GBDe 2005 Issue Group

Cyber Security
Overview on Challenges and Recommendations for Secure Cyber Society

October 17, 2005

Issue Chair: Mr. Buheita Fujiwara, Chairman, Information-technology Promotion Agency, Japan

1. Overview

This report is intended to give overall view of the issues and challenges facing today's Internet society as well as the summary of current activities to make the Internet world better and reliable, and to present suggestions and recommendations toward the better future of the Internet for the benefit of all the players from governments, to institutions and corporations, to citizens and individuals.

2. Issues and challenges of today's Internet

Hidden vulnerabilities in operating systems and other software are occasionally discovered and exploited to make attacks and frauds. Attacks and malicious use of the Internet include:

- Viruses and Worms that spread over network by itself to give harms to PCs, systems and network,
- Hacking to break into computers to steal information from and wrongly manipulate them,
- Distributing Trojan Horses and BOTs to steal information through Spyware, remotely manipulate PCs to make DoS and other attacks,
- Spams that negatively affect the business efficiency and network traffic,
- Phishing that makes frauds to illegally obtain sensitive information, typically bank account and credit card numbers with associated PINs, and
- Information theft either through hacking, Spyware, Phishing or other frauds.

3. Countermeasures and mitigation efforts

Variety of efforts are being made to solve the issues and mitigate the threats by every kind of stake holders of the Internet, including governments and government agencies, Internet Exchange and Internet Service providers, PC and software venders, IT security tools and services venders, and voluntary citizens. Typical activities to name some are:

- Vulnerability Information Handling Framework in which non-government, non-private organizations coordinates among the vulnerability discoverer, software vender, systems integrators and end users to control the secrecy of the vulnerability and rapid and wide spread of the countermeasure information,
- CSIRT or Computer Security Incident Response Team, formed in many countries and industries, to support users in case of computer emergency and incidents. They also play important roles in vulnerability information handling referred to above,
- International Track Back Network, a international collaboration to trace back the packet flow to identify the origin and the attacker in case of suspected attacks,
- Common Criteria, reference and evaluation standard for security and other products,
- ISMS, the international standard and evaluation framework for information security management, and
- Trust Mark and Privacy Mark, the evaluation schemes for privacy information protection which provide marks to evidence compliance to the requirement.

4. Challenges toward the Future

Further efforts and challenges are taking place by various players and participants of the Internet, both from public and private sectors. Typical activities we should note are:

- Culture of Security, the idea that security should become more common sense and a part of culture. Toward that goal, public editorial initiative, private education services and awareness development efforts are promoted.
- Information Security Governance, an initiative to develop more awareness on security from corporate management perspective. The initiation came from government, e.g. Sarbanes Oxley in the US and METI of Japan. Corporate efforts and actions are expected.
- Next Generation Network has been studied and discussed by variation of Internet participants including academism and industry as well as international organizations to resolve many issues associated with open and flexible network architecture and operation of current Internet.
- Ubiquitous Society perspective also involves features of security in view of RFID going to distribute to every piece of day-to-day consumption and even refrigerator being connected to the Internet. All of those means security is requisite.
- Security Level Evaluation and Digitization Approach being expected as possible indicator of security maturity of a society, such as a country, municipals or corporations.

- Damage Calculation Model for Virus Infection is intended to measure the loss of virus infection and provide decision making metrics for IT security expenditures.

5. GBDe Recommendations and Suggestions

In view of today's headaches on the Internet and activities and efforts to mitigate threats and problems as sighted above, the GBDe would like to make recommendations and suggestions in following points:

- Literacy and Education

  When education effort is successful and certain level of literacy is achieved, people can be aware of the danger of keeping BOTs and Zombies, as well as being compromised by Phishing and Pharming. Thus the social risk should be reduced drastically. So, it is recommended that governments facilitate stimulation for IT security awareness and encourage people to obtain better knowledge of the risk of Internet usage. At the same time, industry players are expected to provide people with Internet security education opportunities either commercially or complementarily.

- Information Security Governance

  Information Security Governance is another aspect of security literacy applicable to corporations and institutions. Company executives should be most aware of threats and potential harms of the Internet in addition to the benefit of it. Such awareness would be realized in implementing Information Security Governance into corporate management. Governments can promote it by introducing encouraging guidelines and incentives such as tax discount, special-aim funds, governmental requirements and recommendations, or law enforcement. Corporations can also pay efforts for Information Security Governance. Security reports as part of CSR is one example. Business continuity planning can incorporate Information Security Governance programs as a part, and will contribute to better corporate management. Thus, Information Security Governance is the field that both government and private sector can work severally towards the ultimate Internet security.

- Next Generation Network (NGN)

  Next Generation Network (NGN) is a bunch of concepts and ideas that provide such positive features to the network as traceability, definitely tagging source and destination, assured service level and security level. When NGN is realized, many of problems facing today's Internet will be solved. NGN can provide a basis for critical telecommunication infrastructure, and the whole network will work to the benefit of all the players in the area of politics, academy, business, culture and human life.

The GDBe is now focusing on the promotion of NGN. The activities will concretely take place towards the next year, and is expected to be influencing various NGN development initiatives.

- Vulnerability Information Handling Network

There is some successful experience to fight against possible threats by making up cooperative framework among vulnerability discoverers, manufacturers and coordinators in Japan as well as the US. GDBe will suggest that such framework should be established in most of the Internet- advanced countries and such activities should be interconnected. If the interconnection is realized and properly operated, it should be a good basis for multi-purpose, multi-functional collaboration network to cover the world and contribute to the Internet security.

- Network Traceability

  When traceability over the Internet is established, it would work towards prevention of Internet attacks and unrealized dissemination of harmful communication, and people would become more careful about being affected by viruses or worms, keeping Zombie programs without knowing, sending out virus-affected or otherwise offensive network packets. On the other hand, there is an argument that the anonymity is the feature that gives democratic and creative nature to the Internet. It is, therefore, recommended that traceability over current Internet could be considered and appropriate actions to be taken by taking it into consideration that such work should not negatively affect the freedom of the Internet as well as the option of realizing it in NGN as an alternative.

This report is expected to provide some perspective over cyber security. Several topics were picked up as recommendations and suggestions. With those challenges and topics, the Cyber Security Issue Group will contribute to cyber and ubiquitous society. While encouraging all the GBDe members to speak loudly about Cyber Security and to contribute the stability of IT world, the Cyber Security Issue Group is committed to promote the topics referred to above.

Contributions from the Issue Group Members were provided by: Deutsche Bank, Germany; Institute for Information Industry (III), Taiwan; Multimedia Development Corporation (MDC), Malaysia; Fujitsu Ltd., NEC Corporation, Nomura Research Institute (NRI), and TEPCO (The Tokyo Electric Power Company, Incorporated), Japan.

GBDe 2005 Issue Group

Cyber Security
Overview on Challenges and Recommendations for Secure Cyber Society

October 17, 2005

Issue Chair: Mr. Buheita Fujiwara, Chairman, Information-technology Promotion Agency, Japan

1. Overview

Thanks to the great advance of Information and Communication Technology, the Internet is now an inevitable infrastructure for all the players of human world: from individuals, families, schools and municipalities to governments, institutions and corporations.

The concept of the Internet started from colleagues' and buddies' bona-fide communication within academic society; therefore, it is by nature innocent. After the Internet has been operated commercially, its innocent nature makes itself vulnerable: it makes instant and low-cost communication possible that contributes e-commerce dramatically, but its feature of anonymous becomes uncertain factor for business environment. Since the Internet connection further spreads via broadband and wireless connectivity, variation and significance of threats emerge rapidly. The threats vary from viruses, worms and malicious attacks to frauds and abuse of or over the Internet, which especially shake users' trust in all levels and hinder the development of e-commerce. Thus the Internet security issues became obstacles for not only network communications, but also every aspect of social and economical activities taken place on and over the Internet. As we benefit from widely spread Internet network, we need to make it tolerant to those who behave differently.

Vast amount of efforts have been made in a variety of areas, locations and players. We can take advantage of the fruits of such efforts and start enhancing and reorganizing what we can do to make cyber space safer and stable. Now we, the GBDe, can review the results of past studies and set forth possible countermeasures so that we can make full use of the advantages of the Internet and mitigate the negative aspects of it.

The Cyber Security Issue Group is committed to address these issues and discuss what the threats are, how they affect the society, and what are the possible mitigations and solutions. Such discussion should lead to constructive suggestions and proposals that can contribute to the international IT network society.

2. Typical Threats, Frauds and Embedded Weakness Facing Security of the Internet

2-1. Vulnerabilities

As computer software becomes complex and interconnected, small bugs and holes could lead to big threats where such defects may allow attacks to take place to manipulate victim computers act improperly or harmfully, and/or result in loss of valuable data or information.

Wide spread of commonly accepted operating systems and other system software magnifies the threats and possible damages once such vulnerabilities are explored and exploited. Microsoft is earnestly fighting against this serious issue. UNIX and Linux components are also reported for some vulnerabilities. Potential threats also exist in mobile phones, automobiles and electric appliances. All of these employ embedded software. When ubiquitous realizes and everything is networked, same threats of possible vulnerabilities and their exploits will become real.

Today, to our regret, vulnerabilities in PCs are reported almost everyday, and the exploits appear in a very short cycle time, before people apply appropriate patches. This makes the network vulnerable and harmful.

2-2. Viruses and Worms

Computer viruses and worms became common living things in the network. Many of them give harms by doing any of the followings;

1) making computers malfunction or hung,
2) causing loss of data and information,
3) sending out mails that would send copy of themselves and/or would consume network devices and circuit capacity,
4) injecting programs called Trojan Horses or Zombies that silently work to send out critical information or attack designated targets at designated timing, and
5) sending out significant number of the Internet packets.

In many cases they have capabilities to spread their copies by themselves via e-mails, shared files and storage resources, web browsing, and file downloads and transfers. Most of them exploit vulnerabilities. In many cases, Trojan Horses provide back doors to allow attackers (often called hackers or crackers) to walk into victim computers and to manipulate them.

According to recent survey report from IPA (Information-Technology Promotion Agency, Japan), 70% of Japanese respondents report encounter with virus (found or affected) in 2004. The similar survey results also show 71% in the US, 71% in Germany, 62% in Korea, 62% in Australia, and 37% in Taiwan. Names of most frequently encountered viruses are; W32/Netsky, W32/Mydoom, W32/Bagle, and W32/Klez. These are common among the countries surveyed.

2-3. Hacking

Hacking, or cracking according to some definition, is an attack to a computer usually from a remote place. In many cases, the attackers log on computers by compromising identification and authentication process. They can find out passwords by variety of methods from brute force to peeping password files to social engineering. Some tools to automate such attacks are available on the Internet. They manually, or in many cases by using such tools, invade into someone else's computer. Once they get control of computers, they use the victim computers as foothold for new attacks, network abuse and fraud, and DoS (Denial of Service) attacks.

In such cases, they typically leave backdoor programs to revisit later and erase logs before they get out. Thus, malicious attacks link from one to another, and allow attackers to behave freely in the Internet world.

Malicious attacks may cause damages to the victim computers in the form of theft of information or even money. Other typical malicious use is to rewrite web pages either to send messages, or work fraud. Another mal use is DoS (Denial of Service) attacks. DoS generate very frequent network access and negatively affect network traffics. Such attacks are typically done by Trojan Horses and BOTs as referred to in the next section. When they want to damage a certain network node like a server or a router of famous or important entities like, governments or large enterprises, they can do it at any time they want and without much difficulty.

2-4. Trojan Horses and BOT Net

In many ways unsolicited programs can be set on computers only if it is somehow connected to the Internet. Such programs are called Trojan Horses. Typically they are implanted by worms. Some types of Trojan Horses can be manipulated remotely so that they can generate network attacks. They are typically called BOTs, a derivative of "robot." BOTs live on variety of computers over the Internet and at some timing they conduct network attacks to designated destination according to commands remotely sent or programmed in advance. BOTs can also work as information stealing agents. The threat of BOTs has become increasingly serious.

2-5. Spams

Spam or Spam Mails are the generic names of unsolicited mass mailing. Many of them are for advertising or marketing purposes, and sent out indiscriminately. In many cases, they are unfavorable or undesirable solicitations. As the number of Spam mails is tremendously big, it compromises efficiency of business and badly affects network traffic. Business people have to spend much time to tell and remove Spam mails.

Network infrastructure is used to handle meaningless or harmful mails. Some statistics say that more than half of mails a typical business person receives are Spams. By its mass power, Spam is another threat for the Internet society and its normal, innocent users.

2-6. Phishing

Phishing is an emerging threat of the Internet world. Typically a computer user gets a mail, which tends to be a Spam mail, soliciting the receiver to visit a web site camouflaging a real site of existing companies; typically banks and credit card issuers. They are guided by the mail and the web pages to give proprietary information like card or account numbers or other IDs and PIN, or passwords. Once the offender gets such information, they can do any monetary fraud instantly.

This is a new type of threat. Typically, they combine 1) Spam mailing, 2) tampering or camouflaging URLs and web pages, 3) social engineering.

A similar fraud has come up and named Pharming. In case of Pharming, the URL people are led is real URL of right web site, but the connection is tampered to go to the fraud site. In this case, the user hardly tell he or she is led to a criminal site. Pharming is same fraud as Phishing, but is more serious because of the more sophisticated method.

This implies there could be new types of crimes using IT and exploiting lack of knowledge or appropriate care.

2-7. Information Theft

Once a computer is compromised, any information in the computer, unless properly protected by passwords and/or encryption, is opened for the use by an attacker. In many cases it results in invasion of privacy, theft of proprietary information or trade secrets, loss of money, loss of business opportunities and threats of social hazards. It may further result in damage to individuals' health and life or daily operation of society in worse cases.

Recently Japan experienced series of incidents of individual information being stolen or compromised. The maximum number of IDs stolen in one incident was nearly 5 million. In the case of a convenience store chain, the compromised company gave 500 yen or roughly US$5 per person as compensation or token of apology to its customers whose personal information was suspected to be stolen. This rate applied to the 5-million ID theft case, and is regarded as eventual common rate in similar cases. This means a loss of large number of individual information might result in bankruptcy and thus Information theft suddenly becomes serious threat for companies and institutions.

3. Typical Activities to Fight against and Mitigate the Internet Threats and Risks

3-1. Vulnerability Information Handling Framework

Network attacks to vulnerabilities in software, including operating systems, communication protocols and applications are discovered and reported almost every day.

Such vulnerabilities allow malicious players to exploit them. To prevent successful attacks and compromises, all the users must apply patches and make software updated.

The challenges here are at several aspects. Vulnerability information first must be kept secretly. The source code owner has to verify the reported vulnerability and prepare countermeasures before known to hackers. So that each measure here should be treated quietly and deliberately in this phase.

When workarounds and/or patches are ready, the vulnerability and the way to mitigate/rectify are announced to encourage all users to take appropriate actions to modify the vulnerability. Such measures must be announced immediately and widely so that everyone can protect before attackers are ready to exploit the vulnerability. This should be a frantic phase where variety of information exchanges back and forth.

All the processes must be conducted carefully and promptly. Doing something in confidence is always difficult. To distribute all end-point users accurate and understandable information as immediately as possible is another challenges.

Efforts taken in Japan in 2003 and 2004 were initiated by the government and worked out under the initiative of IPA as public-private cooperation scheme. The vulnerability information handling framework was named as “Information Security Early Warning Partnership.” IPA plays the core role as the POC (Point of Contact) for finders/reporters for any of vulnerabilities and is the center of the handling process. JPCERT/CC collaborates with IPA to work as the coordinator in between vendors to prepare countermeasures. The countermeasures should be coordinated among IPA, JPCERT/CC, the finder and the software vendor in advance prior to its announcement. All the relevant parties including vendors and user associations work widely to spread the information within the respective communities. The database relevant to that information was prepared by IPA and JPCERT/CC and is available for public. This database is called “JVN” or “JP Vendor Status Notes” (http://jvn.jp/) and provides information relevant to vulnerabilities and vendor reactions. The database is currently operated and maintained by the joint team organized by IPA and JPCERT/CC. In the US, US-CERT provides similar service at its web site “http://www.kb.cert.org/vuls.”

3-2. CSIRT and CSIRT Network

CSIRT stands for “Computer Security Incident Response Team” and in some case it is also called CERT or Computer Emergency Response Team. CSIRT is a non-profit organization and provides coordination, suggestion and communication aids when it gets enquiry upon a computer or a network troubles caused by attacks and viruses.

CSIRTs are typically formed country by country, or by other types of community such as academism or industry, and provide emergency aid services. The role of CSIRT has been expanding from existed/passive roles upon inquired basis to the proactive efforts viewed in 3-1. such as network monitoring, a real time network security observation, and vulnerability handling coordination, etc.

They form communication network among CSIRTs in countries and economies to exchange information and do international coordination. APCERT is a network of Asia-Pacific region CSIRTs connecting 17 entities from 14 economies.

CERT/CC (CERT Coordination Center from US), NISCC (UK) and JPCERT/CC (Japan CERT Coordination Center) form another hotline which focusing on vulnerability information handling.

CSIRTs and their collaborative network contribute to mitigate network threats and risks.

3-3. International Track Back Network

Tracking back and identifying the physical network location of hackers is an effective way to mitigate potential threats and risks that lead attacks. CSIRTs and SOCs (Security Operation Centers) form an international network to track them back to identify the hacking origins.

Since all processes should be done as immediately as possible; and thus, there may lays variety of challenges. These processes, thus, should be sustained by collaborative network among many network service players from many countries as possible.

3-4. Common Criteria

Common Criteria or CC is the international framework to evaluate and certify IT products and its systems. CC prescribes ISO/IEC15408 as the international standard. Developers and manufacturers who wish to be accredited by the CC standard on their security products and systems are required to develop the Security Target as security specifications for their products which are to comply with the Protection Profile prepared by themselves or third parties. When the product is evaluated and certified, it is assured that it is conformed with a certain security level. There provided 7 security conformity levels under the certification scheme. In case it is procurement by public sector, typically EAL3 and/or EAL4 is required (EAL: Evaluation Assurance Level). Thus a common measurement of security conformity level can be defined and assured. CC helps to standardize a certain security measurement and provides a common scale and system integration on procurement.

3-5. ISMS (Information Security Management Systems)

ISO/IEC17799 is the international standard for administrative framework of information security. The origin of this standard is British Standard #7799. BS7799 consists of part-1 “guideline” and part-2 “requirement.” BS7799 part-1 became international standard in 2000 as the ISO/IEC17799 which provides the best practice of recommendation. BS7799 part-2 which provides specification for establishing, implementing and maintaining ISMS controls is incorporated in the ISO/IEC17799.

