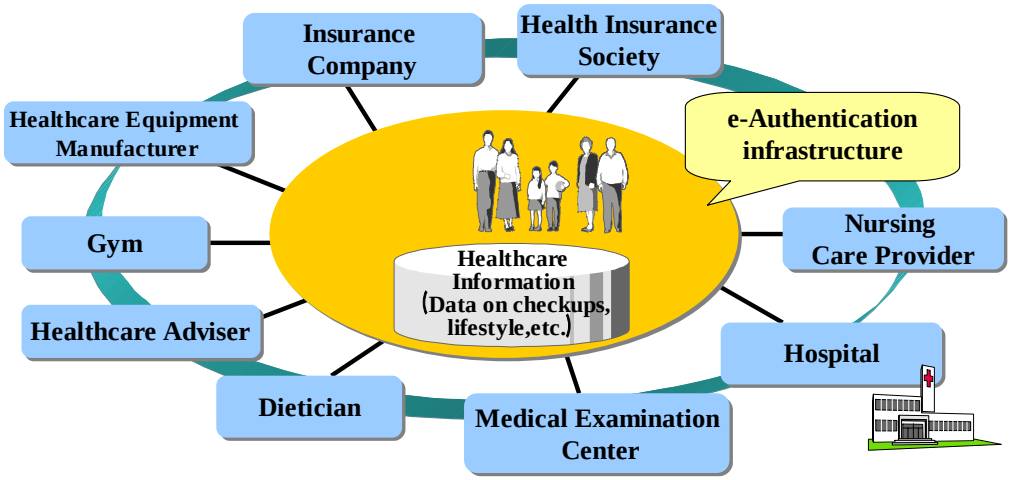


Figure 3.4.2 Application of PKI to Healthcare Promotion

3.4.3 System configuration

In December of 2001, the Ministry of Health, Labor and Welfare publicly announced its "grand design for the digitization of the medical field." Around this central impetus, a national strategy has developed to enhance the medical industry through the use of information technology. The primary components of this "grand design" are the establishment and diffusion of an electronic system for medical records and one for health insurance claims. As for the utilization of PKI, this grand design will also involve a certification system for individuals and their qualifications. Using PKI, the system will confirm the qualifications of both the medical service provider (the doctors, nurses, etc.) and the service user (the insurance holder) and will automatically register the user's medical information.

Among the issues being brought up concerning the infrastructural base for certification technology (commonly referred to as HPKI), one is the debate about the qualification confirmation of medical personnel. Under the given HPKI framework, the system will not only be able to confirm the natural person, the same way it is done by the public certification service for individuals, but it will also be able to record on a certificate the national qualification information of a person in the healthcare field – e.g. medical doctor, dentist, pharmacist, nurse, care manager – in accordance with international regulations (the hcRole of ISO/TS 17090). Thus, if HPKI is implemented, documents that had once required the seal of a doctor, documents such as a letter of introduction to a new healthcare institution (i.e. a letter providing the examination and treatment information of the patient) and examination reports that need to be attached to various applications such as worker's compensation will be digitized and made immediately available online. As of 2004, the industry has begun drafting a common Certification Policy (CP) for all healthcare fields. The plan going forward is to set forth the details of the HPKI system and the reliability structure for the HPKI system that will be built based on this CP and to then consider running a demonstration experiment.

There is currently no precedent in PKI utilization for the services that confirm the qualifications of service users (insured patients) or that automatically transfer personal data. What is being proposed here, however, is the replacement of the health insurance certificate with an IC card; and there is

a performance record for the use of IC cards with insured people. This precedent was established by the Social Insurance Agency in an experiment it conducted in Yatsushiro City of Kumamoto Prefecture that began in 1995 and lasted for almost 10 years until September of 2004. During the operation, nearly 80,000 IC cards were distributed, one card per person, to people that were members of National Health Insurance, Government Managed Health Insurance, or one of many corporate health care groups, and who were patients of over 95% of the city's medical institutions. Because the period of operation was so long, the general users could be firmly established. The operation consisted of two main systems: a reception desk system and a medical history display system. The reception desk system was setup to reference the information of the insured person. Under the system, if the card was lost or stolen, the information on the card could be invalidated by submitting a written statement. Under the medical history display system, each person's health examination history was stored in the IC card enabling users to reference medical check-up information and other health related information through a terminal. The access cards distributed to medical personnel were managed so as to restrict their access to the personal information of unrelated patients.

3.4.4 Effects

As is envisioned by the HPKI framework described above, the importance of the healthcare field including medical treatment will only grow in the future. As it does, the generation, storage, and utilization of information concerning health and medical treatment will become important services. From the beginning, it has been said that the most effective measure for reducing medical and social welfare costs is the prevention of sickness itself. Thus, while individuals will have the need to access general information pertaining to health and sickness prevention, they will also need to access information about themselves. The contribution of PKI is the construction of an environment in which this information is securely encrypted and in which access to this information is safely regulated.

3.4.5 Further developments

Currently, the Ministry of Economy, Trade and Industry (METI) is implementing

the “Support Operation for the Generation of a Healthcare Service Industry (fiscal year 2004),” a project whose goal it is to generate a new industry in the healthcare field. In each region of the country, frameworks are being built for the generation of new business models and IT utilization is being explored.

In one example, Kumamoto University, Kumamoto Prefecture, Japan Red Cross Society Kumamoto Healthcare Center, and Kyuden Infocom Company, Inc., have come together to form the Kumamoto Healthcare Infrastructure Promotion Consortium. This consortium aims to generate new healthcare services by utilizing a foundation of regional healthcare data banks. Having recruited a monitoring group now numbering in the hundreds, the project says it is in the development stage. By utilizing the regional healthcare information data banks setup within the data center, the consortium is interested not only in providing health services for individuals, it is also engaged in supporting the cultivation of a new healthcare service industry.

3.4.6 Other issues

With respect to the fields of medical treatment and healthcare, issues have been raised on how to properly manage the storage and transmission of medical and healthcare information. There are concerns about how to prevent interception and fraud on the networks for example. In another instance, the discussion about the joint ownership and collaborative utilization of the healthcare network databases came up against the question of what to do about the external storage of healthcare information. Institutions like the Japan Medical Association will not back down in their cautions about external storage. It is clear that going forward the issues of information security management at medical institutions, including the question of external storage, cannot be avoided. The demand for an infrastructural system that would provide a quick solution to such problems is very strong. PKI being a viable provider of this solution, the market for PKI utilizing businesses is now ripe.

3.5 "Electronic Account Receivables for Small-Medium Enterprises" (Japan)

3.5.1 Business Background

In the field of small-medium enterprise financing two general reforms are needed. First is the simplification and streamlining of the financing processes in order that the capital procurements of SME's can proceed more smoothly. Secondly, the paperwork for credit guarantees can be made more efficient and credit information can be enhanced so as to reduce the financial risk of financial institutions. One specific need, for example, is a speedier collection of account receivables by SME's and the more efficient use of these account receivables as deposits for capital finances.

What is necessary in order to make this process more efficient is the safe and fast circulation of financial information. A great deal of attention is now being given to the representative business model of electronic account receivables, a possible answer to this need.

3.5.2 Structure of the case

The electronic signatures and electronic authentications of PKI can ensure a fast and secure circulation in what is expected to become a high liquidity loan market where account receivables are transferred and re-transferred.

An electronic billing service has already been established by the Shinkin Central Bank in 2003. In their conception for electronic billing, digitization is not merely a logistical mediator for paper based bills. Rather, the digital process serves as the account receivable transaction itself. In other words, the entire life cycle of the loan from its creation, its transfer, its reduction, to its settlement takes place purely electronically.