The information security management controls provided under ISO/IEC17799 was revised as the ISO/IEC17799:2005 in June, 2005 which covers the following areas:

1) Security Policy
2) Organizing Information Security

3) Asset Management
4) Human Resources Security
5) Physical and Environmental Security
6) Communications and Operations Management
7) Access Control
8) Information Systems Acquisition, Development and Maintenance
9) Information Security Incident Management
10) Business Continuity Management
11) Compliance

Over all, the new version (ISO/IEC17799:2005) added a new chapter about Information security incident management, new controls on employees, contractors and third party user management, and so on. The revision highlights the importance of Information Security Governance in corporations.

ISO/IEC17799 and BS7799-2 are widely applied as national standards in many of developed countries and provides the international baseline for organizations' information security management framework that contributes to local and international mutual confidence in communications and transactions.

ISMS evaluation and certification program is introduced in several countries. Taiwan Government encourages both public sectors and private sectors to establish their own international standard based on the ISMS international standard ISO17799 (ex-BS#7799). Further, considering that service providers should have enough robust capacity to protect system security than the one of consumers', the Taiwan government rules a model contract to increase the service providers' responsibility. In Japan, ISMS evaluation and certification program was introduced in 2002. JIPDEC (Japan Information Processing Development Corporation), one of the Japanese accreditation bodies said that more than 1,100 certificates have been issued worldwide. The top 5 nations are; Japan (510), UK (185), India (82), Taiwan (45) and Germany (36), according to its recent report. (More recently JIPDEC announced Japanese certification issuance counted to 1014 as of August, 2005.) Related information is available from ISO17799 news site at http://www.iso17799-web.com and International Users Group at http://www.xisec.com.

ISMS, based on the ISO/IEC17799:2005 is going to be reorganized into ISO/IEC27000 series in November-December time frame of 2005. Under the reorganization, ex-BS#7799 part-2 becomes ISO/IEC27001 to provide ISMS Requirements and the ISO/IEC17799:2005 becomes ISO/IEC27002 to define security controls. Risk Management, Metrics and Measurement and Implementation Guidance will become independent standards under the 2700 series.

3-6. Trust Mark and Privacy Mark

Consumer confidence has been one of the major interests of the GBDe activities. It is the basis of economic activities over the IT network. In 1980, Organization for Economic Co-operation and Development or OECD issued Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. (http://www1.oecd.org/publications/e-

book/9302011E.pdf) The EU Directive issued in 1995 required actions for protection of individual information. This called up a discussion among EU, US and Japan to take certain actions to protect personal information. Such arrangement is called “safe harbor.” In the US, BBB and Truste severally issue privacy or site-confidence certification. In Japan, Privacy Mark certification framework was established and introduced in 1998.

3-6-1. Trustmark

Trustmark was discussed in the GBDe issue workshop on September 26, 2000. The introductory part of the session paper addresses key requirements for the Trustmark as follows:

1) Be affordable, in particular to SMEs
2) Be enforced rigorously, by providing clear monitoring and reporting mechanisms and guaranteeing neutrality of their enforcement decisions
3) Be broadly disseminated and easily accessible to consumers when accessing commercial web sites
4) Be developed in consultation with all stakeholders
5) Use appropriate security measures to prevent misuse of Trustmark
6) Offer a mechanism for consumer redress along the lines of the GBDe ADR recommendations
7) Require minimum standards of behavior by merchants in the areas of online business practices, privacy protection and complaints handling, in line with GBDe recommendations.

The most recent development in the trustmark area is the establishment of Asian Trustmark Alliance (ATA) and Global Trustmark Alliance (GTA). The Organizing Committee for GTA was launched at the GBDe summit in Kuala Lumpur in November, 2004.

3-6-2. Privacy Mark Program in Japan

The major mark (seal) system of personal information protection used in Japan is Privacy Mark (P-Mark) operated/managed by JIPDEC (Japan Information Processing Development Corporation).

The criteria of the recognition of this mark are to conform to JIS (Japan Industrial Standard) Q15001 “Requirements for compliance program on personal information protection”. The enterprise that wishes to receive the recognition of this mark program should pass the documentary examination and the site survey by JIPDEC to confirm that they put in place a compliance program and handle personal information in accordance with the criteria. The validity term of this mark is only two years, and that enforces the mark bearers to pass the documentary examination and the site survey every two years in order to keep the mark on their web site. Since conditions of the criteria are severer than the requirement of Law Concerning the Protection of Personal Information, this mark is gathering consumers’ trust in Japan.

This service has been started in 1998, and the number of the enterprises received the recognition of this mark is about 1,700 as of July, 2005. Since the Law Concerning the

Protection of Personal Information became fully effective in April, 2005, the number of enterprises that try to receive the recognition of P-Mark is increasing rapidly along with the rise of the concern to personal information protection.
This mark program can be mutually recognized with the privacy seal program of BBB Online in the US and is called mutual BBBOL Mark. The recognized enterprises of P-Mark can also be recognized by the mutual BBBOL Mark by additional procedures and some fees without any examination by BBB Online.

Also the enterprises in the US recognized by the privacy seal program of BBB Online can append the mutually recognized mark on their web sites to show it to on-line customers in Japan.

3-7. Initiatives and Efforts from Governments and Public Sectors

3-7-1. Taiwan

1) Viruses, Worms, and Malicious Attack

In order to overcome the viruses and worms as well as malicious attacks, Taiwan had amended Criminal Code by including a Cybercrime Chapter in 2003. It criminalizes 4 types of conduct: Unauthorized access to computer facility, Illegal interception, Illegal interference, and Programmer who create hacker tool specifically for the perpetration of the above types of crime. Moreover, if a targeted is a governmental facility, the offender will be severer punished with the extent not to exceed more than one and a half of the prison term for which originally been set.

As for Trojan Horses and BOT Net, they are still considered as a management issue. Taiwan Government encourages both public sectors and private sectors to establish their own international standard based on the ISMS international standard, ISO17799 (ex-BS#7799, part-2). Further, considering that service providers should have enough robust capacity to protect system security than the one of consumers', the Taiwan Government rules a model contract to increase service providers' responsibility.

2) Phishing

Phishing crime not only via the Internet, but also via SMS (short message) on mobile phone gets worsen, the Taiwan Government has requested telecommunication service providers play the role as a gatekeeper to filter out quasi-fraud messages. The Taiwan Government is also drafting regulation amendments to require both the Internet service and telecommunication service providers to have the capacity to assist on-line tracking of such criminals.

Besides, the Taiwan Government also required banking service providers to upgrade their ATM systems, change their magnetic cards to smart IC cards and limit their transaction amount up to NT$30,000 per transaction per card.

3) Information Theft

In order to protect people from information misuse, the Taiwan Government is proposing "The Computer-Processed Personal Data Protection Law Amendment", which is on the floor of Congress since March, 2005.

According to this law, personal data is defined as one's name, date of birth, personal identification number and other information sufficient to identify a natural person. It covers the rights to search or read the data, reproduce the data, supplement or revise the data, stop further processing or use of the data; and delete the data. The major changes include:

(1) Expanding the covered fields of all kinds of data processing relevant to natural person not limiting to computer-processed data.
(2) Be applicable to all business and government agencies.
(3) Agencies should notify the individual whose data is belonging to before its use no matter how the data is being collected.
(4) Increasing the total amount of compensation for the damages.
(5) Empowering the government authority to supervise infringement cases.
(6) Establishing a non-government agency to offer legal assistance.

3-7-2. Malaysia

- Information Security Initiatives in Malaysia by NISER –

1) Services Provided by NISER

The National ICT Security and Emergency Response Centre (NISER – www.niser.org.my) is the technical agency formed by the National Information Technology Council (NITC) and started its operation in November, 2000. NISER has been specifically tasked to support the nation's Information and Communications Technology (ICT) security and cyber defense initiatives to avert potential intrusions and unlawful cyber-actions that could threaten the nation's critical infrastructure.

Services provided by NISER include Incident Response, Computer Forensics, Security Assurance, Security Management and Implementation:

(1) Incident Response

The Malaysian Computer Emergency Response Team (MyCERT – www.mycert.org.my) was established to provide incident response services to the Malaysian Internet users. Over the years, MyCERT has been providing assistance in handling ICT security incidents such as intrusions, denial of service attacks, hacking attempts, malicious code attacks, email abuses, social engineering, and named quite a few.

(2) Computer Forensics

Computer Forensics services provide data recovery and digital evidence services to agencies and organizations. Computer Forensics services also include training to law enforcement and other government agencies.

(3) Security Assurance
Security Assurance services provide trusted evaluation services on IT products and their systems and are involved in security system audit for government agencies such as the Human Resource Management Information System, Electronic Budget and Financial Planning System and Pensions Online Workflow Environment (POWER).

(4) Security Management and Implementation
Security Management and Implementation is active in the information security standard development and implementation in Malaysia including Information Security Management Systems (ISMS) and Business Continuity Management (BCM).

2) International Collaboration
At the international arena, NISER (MyCERT) is a member of the Asia Pacific Computer Emergency Response Team (APCERT). Through APCERT, NISER (MyCERT) collaborates with other CERTs in the Asia Pacific region including Australia, Japan, Singapore, Thailand, the Philippines, Indonesia, Hong Kong, China, Taiwan, Vietnam, Brunei and South Korea.

3-7-3. Korea
In Korea, we can see remarkable progress in the Internet society development and information security.

1) Government initiatives in cyber society development
In 1995, Korean Government enacted the baseline of the Law to Promote Information Society (amended in 1999 and 2000). Based on this law, its principal concept was set up in 1996 and the Information Promotion Committee was formed within the Cabinet. This was the year when KISA, Korean Information Security Agency was formed and CERTCC-KR has started its operation within KISA.

CyberKorea21 plan was generated in 1999 aiming at a creative and intelligent nation based on broadband infrastructure. In 2002, the CyberKorea21 was reformed into e-Korea Vision 2006. In this initiative, 3 objectives were defined; 1) a scheme to prevent and respond to cyber terrorism, 2) security technology and human resources development, and 3) establishing healthy, sound and ethic cyber space.

The idea of e-Korea Vision 2006 was then redirected to a new initiative, Secure e-Korea 2002-2007, a mid-long-term Information Security Master Plan. The subjects set forth under this initiative were; 1) enhanced infrastructure of highly intelligent information society, 2) promotion of digital signature to secure reliable e-commerce, 3) cryptography application foundation for secure cyber environment, 4) private information protection and Spam Mail control, 5) healthy cyber sphere development, and 6) strategic incubation of information security industry.

The organization is consisted by several governmental agencies such as National Security Council as command center, Defense Intelligence Center under Ministry of National Defense (military), National Cyber Security Center under National Intelligence Service (government) and Korean Information Security Agency under Ministry of Information and Communication (civil sector).

2) Serious and various incident experiences

The biggest and most remarkable incident that Korea has ever experienced was the Internet Blackout on January 25, 2003 caused by SQL slammer worm. The network damage resulted Korea a fatal damage and the economic loss was also huge because the worm hit the peak hours of consumers' access. This world-famous incident was followed by other typical virus incidents such as Sobig, MS Blaster and Sasser, and associated by several incidents including; citizenship number theft, spam mails, sensitive personal information leakage from National Education Information Systems and credit card number theft coupled by ID information for 470,000 citizens.

The Ministry of Information and Communication summarized the trend of cyber attacks after the Internet Blackout as follows; 1) paradigm shift from system attacks to network services attacks, 2) increased complexity and maliciousness, and 3) shortened lead time and accelerated spread speed of damages.

3) Cyber Security Activities

Private-Public collaborative activities seem to be well organized and function effectively in Korea. The public sectors are actively approaching to set up political initiatives and organizational formation, promoting technical and human resources development, and stimulating information security industry growth. The private sectors are rather active in formation of collaborative scheme including CERTCC-KR, CONCERT (CONsortium of CERTs), and ISAC: KISA is leading such activities. Variety of venture companies is playing important roles in providing local-origin IT security technologies and products.

3-7-4. Japan

Japanese Government introduced Individual Information Protection Act in 2003 which became fully effective in April, 2005. The law requires that entities who own certain number of individual information in any database structure should provide physical, organizational, technical and operational security measures. As an effect of this law, many companies and local governments are to acquire Privacy Mark certification in advance when they transact using above mentioned individual information.

Privacy Mark certification system which assures appropriate protection of privacy information in view of emerging e-commerce and Internet-based transactions was introduced in Japan in 1998. After several years, Privacy Mark is becoming very popular due to the newly introduced Individual Information Protection Act. There plans to review the framework of the certification so that the scheme will become further efficient and workable. This should lead to an internationally consistent certification standard.

Japan used to apply to authorization system of safety countermeasures employment for information processing firms. The authorization system was incorporated into ISMS certification framework in 2002. The certification framework is modified to better meet up-to-dated and international requirements for information security.

A similar system named Information Security Audit System was introduced in 2004 to provide more flexible framework for SMEs. The purpose is to provide supports and suggestions towards security management practice in addition to demonstrate assurance of a certain security level.

3-7-5. United States

Cyber attacks reported to CERT/CC (CERT Coordination Center) have been exponentially increasing in recent years; 21,756 in 2000 expanded to 137,529 in 2003. Many of the attacks are performed by automated attack tools called BOTs or Trojan Horses which typically distributed by worms. While viruses and worms are the majority of those that affect adversely the reliance and performance of network: recent development of network threats is not limited to Trojan Horses and BOTs, but spreads to spam, spyware, phishing and pharming.

In addition to attacks and malicious codes, network fraud becomes increasingly harmful. By way of hacking and/or Spyware, information theft and fraud has been made pretty often, and the damages are huge. People are concerned of their ID theft and fraud leading to credential destruction which means civil life to become difficult due to loss of monetary credibility.

The government efforts to fight against cyber threats and crimes are centralized to National Cyber Security Division (NCSD) under the Department of Homeland Security. NCSD was established by assembly of Critical Infrastructure Assurance Office (CIAO) of the Department of Commerce, National Infrastructure Protection Center (NIPC) of FBI, Federal Computer Incident Response Center (FedCIRC) under the Federal Procurement Agency, and National Communication System (NCS) of the Department of Defense. Due to broad coverage of Homeland Security, NCSD's activities are somewhat limited in terms of empowerment and funding. As for the supplemental purpose, the Department of Justice plays part of it. FBI experts are also sharing competency with NCSD in cyber crimes.

As globally known, the US is one of the leading countries to provide high level IT security technology and products. Historically, the US has been mainly providing anti-viral products, firewalls and intrusion detection systems. Recent development in IT security technology includes; Wireless LAN Security, End Point Security which comprehensively covers desktop and mobile devices, and Trusted Computing. Trusted Computing is a relatively new industry initiative, supported by Trusted Computing Group (TCG), aiming at securer computing platform consisting of a specific hardware. The hardware so called Trusted Platform Module or TPM contains an encryption key, digital certificate, password and other security features. They are safely stored in the chip, tolerant to tampering and fraud, but destroyed when taken out of the chip. While this

defines limited free and flexible computer use, yet it can provide safer computing and communication environment over the Internet.

Due to the increase of such damages by information and/or ID theft and expansion of people's concern, federal and state governments set up laws and regulations. Those laws and regulations currently effective are: Sarbanes Oxley Act, HIPAA, GLBA and FTC regulations at the federal level, and Security Breach Information Act of 2003 of California is a typical state-level legislation example. Several bills, including Comprehensive Privacy Act, Social Security Number Misuse Prevention Act and Identity Theft Prevention and Victim Recovery Act are on the House for deliberation.

Private sectors are also active and cooperative for government's variety of efforts. Besides TCG, NCSP, the National Cyber Security Partnership, consisting of Business Software Alliance, Information Technology Association of America, TechNet, US Chamber of Commerce and others is active in terms of calling for action for Information Security Governance. National Cyber Security Alliance (NCSA) is a non-profit, public-private partnership consisting of businesses, consumer groups, government agencies and educational institutions dedicated to raising the awareness of cyber security issues and best practices. The NCSA provides tools and resources to empower home users, small business, and schools to stay safe online.

While the US is yet suffering from cyber attacks and frauds, both governmental, academic and private sectors are rapidly becoming active and cooperative to accomplish safer cyber security.

3-7-6. Germany

CERT in Germany looks very active in handling virus, worm and intrusion response and coordination. The vulnerability handling framework is not yet established. Public or non-profit organization is not very much involved in fighting against phishing. No official regulation on phishing are not yet realized, while industry's voluntary countermeasures take place.
Germany has a law to protect personal and privacy information. The enforcement is very comprehensive and covers from personal reference to social identification to private, sensitive information.

4. Challenges toward the Future

From the viewpoint of a large sense, people are doing good job. The problem is that the people in the other world are also doing "good" job. That means we need to continue the current effort ever better, and do more to realize virus free, worm free and any of cyber attack free in the future.

In this chapter, we would like to discuss an overview on new challenges and the areas we need to focus more to establish the better future of the Internet world and cyber security.

4-1. Culture of Security

As IT penetrates to our society, IT changes the order and the sequence of social structure and activities, the culture dominating there must change. Everyone in the IT-nised universe must know what "ubiquitous" means and might mean in terms of convenience, AND threats as well.

When you connect to the Internet, you should know what it means. You click for something convenient, and you should know what potential risks you are approaching. This kind of knowledge cannot come to you automatically. You can certainly learn from your experience, but that is definitely not enough. Thus, you are to maintain security awareness training: to that end, a certain level of security education is definitely required. Security literacy is not only for user's own security, but more importantly inevitable for cyber society security.

Players and beneficiaries in every field are taking actions. National requirement for privacy protection and security governance responsibilities stimulates corporations towards thinking more about IT and information security. Corporations are now seriously trying to develop and improve their employees' security awareness. Operating system vendors have been paying efforts to make their products safer, and make their users know about security better. Internet service providers extend security check services and let their users know about security better. Security tool vendors, especially anti-viral vendors, provide opportunities to have users know better about threats and damages.

Security education has established itself as a market segment. Education providers vary from school operators to security tool vendors, from consultants to systems integrators. Conditions for cultural security have been ever improving. Yet, numbers and frequency of virus outbreaks steadily grow. Incidents relevant to information theft or lost come out one after another. Most of such outbreaks and incidents are from known or controllable causes. That is, if people are sufficiently trained of security and certain protective measures and are cautious, such security incidents should have been prevented. Further efforts for literacy improvement on security are expected.

4-2. Information Security Governance

Threats and risks certainly exist and cannot be mitigated or removed easily. It is, therefore, inevitable that all the participants to the Internet world should be aware of the risks. In case of corporations, it is not easy to justify or determine to what extent they should do in the investment and expenditure for the Internet security.

If there are guidelines and measurements for network security expenditure, it is much easier for corporations to prepare for threats and possible damages. Nippon Keidanren, the leading association of national economic entities in Japan, recently issued a report referring an expectation to a common understanding on security management. The report says, if corporate efforts for network and information security can be measured and assessed from corporate governance and management evaluation perspective, it should effectively support corporate executives.

Ministry of Economy, Trade and Industry (METI) of Japan recently conducted a study on Information Security Governance and publicized the report on their study. From both corporate sound management and social cyber security perspective, METI thinks the ways to justify and evaluate corporate security investment must be established. This corresponds to the proposal from Keidanren and represents voice of the majority of corporate management executives.

The METI report points out 3 aspects of Information Security Governance realization:

(1) Information Security Benchmarking
This is a kind of an indicator or a measure to assess how and to what extent a company should take actions and spend money for Information Security Countermeasure. Typically SMEs can benefit from this because it may not be easy to set up criteria for security expenditure without such benchmarks.

(2) Information Security Report Model
This is a kind of template or guideline to make report on corporation's information security activities and efforts. To get fair evaluation and justification for security investment, it will be helpful if some reference for reporting is presented. A study is going to be conducted to set up such reference model. It is also expected that formats and methods will be developed to calculate and evaluate security costs and the expected effects, and some security accounting methodologies are introduced.

(3) Business Continuity Planning Guideline
Information security can also be defined as a portion of BCP program. BCP can be another approach as to how a corporation can justify and digitize the significance of security investment. Typically, when an IT system is compromised, its corporative activity could be disrupted resulting in vast damages and losses of business and money.

So, when a BCP can address information security as an integral part of it, this is another way to evaluate and justify efforts and spending for information and network security.

4-3. Next Generation Network (NGN)

The Internet is a communication medium based on the best-effort concept. There is no assurance of latency, accuracy, error-free and security. We have been experiencing its volatile and fragile nature and such concern naturally leads to an alternative or extra internet. The concept of extra internet comprises of two elements: reliable network and reliable participants. The network service is provided by reliable carriers who can provide service level agreement tolerable of critical communications. In such reliable world, only reliable and identifiable players behave in an appropriate manner so that bona fide participants can depend on the reliance of the network.

Such concept of extra Internet is called Next Generation Network or NGN. Variation of NGN activities spreads over the world. Examples of such study includes; PlanetLab funded by National Science Foundation (NSF), US, NCOIC (Network Centric Operation Industry Consortium), a private entity by industry and university players to aim at

interoperability of networks, Internet Project sponsored by NSF operating Abilene network and FP-IST FET from EU. International organizations including OECD and ITU are also active. Severally, there is a study in Japan carried out by COCJ (Committee on Competitiveness of Key Technology Institute-Japan).

A report to overview these activities and present the future expectation is being prepared separately by a workgroup for NGN within the GBDe, and is going to be submitted separately from this report.

4-4. Security in Ubiquitous Society

IT is evolving every day and brings IT armament capability to everything that consists and drives our day-to-day life and activities. Such movement and vision is called "ubiquitous," meaning IT everywhere. "Ubiquitous" state realizes the Internet connection to everything and everywhere. Typically, RFIDs or IC tags will be attached to every object in the world. That will bring you such convenience that you can monitor and control your home appliances and check your home security from remote. It also can realize identification of every dietary objects and traceability in dietetic security. That also means malicious people can have the same access somehow unless appropriate protection is provided or maintained. Cyber attacks and frauds become much easier to take place.

The security of information, typically privacy information, is also at stake. All the subjects and objects in the world can be retrieved electronically; that means someone can know when and where you are and what you are doing at anytime he or she wants to do so. This is a serious concern about privacy.

4-5. Security Level Evaluation and Digitization Approach

Security is technical, cultural, and thus, a social issue. While every individual player, both people and corporation, need to fulfill respective responsibilities, public sectors must play active roles in various aspects. On one hand, it would be funding for R&D and literacy development. The other aspect may include guidelines and indicators generation. Japan is now trying to introduce a digitization approach for national security level which includes security scoring. Korea has been developing this method, and IPA is cooperating with KISA to further it.

The Information Security Evaluation Index is developed to measure the nation's security level based on various basic data such as information security measure status (e.g. rate of firewall introduction), and IT infrastructure development status (e.g. rate of PC usage).

By measuring these indexes for many years and gathering data for reference, the index is expected to contribute to the improvement of security countermeasures. Grasping the changes of security countermeasure solution and grasping the cost performance of the measures to security investment would provide the basis for comparison and benchmarking.

Currently, in reference to the index developed by South Korea, Japan is also developing its own index. The joint project between Korea and Japan is planned to develop an index to be accepted from all over the world on the basis of the South Korean index.

4-6. Damage Calculation Model for Virus Infection

Evaluation is also expected in the area of assessing damages of infection. Some approach has been made to establish a formula to calculate damage of virus infection.
IPA has developed the Virus Damage Estimation Model to figure out monetary damage amount. It is calculated based on data such as network down time, required human resources to recover system and business, labor cost and degree of IT dependence. Questionnaires, and statistics are studied to extract parameters. When they are figured out and the formula is established, the monetary damage amount can be easily estimated.

5. Conclusion

Above mentioned are the major topics that have relatively big effects to cyber security. The topics represent major areas that IT-nized countries have been active to improve the situation surrounding the cyber security issues. Reviewing current states of the topics would be a good opportunity to get a comprehensive view of where we stand today. It would lead to a view of future challenges for making a better cyber society.

Cyber Security is not simply a social issue. It is a complex of every element of society: technology, science and engineering, business, literal, social, educational, cultural and thus political and administrative. All the participants are expected, and have to, play respective roles so that cyber space works for the best benefit of all the participants.

From such point of view, the GDBe will recommend the following points as where actions, initiatives and leadership are expected to take place by governments and private sectors:

5-1. Literacy and Education

People as individuals tend to lack knowledge about the danger of the Internet connection. Without properly applying anti-viral software, they can easily be affected by viruses and worms. That results in infection by Trojan Horses and BOTs. When they become active, they may offend the network, or alternatively, they can easily be led to fraud web site to be stolen of their bank account numbers or credit card numbers.

The only way to avoid this kind of hazardous situation is that they know the danger of the Internet and risk of doing something over the Internet without proper protection and precaution. Thus, education and literacy development become the most important subjects to be observed and realized. The less they are aware of the risk, the less they are willing to pay money or spend time for getting knowledge of the risk. That means public leadership to make them aware of, and encourage them to learn about the risk is expected ever seriously. At the same time, messages from the Internet service providers, PC

manufacturers and software vendors about the risk and how to protect the client environment are requisite.

When education effort is successful and certain level of literacy is achieved, the risk of keeping BOTs and zombies, as well as the risk to be compromised by phishing and pharming should be reduced drastically. So, it is recommended that governments facilitate stimulation for IT security awareness and encourage people to obtain better knowledge of benefit and risk of Internet usage. At the same time, industry players are expected to provide people with Internet security education opportunities either commercially or complementarily.

5-2. Information Security Governance

Information Security Governance is another aspect of security literacy. Security awareness is most important at individual level. The same can apply to corporate citizens. In case of corporations, it can be defined as Information Security Governance. Company executives should be most aware of threats and potential harms of the Internet in addition to the benefit of it. The concept of Information Security Governance was discussed in section 4-2.

Such awareness would be realized in implementing Information Security Governance into corporate management. Governments can promote it by introducing encouraging guidelines and incentives. Such incentives could be tax discount, special-aim funds, governmental requirements and recommendations, or law enforcement.

Corporations can also pay efforts for Information Security Governance. Security reports as part of CSR is one example. Business continuity planning can incorporate Information Security Governance programs as a part, and will contribute to better corporate management. Securities market rating should incorporate Information Security Governance as risk assessment element, and can provide pressure or incentive to corporations for consideration of information security.

Thus, Information Security Governance is the field that both government and private sector can work severally towards the ultimate Internet security.

5-3. Next Generation Network (NGN)

The Internet world contains countless issues to be addressed and discussed. Some of them were briefly observed in section 4-3, and discussed in detail in the report of NGN. GDBe recommend that NGN will be realized in the near future and will extend a basis for critical telecommunication infrastructure. When it is realized, the current Internet can coexist with NGN, and then the whole network will work to the benefit of all the players, from government to citizens, from corporations to employees, and from vendors to consumers.

GDBe is now focusing on the promotion of NGN. The activities will concretely take place towards the next year, and is expected to be influencing various NGN development initiatives.

5-4. Vulnerability Information Handling Network

Vulnerabilities are one of the most concerned subjects of Internet security. There is some successful experience to fight against possible threats and make up cooperative framework among discoverers, manufacturers and coordinators as seen in section 3-1. The framework is currently working in several countries including the US and Japan. The GDBe will suggest that such framework should be established in most of the Internet-advanced countries and such activities should be interconnected. If the interconnection is realized and properly operated, it should be a good basis for multi-purpose, multi-functional collaboration network to cover the world and contribute to the Internet security.

5-5. Network Traceability

There is a consistent argument that if every communication over the Internet is traceable, it would give various benefits to the Internet world. People would be more careful about being affected by viruses or worms, keeping Zombie programs without knowing, sending out virus-affected or otherwise offensive network packets. That implies when traceability over the Internet is established, it would work towards prevention of Internet attacks and unrealized dissemination of harmful communication.

On the other hand, there is an argument that traceability may compromise the anonymity of the Internet, which is one of the features of the Internet and respected by some participants. This feature provides an environment for criticism, claims, performance and experiments. It can work as a cradle for democracy and creation, and in that meaning can work for the benefit of many of the Internet users.

It is, therefore, recommended that traceability over current Internet could be considered and appropriate actions to be taken by taking it into consideration that such work should not negatively affect the freedom of the Internet.

This report is expected to provide some perspective over cyber security. Several topics were picked up as recommendations and suggestions. With those challenges and topics, the Cyber Security Issue Group will contribute to cyber and ubiquitous society. GDBe is now committed to the cyber security in various aspects including SET, Ubiquitous, RFID and NGN. While encouraging all the GBDe members to speak loudly about Cyber Security and to contribute the stability of IT world, the Cyber Security Issue Group is committed to promote the topics referred to above.

Contributions from the Issue Group Members were provided by: Deutsche Bank, Germany; Institute for Information Industry (III), Taiwan; Multimedia Development Corporation (MDC), Malaysia; Fujitsu Ltd., NEC Corporation, Nomura Research Institute (NRI) and TEPCO (The Tokyo Electric Power Company, Incorporated), Japan.

GBDe 2005 Issue Group

e-Government

October 17, 2005

Issue Group Chair: Mr. Kazuo Furukawa, Executive Vice President, Executive Officer & Chief Executive Officer, Information & Telecommunications Systems, Hitachi
Sub Issue Group Chair: Datuk Dr. Mohamed Arif Nun, Chief Executive Officer, Multimedia Development Corporation (MDC) Sdn. Bhd.

1. Introduction

The GBDe has made a number of recommendations on e-Government since it first addressed this issue four years ago.

2001: On the adequate conditions of e-Government from the perspective of the relationship between the Government and private sector.

2002: On the adequate conditions of e-Government from the perspective of the relationship between governments and citizens.

2004: On the conditions of businesses/citizens-participation systems in the processes of making policies, regulations and laws, and on the construction of the systems.

One of the reasons the GBDe has focused on specific recommendations on e-Government is that central and local government are the largest procurement agencies, purchasers, and data/contents holders in our countries and communities. Thus the digitalization of administrative operations and the provision of Internet services to businesses and citizens will accelerate the improvement of IT infrastructures and the promotion of e-commerce.

In fact, the realization and promotion of e-Government has been established as one of the major policies in many countries, including developing countries. According to the "UN Global e-Government Readiness Report 2004", more than 170 out of 190 UN member countries have facilities for the Internet. (http://www.unpan.org/egovernment4.asp). In particular, online services for registration, application and declaration of various administrative procedures are being implemented by central governments in many countries.

In local governments, those services are not always as developed as those in central government due to lack of finance and human resources. However, most of the businesses usually interact more with local government on a daily basis. Therefore, the promotion of e-Government at a local level is an important priority.

In 2005, the GBDe is supporting the promotion and adoption of Open Source Software (OSS) as one of the solutions for further realization and promotion of e-Government.

2. Definition and Features of OSS

(1) OSS is a generic term for software that is allowed to be used and distributed under license agreements which have some common features. The features of license agreements are:

- OSS is free to be distributed and redistributed.
- OSS is licensed for free.
- There is no limit to the objects and uses of OSS.
- Source code must be disclosed and distributed.
- Source code is allowed to be modified.

It is important to note that license conditions are different for each OSS license in the same way that commercial software is sold under various agreements. In addition, OSS is NOT free software. It is licensed for free, but there are usually charges for additional services such as maintenance, technical support and distribution. Linux is the best known OSS software.

(2) The following effects are expected by adopting OSS.

1) Vendors will be able to compete with each other on the same infrastructure when Governments procure software products with specifications that are disclosed to the general public and which can be implemented by anyone in accordance with open standards. Accordingly, Governments will have greater opportunity to provide e-Government services at low cost.
2) Interoperability between information systems will be realized by adopting software products whose specifications are disclosed. Consequently, Governments will be able to respond to requirements of the development, maintenance and transition of systems, avoid locking in particular products or services, and ensure the flexibility of procurement in the future.
3) The flexibility of procurement will be assured by disclosing the specifications of software. Therefore, it can be expected to reduce risks associated with skill training for people required for transition of systems, data conversion, and system operation.
4) Interconnection and data exchange between relevant organizations, including different government agencies, will be realized by assuring interoperability between systems. As a consequence, Governments will be able to provide services required by businesses, citizens and organizations concerned in a timely and effective manner.

5) Even people other than the developer of relevant software can engage in inspection of the source code, which is disclosed and allowed to be modified. Thus, there will be less risks that “black hat hackers” leak confidential and personal information. Even though security holes may be found in software, third parties will be able to fix the problem without relying on the software developer.
6) Software itself or source code can be reused as a part of the other software which builds e-Government infrastructure because there is no limit to the objects and uses of software.

3. Current Trends in OSS

The following reports on the adoption/application of OSS provided by GBDe member companies and cooperating organizations and associations illustrate the growing importance of OSS throughout the world.

3.1. OSS Global Overview

IT research and consultancy firm Gartner says OSS is the hottest IT topic and trend for 2005. Gartner says that by 2010, global 2000 IT companies will consider OSS products in 80% of their infrastructure-focused software investments and 25% of business software investments. OSS is expected to revolutionize software markets by moving revenue streams from license fees to services and support.

Major governments outside the United States either have adopted Linux and open-source software or have begun the processes that will lead to adoption. Open-source software, especially Linux, has spread globally to countries and regions that regard it as the best model of software development and an engine of economic growth. Governments see adoption as a way to exploit a promising trend.

The starting point for global Linux adoption began in Europe approximately four years ago. In 2001, the German parliament adopted a resolution that declared the government should use open-source software "whenever doing so will reduce costs". Two years later, a technology advisory group to the European Commission issued a report that called open-source software "a great opportunity" for the region that could "change the rules in the information technology industry", reducing Europe's reliance on imports.

In 2004, $19.5 billion of Linux-related technologies were sold in Poland and Russia alone. During the same period, seven leading Indian enterprises began porting application software and development work to Linux. Those companies included BSNL; Indian Railway Catering and Tourism Corporation; South Asian Petrochem, Ltd.; Kotak Mahindra Bank; IDBI Bank; Central Bank of India; and the Department of Treasury, Government of West Bengal.

In Latin America, the six largest markets comprise the fastest growing region for Linux adoption anywhere. The six markets include Argentina, Brazil, Chile, Colombia, Mexico and Venezuela. According to a recent IDC report, "the Linux operating system is gaining

broader acceptance in the vendor and user communities in Latin America, making it one of the fastest-growing segments within the operating system software market".

3.2. OSS in Asia

The CICC (Center of the International Cooperation for Computerization), a public-interest corporation in Japan, held “The 1st Asia OSS Symposium” (in Thailand, March, 2003), followed by the 2nd (in Singapore, November, 2003), the 3rd (in Hanoi Vietnam, March, 2004), the 4th (in Taiwan, September, 2004), the 5th (in China, March, 2005), and the 6th symposium (in Sri Lanka, September, 2005), under the auspices of the Japanese Ministry of Economy, Trade and Industry (METI). Interested parties from Governments, business sectors and academies of more than 10 Asian countries participated to discuss the promotion and adoption of OSS in Asia (cf. http://www.asia-oss.org). According to the report, some countries such as Malaysia, South Korea, India, Indonesia and Vietnam officially set the promotion of OSS adoption as a national priority.

3.3. OSS in Japan

The Japanese government supports the promotion of OSS development, mentioned in “e-Japan Strategy 2004”, as part of its national IT policy. Within this context, the IPA (Information-technology Promotion Agency), a member of the GBDe, is playing a central role in the development of OSS infrastructures in Japan, and in the promotion of information exchange among Japan, China and South Korea regarding the technology assessment, the development of human resources and the standardization, with assistance of METI.

According to the result of the experimental introduction of OSS into schools conducted by IPA, 70% of the teachers appreciated Linux as suitable for use in classrooms. The Ministry of Economy, Trade and Industry (METI) has a plan to conduct further experimental introduction of OSS into local governments this year. The Japanese government is also in the process of formulating new guidelines on OSS procurement in accordance with the “IT Policy Package 2005” designed by the Strategic Headquarters for the Advanced Information and Telecommunications Network Society (IT strategic Headquarters). In addition, in local governments, OSS is increasingly being adopted at the prefecture-level such as the e-bidding system (e-procurement system) of the local government of Shimane prefecture; collaborative outsourcing system of the local government of Hokkaido prefecture; and estimation and calculation system of the local government of Nagano prefecture; to the town-level such as a website for regional specialty goods of Amagi-cho, Kagoshima prefecture. Eight local governments, including Kochi prefecture and Okayama prefecture, have jointly developed basic operational package software utilizing OSS. Furthermore, the “Japan OSS Promotion Forum” has been established as a public-private partnership at the initiative of private enterprises to discuss solutions for challenges which will emerge with the diffusion of OSS. There are also plans to send experts in OSS from the private sector to act as CIO advisers to central and local governments to support OSS adoption.

3.4. OSS in Malaysia

The Malaysian government's initiative for its Public Sector Open Source Software (OSS) is spearheaded by the Malaysian Administration Modernization and Management Planning Unit (MAMPU), an agency under the Prime Minister's Department.