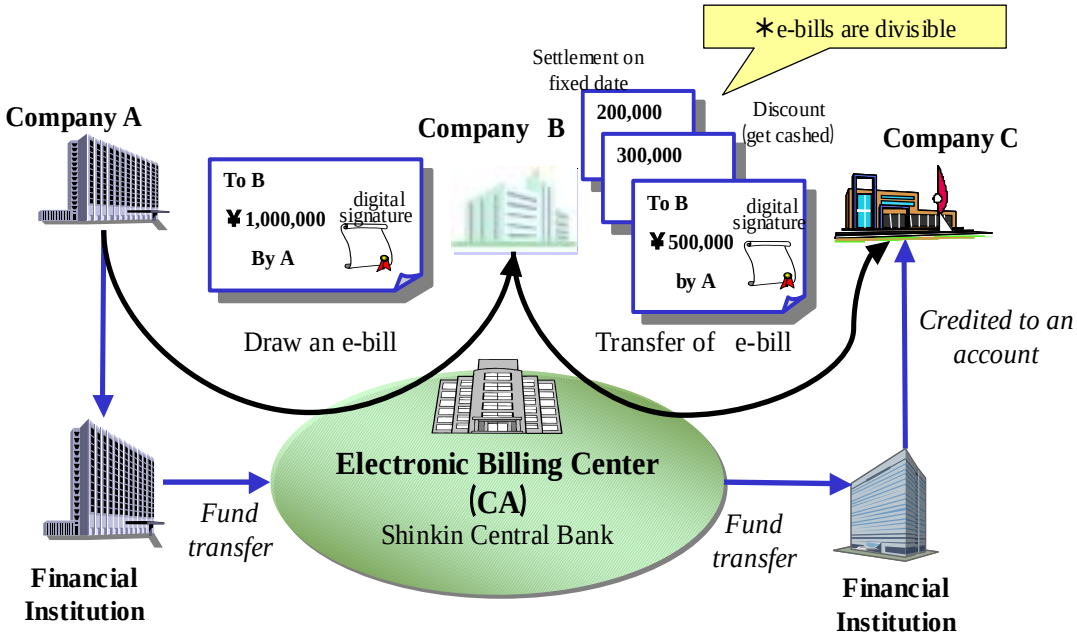
3.5.3 Configuration of the System

In providing its electronic billing services, the Shinkin Central Bank established a Certifications Department and issued Public Key Certificates. The user corporations utilize an online electronic billing platform and are able to

electronically carry out billing transactions – e.g. drawing on their accounts or transferring money – that previously had to be done through paper exchanges. A demonstration experiment for electronic loans, in which the electronic billing service is used, has been underway since December of 2004 in Okinawa. Participating in the experiment are three regional banks, the local Okinawa credit union and approximately 100 customers from these banks. The financial activities being performed through the electronic billing services are not mock activities but actual business transactions.

[Figure 3 Electronic Billing Service]

3.5.4 Effects



According to a report by METI, Japanese SME's (companies with a capitalization of under 100 million yen, approximately USD 1 million) possessed about USD 800 billion in account receivables. In other words, their capital scope was on par with the value of their land. At present however, only a very few companies are using these receivables as deposits for capital finances. The diffusion and circulation of electronic loans can greatly enhance the financial procurements of SME's.

Under the current laws and regulation, however, the risk of an overlap between an electronic loan processed through the system and another loan processed through paper still exists. Many are now demanding that

legislative measures, such as a law on electronic loans, be taken to secure the safety of such transactions. If such laws are successfully put in place and e-commerce sees the development of an electronic loan system that encompasses the whole cycle of a loan from establishment to settlement, the system can be extremely effective. In other words, combined with the streamlining of financial procurements, the acceleration of commercial transaction and the reduction of loan management costs will bring about great advances in efficiency.

3.5.5 Further development

Electronic account receivable financing is another viable business model with respect to the electronic billing business. This is a service that is actually being provided, as of June 2004, by the financial service provider Gallia Plus and the accounting type IT vendor Miroku.com. The aim of this service is to stimulate finances by targeting the market for mid-level interest rates that lie in between the low rates of financial institutions like banks and the high rates of commercial moneylenders. By electronically storing the credit information of SME's that request capital, they are able to conduct the investigation process much more efficiently than other financial institutions.

Gallia Plus and Miroku.com are also collaborating to provide an ASP service that conducts account receivable financing investigations through the Internet. Public Key Certificates are used to authenticate users who log on.

3.6 PKI applications in e-Government (Chinese Taipei)

3.6.1 Business Background

Taipei City Government is striving to make Taipei a competitive international metropolis within this restricted land area. It can only achieve this goal by replacing unnecessary physical journeys with electronic ones—in short, by creating a cyber-city. (http://english.taipei.gov.tw/TCG/index.jsp?recordid=1994) PKI stands for the multi purpose card system, secure e-mail system, attendance management system, and personal document encrypt/decrypt system at this amazing and

world first project.

The other one is e-Land county government, to build up a digital signature authentication and management system for single sign on and dual-smart card solution.

3.6.2 Structure of the case

In this e-Government project, hardware token/IC smart card stands on an important place. Smart card could provide authentication and identification for single sign on login purpose. And then the validation authority system coordinated with different CA on internet to provide the certification though internet. In this multi tier structure, the end customers, such as: government staffs, employees of supporting companies, citizens, and other related members, the authority identified institutes, and other information nodes knit this complex system together.

For example, e-Government though different interface, e.g. TANet, GSN, and the Internet, to connect or log into the services systems, such as e-Document, e-Taipie Portal, e-Citizen, and Computer Education Center. The backend databases, uPKI system, validation service center, and so on will provide the back end support, authenticate, and certify for the front end services. Figure 1 show where does ARES uPKI stand on this e-Government project.

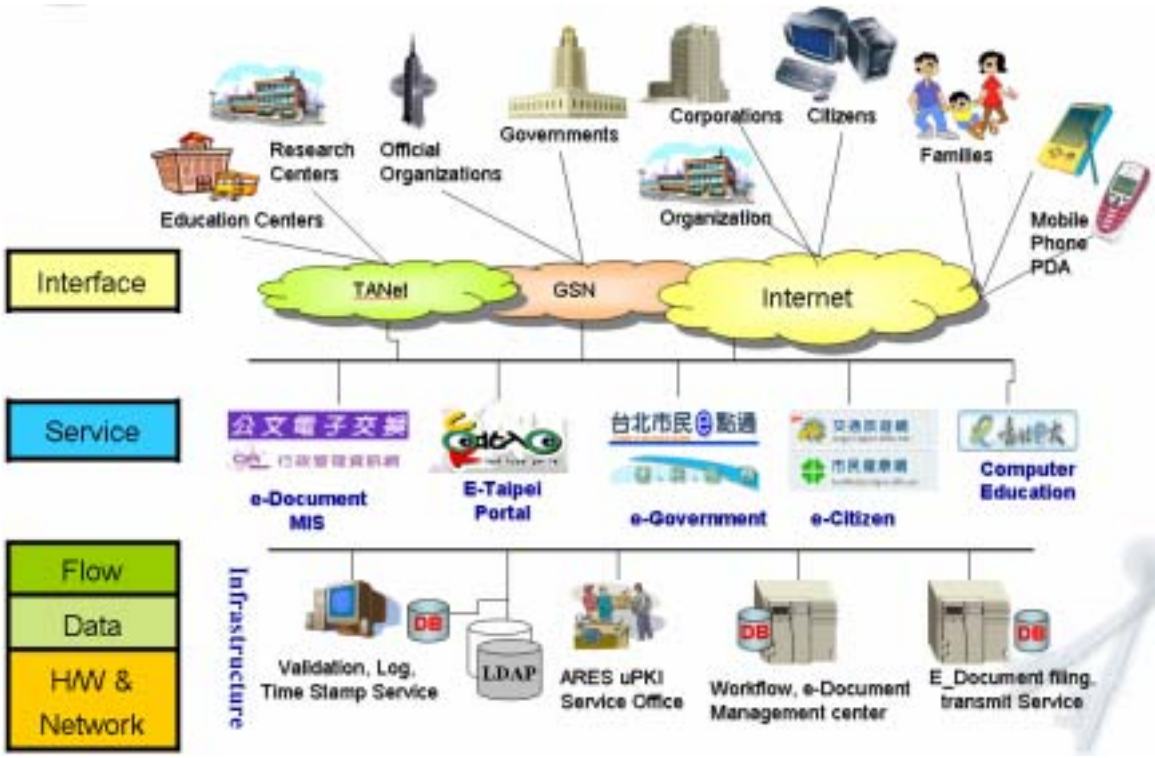


Figure 3.6.1 e-Government conceptual structure

3.6.3 Configuration of the System

The major propose of the uPKI system is to verify the digital signature from smart card and single sign on system. The mainly schedules are 1. Using smart card to login by entering account/password or digital signature (smart card); 2. Authentication at single sign on system though the uPKI security API; 3. Verify the digital signature at uPKI validation authority system; 4. Log and record the important transaction data; 5. Retrieve CRL from each CA by schedule. Figure 3.6.2 present the uPKI system architecture of e-Government project.