With the vision to create and enhance value using OSS within the Public Sector ICT framework in providing efficient, secure and quality services, the OSS initiative has been established with the objective to:

- Reduce total cost of ownership
- Increase freedom of choice of software usage
- Increase interoperability among systems
- Increase growth of ICT industry
- Increase growth of OSS industry
- Increase growth of OSS user and developer community
- Reduce digital divide

This is in line with the Malaysian government's public sector master plan, targeting to:

- Establish strategic direction and framework
- Develop an implementation plan and roadmap
- Establish an Open Source Competency Centre to support OSS implementation in the public sector
- Formulate policies, standards and guidelines

Amongst others, key advantages for the OSS implementation include:

- Avoid vendor lock-in
- World-wide, royalty-free, non-exclusive and perpetual licensing
- Free source code version control management software
- Better software security
- Configuration management (platforms used & compilers supported)
- Software modifications/enhancements and testing
- Debugging without charge or limitations on modifications and future distribution
- Updated documentation
- Benchmarking and performance tuning

Moving ahead with the implementation programmes, an Open Source Competency Centre (OSCC), functioning as the single point of reference for support and guidance in the implementation of OSS in the public sector was created with the role to:

- Maintain knowledge bank for sharing of knowledge and experience
- Create greater awareness, promote OSS and the OSCC
- Conduct and coordinate OSS training and certification programmes for public sector personnel
- Facilitate, coordinate, advise and assist Government agencies in OSS implementation

- Conduct, facilitate, coordinate and monitor OSS research and development programmes
- Formulate OSS policies, guidelines and standards to facilitate OSS implementation

The Centre's targets for 2005 include:

Activities	**Target**
Awareness	100% of CIOs and IT Personnel are OSS literate
Re-skilling	60% of IT Personnel are OSS trained
	10% of IT Personnel are OSS certified
	20% of teachers responsible for School IT Labs are OSS trained
Education	40% of Institutions of Higher Education utilized OSS education and teaching tools
	20% of School IT Labs utilize OSS education and teaching tools
Procurement	60% of all new servers (hardware) procured are able to run open source operating system
Implementation	20% of School IT Labs have OSS installed (e.g.) office productivity
	60% of web servers (software) use OSS
	30% of office infrastructure (email, DNS, Proxy) use OSS
	30% of desktop solutions (e.g. web browser, email reader) use OSS

3.5. OSS in Taiwan

(1) Background

The growth of the Open Source Software industry has become a key indicator for measuring the development level achieved by a country's IT hardware and software industries. Open Source Software will also provide an important platform for enhancing the overall competitiveness of Taiwan. In order to make it less expensive for business enterprises to use free software, and to strengthen the overall competitiveness of the Taiwanese software industry, on June 3, 2002 the Sci-Tech and Information Committee of the Legislative Yuan held a meeting to "Encourage the Independent R&D of Software in a Barrier-free Software Development Environment to Enhance the Competitiveness and Independence of Taiwanese Industry" at which representatives of various agencies and institutions were invited to discuss the strategies that Taiwan should adopt.
And on June 20, 2002 Executive Yuan convened a meeting for the promotion of free software. During this meeting it was agreed that the Ministry of Economic Affairs, would be responsible for organizing the free software promotion work team and for establishing the relevant promotional mechanisms, as well as for planning out the division of responsibility and the timetable for work item implementation. Subsequently, at the sixth meeting of the National Information and Communications Initiative Committee (NICI), Executive Yuan, it was decided that the Free Software Steering Committee would be established, and a free software promotion team would be formed by the Industrial Development Bureau of the Ministry of Economic Affairs. This plan - Free Software Industry Encouragement Plan - has been drawn up in line with these decisions. It is hoped that the implementation of the plan will facilitate the development of the Taiwanese free software industry and help encourage the use of free software in Taiwan, thereby contributing to the sharing and exchange of information.

(2) Development Strategy

1. Strengthening of the legal framework and development of appropriate incentive measures.
2. Greater emphasis on R&D and manpower cultivation.
3. Promotion of product development and model applications.
4. Establishment of industry standards and certification mechanisms.
5. Promotion of free software community development and international collaboration.
6. Strengthening business opportunity and market development.
7. Furthering the commercialization of free software.
8. Expansion of the free software user base.

(3) Key Implementation Measures

1. In order to ensure effective overall control of the planning, promotion and appraisal of free software industry development, to further the development of free software R&D and bring about the creation of a suitable environment for free software application development, the Government has established a Free Software Steering Committee (FSSC) under the National Information & Communications Initiative Committee (NICI). Under normal circumstances, the FSSC meets once every three months; additional meetings may be held as necessary to deal issues of particular urgency.
2. The Industrial Development Bureau, Ministry of Economic Affairs has also established a Free Software Working Committee under the NICI. The Working Committee serves as an advisory body to the FSSC, implements the tasks entrusted to it by the FSSC, plans the development strategy for the free software industry, implements the Free Software Promotion Initiative, and reviews work performance and achievements.
3. In order to assist in the establishment of a suitable environment for the development of the free software industry, the government provides product compatibility certification, formulates industry standards, provides manpower cultivation services and fosters international collaboration.
4. The government encourages universities, vocational colleges and research institutes to participate in free software technology development, thereby helping to cultivate the talent that the free software industry needs.
5. The government identifies key free software industry development areas to which particular attention should be given, draws up strategies for plan implementation, and formulates the necessary incentives and ancillary measures. Key development areas will be selected every year on an ongoing basis; after selection they are submitted to the FSSC for approval. The key development areas for 2004 were industry development and promotion, product testing and certification, community development and technology applications.
6. Formulation and revision of laws and government procurement regulations relating to free software industry development, so as to strengthen the mechanisms for protection and management of free software copyright and licensing terms, and to encourage the creation and distribution of free software.

7. Encouraging the domestic free software community to participate in international free software community exchange activities, thereby helping to upgrade both the size and quality of Taiwan's free software community.
8. Establishment of mechanisms to foster "cross-strait" collaboration between Taiwan and mainland China with respect to free software industry development, with the aim of developing the international Chinese-language software market and strengthening the provision of free software industry information services, to ensure that the products developed by the free software industry meet the market's needs.
9. Encouraging the adoption of free software solutions for the government's Technology Development Programs and the selection of free software when undertaking purchasing for public construction projects.
10. Utilization of the Ministry of Economic Affairs' industry-specific Technology Development Programs, key product development programs and project loans to encourage R&D in order to provide assistance for free software companies in the areas of technology, products and market development.
11. Encouraging government agencies to insist on the adoption of open source code methods when outsourcing software projects, so as to ensure maximum transparency in the government's IT construction and achieve the government's aim of sustainable development.

Making effective use of government procurement and the eTaiwan plan to stimulate market demand for free software (in so far as this does not violate the principles of fair competition).

3.6. OSS in Brazil

On 29 October 2003, Brazil's President Luis Inacio Lula da Silva, signed legislation establishing eight technical committees aimed at the promotion, planning and implementation of OSS, Digital Bridge and Government systems integration. The coordination of OSS promotion and implementation has been assigned to the National Institute for Information Technology (ITI), organization directly connected to Presidential cabinet (www.iti.gov.br).

ITI has approved the final report that defines the objectives and actions for the implementation of OSS in the public administration in Brazil. 18 guidelines, 12 objectives and 29 main actions have been defined:

The adopted guidelines are the following:

1) Prioritize solutions, programs and services based in OSS to promote cost reduction on IT initiatives;
2) Prioritize web platform for the development of systems and user interfaces;
3) Adopt open standards for the development of ITC (Information Technology and Communication) platforms for services and applications;
4) Promote the general use of OSS;
5) Improve the services for citizens through the use of OSS;

6) Citizens must no be obliged to use proprietary platforms when accessing public services;
7) Utilize OSS as a base for Digital Divide programs;
8) Assure full accountability and security for the systems, considering the legislation for privacy and security;
9) Promote the interoperability with legacy systems;
10) Limit improvements on current proprietary systems;
11) Promote the gradual migration of legacy systems to open systems;
12) Prioritize hardware acquisitions compatible with OSS;
13) Assure the free distribution of OSS systems in voluntary and collaborative ways;
14) Promote the improvement and sharing of OSS within and outside the central and local governments;
15) Promote the adoption of new business models based in OSS;
16) Promote culture changes in the public organizations for the adoption of OSS;
17) Promote the training of government employees for the use of OSS;
18) Formulate national policy for OSS.

OSS has been set as national policy on October 2003 and is called "SOFTWARE LIVRE Initiative", coordinated by National Institute for Information Technology (ITI).

Brazilian government agencies, cities and states setting OSS adoption as the policies:
In Brazil, the use of OSS has been officially recommended by Brazilian central government since November 24, 2003. Since then, various public organizations have begun gradually migrating systems, such as Brazilian Senate, Federal Deputy Chamber, Economy Ministry, Federal Data Processing Company (SERPRO), Brazilian Company for Agrobusiness Company (Embrapa), Eletronorte, Petrobras and Sao Paulo Metro Company.

Brazilian States adopting OSS:
Eleven of 27 Brazilian States have issued recommendation for the use of OSS on public systems. The initiatives are called "Projeto Software Livre" and are adopted in the following Brazilian States: Bahia, Sao Paulo, Mato Grosso do Sul, Rio Grande do Sul, Parana, Espirito Santo, Minas Gerais, Pernambuco, Rio de Janeiro, Santa Catarina and Distrito Federal. Some states, such as Santa Catarina and Pernambuco, officially adopted the initiatives, while others remain as non-government organizations.

Some Brazilian cities adopting OSS:
In 2001 Rio das Ostras City, Rio de Janeiro State, officially adopted OSS as standard and created its own distribution called TATUI, widely deployed on all computers.
Recife City, capital of Pernambuco State instituted the use of OSS by law number 16.639/2001 issued in 2001.

Advantages and Challenges of OSS adoption pointed out in those policies:
Rio das Ostras city and other Brazilian organizations pointed out that in addition to the cost reduction with software licenses, the flexibility to customize the software for their needs and possibility of using limited microcomputers to run OSS applications are the

main advantages. As the main challenge, they pointed out the need for training of public employees.

3.7. OSS In India

In August 2005, two vendors launched entry-level PCs that run Linux and are priced at about US$230 (Rs 9,990). These initiatives have been backed by India's Minister for Communications and Information Technology. Currently, 15 million people in India own a PC and there are 5 million Internet connections in the country. The aim of the Indian government is to increase the number of people owning a PC to 75 million and the number of Internet connections to 45 million by 2010. The Indian government has also set up an open-source center in Chennai to develop open-source software to get around the high cost of proprietary software.

3.8. OSS in China

International pressure against software piracy has encouraged development of OSS in China. Red Flag Linux claims that its Asianux is one of the most popular Linux distributions in the world. Besides being especially strong in servers, it is also the market share leader for Linux desktops in China. It has been reported that the software industry in China has been growing at 30% per annum.

3.9. OSS in GCD Member Cities

According to some cities of the Global Cities Dialogue [www.globalcitiesdialogue.org], local authorities are more and more aware of the important role played by OSS as regards to the implementation of e-Government. Even though few interviewed cities have adopted a favourable policy in this field, most of them are currently implementing OSS applications (75% of the polled cities) or are counting on OSS to support the application of Information Technologies in the city administration and to develop projects aiming to reduce the digital divide [s. the experience of Brazil].

On one hand, the status of implementation of OSS in local communities is still considered as unsatisfactory. On the other hand, the will to develop OSS-based running systems and office applications seems to be increasing.

Cities surveyed by the GCD mainly use OSS applications for their servers, web sites and Intranet networks. The advantages of OSS which are most praised are not only the lower costs, the ease of use, as well as the higher flexibility and independence from the vendors, but also the possibility "opened" by this kind of software to improve the communication between citizens and administrations. In particular, open source software and contents are considered as "a new way to promote the creativity and productivity of the community as well as to strengthen the civic and public aims of the city's portal" (e.g. the Municipality of Bologna with the "Iperbole" city network).

OSS has been largely applied in Germany to develop online services of the public administrations for citizens and business (from the registration to the assignment of public contracts), as well as to implement e-government solutions based on innovative signature and encoding techniques, including electronic paying systems for public

administrations at national, regional and local level (e.g. the Free Hanseatic City of Bremen with the "Governikus" system).

In France a cooperative platform named "AdmiSource" has been proposed to the administrations to allow the development of free software and to support the implementation of e-Administration projects. The importance of OSS and free software as motor of e-Government has been even recognized by the European Parliament, which has recently rejected the directive on the "patentability of the inventions realized by computer", proposed by the European Commission (6 July 2005).

Indeed, as regards to the implementation of OSS in the public administration, success will depend on the extent in which this new software will be accepted by users. Therefore, it is essential to involve the citizens in this process and take their expectations and needs into account. This should also help to overcome the obstacles of software producers who are not always favourable to invest in the development of OSS, if there is not a strong demand from the users [s. the experience of Munich, Germany].

4. Challenges and Solutions on the promotion of OSS adoption into e-Government

The following challenges have been frequently pointed out, however, the GBDe would like also to offer some solutions:

Challenge 1: Due to the lack of precedents of OSS adoption, the effects offered by OSS have yet to be fully recognized.
Solutions: - Develop and publish policies at central and local government level to support the adoption of OSS into information systems.
- Establish pilot OSS projects and then evaluate and publish the results of these projects.

Challenge 2: A lack of competitive growth among OSS vendors means benefits of OSS adoption have sometimes been difficult to identify.
Solution: - Implement a software engineering development policy through industry-academia-government collaboration.

Challenge 3: A lack of investment in personnel training and education, which has resulted from IT vendors' concerns about the negative effects on business activities such as shrinking of the market size, is hampering development of OSS.
Solution: - Governments should apply savings gained by OSS adoption to IT vendors' services to build the advanced systems.

Challenge 4: The standards necessary to ensure interoperability between OSS systems at a global level have not yet been specified.
Solution: - Consider the establishment of organizations and develop conferences so

to encourage cooperation between countries to create the appropriate standards in proper sequence.

OSS is not, of itself, a panacea which will enable the realization of e-Government. Nevertheless, it is fast becoming an important component in the provision of easily accessible and low-cost services to citizens. As representatives of private enterprise, the GBDe will endeavour to support the efficient and widespread adoption of OSS.

Contributions were provided by the Global Cities Dialogue (GCD); CICC (Center of the International Cooperation for Computerization), NEC Corporation, Japan; Multimedia Development Corporation (MDC), Malaysia; Institute for Information Industry, Taiwan.

GBDe 2005 Issue Group

International Micropayment

October 17, 2005

Issue Chair: Shyue-Ching Lu, President, Chunghwa Telecom, Taiwan

1. Introduction

From past investigation, there is no doubt that the existence of appropriate payment systems is vital for the development of e-commerce. The real experience indicates that the volume of micropayment has dominated the transactions of B2C e-commerce in the past three years. The percentage of micropayment transactions as a percentage of total B2C e-commerce has risen significantly from 2004 to 2005. In the meantime, the average user's age has decreased gradually every year, in particular, teenagers have become the major users, especially for digital content transactions.

Micropayments are a means for transferring money (less than US$15 for each transaction and less than US$ 100 for each billing period) in situations where collecting money with the usual payment systems is impractical, or very expensive, in terms of the amount of money being collected. Generally, micropayment systems accumulate many micropayments and collect the accumulated amount of money as one regular payment either before or after the transactions. Examples of situations where micropayment systems are often used in the United States include public transportation systems, university student dining rooms, and tolls on roads. These are all areas where it would be very impractical to collect the price of the service from the consumer each time a service is rendered. There has been a great deal of recent innovation in micropayment systems, in order to facilitate providing content for a fee over the Internet. Many payments are made with credit cards, but processing a credit card payment typically costs the merchant a fee with a minimum on the order of 20¢ plus a few percent of the amount of the charge. Clearly charging a customer an amount less than the fee is impossible.

The basis of micropayments is to maintain and take advantage of the very high volume of viewers by offering content for a very small charge. For example, a web comic author would make his online comic book available for 25¢ (USD). Other variations on the idea propose charging fractions of cents (that is smaller than the smallest possible amount of

hard currency) for equally fractional amounts of content, for example, a tenth of a cent per single web page of an online magazine.

Imagine what you, as a potential user, would do in the following two scenarios:

Scenario 1:
Suppose you are now in Taiwan, interested in watching a Korean drama that is available on a Korean website. How do you get it? How do you pay for the service?

Scenario 2:
On your business trip to Japan, after your business activities, you sit in a park where Forma/WLAN is available. You would like to get on to the Internet. How do you do it and how do you pay for it?

Scenario 3:
Suppose you are now in Taiwan, interested in browsing some pages of Discovery magazine that is available in worldwide website. The service is charged by the page. How do you get it? How do you pay for the service?

The scenarios mentioned above could very likely happen in our daily life. However, the corresponding payment mechanisms satisfying the users, especially teenage users, in a cross-border transaction scenario are few and far between. The major barriers can be summarized as:

1. The payment tools are not readily offered to all users, especially not available for the group of major users, namely, teenagers.
2. The psychological barriers include lack of consumer confidence, fear of disclosure of privacy data and the possibility of cross-border transaction dispute.
3. The shipping/handling is still poor for cross-border transactions.
4. The operators are skeptical about the viability of the investment required to set-up international payment mechanisms.

As the level of consumer's concern grows proportionally with the level of accompanied transaction risks, including the real loss and the impact of inadequate privacy protection (data disclosure), we believe that the promotion and establishment of international micro-payments will be better accepted than Internet payment, especially for digital content transaction.

At this time, widely adopted and trustworthy international micropayment mechanisms are still lacking in most countries although some micropayment tools have been applied to e-commerce transactions in individual countries. In this recommendation we begin with providing an overview of current developments in micropayment, then identify reasons for the current stalemate despite an urgent need for the marketplace, and finally point out a possible approach to overcome the problems.

2. Existing Micropayments

Current status of development and application in member countries

Some countries apply micropayments to services such as digital content transactions, (vending machine) drink purchase, public transportation systems, university student dining rooms, and tolls on roads. They have already started to issue digital e-wallets that may be used in daily life. Most of digital e-wallets are contactless-card based with a virtual ID embedded and can be used for e-Government as well as commercial purposes. Below we list a few examples:

Japan

- **Micropayment by prepaid (online):** For this kind of micropayment, the customer usually has to previously pay the money by cash, credit card or ATM then transfer an equal-value of virtual money amount into his web account. WebMoney, BitCash, NTT-Communications Chocom, Nippon Shinpan Digicoin, C-Check, QQQ Card and QUO all belong to this kind of micropayment.
- **Micropayment by ISP account:** NTT Communication has launched a micropayment solution - "CoDen" service since Oct. 2004. The CoDen service is an agency receipt service using monthly phone bill. By May 2005, there were at least 30,000 users of CoDen. Nifty, @pay, Biglobe E-MYCASH, OCN PayOn and So-net Smash are other likely payment systems.
- **IC-card based:** Among micro-payment systems in Japan, profusion of DoCoMo's i-mode mobile phones is noteworthy. The number of i-mode subscribers has reached over 42 million. Since i-mode was already equipped with infrastructure with functions such as user authentication, terminal authentication, and payment services for data usage, it was relatively easy to implement copyright protection and content billing as represented in the music download business. Therefore, i-mode provides a micropayment platform that combines IC-card payment with the functionalities of a mobile phone. As actual business transactions using i-mode, approximately 150 billion sales of billable contents and hundreds of billion yen sales in e-commerce are reported in this market. It should be noted, however, that other mobile phone companies are also providing competitive services (as of October 2004).

  Edy and Suica, using same technology platform called Felica, are in the mainstream. For Edy, mobile phones mounted with functions of Edy (Felica) have been made available lately. The total number of smart cards and mobile phones equipped with Edy functions amounts to 7.4 million and the number of stores ready to accept Edy is reported to be 14 thousand (as of January 2005).

  Suica started as a non-contact railway pass system run by JR East but has largely expanded its functionality today as electronic money. In addition to the convenience of electronic money, convergence with other uses such as credit cards, employee ID and student ID cards is progressing. The number of Suica

cards issued to date is approximately 8.3 million and stores ready to accept Suica are reported to be in the range of 35 thousand (as of March 2004).

PiTaPa and JCB Quickpay are the likely payment tools.

- **Other micropayments:** There are two kinds of micropayment, Internet banking and credit card solution in addition to the three kinds of micropayment mentioned above.

Taiwan

- **Easy card:** In 2004 Taipei city government started to extend the Easy card to other traffic payment services such as taxis and public buses. Before 2004 the Easy card was only utilized for subway tolls. It is rechargeable and number of issued Easy cards reached 1 million by the end of 2004. Easy card is forming a partnership with 4 banks at present. This may involve the adoption of an IC-card specification which will enable it to work as i-Cash; which means it will probably be able to enjoy wider application.
- **Financial IC card:** The IC card-based payment tool has been integrated and has been popular in Taiwan but is limited to domestic applications only. The IC cards are all issued by the banks and the issued amount achieved 17,000,000 in May 2005. The amount will have risen to 25,000,000 over the next year. However, the financial IC card applies only to domestic transactions except for that issued by few banks. Even in the case where IC cards can be used in other countries, there are very few stories or ATM services ready to accept them.
- **E-coin:** Yu-San bank issued e-coin micropayment to overcome the usage barriers such as teenage use and transaction processing costs. Up to 2004, it recruited more than 300,000 members, among which some 210,000 were active users. Usage of this micropayment is confined to domestic transactions at the member stores of Yu-San banks.
- **I-cash:** This micropayment solution is provided by a major convenience store chain (7-eleven). I-cash is a pre-paid and rechargeable virtual card with a specification similar to an IC Card. The customer has to purchase and charge the card at a physical convenience store. The transaction processing fee is charged only when money is retrieved out from the I-cash account. By the end of 2004 some 17 million I-cash cards were issued.
- **Paypal:** e-Bay made a pre-paid digital e-wallet available to all its bidding members. By the end of 2004 about 78 million user accounts in the world had paid for transactions with Paypal.
- **Micropayment by phone bill (ISP account):** The payment service by monthly phone bill has been available since 1998. Up until the end of 2004, there were around 5 million transactions per month totaling about 0.3 billion Taiwan dollars. The annual growth rate is for the amount of transactions is 33% and the total number of customers has reached 2 million. The purchased objects include digital content such as recharging of online games, music download and movie download. HiNet AAA, emome 839 and I-style are the typical payments.

Korea

- **Payment by phone bill - Teledit:** The teledit micropayment is operated by Danal company. It achieves 53% of the market share and is the biggest one in Korea. The participating websites have reached 6,000 and the total transaction fees have risen to 2 billion Korean won. This is a similar to the e-coin micropayment method. Its market share is about 20% of the phone bill payment market.

Europe

- **Direct debit transfer:** In Germany there is a very efficient banking system that allows money transfers as well as direct debit for transaction costs of 5-20c (for large vendors, prices might even be below 5c). For other Europe countries, direct debit transfer is also a dominant payment method. Many people have flat rates that allow them to transfer money without any additional costs. Hence, money transfers are used for micropayments. For example, there have been reports of charges as low as 0.89 EUR via regular direct debit money transfer and transfers of between 1 and 5 EUR for purchases on e-Bay. It is possible to have a money transfer all over Europe (project SEPA - single European payment area). However, prices might be higher for cross boarder transfers. GeldKarte and Paysafe card are the typical solutions.
- **Debit/Credit card based:** Basically, this kind of micropayment is a prepaid solution. Firstgate Click&Buy and infin micropayment are the typical examples.
- **Payment by phone bill:** Services that are provided by a telephone company are charged to the telephone bill (like any kind of services). In addition, there are aggregators for Internet payments (like, e.g., Firstgate Click&Buy and others) which charge a certain amount (e.g. 10 EUR) via direct debit to your account, which you might spend in small pieces at Internet shops. However, these payment providers come along with a high disagio (in most cases more than 10%) which makes them attractive only for niche markets. T-Pay, MobiPay and DaoPay are similar micropayments. DaoPay is available for cross-border payment. The payment gets from everybody with a phone.(?)

United States

- **Email-based payment systems**, including PayPal/X.com and Flooz, bill the sender's credit card or bank account, or deduct the payment from an account prepaid by check or money order. PayPal recipients may receive payment by check, or have it directly deposited to a bank account; Flooz recipients may use their payments at certain online merchants.
- **QPass** is another wallet-based system that bills the buyer's credit card for aggregated purchases, relieving merchants of some of the per-transaction burden of other credit-based online micropayment systems. The New York Times Neediest Cases Fund used QPass in November, 1999, to receive online donations.
- **Cybercoin**, the micropayment system developed by Cybercash. Through partnerships with ISPs like Concentric Networks, Cybercash may be able to offer other e-commerce packages that will include micropayments.

- **Millicent**, a micropayment system implemented by Digital Equipment Corp, now owned by Compaq, with wallets starting at 1000 yen and payments as small as 5 yen (approximately $0.04 at launch time).
- **E-gold** for a modest fee, stores the entire "e-metals" (gold, silver, platinum, and palladium) account you purchase and allows you to conduct electronic transactions of all sizes with other account holders.
- **Bee-Tokens** are a virtual currency purchased from Bee-Tokens.com. Bee-Tokens are accepted by any website that participates in the Bee-Tokens currency method. Each Bee-Token is worth USD $0.10. Bee-Tokens are used to pay for pictures, fan fiction, music, white papers, essays, horoscopes, donations, and other Internet merchandise.
- **Phone-bill/ISP account based:**
    - Trivnet's WiSP merchant server, which does not require buyers to download a wallet, bills micropayments to the consumer's ISP account. Its e-commerce solution is still used by credit-card, and m-commerce solution is billing by mobile ISP account.
    - iPIN also bills digital content purchases to the buyer's ISP account. In September, 1999, it entered into agreements with several digital music companies to handle web-based payments for their online musical content.

3. Problems Faced when Extending Payments to Cross-Border

Most of the micropayment systems mentioned above are only available for domestic transactions. What problems do we face to when the payment is extended from domestic to cross-border? Fig. 1 is the system architecture diagram from micropayment to international micropayment (IMP), taking an example for the cross-border transaction between Japan and Germany. The figure is helpful for thinking about these issues. There exist six kinds of role in the IMP system, including merchant (content provider), user, payment service provider (PSP), IMP center, ADR organization and government.

Most of the micropayment services are provided by MSP (Micropayment Service Provider). The role of MSP is to relay the paid value as the intermediary. This means that the paid value is transferred in two stages; consumer to MSP and MSP to shop/merchant. The real value transfer related to these stages might occur independently on the corresponding trade. In any case, the role of the MSP is twofold: one is that of collecting/receiving the money from the consumer and the other is the role of delivering the money to the shop/merchant. This role model is not only applicable for micropayment, but also applicable for credit card-based payment. In the case of credit card-based payment, the service provider for the consumer is called issuer and the service provider for shop is called acquirer. These service providers, under the international credit brand, provide the credit payment services collaboratively. A similar business model might be applicable to global micropayment services. This means that the micropayment service providers for consumers and the micropayment service providers for shops in another country could collaboratively provide payment service for cross-boarder e-trading. Interoperability agreements might be established between two types of

micropayment service providers. These agreements would act as the international coordinator for IMP.

In general, the issues faced when extending the payments to cross-border include multiple system integration, business concern, tax regulation, legislation gap among countries, transaction dispute handling and security and consumer confidence.

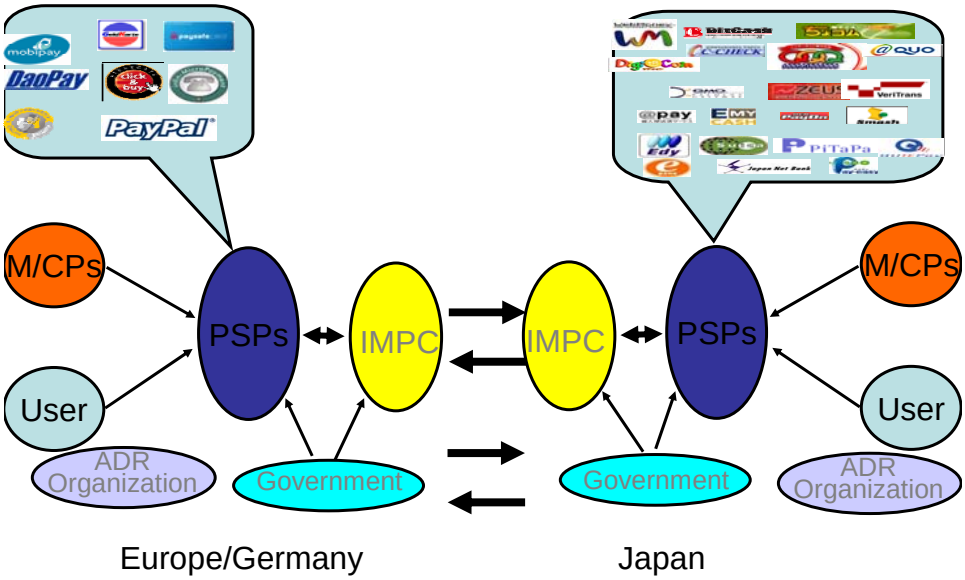

Fig. 1: Interacting Roles in International Micropayments

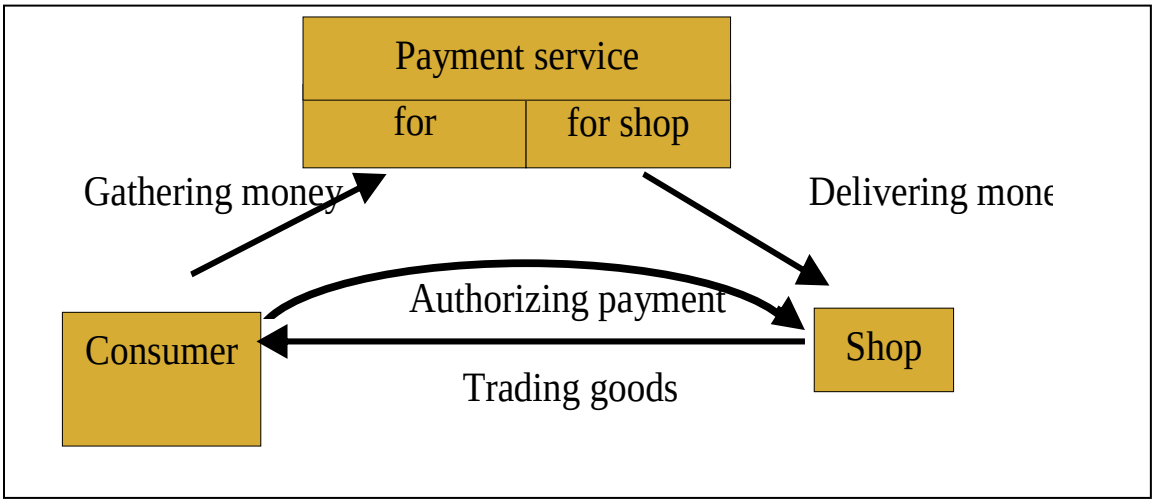

Fig 2: Payment Service Model

System Integration Issues (multiple system and multiple technical specifics)
Before applying a micropayment to cross-border transactions, it would be very helpful if there was an integrated and simple payment platform which ran well in a domestic setting. The existence of a common protocol for system interface is essential for the

integration of multiple micropayment systems. Unfortunately, most of the micropayments systems have no common system interface at this moment. This phenomenon is typical in the case of client device or payment work flow or system interface. Even though technical issues as such are not the most difficult part, they still need to be dealt with.

Various technologies or business models for MP were identified in a mid-2005 GBDe meeting in Taipei. For example, it was mentioned that there are well-known micro-payment services based on stored value card, such as SUICA and Edy. Although these types of micropayment are successful in a local or domestic environment, they might not be feasible for an international scheme. As stored value based micropayment requires using same technology for both consumer side and shop side, which might not be a big problem in local market, it will be a significant obstacle for global acceptance in international market. Therefore, it appears that some MP technology might need to be excluded from IMP consideration in order to facilitate our work in the initial stage.

Business concerns (cost, marketing)
Motivation is always a key factor in successfully realizing a new idea. This phenomenon is more obvious in the business context. Hence, the transaction volume and marketing demand for cross-border transaction are often the issues that the cooperating partners care about most. Until now, there has been no objective investigation indicating how strong the demand for cross-border transactions is or how much profit they will generate. The operational experiences from many websites indicate that 20% of the users are from the foreign countries even though there is no real data to support this contention. On the other hand, since there is no boundary for commerce over Internet, it is predicted that the demand for IMP will grow stronger as e-commerce booms. A major concern from the merchant's side is the cost of processing. It is expected that the cost should not increase too much if the selected micropayment system has already been in operation in the domestic setting. For merchants it will be a good incentive if a well functioning cross-border payment can extend their market to foreign countries. In current e-commerce, credit based payment services are widely accepted even for international transactions. Therefore, any payment service applicable for e-commerce should be provided at a competitive level of cost with that of the credit based payment. Otherwise, it will be difficult to achieve critical mass. In general, the merchants evaluate the operation cost against the directly added revenue. Here, the cost includes the loss incurred by bad debt, extra hardware and software setup, and revenue share of payment providers.

Tax regulation (VAT gap and different tax policies among countries)
In most parts of the world, it is commonly required to pay the value added tax (VAT) with each transaction and the differences of tax rate among countries can be significant. A 5% VAT is popular for the countries in Asia, while 10% or more in Europe and North America is often seen. With different tax rates, goods' price will be variable for the customers from different countries. This means that there needs to be a common and clear understanding regarding a varied pricing list for different countries from customers and stores. Otherwise, numerous transaction disputes are bound to arise. Additionally, the policy of withholding tax is different in different countries, even within the same region (e.g. Asia). This problem makes the process of revenue sharing among the agencies and

stores more complicated. Furthermore, to reduce as much as possible the cost of conversion between different currencies among the banks is very important, as it will affect the final revenue to be shared among agencies and stores. The situation is more obvious for IMP because the transaction fee is in micro scale. In other words, the profit of store will be decreased if the agency fees are kept, which will affect the willingness of the store to adopt IMP.

Legislation gap among countries (operator constraint, banking law, consumer protection law for different countries)
In addition to the tax issues mentioned above, the legislation gap among different countries is yet another issue. For example, while the German "Fernabsatzrichtlinie" (federal distance selling policy) ensures that the customer has the right to annul the agreement within two weeks (without having to state a specific reason), related policy is different for countries in Asia, where the right to annul the agreement within one week is common practice. Differences, as such, will inevitably cause the problems of increased operational cost and transaction disputes for stores and customers respectively. Furthermore, the license constraint for settlement vendors in banking law may not be the same in different countries. This allows the vendor to play a clearing-house role but not to operate as a settlement vendor in law. The solutions or alternatives of all these problems are pressing concerns for IMP.

Transaction dispute handling (how to inquire and process efficiently and reliably)
Transaction disputes are normally handled in accordance with related laws or regulation, while ADR is reserved for handling the exceptional cases. For example, the customer might expect to receive the goods or services, however this does not turn out to be the case even after successful authentication and authorization of payment; or the customer might not be satisfied with the received goods after paying the money; or the charged bill is not consistent with the customer's understanding. As transaction disputes always exist, a convenient mechanism and a trustworthy organization is indispensable to facilitate the growth of IMP, even if each user's individual loss (of the payment) may not be so much.

Security and consumer confidence (security requirement for different payment tools, trust strength, operator credit and user recovery)
A large number of security and consumer confidence problems are due to human psychology. While a very popular payment service complying with regulation in law and security always attracts more users to join it, past experiences reminds customers that there are always risks with network transactions. Customers need to be constantly reassured that due diligence is present. Fortunately, as transaction risks are proportional to the transaction fee, this issue but might not be as critical. However, privacy in an open society requires anonymous transaction systems, and this is especially true for digital content services.

Although e-commerce is borderless, most e-commerce today remains within national boundaries. Latest statistics show that in Germany more than 99% of e-commerce is domestic. One reason might be that the usage of German language is not common in

international shops. Another (and probably more important) reason might be that people in Germany trust German shops more than international ones.

Thus, requirements to facilitate development of micropayments are:
- everyone should be able to use the system without additional subscription etc.
- systems should be based on people's experience with payments
- low transaction fees.

4. Current Situation in the World for Solving IMP issues

Most of the governments in the world care about the development of e-commerce, especially for the financial business and tax. The phenomenon is more obvious for the countries where e-commerce is growing most rapidly. However, the efforts and concrete adopted results in the IMP is not enough.

System integration

- **Taiwan**

Currently, there are at least 17 operating micropayment systems for internet transactions in Taiwan. To reduce the number of micropayment systems through system integration and marketing examination has become a common sense approach for all payment operators. Before carrying out system integration, the environment on the client side has to be examined. For example, to integrate micropayment systems based on a physical card, a compatible card reader and system platform is needed. A solution plan using a 3G USIM card has progressed under a Government initiative. However, the evolution of current micropayment systems on the Internet still does not show the trend toward integration. Except for the phone bill micropayment, there exist differences in the whole transaction flow for most other systems. From the driving force in customer base, it appears that phone bill micropayment and Paypal of e-Bay have their own advantages even when extended to cross-border payment. An integration of phone bill micropayment with up to 95% coverage rate in customer base in Taiwan has been provided by Chunghwa Telecom, starting from 2005. Chunghwa Telecom’s experience shows that with the integration of one usable IMP system for phone bill payment, technical issues are less of a problem; rather the tax and regulatory issues are major concerns.