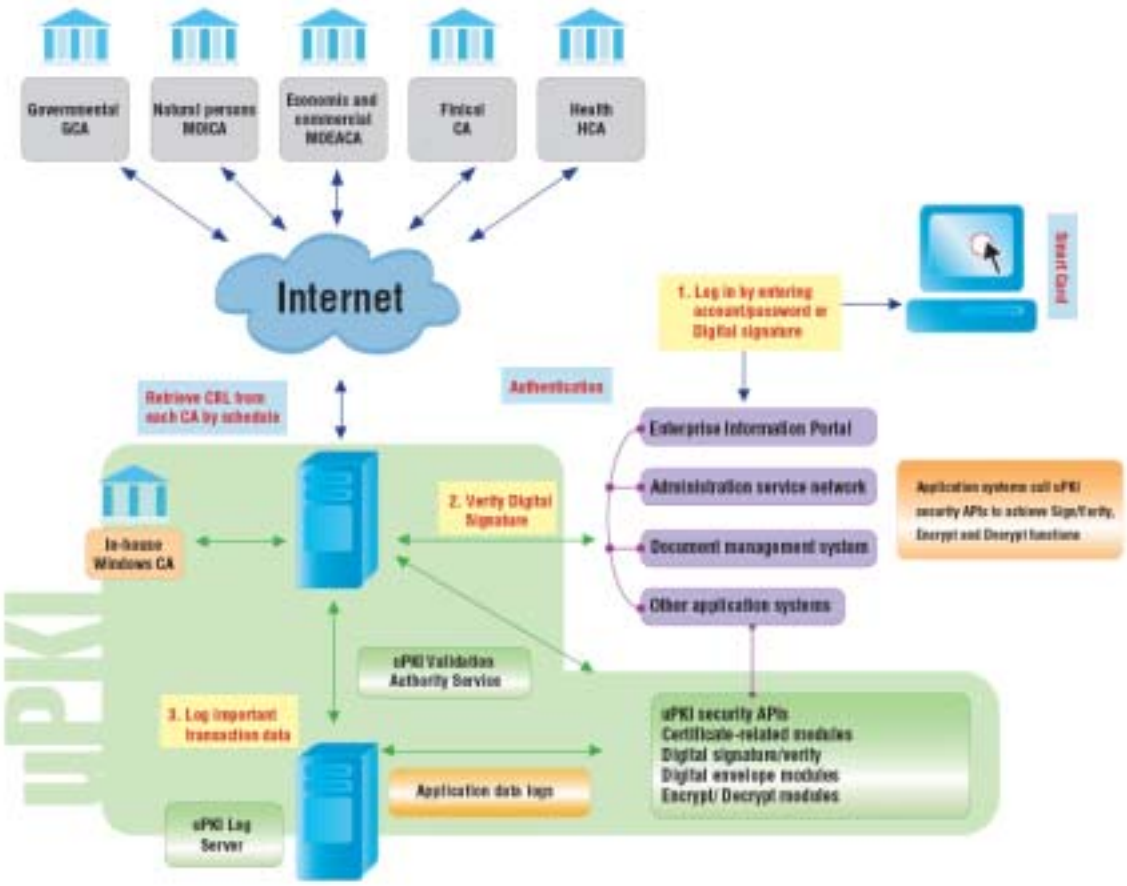


Figure 3.6.2 uPKI System Architecture of e-Government

From the software point of view, the uPKI system was built between PC/SC interface and IE browser. We used standard and non-standard API to communicate each other and coordinated with certificate, XML, CRL, OCSP, and other protocol and technology to provide the highly security, integrity, and easy identification. Figure 3.6.3 show the architecture by each layer and mark the self develop software made by ARES.

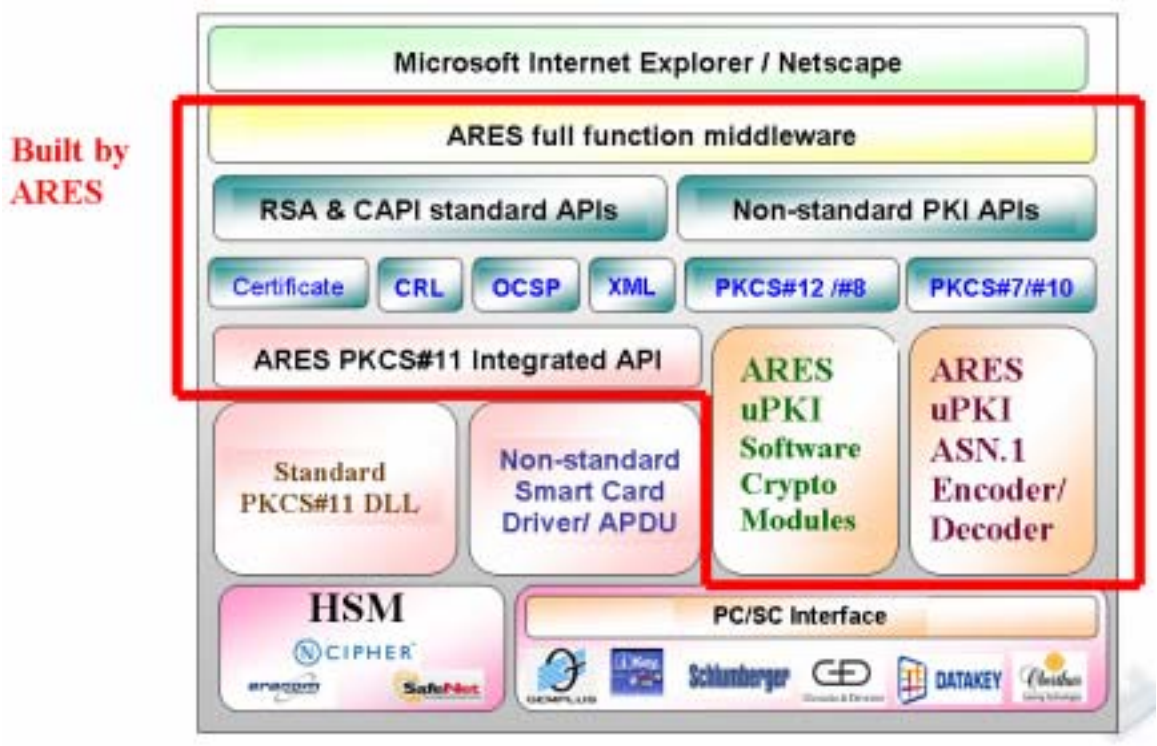


Figure 3.6.3 uPKI S/W architecture

3.6.4 Effects

The uPKI module provides a secure, integrity, convenient management and using system for every citizen, employer, and government itself. This project brings the efficiency and security though the Internet and multi secure settings. The main expectation of this system will be to give every citizen a new and convenient government service and get a higher satisfaction. For example, the Taipei-eLife.net almost have 400,000 visitor visited in these short days. Up to now, the poll and the survey of the e-Government so far are pretty incredible. People pretty like this multi purpose card and online government services.

3.6.5 Further development

The Research, Development, and Evaluation Commission, Executive Yuan has an eTaiwan project http://enable.rdec.gov.tw/eng/index.htm). uPKI just one of the important component of the G2B2C project, which is one of the eTaiwan leading project. All the central and local government will continually develop their uPKI system and will be combine and connect together afterward. Thus, every citizen of Taiwan could easily though the Internet and

other interface to access the services online. No mater the territory lies on central or local government.

3.6.6 Other issues

The e-Government project must be changed the usual life of every single citizen of Taiwan in a very soon future. That means the e-Government may bring the new custom for that people already used to before. We can expect some important issue while and after the e-Government system had been built.

The first one is the information security issue. Every personal detail info of each person will be stored in the government database. People could easily access their information online to apply ID or recharge the transportation card. But we still need to consider the security problem. The more easy and convenient way usually means the more danger way. The network and information system should notice this issue and prevent its damage.

The second one is the people expectation changed. That means people will rely on the information more than before. Even the employees of government will lean on the electricity mail rather than the original physical mail to communication and recording. That may bring more efficiency but still need to find another way to keep it safer.

The third one will be the information education. If we want to let the e-Government more powerful and more popular, the end-users information education is the key point. No mater the data keyin staffs or end using customers, providing highly information education for each of them will be more important then before.

However, we still look forward the new era that e-Government will bring in.