- **Japan**

From a system integration point of view, Japan is better than other countries. For smart card based micropayments, a common platform - Felica almost dominates the micropayment market in Japan. The favorable environment is due to the fact that large companies mandate the setup of a common system interface. On the other hand, other micropayment systems have their own business policy for system integration, such as the case of NTT communication CoDen services.

- **Germany**

The micropayment systems are fewer than in many other countries. This situation may be related to the different consumer behavior in Europe, where people are accustomed to paying bills by credit card in similar situations. Hence, system integration for various micropayment systems is probably not the first priority, rather a common trustworthy infrastructure for strengthening consumer confidence is the important requirement. This may also apply to situation in North America.

- **Business concern**

For IMP, in the aspects of transaction amount and invested cost, there is presently not much difference among various countries. The study and investigation of customer needs is progressing. However, judging from the example of Korean fans and Japanese fans in Taiwan, it is predicted that will be a strong demand for IMP. This phenomenon is particularly obvious in the countries with a shared traditional Asian culture.

- **Tax regulation**

For e-commerce, the trend of tax policy is towards being low and simple, although VAT likely to be imposed on cyber biddings in some countries. While e-commerce is highly encouraged in Taiwan, it is still hard to avoid basic VAT. The withholding tax is expected to be waived for IMP in the future for the transaction of digital content.

In Japan, the tax regulation is similar to Taiwan. The 5% VAT is the basic tax (same as in Taiwan and in Korea). So the gap among the countries in Asia is smaller than in Europe and America. This condition should facilitate the realization of IMP in Asia.

- **Legislation gap reduction**

The differences in law among different countries cover the law of consumer protection, money transfer and operating constraint for settlement vendors in banking law. Addressing this issue is an important objective.

- **Transaction dispute manipulation**

ADR is always a key issue for e-commerce. This is true not only for IMP but also for other Internet transactions. Fortunately, the concept of an ADR alliance has made significant progress during the past three years. A global alliance organization is being set up through the cooperation of trust-based organizations such as BBBOnline of the USA, as well as ECOM of Japan and SOSA of Taiwan.

- **Security and consumer confidence**

Currently, a common secure transaction protocol called secure socket layer (SSL), with 128 bits triple DES encryption algorithm, is widely adopted for Internet payments. The protocol can also be applied to IMP. Personal privacy and data protection are still primary concerns with IMP. In Taiwan, the protection of personal privacy data has risen to the legal level. It is expected that the related legislation will facilitate the progress of IMP. In the system design for IMP, it is very important to ensure that order information and privacy payment information are kept separately and protected securely by the

appropriate parties. In the meantime, a transaction/settlement policy by service deliverers emphasizing customer-protection will be positive for boosting consumer confidence, especially for the customers in Europe.

5. Recommendations

Undoubtedly, most of the issues regarding Internet payment still need to be resolved for IMP. While some issues may not be as sensitive in the case of IMP, due to smaller individual transaction fee, some issues will be more critical, such as requirements for transaction performance, cost per transaction and convenience. The GBDe believes that the identification of specific business domains and inter-connecting service providers with the micropayment systems widely used in those domains will enable phased implementation. For example, a small scale field trial through the vendors from different countries, say, between Chunghwa Telecom and counterparts from Korea or Japan should be tested for the feasibility of the model.

Nevertheless, the danger is that without a sustainable model, IMP by itself will not grow into a big business and that subsidizing the expense to ensure connectivity among service providers will be difficult. Hence, IMP is a “hard” business. However, due to its nature, it will be easier and more successful for specific transactions such as those involving digital content.

Realization of a micropayment system is most likely to be successful if it is driven by existing major players (like banks or telcos). However, even with that, it does not seem to be sufficient. The following aspects should be taken into consideration when planning IMP in a real market.

- The usage in real-world may be not a killer application because people still prefer established payment behaviour. This should not be neglected when implementing IMP.
- Extra and expensive equipment (like card readers) will raise the barriers toward widely-used payment.
- Even in cases when usage is convenient (like being in a parking garage without sufficient coins), there could be situations when the system cannot be used, e.g. because money needs to be stored on the card prior to a purchase. Hence, both an easy-use e-wallet and a ubiquitous environment to charge money are essential for card-based micropayment.
- Eliminating doubts from consumer and reducing the risk of shops are two important issues to be addressed in building IMP.

Recommendations for Governments

The recommendations for governments are:

- Removing international differences in legislation and tax is a priority for the provision of international micropayment. Tax incentives are needed to encourage IMP.

- Governments should lift restrictive regulations and allow non-banks to enter the micropayment arena. Governments should also encourage dialogue among various electronic payment service providers, including banks, telecommunications and e-purse companies to ensure safe and seamless integration. This could include dialogue on issues such as:
    - Industry self-regulations and mutually accepted business practices, e.g. settlement rules and dispute resolutions.
    - Applications of innovative online payment technologies and installation of related business agreements.
    - Compilation of review opinions on relaxations of current legal environments, e.g. digital signatures and bank deposit policies.

- A convenient and trustworthy ADR network for international transactions is needed to be established as soon as possible with Government support.

- For each country, integrating multiple micropayment systems into a single transaction platform for each class of micropayment system is essential.

- Specifically, governments should take an active role in fighting the rapid growth of cyber-crime to ensure privacy online and to protect payment and transaction information. Other related priorities include:
    - Online transaction information and privacy should be carefully protected in both public and private sectors.
    - Outsourcing services on e-payment should follow strictly enforced security procedures to ensure continuing growth.
    - High awareness of cyber-crime through consumer education, e.g. phishing & skimming and others.
    - Rapid modernization of laws and regulations in related areas.

- Governments should support cross-border e-commerce, e.g. rapidly growing digital content or online media services. States should work towards establishing a more convenient, transparent and more fully integrated environment for international micropayments. The following measures should be considered:
    - Periodical update and dialogue between the Government and private sector regarding changing industry needs.
    - Comprehensive review of regulations to suit new technologies.
    - Harmonizing of consumer protection, banking, taxation and invoicing policies in different territories to facilitate cross-border e-commerce and e-payment.
    - Providing incentives for digital content or online media industries which are among the most widely subscribed cross-border paid services online today.
    - Developing certification systems for various micropayment services to guarantee honest services from online payment service providers domestically and overseas.

Recommendations for Business

- The private sector should seek to form cross-industry and trans-disciplinary e-payment service organizations which could then influence governments in promoting m-commerce and e-commerce.

- Such trans-disciplinary organizations should share business practice consensus and adopt minimum security requirements in order to facilitate cross-border integration, particularly with regard to mobile payments.

- e-Payment industry integration should include establishing common interfaces for consumers' convenience and confidence. It should also cover common policies on ADR, privacy and security.

- Industry should recognize cultural and business differences between countries and should take lead in building consumer trust through harmonized ADR, trustmark and escrow mechanisms.

Contributions from Issue Group Members were provided by: Deutsche Bank, Germany; Institute for Information Industry, Taiwan; Multimedia Development Corporation (MDC), Malaysia; NEC Corporation, Nihon Unisys, NTT DATA, TEPCO (The Tokyo Electric Power Company, Incorporated), Japan

GBDe 2005 Issue Group

Next Generation Network

October 17, 2005

Issue Chair: Mr. Kazuto Kojima, Special Representative, Fujitsu Limited

1. Introduction

The current Internet is facing so many challenges. First of all, service is on a best- effort basis. There is no guarantee that an email message really goes through to the other end, and no one knows how long it takes. Furthermore, no one knows that the party on the other end is the person intended to receive the communication and/or the party sending the mail to this end is a trustworthy person with good intentions. This is the weakness of the current Internet and has been one of the main causes of problems such as SPAM mails, Phishing, Viruses, Net Fraud, to name a few.

A lot of countermeasures are taken to cope with this situation. They are, however, a patchwork of solutions for individual problems and never a total protection against these malicious activities. When the Internet was first envisaged and realized, it aimed to be a communications media among a limited number of trustworthy members. But, once the Internet expanded and became the communications tool for the anonymous many, the system, based on "the ethical doctrine that human nature is fundamentally good," revealed serious weaknesses.

Worried about these conditions, engineers and researchers have started investigating the possibilities of a truly safe media for communications and e-commerce by building new networks where malicious activities and criminal actions are not possible.

At the same time, the current Internet has become an important tool for society used daily by the billions of people in the world at reasonably low cost. Even if totally new and safe networks are physically feasible, it does not make sense because construction cost would be so high and only a small number of people can afford to use them. Furthermore, the Internet traffic is explosively increasing and could eventually burden the capacity of certain networks. The Internet is currently relying on certain networks built by telephone operators for telephone connections. Who should be responsible to build new networks that have the capacity of handling all the demands in the future, spending large amount of

money? We need to address this issue from the view point of the "Internet Economic Theory".

Anonymity is said to be the shortcoming of the current Internet. There is, however, an opinion from a sociological point of view that it is necessary to guarantee the freedom of speech of the people and to ensure democracy. The system that is always capable of identifying the party on the other end might have a danger to suppress the free expression of opinions, hindering the sound progress of democracy. How we should strike the appropriate balance between the human rights and public safety?

Being aware of these issues, the GBDe started a study of the NGN this year. But, as you may know, the issues relating to the NGN cover a wide range of topics from sociology to technology. The studies by interested organizations have already started, and any agreements, if made, on the NGN may well take several years to two decades.

In this Issue Group, therefore, the GBDe investigated, as a first stage this year, which governmental/international/private sector organizations are doing what kind of research on the NGN. Some issues will naturally overlap the study by other Issue Groups such as the Ubiquitous Issue Group. These issues will be sorted out in due course.

2. Situations by Country

1. Japan

1) COCJ (Committee on Competitiveness of Key Technology Industries- Japan)

In Japan, the COCJ, consisting of members from 24 major companies, the Tokyo Institute of Technology and Osaka University, have started a study on the "Development of the Safe and Trustworthy Next Generation Network," since January of this year at one of the working groups in the committee.

The basic concepts of the NGN they are proposing are:

a) Capable of providing high quality communication
   - High speed virtual private network
   - Resilient emergency communication

b) Safety
   - With the trustworthy authenticated identifiers put at the end of each packet, we can always be sure that who sent the message from where and when

c) Reliability
   - Network monitoring and fast detour building capability in case of line failures
   - Mechanism to secure communications measures in case of disasters

d) Major development items
   - IP based network technology
     Total architecture; Technology to secure quality, security and reliability of the network; Router and switching technology; Disaster-proof communications technology

- Applications development
  Next generation development technology of applications (such as information content security)
- Basic component
  Optical IC; Low power consumption devices technology supporting the network
- Making use of current national project relating to quality assurance, high reliability and security of networks. The followings are on-going national projects:
- Research and development of ubiquitous network technology (MIC: Ministry of Internal Affairs and Communications)
    - Research and development of next generation backbone trunk lines (MIC)
    - Research and development of authentication infrastructure technology (MIC)
    - Photonic network (MIC, METI)
    - Next generation high speed communications equipment technology development (METI)
    - Research and development project for the realization of the cutting edge IT nation (Ministry of Science and Education)
    - Research and development of basic technology supporting the safe ubiquitous society (Ministry of Science and Education)

2) Study Group on Next Generation IP-based Infrastructure

Since December 2004, the MIC (Ministry of Internal Affairs and Communications) has held meetings of the "IP-based Networking Group" under the "Study Group on Next Generation IP-based Infrastructure", which is to deliberate upon (i) issues to be resolved accompanying introduction of totally IP-based communication infrastructures, and (ii) adequate policy measures for addressing thereof. On August 11, 2005, the Group has compiled and released a report "Toward Smooth Migration from PSTN to IP-based Networks" as its third report.

The report says, on totally IP-based communication infrastructures, safety, reliability and interconnectivity will be maintained, and that safe and convenient service should be provided. It then proposes that, while promoting the smooth migration to IP-based networks, steps toward the migration should be clarified and that it is vital for related parties to have a common understanding. The MIC will implement necessary policy measures, paying due respect to this report.

3) Council on Information and Communications

The discussion on the NGN standardization in Japan is held at the NGN Working Group of the ITU-T Committee under the Information and Communications Technology Committee of the Council on Information and Communications. Also since April 2005, they are holding meetings together with the NGN Up-stream SWG of the Specialized

Committee on Architecture under Telecommunication Technology Committee to pave the way for persons involved in the standardization of NGN.

4) TTC (Telecommunications Technology Committee)

This committee is cooperating with the NGN Working Group as stated above. Their NGN Architecture Committee is working closely with the standardization organizations of Korea and China and has established CJK NGN WG.

2. United States

1) NSF (National Science Foundation)

- Held a workshop in April 2003 and identified the future trends of the network and the vision for the future.
- Developed new network theory, architecture and technique to develop next generation services and applications.
- The new themes identified include:

a) Resilient Network Development: This is a network which will detour communication route automatically to avoid interruption, in case some parts of the network are destroyed by large scale earthquake, disaster or by war. Although it is believed that the current Internet already has this capability, Internet operators generally direct other packets than their own to go through different routes to reduce the traffic burden in their own network. This creates bottlenecks in times of emergencies. Further, the current trunk lines may not be able to deal with the explosive increase of network traffic. For most of the private sector operators that are suffering reduced profits due to excessive competitions, investments on the new network seem to be almost impossible. Large-scale investments in building new networks would require international governmental policy and agreement from the view-point of economic theory on the network.

b) Overlay-Network Design: To add another network layer on the top of the current network which handles the flow of packets. In actuality, what happens is that various functions will be put in the nodes of current network. For instance, time stamps are recorded at the nodes of sending, in the middle and receiving to always monitor the time needed. This will make service class (urgent and ordinary services, etc.) possible. Also for the purpose of testing various software for the network functions, researchers need to install the experimental software into the nodes. To do this physically is difficult, but if each node has functions called Virtual Machine and VM Monitors, they can do it very easily. (The experiment is in place as a project named PlanetLab in more than 20 countries with 500 servers. Details below.)

c) Environment Sensing: For example, sensors for temperatures and humidity could be placed around us. We can use the information sent through wireless link for the environmental control in the building. If the sensor is sensitive enough to capture the nominal change in temperature, we can detect the intrusion of the unwanted persons. Of course, military application is possible. Thickly deployed sensors of movement of human beings in the war front can

instantly tell us where the enemy has caused some actions. If we put tags to each person in the warehouse, we can know who accessed which shelf most. This information can be used for the most efficient arrangement of materials or goods in the warehouse. Vibration sensors placed in the walls during the construction will provide information on earthquakes. For the realization of this sensor network, we have to clear the hurdles of miniaturization of sensors, batteries wireless communications between sensors and routers, etc.

d) Wireless Network Theory: In order to realize the sensing network stated above, sensor network using wireless communication is indispensable. We need to develop the theory and technology for it.

- The GENI (Global Environment for Networking Investigations) Initiative
  This is an initiative of the Directorate for Computer and Information Science and Engineering (CISE) at NSF announced on August 24 this year, to advance their past R&D results on NGN obtained in cooperation with the projects such as PlanetLab.

  The objective of the initiative is to develop new networking and distributed system architectures that: build in security and robustness; enable the vision of pervasive (ubiquitous) computing by including mobile, wireless and sensor networks; include ease of operation and usability; and enable new classes of societal-level services and applications.

  For this purpose, CISE is encouraging a broad community effort that engages other agencies, other countries, and corporate entities. The actual R&D will be conducted using the network such as Internet2. Further, it is noteworthy that it will analyze, from the viewpoint of Internet Economy, the construction of new networks and creation of new services to see if these service providers can be financially successful

2) Cooperative Studies by Government-Academia-Private Sector

a) 100x100 Project

A project started in 2003 aimed to provide 100Mbps lines to 100Million homes, identifying the limitations of the current network, necessary characteristics of the new network services to be offered, basic architecture, protocol, etc. The goal is to draw the blueprint of the network exceeding the current network by the participants including scientists, network engineer, network operators, from Carnegie-Melon University, Stanford University, Rice University, UC Berkley, Internet 2, AT&T, and others.

b) PlanetLab

A project started in March 2003 to put a new layer over the current Internet for advanced research and services. Major participants include: Princeton University,

Cambridge University, MIT, UC Berkley, INTEL, HP, AT&T, France Telecom, and NECLab.

c) NCOIC (Network Centric Operation Industry Consortium)

This is a consortium established in September 2004 by 28companies including Boeing and Lockheed Martin. Currently, the members expanded to include Johns Hopkins University, Carnegie Melon University and over 50 companies including Cisco, Oracle, Intel, Raytheon, Sun Microsystems, Northrop Grumman.

Although the efficiency of the network has been improved dramatically, integration of networks among Federal Departments has not been achieved due to the lack of technique to make different systems work as one network. NCOIC was established to promote the interoperability of the networks including not only those of the Federal Government but also of the private sector.

The research and development at the NCOIC is conducted through cooperation among government, academia and the private sector and is aimed at building interoperable networks with security and high reliability. Member companies are benefited by reduction of administrative costs and by the improved efficiency of joint operation through open standards and with system engineering tools. The information and knowledge produced by NCOIC are to be provided first to defense industries through many initiatives and later to the private sector.

d) Internet2

The Internet2 is a research project for the NGN started in 1996 by NSF funding and a partnership of 34 universities. Currently, it has members of 207 universities and 70 companies.

To achieve the mission of cutting edge technology research and development, universities are more and more required to make their knowledge commonly held through exchanges of personnel and also to integrate their facilities (computer hardware) located all over the US. But the current Internet does not have the capacity to realize this objective. The academia and research community therefore started building the Internet2 by themselves.

At Internet2, research for network related technology is carried out including next generation internet protocol using ultra high speed network for the purpose of high speed and low cost networks specialized for educational and research use. Advanced applications research and development also is conducted. Participating member organizations provide funds and equipment free of charge.

The operation of Internet2 is administered by the UCAID (University Corporation for Advanced Internet Development), a non-profit consortium of universities.