3.7 "Expanding Finance Certificate Application Range" (Chinese Taipei)

3.7.1 Business Background

There are three major topics relative to Finance Certificate Application: Online Bank, Stocks/Futures Online Trading, and Online Insurance and Other Application.

(1) Online Bank:

Online Banks provide their clients/customers services including funds transfer, taxes paying, expenses paying and some other transactions online by connecting to Bank's Website open for 24 hours a day and 365 days a year. In addition, under Taiwan C Program –Money Flow Operation, industries are provided for: paying on-line for Purchasing Operation, financing on-line for Production operation, financing dispatching on-line for Financial Management, and automatically canceling account for collecting and paying bills operation.

Currently, enterprise clients directly designate bank for payment, the money flow and the electronic business affair are not integrated. Business transaction security is looked at attentively.

Furthermore, the bank chip card changing ratio was low, and it was 8-10 million cards till late 2004. Since the bank chip cards reserve the storage space for certificate, the upgrade policy for bank card will be the big advantage for popularizing PKI.

(2) Stocks/Futures Trading On-line:

The Stocks/Futures Online Trading is launched for years as one of the major trading methods. Additional, SECURITIES & FUTURES INSTITUTE (in Taiwan) allowed the shareholder can e-voting online at shareholder's committee.

(3) Online Insurance and Other Applications:

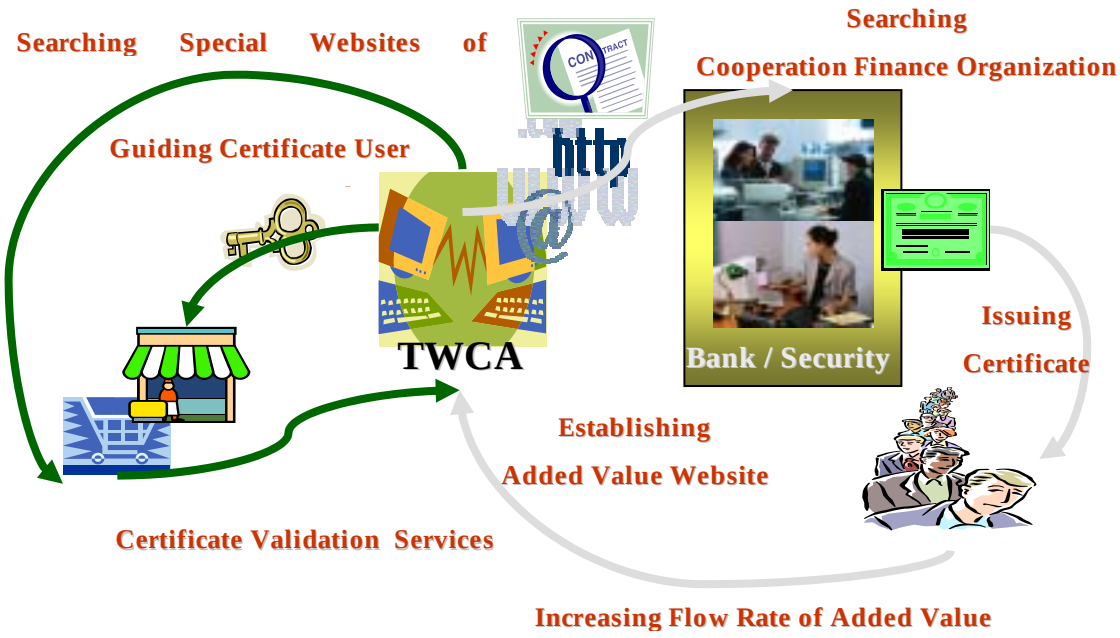
Online Insurance provides: third-party liability insurances of car/motorcycles accidents, and travel insurances. There are some other applications relative to electronic documents guarantee services, electronic check, and electronic document exchange services.

All of these financial PKI application must be integrated because the establishment of financial holding corporations. Taiwan's financial industries are consolidated secondly, fourteen financial holding corporations will become to half before late 2006 expectantly. They needs unified token, unified API and unified PKI hierarchical to let all issued financial certificate can be used in each field.

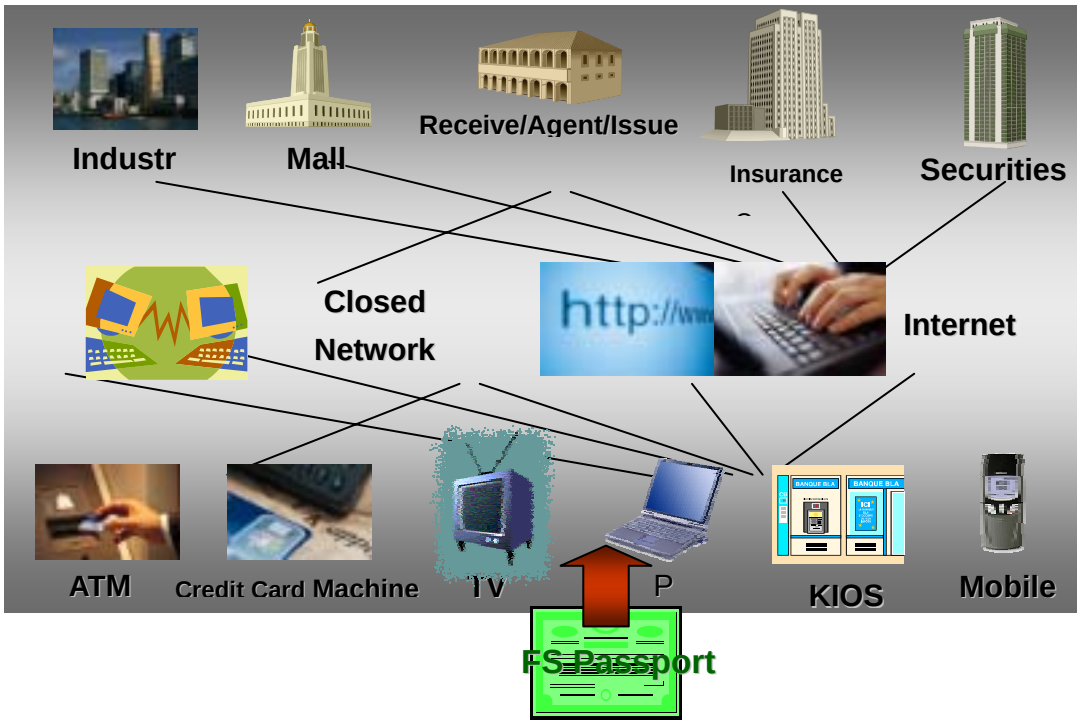
3.7.2 Structure of the case

System Framework

The picture shows the stakeholders of Certificate Application Service Value Chain. TWCA Certificate Added Value Website performs the vital role of the case.



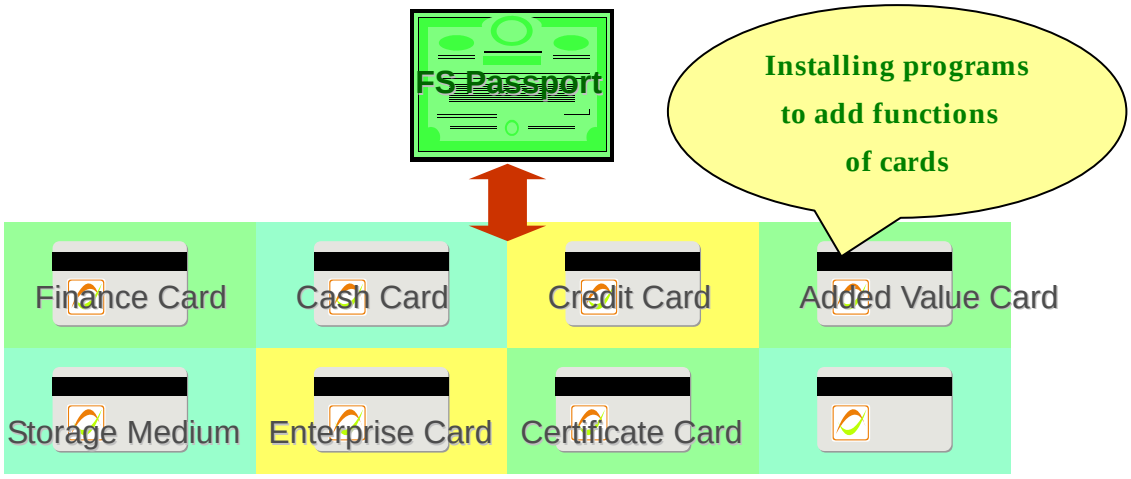
The bellowing picture shows that Financial Service Passport (FS Passport) offers quite completed services in e-Commerce. Here the functions of **Financial Services Passport** applications are clearly shown.



3.7.3 Configuration of the System

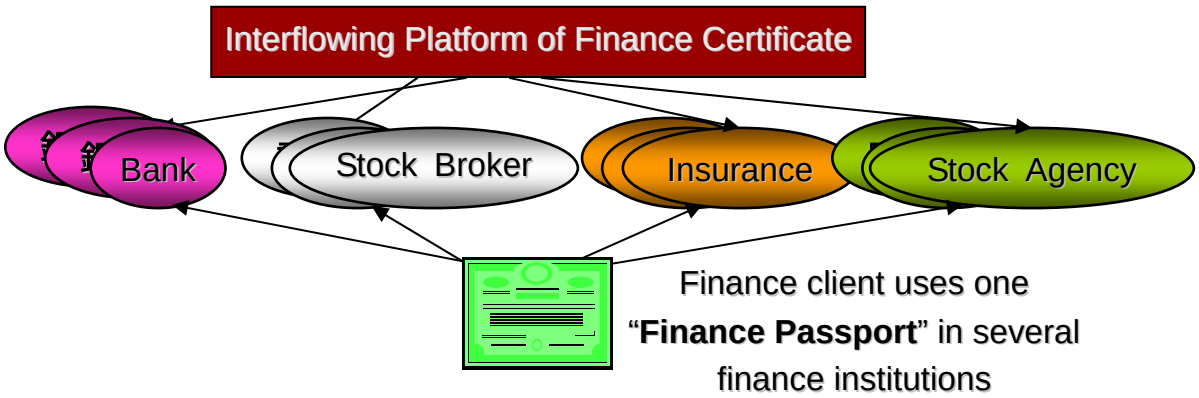
Security foundation construction generally comprises numerous effects. Universal foundation construction of Finance Passport can be generally used for various finance business transaction and other electronic commercial affair business transaction, and can be added appending security organization, password for example, due to business characteristic. Integration of substance transaction and virtual transaction promotes the value and user's will to utilize, and supports various commercial applications effectively. Digitial Certificate plus Chip Card is one of the most practicable molds of Finance Passport for information security foundation construction. Additional, for the added value application feature of Finance Passport, finance institution provides the security organization for other electronic business affairs transaction, and supports the integration of information flow and currency flow.

The below picture illustrates the Function of FS Passport.

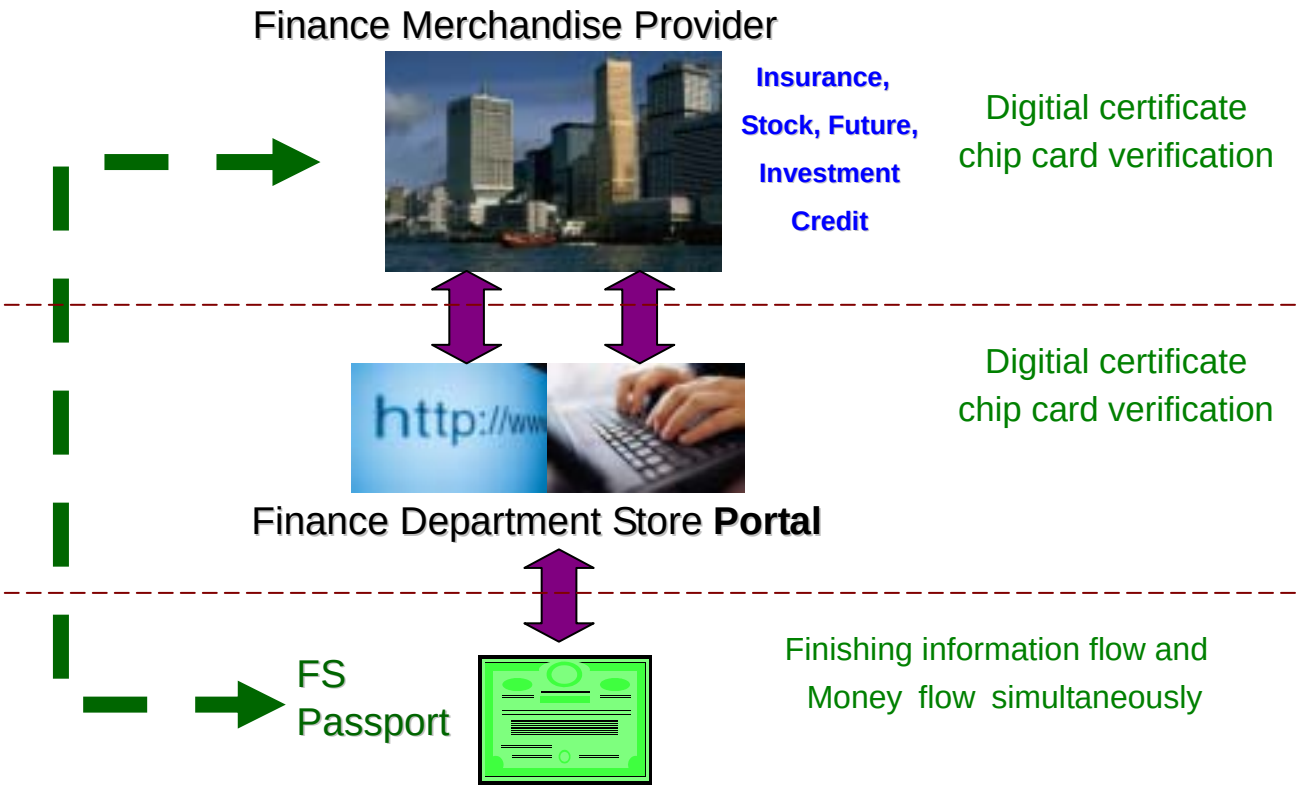


The Functions of Chip Cards defined by Business catalogues

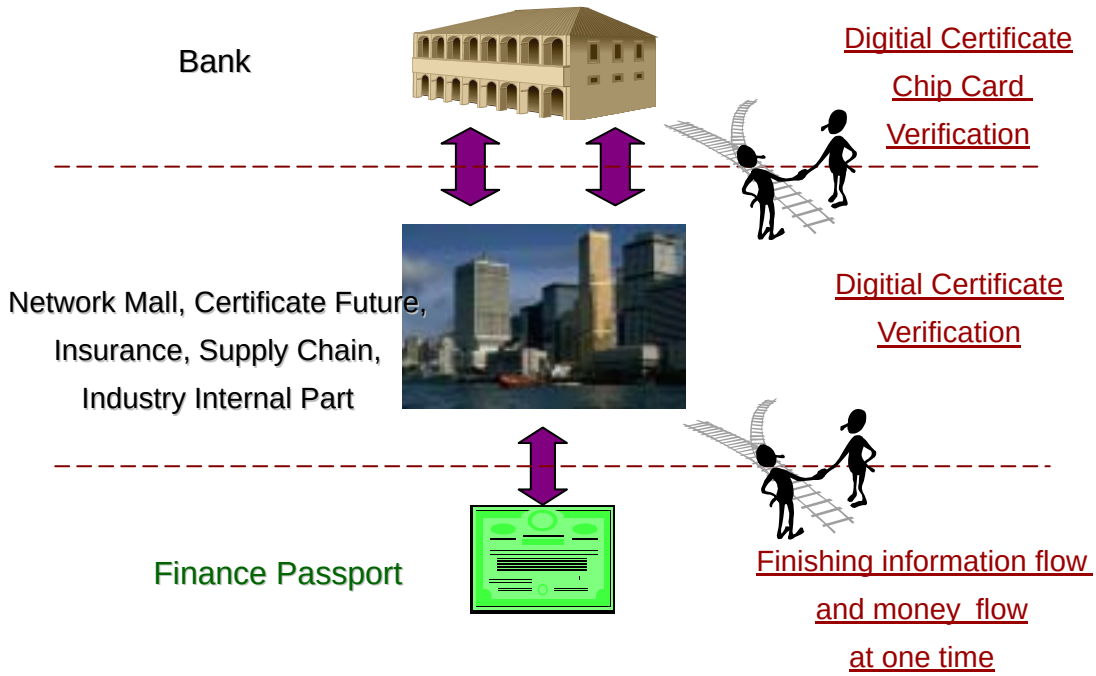
The below picture shows that user can travel with Finance Passport everywhere. Digitial Certificate user is attracted that the certificate is like a "Finance Passport" and used in any finance institution. Digitial Certificate can be combined with Chip Card into the Finance Passport Card. It accelerates integrating finance controlling, and extends the attraction of different trade alliances, such as certificate, future, insurance, to increase profit.