The most important achievement of the Internet2 is the backbone network called Abilene that started operation in February 1999. The Abilene is a fiber-optic

network spreading to 20,000km in total, provided by Qwest Communications and Cisco Systems for free. In 2003, the network had the speed of 10Gbps with 47 domestic access points. Since Abilene is suited for not only IPv4 but also IPv6, the next generation Internet protocol, Internet2 is tackling with the IPv6 network on Abilene. It is aimed to develop monitoring tools for network security and new multi-homing technology by the end of 2006.

3. European Union

1) EU FP-IST FET (Framework Program- Information Society Technologies Future and Emerging Technologies)

The Framework program is a project conducted by the EU to promote science and technology and is now in its sixth stage (FP6: from 2002 to 2006). Information and Communication is taken up as one of the most important subjects and is divided into several research categories. Future and Emerging Technologies is one of them. This is to identify the communications paradigm for 2020. The RFP was issued in 2004 and submissions of proposals were closed in March 2005. The Award is to be announced in autumn 2005.

As is the case in the NSF in the U.S., the Situated and Autonomic Communications (COMS), a ultra distributed communication system that autonomously controls and reorganizes itself to the changes in circumstances, is the main subject of study.

There are 16 other research projects in connection with the NGN. These are all composed by more than three companies and/or organizations, funded by EU and themselves. These projects are:

a) European Research Network on Foundations, Software Infrastructures and Applications for large scale distributed, Grid and Peer-to-Peer Technologies (Code Name: COREGRID)
b) Being on Time Saves energY continuous multimedia experiences on network handheld devices (BETSY)
c) Distributed European Testbed Laboratories (EUROLABS)
d) Mobility and ADaptation enAbling Middleware (MADAM)
e) Access to Knowledge through the GRid in a MObile world (AKOGRIMO)
f) Co-ordination Action for Libre software Engineering for Open Development Platforms for Software and Services (CALIBRE)
g) Understanding Networks of Learning Design (UNFOLD)
h) Flexible Gateways Architecture for enhanced access network services and applications (FLEXINET)
i) Realizing the semantic web (KNOWLEDGE WEB)
j) Digital Switchover, Developing Infrastructures for Broadband Access (ATHENA)
k) Exploring new limits to Moore’s law (MOE MOORE)
l) Design and Engineering of the Next Generation Internet towards convergent multi-service networks (EURO NGI)
m) Network of Excellence on Digital Libraries (DELOS)
n) Broadband services for everyone over fixed wireless access networks (BROADWAN)

o) Next generation Optical network for broadband in Europe (NOBEL)
p) Ultra High Bit Rate Over Copper Technologies for BROADband Multiservices Access (U-BROAD)

Regarding the Framework project, drafting of the scheme for the next framework (FP': from 2007 to 2013) has started. The recommendations for it were submitted to the European Parliament and Board of Ministers by the Directorate for Research and Development in June 2005 for discussion in autumn and beyond.

2) COST - European COoperation in the Field of Scientific and Technical Research
This is a project co-funded by European countries started in 1971 to keep European leadership position in many scientific areas such as ICT, Biotechnology, Medical Science, Physics, and Social Science. COST held a joint workshop "Nextworking 2003" with NSF in Greece in June 2003. Participants included INTEL, AT&T and Microsoft. The main objective of this organization is to exchange opinions on emerging technologies regarding networking and to share the knowledge.

3. Situations at International Organizations

1. OECD

The "Working Party on Telecommunication and Information Policies" under the "Committee for Information, Computer and Communications Policies" of the "Directorate for Science, Technology and Industry" published a report "Next Generation Network Development in OECD Countries" in January 2005 addressing policy issues relating mainly to the transition from the PSTN to IP based networks and the changes in business models to VoIP. This is not directly related to the issues the GBDe is tackling in terms of the current Internet. However, it shows that we need to carefully watch the latest investment developments as the operators cope with the expected shortage of network capacity with the arrival of the ubiquitous network society, together with the end-to-end QoS, at a time of uncertain business models.

2. ITU

ITU-T SG 13

The "NGN 2004 Project," started in January 2001, is based on the outcome of the "Global Information Infrastructure Project" (started in 1995). The main themes include: Fundamental Characteristics of the NGN (IP based); Necessary Functions (Separation of Services and Network); Objectives (Promotion of Fair Competition and Private Sector Investment); Architecture; Security; Mobility; Numbering; and Routing. The first recommendations were announced in June 2004.

According to the recommendation, NGN is placed in the most important theme for standardization in the current term (from 2005 to 2008). A study group (SG13) in charge of NGN was established and standardization of NGN is accelerated at FG NGN.

The discussions at the ITU are focused mainly from the viewpoint of the carriers. Priority areas are subjects like Universal Service, Interoperability, Seamless Provision of Application Services, and the Standards for these.

3. ETSI (European Telecommunications Standard Institute)
At ETSI, the so- called TISPAN Project, which is an integrated project of TIPHON (Telecommunication Internet Protocol Harmonization Over Network) and the SPAN (Service and Protocol for Advanced Network) project, is leading the standardization of the NGN. Because of the delay in the planned issuance of the NGN Standard Release 1 in June 2005, partial releases are expected.

4. APEC (Asia Pacific Economic Cooperation)
At APEC, the NGN is taken up by the Telecommunications and Information Working Group under the Telecommunications and Information Ministerial Meeting and ECSG (Electronic Commerce Steering Group), together with the issues of information security, and the ubiquitous society.

5. ATIS (Alliance for Telecommunications Industry Solutions)
In the US, the NGN FG was established under ATIS. The requirement is basically the same as ETSI-TISPAN NGN Release 1, except for the parts regulated by the US laws.

6. 3GPP (3rd Generation Partnership Project)
This is basically a forum relating to the third generation mobile phone, but the IMS IIP Multi-media Subsystem) technology developed by the project is used for the core network of the NGN.

7. Other International Fora

1) IETF (Internet Engineering Task Force)
The IETF activities are centered around specifications for components of technology including SIP (Session Initiation Protocol), MPLS (Multi-Protocol Label Switching), GMPLS (Generic Multi-Protocol Label Switching), and IPv6.

2) MSF (Multi-service Switching Forum)
This forum is devoted to developing the NGN specifications. Standards used are based on the ITU-T recommendations and specifications by IETF.

4. <u>Results Derived from the Study</u>

1. Expected Timing for the Realization of NGN

The NGN that enables safe and secure communication will be realized incrementally and part-by-part, not in a big bang on someday in the future. Therefore, the timing differs depending on the aspects of the NGN. For the standardization aspect, 2008 seems to be the common target year. For building new network infrastructure and new services, somewhere in between 2010 and 2020 is targeted by many institutions involved.

2. Technologies to be Used

IP-based ultra high speed network using packets and technologies such as IPv6 seems to be the goal, where packet transporting layer and monitoring layer will be separated to make many new services available. Also, an ultra distributed communication system architecture that autonomously controls and reorganizes itself will avoid interruption in any changing circumstances.. Regarded as very important, technologies relating to the NGN, Wireless and Sensing Network technologies are under development as well.

3. Role of Governments

Since the NGN is, by its nature, a global infrastructure which is beyond just one country or one company, governments should: bridge the gap among governments; make necessary investments for R&D and building and/or upgrading network infrastructures; and support the activities of private sector for creating new business models. In close cooperation with the private sector, governments should investigate the societal issues including anonymity (traceability) to reach certain agreements among the stakeholders.

4. Role of the Private Sector

Reflecting the importance of the NGN as a global infrastructure, the private sector will cooperate with governments, international organizations and other private sector organizations and companies: to facilitate the technological advancements by making the best use of their capabilities; to reach agreements on the societal issues stated above; and to enhance the living standards of all the people on Earth.

5. Conclusion and Issues for Continued Study in 2006

This year, the GBDe has gathered the current activities of governments, international organizations and some private sector initiatives on the NGN. The status of such developments is quite different based on the objectives of each institution. This situation is far from initial expectations that a clear image of the NGN could be presented. Internet related organizations including ISPs, content providers, payment clearing house and equipment manufacturers, are targeting the creation of new business models that provide safe and secure services. The telephone operators are mainly interested in the change in technology for their networks from PSTN to VoIP. The organizations such as the ITU are working on the most appropriate standards for the NGN. Academia is looking with great interest at the possibility of a new democracy where citizens can directly disseminate their beliefs and can be directly involved in the politics, with the pros and cons of the keeping and losing their anonymity on the Internet. The areas of interest are different, although some are overlapping, as the NGN contains vast aspects of issues to be addressed. It is very difficult to reach a common view, because it is as if we are shooting at a moving target from a moving car. Of course, we can be optimistic to believe that we can reach an agreement/conclusion after a certain amount of time, even if we conduct R&D separately, recognizing that other R&D can be conducted in other organizations in parallel.

The GBDe will therefore take one step further and create a forum next year to watch the progress of NGN developments; to exchange information with governments, the private

sector and academia; and to submit timely recommendations to the related parties so that we can contribute to the advancement of the NGN.

Also, in building the NGN in the future, we would like to ask governments to listen to the opinions of the private sector, when they are setting standards and/or making regulations and rules on the NGN. In the area of e-commerce, the private sector and governments have maintained good dialogues and, as a result, our recommendations have been reflected in corresponding government policies. The private sector has to build much more cooperative structures, leaving behind current unproductive practices which will be required to achieve a better corporate financial performance, especially in the area of standards relating to the recordings of visual/information data.

Further to this point, if we are focused only on the viewpoint of carriers that see the NGN just as a shift from the PSTN to networks using IP, the vision concerning the NGN framework may become too narrow. We request, therefore, that the NGN discussions be wide open, taking into account the full spectrum of activities and possibilities.

Although we do recognize the importance of promoting standardization with regard to the NGN, we should not be put in a position of waiting for unnecessary delays due to the time needed to adjust different opinions among various organizations involved.

Last but not least, governments have a very important role in the financing aspects of the NGN. It relates to the cost of building new networks to solve the problems of our current networks in terms of capacity and functionality. The private sector has invested in these areas, motivated mainly by competition. The current situation, however, is that private companies are in weakened financial conditions because of too much competition, and cannot afford major new investments. Governments should consider investment in this area as the NGN is positioned as a global infrastructure. Actually, the US Government provided $373.7Million in 2004 for NGN-related activities, and the EU is providing 3,625 Million Euro for the FP6IST project over five years. With such public investment in the NGN, the private sector will also respond positively with additional resources devoted to NGN projects and deployment.

Contributions from the Issue Group Members were provided by: Institute for Information Industry, Taiwan; Information-technology Promotion Agency, Nomura Research Institute (NRI), NEC Corporation, TEPCO (The Tokyo Electric Power Company, Incorporated),, Fujitsu Laboratories, Ltd., Japan.

GBDe 2005 Issue Group

Securing Electronic Transactions

October 17, 2005

Issue Chair: Dr. Thorsten Demel, Chief Operating Officer, Global Technology, Deutsche Bank AG

1. Introduction

The ability to use electronic channels for legally binding transactions is a keystone for the future development of e-commerce and e-government. Internet payments are the most prominent class of such transactions. However, legally binding transactions also occur in e-government and whenever a contract is signed.

Therefore, the GBDe has frequently addressed the issue of trust infrastructures in its work over the last years. In the meantime, a significant number of governments have picked up the issue of secure identification and authentication in the Internet.

The GBDe welcomes this development. Most current initiatives are, however, on a national level only. Therefore, the GBDe wants to contribute in an international discussion on:

- legal harmonization and international recognition of national trust infrastructures,
- chances that derive by public and private sector using a joint trust infrastructure,
- ways to achieve a broad public acceptance of new infrastructures.

2. Different Approaches to Trust Infrastructures – case studies

The GBDe started with some prototype case studies, which show different approaches countries follow.

Germany

Germany was among the first countries to enact a digital signature law in 1997. Electronic signatures that may serve as an equivalent to a hand-written signature require a smart card and a dedicated registration process. The legal framework, however, has not produced a break-through in PKI implementations. In contrast to expectations, the 1997 signature law became rather a barrier to implementation: The high security standards made the system too expensive for a mass market; and critical mass could not be

achieved. In January 2005 an amendment to German signature law was passed which now allows a combination of existing (smart card) infrastructures like bankcards.

At first, the German Government did not plan to run a trust infrastructure. But with chips being required in passports and ID-Cards, it was decided to combine passports and ID-cards with a PKI. This digital ID is mandatory and fitted with an authentication certificate; a certificate for signatures can be downloaded at the holder's expense. Since ID cards are valid for 10 years, the card exchange will last from 2007 until 2017.

The public private initiative "German Signature Alliance" was founded in 2002 and defined technical standards enhancing existing international ones. The German Government declared an eCard Initiative in 2004 based on the results of this Signature Alliance. A critical mass of cards, certificates and applications is expected when digital IDs and bankcards with authentication/signature-functionality will be implemented on a large scale.

(Similar digital ID projects have been started in France, Great Britain and Spain. Most EU member states such as Netherlands or Italy are currently discussing the introduction of digital ID cards.)

Finland
Finland was the first EU member state to introduce a digital ID in December 1999. The digital ID was optional and came along with additional costs (€40 for 3 years). As a result, only about 14,000 cards had been issued to the 5 million citizens in the first 3 years.

The cards were designed to work in public and private environments. In particular, they could be used for online-banking or insurance services. The number of applications, however, never reached a level that citizens were willing to pay for the digital passport. In the meantime, banks implemented alternative authentication schemes. As of April 2005, about 63,000 citizens had certificates based on electronic ID cards, bank cards or mobile SIM cards.

Belgium
In Belgium, the government started to introduce a mandatory digital passport in 2003. Substitution of the non-digital IDs will be not be completed until end of 2009. Each digital passport is valid for 5 years and can be used for private and public purposes. The digital passport comes along with a qualified certificate. The certification authority is under public responsibility, but operated by private companies.

Like Belgium, Estonia and Sweden have launched mandatory digital IDs. In Estonia, a digital ID has been issued to about half of the total population.

Taiwan
Based on the 2002 Signature Act, the Taiwanese government issues electronic ID cards that can be used as signature cards. The cards can be used for e-Government as well as private purposes. The number of e-commerce as well as e-Government PKI applications is more than 353 (G2G:50, G2B:15, G2C:288), and among them, electronic tax

declaration is the most attractive, with 100,000 users in 2004 and 198,000 users in 2005. As of September 2005, about 881,000 cards were distributed to 23 million citizens.

Until the end of 2004 the signature card was free of charge for promotion. Since January 2005 citizens have to pay NTD275 (≈8.5 USD) per annum.

Japan
The Japanese government used to run different certification infrastructures under its responsibility: For inter-central government communication, for inter-local, for business-to-government and for citizens-to-government. By 2003, the Japanese had introduced bridged certification infrastructure which allows all these areas to connect to each other for certification. Japan is on of the first countries to realize this nationwide PKI to secure electronic communication.

The Japanese citizen card (called Jyuki card) is based on smart cards. This signature card is not mandatory and costs ¥500 (~5 USD) for the card itself and ¥500 (~5 USD) more for the PKI function. In two years more than 500,000 Jyuki cards were issued, which is 0.4% of the total population. Jyuki card with PKI may be less than this number.

Citizens may apply for this signature card as a public ID. However, this service is only relevant for citizens who have neither a passport nor a driver's license.

In contrast to most other countries, Japan does not allow the usage of the citizen PKI for private purposes, limiting the possible field of application. Hence, the Japanese citizen PKI is rather an instrument to secure the communication of (local) governments with its citizens than a comprehensive trust infrastructure.

Malaysia
In September 2001 the Malaysian government launched MyKad, a smart card based national ID card. MyKad combines a bundle of public and private applications. Besides the PKI functionality, the card serves as national ID (for entering the country) and driver's license. It covers health information and can be used as electronic wallet. It is even possible to connect the card with an existing bank account and use the MyKad at an automatic teller.

There are two certification authorities offering certificates for the MyKad under the Malaysian Signature Acts of 1997 & 1998. Certificates issued by authorities outside Malaysia, however, are not granted yet. Although MyKad is not mandatory and comes along with some costs (40 RM ~ 10 USD for card and certificate), more than 10 million cards have been issued in the last 4 years. The government plans to reach more than 50% of the population in 2005.

USA
In the United States, as in many other countries, the implementation of trust infrastructures is left to the private sector. Some of the largest certification authorities are located in the US and sell certificates to individuals and companies.

The registration process, as well as the costs, are subject to agreement between the certification authority and certificate holder. The legal status of signatures is decided on a

case-by-case basis. There are no high court decisions yet which clearly indicate the legal status of such signatures.

3. Achievements from case studies

Heterogeneous landscape
The prototypical case studies show that the current situation is highly heterogeneous. On the one hand, one might regret this situation since it hinders the formation of any trust infrastructure to obtain the necessary critical mass on a global scale. There is a risk that we will end with non-interoperable local trust infrastructures and regions without trust infrastructures at all. On the other hand, competition between different solutions increases the chance that the best scheme will prevail.

Existing implementations are under government responsibility
It is too early for a final evaluation of the different approaches. It is a fact, however, that the only successful infrastructures today are the ones operated under government responsibility.

In countries like the United States that leave building of trust infrastructures completely to private sector, PKI is still a niche product. Having a comprehensive legal framework in place might give legal certainty, but seems not to be sufficient to bring private PKI initiatives out of their niche (as the German example shows).

The reasons for the lack of widely accepted private trust infrastructures are not obvious. One might suggest that for many people identification is a core function of a government and they are not used to pay a private company for such a service. It seems, however, that the high initial costs, which come along with building a new infrastructure, is the main barrier for private trust infrastructures.

It is not unlikely that (like the telephone infrastructure 100 years ago) the implementation of a new trust infrastructure requires an initial government involvement, before infrastructure providers can go public in a second phase. Nevertheless, government responsibility by itself does not guarantee that an infrastructure is accepted. The Finish example shows that it is not sufficient to provide a signature card and wait for citizens to apply and applications to be implemented.

Mandatory or optional ID cards
Mandatory ID cards (like in Belgium) certainly have the potential to overcome the critical mass problem. If there is a sufficient penetration, then it is likely that applications will be built up on this infrastructure. Mandatory schemes require a strong political commitment because the initial costs have to be paid by citizens or tax-payers at a time when many citizens do not see the advantages.

The cost for the mandatory digital ID card can be reduced if the certificate (for signatures) is not included. For example, Germany will follow this path. In this case, however, the usage of the ID card is limited unless it is upgraded. There is a risk that the functionality of the not-upgraded card is insufficient for business applications and the number of upgraded cards stays small like in the non-mandatory cases.

It is clear that a mandatory electronic ID comes along with a long transition period and requires a consensus that there is a national ID card at all. This is not easily settled as the examples of United States or Great Britain show (note that there is a political discussion in Great Britain as to whether such an ID should be implemented).