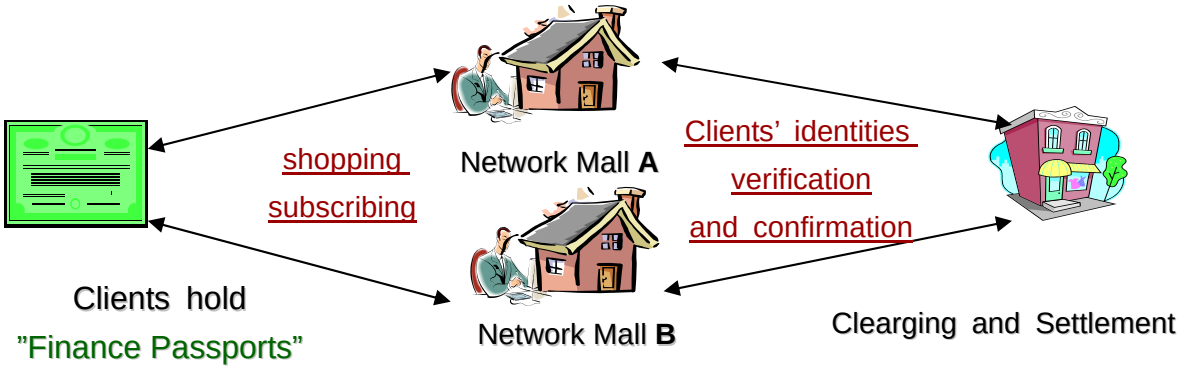
The below picture illustrates one application of Finance Passport: Purchasing Finance Merchandise.



The below picture illustrates another application of Finance Passport: Electronic Business Affair Transaction.



The below picture illustrates another application of Finance Passport: Function of Credit Card. Issuing bank allies with network/substance mall. Client shops and uses credit card with Finance Passport in stores. Utilizing Finance Passport, store manages associate's, accumulates bonuses, and sales electronic gift coupons to promote marketing. Transaction security is protected.

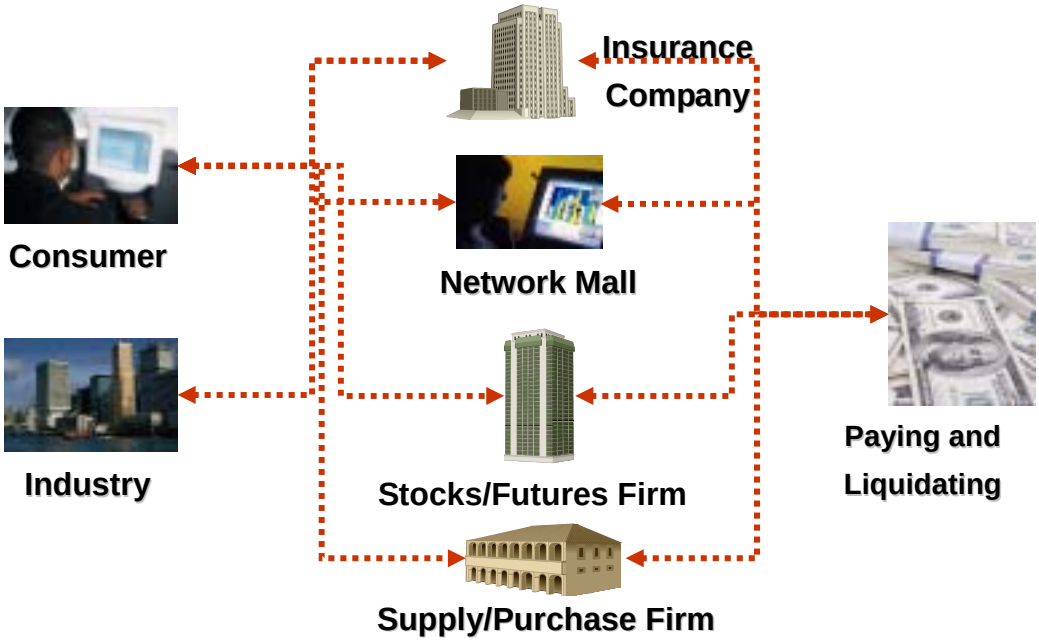


3.7.4 Effects

Finance Certificate Application Business is expectable. On of the development tendency is Integration Financial Service. Under finance controlling corporation structure, integrated finance service will be normalized. The manage money commissioner assists client with various finance business transaction, such as insurance commerce service, stock agency service, stock/future/fund commerce service, investment credit /investment council, deposit remittance service, and new finance merchandise service.

In addition, finance merchandise One-Stop shopping is practicable. Integrated finance service comprises several advantages: one's own finance controlling corporation's finance merchandise, agent marketing or agency other corporations' finance merchandise, and buying all finance merchandise at one time.

The below picture illustrates integration of information flow and currency flow.



3.7.5 Further development

Expanding Certificate Value-added Application regions will be the future perspective of the case. Include:

- Associate login and management organization
- Transaction on-line
- Auction on-line
- Digital content and learning
- E-Ticket of concert, movie, and bus or train
- Integration of industry operation process and faraway access
- Combination of substance and network: purchasing on-line and substance transaction

3.8 "BAROC FXML UCA & i-Security Integrated Trading Security System" (Chinese Taipei)

3.8.1 Business case background

***Industrial Automation & e-Business Promotion Program by Governments**

- Under the trends of Global e-Business, Executive Yaun enacted the project of "Industrial Automation e-Business Promotion Program (iAeB)" in 1999 to drive B2B e-Business, Then, Ministry of Economic Affairs designed the e-Business Project for the IT and major Manufacturing Industries, which were so called as Project A and Project B.
- The Ministry of Finance commissioned Bank Association R O C (BAROC) to plan the money flow project of domestic e-Business. Thus, BAROC set up the "XML-based Inter-bank Common Platform (ICP)". Moreover, under the request of the Ministry of Finance, each member bank of BAROC has to join and to build the money flow platform for the C Project before 2004.

***Plan A、B、C、D、E**

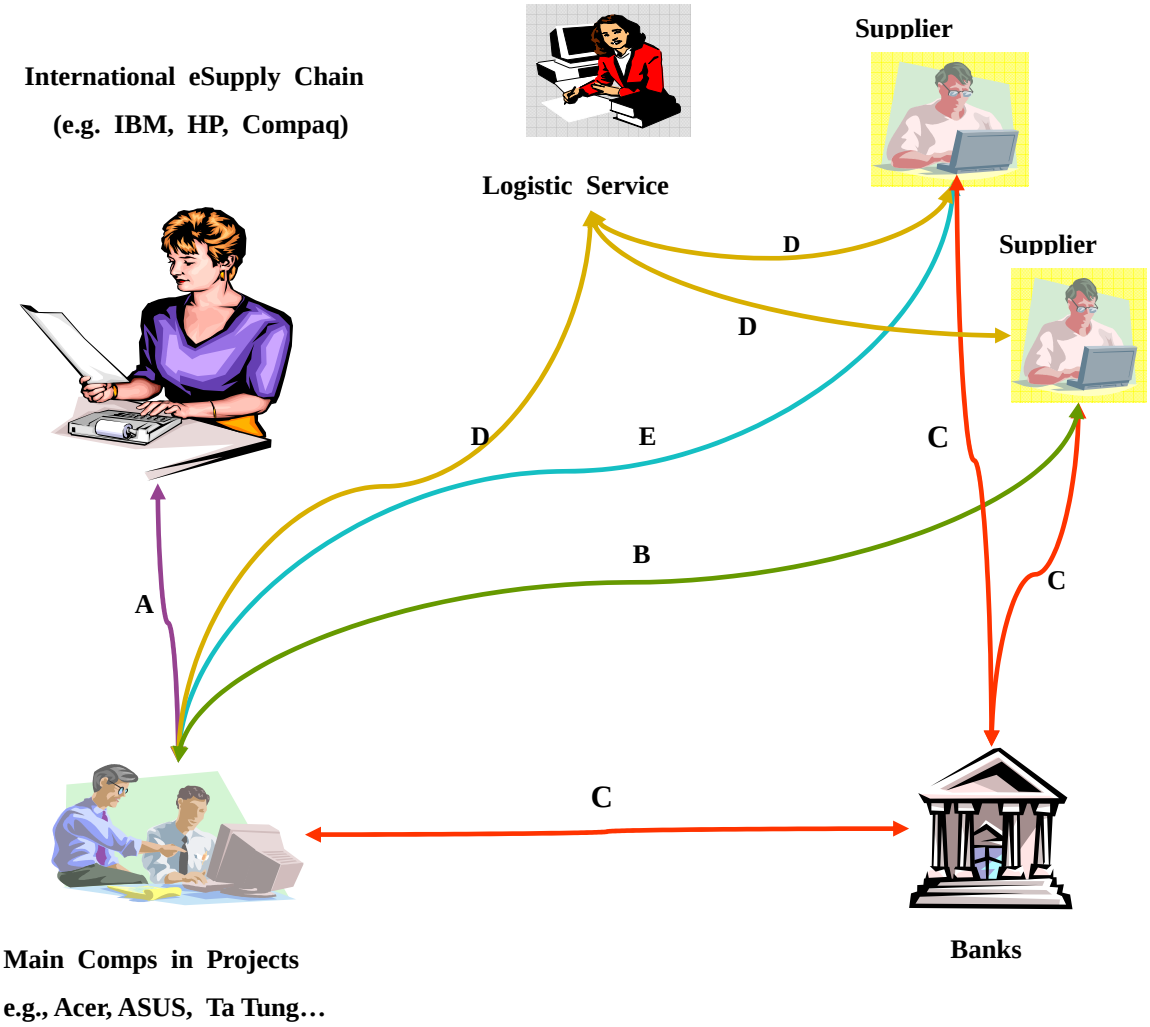
- **Plan A:** Build up e-Supply chain system which could be connected to international procurement system.

- **Plan B:** Build up the e-Process ability of domestic companies by leveraging large enterprises that can drive their small and medium sized suppliers and forming the e-Supply Chain.

- **Plan C:** Accelerate e-Payment, on-line finance, on-line capital management...etc

- **Plan D:** The main points of the plan are the tracking of operation and transportation and logistics...etc.

- **Plan E:** Motivating R&D capability of industries by facilitate the exchange of the R & D knowledge, R & D experience and R&D elements...etc

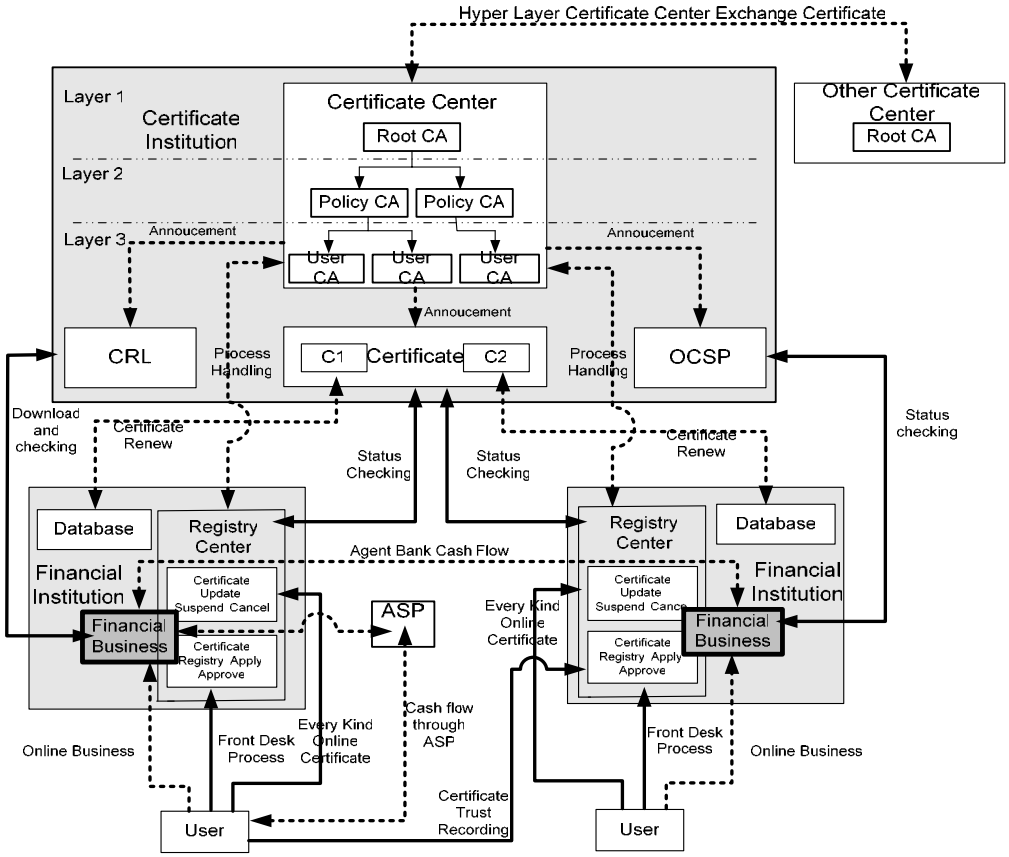


***The PKI Requirement in Plan C**

- PKI mechanism is applied in the high-risk money flow service in plan C—Plan C contains Taiwan Finical Root CA (TFCA) and user CA.
- PKI is much popular in banking services fields. But it has different applications, such as EDI or on-line banking. That is, banks have incompatible PKIs. The problem of interoperability always impedes the motivation of PKI.
- Bank Association ROC defined "Finance XML Certificate Policy" in order to make the e-commerce domestic certificate policy successful.

3.8.2 Structure of the case

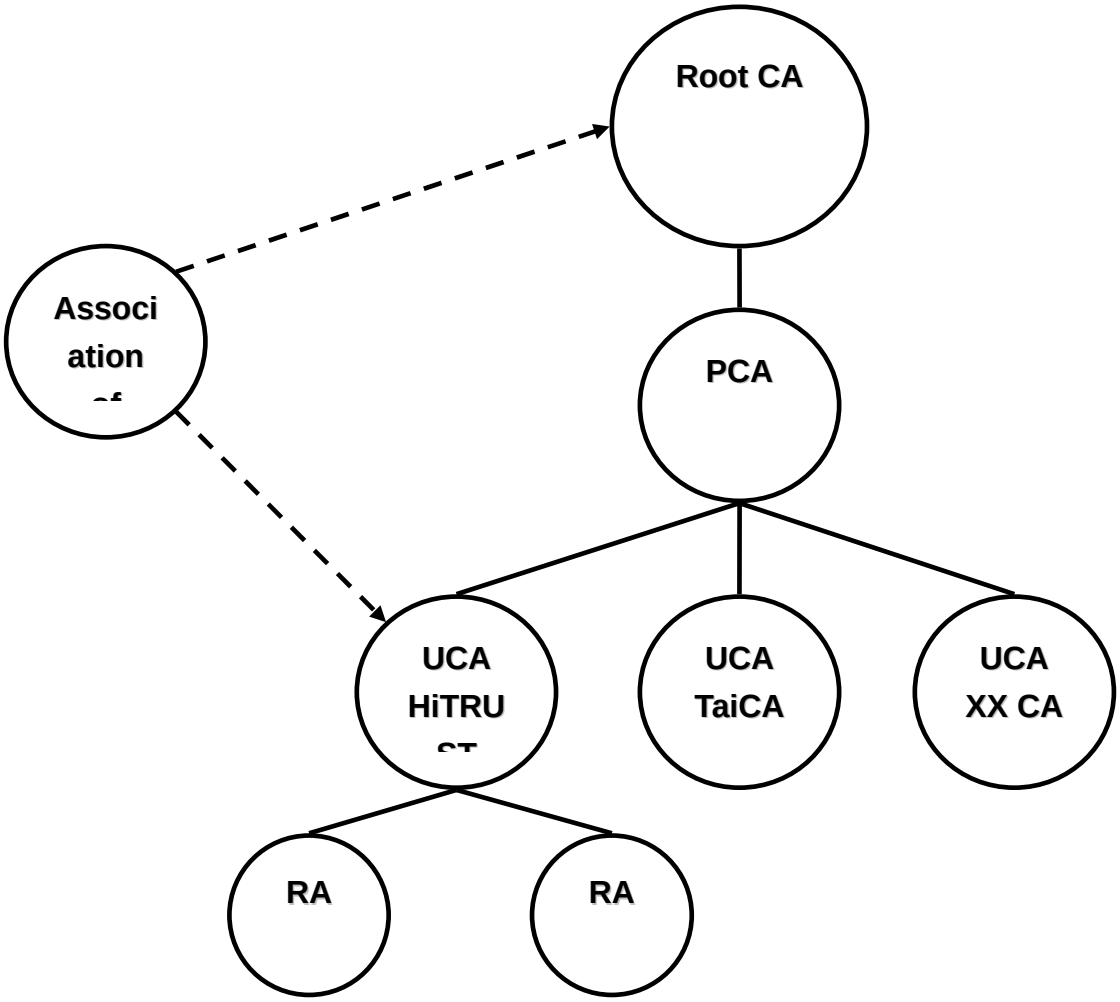
The Structure of Common Regulations of Technique



FXML UCA Service

- Using VeriSign Managed PKI Service
  - Dual Key System
  - End Entity Certificate Profile and modifying it with the association's regulations.
- If certificate policy service providers were qualified, they need to get the PMA certification of the association of banks, and then they can provid the UCA service.
- Granting the certificate of registered center.
- Granting the XML certificate of nature person
- Granting the XML certificate of legal person
- Managing and announcing canceled list and OCSP information.

The Structure of FXML Certificate of the Association of Banks



PMA： The certificate policy management association which is composed from the association of banks manages RCA and grant UCA.

i-Security Integrated Security System

- Four main divisions: registered certificate center RA, check and accept, encryption, and certificate management
  - Providing the system of Bank register and certificate, providing the application, suspension, lifting a ban, and cancellation of certificate.
  - Providing banks and customers the management of certificate.
  - Providing the checking and accept of e-finance documents.
  - Providing the decipherment and decipherment of e-finance documents
- HiTRUST has abundant experience of development and service of finance application programs. We can provide lots of service such as

Payment Gateway, eCheck,...etc.

- Providing total solution (containing certificate service and manage software.

3.8.3 Configurations of the system

i-Security Trading Security System

- W3C XML Signature regulation.
- PKCS#7 electrical envelope regulation
- Common Regulations of Certificate Management System
- Common Regulations of Registering System
- Providing Internet Explorer ActiveX Certificate Module
- Providing Internet Explorer ActiveX Checking and Accepting Module
- PKCS#11 the basic code management system (Extended)

3.8.4 Effects

- Hitrust making lots of profits in 2002 and 2003
- Other Business of Finance application program (e-Check)
- The profit of finance application program is much higher than PKI service.
- UCA Customers:
  - Hua Nan Commercial Bank、Chang Hua Bank、Far Eastern International Bank、Taishin Financial Holding Co.、Taiwan Business Bank、Jih Sun Holding Co.、Hsinchu International Bank、Central Trust of China、Bank of Overseas Chinese、HuaTai Bank、Fuhwa Financial Holding Co.
- i-Security Customers:
  - Financial Information Service Co.、Taiwan Clearing House 、Hua Nan Commercial Bank 、 Chang Hua Bank 、 Far Eastern International Bank 、 Taishin Financial Holding Co. 、Taiwan Business Bank、Jih Sun Holding Co.、Hsinchu International Bank、Central Trust of China、Bank of Overseas Chinese、HuaTai Bank、Fuhwa Financial Holding Co.

3.9 “CORENET e-Submission” (Singapore)

3.9.1 Business background

In the Construction Industry, approvals by various Government authorities are needed before any construction works can commence. Construction plans are typically also exchanged via hardcopies, and these have to be delivered to the relevant Government authorities for approval. The time required for approval by all relevant authorities was very long. There is a need for a one-stop submission system that increases operating efficiency, reduces cost and allows speedy approval of plans.

3.9.2 Structure of the case

What is needed is a comprehensive system for online submission. The business processes in the Construction Industry has to be re-engineered to achieve a quantum leap in turnaround time, productivity and quality. For accountability and non-repudiation, the Qualified Professionals would digitally sign submitted documents using Digital Certificates from a licensed CA. CORENET was thus conceived.

CORENET is an acronym for **CO**nstruction and **RE**al Estate **NET**work and is a major IT master program for the building and construction sector in Singapore. CORENET e-Submission (eSS), which is a subset of CORENET, is a virtual submission system that was developed for Singapore's Building and Construction Industry to ease the approval processes by the various government bodies regulating the construction industry. The initiative is led by the Ministry of National Development (MND) and driven by the Building and Construction Authority (BCA) in collaboration with other public and private organisations.

CORENET e-Submission system is a G2B (Government to Business) internet-based system that enables industry professionals to submit project related electronic plans and documents to regulatory authorities for approval. The System covers all the application types concerning planning approvals, building plan approvals, building maintenance and certification from the various regulatory Authorities, forming a one-stop convenience point for round the clock submission via Internet.

With this System, the public is able to submit electronic plans and documents from their home and offices to 16 different regulatory authorities. In addition, the public is able to track the submission status online at their own convenience.

The System handles project-related documents for whole project life cycle covering processing of plans and documents related to issuance of:

- Planning approvals
- Building plans approvals
- Structural plans approvals
- Temporary occupation permit
- Fire safety certificate
- Certificate of statutory completion

Since 1st July 2002, all building project documents in Singapore must be submitted to the relevant authorities for processing and approval using CORENET e-Submissions. Offline submissions are no longer accepted.

3.9.3 System configuration

Authorities requiring e-Submission include:

- Building and Construction Authority (BCA)
- Central Building Plans Unit of National Environment Agency (CBPU)
- Housing & Development Board (HDB)
- Land Transport Authority (LTA)
- National Parks Board (NParks)
- Singapore Civil Defence Force (SCDF)
- Public Utilities Board
- Infocomm Development Authority (IDA)
- Singapore Power Ltd

PKI is an integral part of the Infrastructure. Qualified Professionals (Engineers, Architects, Electricians, Plumbers, etc) are equipped with digital certificates for digital signing on official documents before they are submitted online. Staffs in regulatory authorities are similarly issued digital certificates to sign on their approval for plans submitted. All documents submitted are archived

securely with the digital signatures intact, and the signatures are verifiable anytime in the future, when required.

3.9.4 Effects

The benefits of the CORENET e-Submission system (eSS) include:

- Providing One-stop convenience to both private and public sectors;
- Providing One-stop point for submission of plans from qualified persons to multiple approving authorities from anywhere, at any time;
- Providing One-stop access for qualified persons to check submission status online;
- Providing One-stop billboard for approving authorities to post submission status online.

CORENET e-Submission has improved work efficiency, reduce turnaround time and reduce the cost of seeking regulatory approvals.

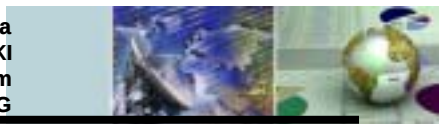
3.9.5 Further developments

An Integrated Plan Checking Systems was planned with the aim to automate the checking process for the various plan types. These are leading-edge systems that require the integration of expert knowledge in plan checking as well as artificial intelligence (AI) and computer-aided design and drafting (CADD) technologies. With these systems, regulatory requirements can be captured more consistently and comprehensively. Any areas of non-compliance with regulations can be detected and amended during the design phase rather than during the approval phase. As a result, less re-submission needs to be done without compromising on the safety aspects of building.

Several government agencies are working together on an integrated plan-checking project to deliver a single plan-checking tool to check building plans submitted by Architects and M&E Engineers for compliance of the various authorities' regulations.

3.9.6 Other issues

The CORENET e-Submission system has been in place since 2002. PKI is an integral part of the system. There are no major issues with the System. Acceptance level is high because of the many benefits of the System.



4. Future approach

4.1 Consideration & Further work

BAWG has been discussed various types of business models for several years. This book covers several representative business models which are reflecting PKI technology and its solution.

We hope that Asia PKI forum members can have more knowledge on newly invented business models and share other region's experience actively. We also hope that we can find a project for all members through exchanging idea about various business models in every area.

4.2 Closing

This is the first time to publish a book in the name of BAWG, Asia PKI Forum. It will be a good start for fruitful discussion among members and industries related to them.

We appreciate members for those who were attended for gathering information, editing and arranging material, and related work for this document.

Business Case & Application

Working Group

Asia PKI Forum

http://www.asia-pkiforum.org