Usage of public infrastructure for private purposes
There is a variety of nuances in which way private initiatives make use of a government run trust infrastructure. At the far end of the interval you will find Japan and Malaysia: In Japan private usage is not allowed at all, while the Malaysian MyKad replaces existing private bank cards.

The usage of a public trust infrastructure has the potential to realize significant cost savings, in particular because one can expect that customers trust in government-initiated infrastructures. Every company has to decide whether the positive effects of cost savings outweigh negative effects caused by dependence on an external infrastructure and the lack of an individual branding. It is clear that a public infrastructure and private applications must be separated in the way that data protection and a fair competition is guaranteed. For example, the trust infrastructure can be used for authentication purposes only and all data stored in the (private) application. Restricting the usage of a government-run infrastructure to a citizen-to-government application, however, limits the value of the infrastructure to citizens and prevents companies from taking advantage of the infrastructure.

4. Recommendations

International coordination and cross-border recognition
The current situation is highly heterogeneous: Some countries issue mandatory digital passports which can be used to process an electronic signature, other countries issue (or plan to issue) such cards on a voluntarily basis, some do not run a trust infrastructure and leave it to the private sector. Although the underlying public key infrastructure (PKI) is mostly based on international standards, there are many differences on a technical as well as policy level. As a result, a trust infrastructure that gains legal acceptance in one country will in general not be valued in another.

There can be no doubt that competition between different solutions is necessary because it increases the chance that the best scheme will prevail. However, there is a substantial risk that we will end with non-interoperable local trust infrastructures and regions without trust infrastructures at all.

Therefore, the GBDe recommends international coordination of the developing trust infrastructures and the underlying policies such that cross boarder recognition is achieved.

The critical mass problem and the role of governments
Infrastructures, in general, face the critical mass problem: The value for each user depends on the total number of participants. In order to be successful, a trust infrastructure needs a critical number of users and applications. A strong government

involvement (e.g. issuing mandatory digital IDs or stetting framework and demand for private trust infrastructures) seems to be one way to overcome this problem. Nevertheless, government involvement by itself does not guarantee that an infrastructure is accepted.

The GBDe recommends that governments clearly identify their role and define strategy how the problem of critical mass should be solved. It is recommended that the private sector is involved in the strategic discussion.

Usage of public infrastructure for private purposes
For private enterprises the usage of a public trust infrastructure has the potential to realize significant cost savings, in particular because one can expect that customers trust government-initiated infrastructures. Every company has to decide whether the positive effects of cost savings outbalance negative effects caused by dependence on an external infrastructure and the lack of an individual branding. It is clear that a public infrastructure and private applications must be separated in the way that data protection and fair competition is guaranteed. For example, the trust infrastructure can be used for authentication purposes only and all data stored in the (private) application.

Restricting the usage of a government-run infrastructure to a citizen-to-government application, however, limits the value of the infrastructure to citizens and prevents companies from taking advantage of the infrastructure. Thus, the GBDe recommends opening government-run infrastructures to private and commercial usage.

Private trust infrastructures
In many countries private trust infrastructures exist, like (smart-) card infrastructures of banks and telecommunication providers.

The GBDe recommends that private and public infrastructures and applications should be designed in a way that interoperability is guaranteed. It should be possible that private trust infrastructures can be used in a public environment and vice versa.

Business case for trust infrastructures
All stakeholders should be aware of the fact that a viable business case is crucial for the development of a trust infrastructure. If an infrastructure is run by private enterprises or if a public infrastructure is not mandatory, customers and citizens must be convinced to take part in the infrastructure. They will only do so, if they see a benefit – which might be a financial incentive or an improvement in personal convenience. Important government applications like tax declaration have the potential to become a killer application. Such killer applications play an important role in order to reach a critical mass of users.

As a conclusion, the GBDe recommends that for any strategy to implement a trust infrastructure a business case for all stakeholders should be looked at as a keystone.

Electronic mass documents/electronic records
When looking at securing electronic transactions, most effort is spent on finding ways to allow private users to authenticate themselves to an e-Commerce or e-Government service. Much less attention is paid to enterprises or governments that want to distribute large number of documents electronically to customers and citizens. Such documents can

include banking account information, an invoice or a tax assessment notice. Often, such records are presented to third parties. Therefore, integrity and authenticity of such records must be guaranteed. Personal signatures, however, seem not to be appropriate for mass documents or records which are produced by the customer on demand (like an account statement).

The GBDe recommends that governments should adjust the legal framework in a way that the requirements for electronic mass documents are clearly defined, such documents can easily be distributed and are recognized by all government authorities.

GBDe 2005 Issue Group

Ubiquitous Network Society Vision

October 17, 2005

Issue Chair: Dr. Teruyasu Murakami, Chief Corporate Counselor, Nomura Research Institute, Ltd. Japan

1. Introduction

The word ubiquitous has been around for many centuries and its meaning is said to be "being everywhere", "in many places at the same time", and "omnipresent", among others. For the last few years, the IT industry has begun using the word ubiquitous often; it was said to be initially introduced by an American researcher in the late 1980's, in search of a resolution to a problem of connecting computers.

The use of the word ubiquitous and its meaning became more apparent in Japan around the turn of the 21st century. This shift is summarized as the "Ubiquitous Paradigm", and includes "Ubiquitous Network", "Ubiquitous Computing", "Ubiquitous Information Society", and other ubiquitous-related concepts. To this day, this movement in Japan is still unique, continuing to spread through society as a whole.

As we approach the decade's midpoint, Internet connectivity continues to increase. Yet as the network has become more complex, allowing anything and everything to be connected, various issues have come into focus.

At the GBDe, there have been a number of issue groups addressing the complex problem of e-commerce in the last several years. As the Ubiquitous Network concept has become more defined in the last five years, and issues related to the Ubiquitous Network and its impact on society have become greater, it now needs to be addressed. This effort was clarified in the GBDe's recommendation on a "Ubiquitous Society Framework" issued in late fall of 2004 at the Kuala Lumpur Summit. In 2005, the ubiquitous society framework as a whole has become the so-called new "Ubiquitous Network Society Vision".

2. National Strategies and Worldwide Activities

2.1. u-Japan

Japan's Ministry of Internal affairs and Communications (MIC) has been working on the issue of a network society for a long time. In recent years, the Ministry has established a conceptual agenda in its "u-Japan (Ubiquitous Net-Japan) Policy". This Ubiquitous Net-Japan may be seen as a vision of ICT, but in fact it is a vision to resolve national issues facing Japan towards the year 2010. National issues to be resolved are based on the fact that there will be a decrease in Japan's total population due to a decrease in birthrates, along with an increase in the senior citizen population and a decrease in the workforce. These facts will cause a variety of social problems.

Before the creation of u-Japan by the Ministry of Internal affairs and Communications, there was the "e-Japan Strategy". This was Japan's first IT strategy, created in 2001 by the Japanese government. e-Japan's mission was to create the world's most IT-advanced nation by the year 2005. The Ministry of Internal Affairs and Telecommunications is now proposing a next-generation ICT society by the year 2010, which will bring about new value and an estimated market size of 87.6 trillion yen.

After the original e-Japan strategy came out in the year 2000, e-Japan itself was implemented in 2001. In 2003, it was revised to bring about the most advanced strategy in the world, with specific focus on infrastructure building and pursuing advancement in usability. In the area of building an infrastructure, deployment of a broadband network is well underway and accomplishing a great deal. These movements were made more instrumental through the efforts of the Ministry of Economy, Trade and Industry (METI). In its "Vision for Information-based Economy and Industries", the Ministry of Economy, Trade and Industry has specified a refinement of the ubiquitous IT infrastructure as one of its five main outlines.

As the u-Japan vision is set towards the year 2010, a mid to long-term R&D program in information and communication technology strategy was examined. The "UNS Strategy Program" came out in July 2005, a long-term R&D project moving toward the year 2015. "UNS" primarily stands for "Ubiquitous Network Society"; at the same time, the U also means "Universal Communication", the N means "Next-Generation Network", and the S means "Security and Safety". Japan is very fortunate to have the Ministry of Economy, Industry and Trade and the Ministry of Internal Affairs and Telecommunications to create these strategies and establish their continuing goal.

2.2. u-Korea and the IT839 Strategy

In Korea, the initial effort to enhance the Internet society was "e-Korea vision 2006". The "Korea IT839 Strategy" effort was created when the "IT839 Strategy" was applied to the e-Korea concept. The term "839" comes from "8 Services", "3 Infrastructures", and "9 Growth Engines". They are further divided into: (1) b8 Services – WiBro services, digital multimedia broadcasting services, home network services, telematics services, RFID-based services, W-CDMA services, terrestrial digital TV services, and Internet telephony

(VoIP); (2) 3 Infrastructures – broadband convergence networks, ubiquitous Sensor networks, and Internet Protocol Version 6 (IPv6); and (3) 9 Growth Engines – next-generation mobile communications devices, digital TV broadcasting devices, home network devices, IT System on Chip (SoC), next-generation PCs, embedded software, digital content and software solutions, telematics devices, and intelligent service robots.

u-Korea's future blueprint will include "U-home", "U-government", "U-commerce", and "U-society", yielding the goals of "Convenient Life", "Happy Life", "Safe Life", and "Rich Life". As the process of u-Korea will span ten years from 2005 to 2015, the Life Revolution Strategy will complement the IT839 Strategy via "Popularization of IT Applications", "IT Benefits for Everybody", and a "Healthy and Safe IT Environment".

2.3 e-Taiwan and m-Taiwan

Taiwan has chosen to build a next-generation wireless network over four years, starting in 2005. It is understood to cover a number of industries in Taiwan, including warehousing; healthcare; public security; environmental protection; libraries, museums, and galleries; travel and tourism; transportation and traffic information services; education; digital content and entertainment; and videophones. As seen in other countries' ubiquitous-related strategies and efforts, Taiwan also started with a concept called "e-Taiwan".

e-Taiwan is also known as "Challenge 2008", established in May 2002 to achieve the most widespread Internet services in Asia. The concept was drafted by Taiwan's STAG Board (Science and Technology Advisory Group). This concept included: (1) e-movement, (2) e-life, (3) e-business, (4) e-transport, and (5) the provision of broadband service to over 6 million households.

With the advantages of the world's top production value of WLAN products and mobile phone penetration rate, the Taiwanese government has also been actively devoted to promoting mobile-competitiveness. The "M-Taiwan Program" is expected to build up wireless networks, integrate mobile phone networks, set up optical fiber backbones, and execute the Integrated Beyond 3rd Generation (iB3G) Double Network Integration Plan. It is also expected to shift Taiwan from an "e-nation" to an "M-nation", and to fulfill the vision of "a mobile Taiwan, infinite application, and a brave new mobile world".

The major focus of the m-Taiwan program is to develop an application environment with a wireless broadband infrastructure that allows any user to access multiple digital applications and services through any network, anywhere, at any time. The m-Taiwan program includes two main projects: (1) constructing broadband ducts and (2) promoting "Mobile Taiwan" access.

Broadband duct construction includes two areas:

- The government constructs broadband ducts, and then leases them to the operators of PSTN, cable TV, and mobile networks.
- Broadband operators can rent ducts from the government and install fiber optic systems given enough market demand.

Promoting "Mobile Taiwan" access consists of the following:

1. Mobile Service
   - Choosing demonstration points to promote mobile service
2. Easy Life
   - Promoting potential operation models of WLAN, encouraging citizen participation
   - Constructing common service platforms for a wireless network
3. Enjoy Learning
   - Integrating domestic education/training institutes, cultivating human resources, introducing application/development personnel to wireless dual network
   - Promoting a mobile "Enjoy Learning" community
   - Popularizing dual-network applications
4. Promoting Dual-Network Integration
   - Dual-network business model research
   - Developing integrated dual-network handsets
   - Legal system research
   - Dual-network integration field trials

Due to the trend in global ICT applications moving towards ubiquitous network society applications, in April 2005 the Taiwanese government started planning a ubiquitous Taiwan program following the e-Taiwan and m-Taiwan effort. The basic idea is to take advantage of the four ICT technology areas, including (1) Internet computing, (2) mobile devices, (3) wireless sensors and context-aware platforms, and (4) user-friendly interfaces, in order to develop "personalized services anywhere, for any device, at any time" application scenarios in Taiwan by 2007. The key milestones of the u-Taiwan program may consist of (1) network convergence in ubiquitous network infrastructures, (2) the promotion of ubiquitous network ICT society industries and ICT-enabled industries, and (3) the development of ubiquitous network society applications.

2.4. i2010—A European Information Society for Growth and Employment

Ubiquitous-related activities such as eEurope2002 and eEuropa2005 have been established in Europe. Now, as eEuropa2005 is approaching the final stage of its mission, a program known as "i2010" is being established, one which features an outlook and various efforts to be focused on over the next five years. In this docket, the European Union is including such items as (1) a Single European Information Space; (2) innovation and investment, yielding more and better jobs; and (3) an inclusive European Information Society, again promoting more jobs, better public service, and a better quality of life. Notably, Europe is trying to promote employment with the creation of new jobs for the community.

2.5. WSIS

WSIS, the World Summit on the Information Society, was established by the United Nations and ITU, the International Telecommunication Union. The first phase of the effort was completed as a gathering of all nations who wished to be included; now WSIS

is in its second phase, and the issue of the digital divide is being addressed for all countries that are currently establishing an infrastructure for Internet access. For those who are well into the ubiquitous phase of the Internet era, supporting efforts such as WSIS is very important for world unity regarding the Internet. The second phase of WSIS places special emphasis on: (1) the role of governments and all stakeholders in the promotion of ICTs for development; (2) information and communication infrastructure, an essential foundation for an information society; (3) access to information and knowledge; (4) capacity-building; (5) increasing confidence and security in the use of ICTs; (6) enabling environments; (7) ICT applications having benefits in all aspects of life; (8) cultural diversity and identity, linguistic diversity, and local content; (9) media; (10) the ethical dimensions of an information society; and (11) international and regional cooperation. These are well defined and spelled out in the Plan of Action paper published by the WSIS organization.

As part of efforts to make WSIS participants aware of ubiquitous network society concepts, the Tokyo Ubiquitous Network Conference was held in May 2005, attended by 600 participants from 85 countries around the world.

2.6. Other Efforts

Other multinational efforts such as APEC are actively investigating ubiquitous network effects in both TEL (Telecommunication and Information Technology) and ECSG (e-Commerce Steering Group). The GBDe has participated in meetings of both APEC bodies, notably APEC TEL31 held in April 2005 in Bangkok, Thailand, and the APEC TELMIN6 Ministerial Level Meeting held in June 2005 in Lima, Peru. For the future, the GBDe will remain focused on all of these advocacy activities with multi-stake holders and continue working with consumer advocates as well.

3. Policy Issues in Ubiquitous Network Society Vision

Several issue categories were identified in order to examine the future of the Ubiquitous Network Society Vision. These issues will be discussed further with their associated technologies and services:

1. Privacy Concerns
2. Security and Social Safety Concerns
3. National IT Strategies
4. Negative Aspects of a Ubiquitous Network Society
5. IPR and Copyrights
6. Introducing e-Commerce in the Developing World
7. Spectrum Allocation, Interoperability, and Standardization

The following are the areas of associated technologies and services to be discussed at this time:

- RFID
- Mobile Applications
- Sensor Networks
- Networked Appliances

- Home Entertainment Networks
- PLC: Power Line Communications

3.1. Privacy Concerns

In a ubiquitous network society, almost all ubiquitous communications are bi-directional. Therefore, just as the ubiquitous user is obtaining information, this same user is also sending information back to the corresponding application. This bi-directional information exchange often occurs without the user realizing that his or her information is being stored and compiled for use by a third party.

RFID: Many consumer protection advocacy groups have already identified some privacy concerns about RFID usage, as have governments. Regarding RFID privacy in particular, the GBDe held two advocacy meetings in the U.S. in the last year, after the release of the last "Ubiquitous Society Framework" recommendation in 2004, addressing privacy concerns and the use of RFID and sensors. Consumer products with embedded IC tags have already been introduced in small numbers, but will increase in the near future.

A person's purchasing pattern and usage of a specific product should remain private information. However, the use of RFID will enhance the serviceability of industries from manufacturing and distribution to supply chain management and retailing, even reducing the operational cost in some cases. The technology could also have other applications in environmental protection and the prevention of unlawful business. Therefore, discussions on the usage of RFID must continue; and the GBDe is committed to working on this issue at the government, industry, and consumer levels. Numbers of RFID usage guidelines and policies have already been published by various governments, so the next step will be to promote and support these policies out of a concern for privacy.

Mobile and Sensor Networks: Another area of privacy concerns can be identified in both mobile and sensor networks. With enhanced technology, a mobile device could be tracked and the user's movement monitored. Similarly, a sensor network will be able to detect "person-to-person", "person-to-object", and even "object-to-object" movement. Information obtained by these mobile and sensor network applications is a privacy concern; this issue must be addressed at the government, industry, and consumer levels as well.

3.2. Security and Social Safety Concerns

Network security, including a safe Internet environment and the protection of personal data and privacy, is of utmost importance to a ubiquitous society. This is especially true from the ubiquitous user's point of view, and many preventive measures have been put into force to protect personal data.

In recent years, however, there have been many threats to this society from various factors. The threat most commonly discussed and addressed is terrorism. Unfortunately, we must all protect ourselves and ubiquitous technology could be utilized to ensure social safety. The issue is a double-edged sword, where system misuse and abuse may harm a ubiquitous society, but proper utilization of the same system will enhance social safety.

RFID could be utilized for tracking and electronically sealing the movements of objects. Additionally, mobile and sensor network applications could be used to monitor any harmful activities, while at the same time being used as safety alert mechanisms. As the world has gotten smaller thanks to international travel, cross-border standardized technologies are needed to create a fully safe and sound security environment. Such movement could be seen in the endorsement of IC tag-embedded passports, which have been introduced in many Asian nations and are now spreading throughout the world.

3.3. National IT Strategies

In order to excel at building a ubiquitous society, it is necessary to establish a national strategy and accept convergence. The term ubiquitous is now widely accepted and used in many different regions of the world, but different words are also being used to convey the same meaning: Ambient is the term used in Europe, and Extra Internet is perhaps the term used in the United States. Even with these different terms, the goal to be achieved is the same, and this goal cannot be achieved unless there is a government-level effort to establish a national strategy.

Convergence is also very important, and must be taken into consideration in order to succeed dynamically in any given national strategy. It is a factor that will complement national strategies in a process of realization, change, and enhancement. Technologies, applications, and uses in a ubiquitous society are very dynamic, with new concepts converging at a significant rate every day. Any given strategy must take into account the importance of convergence.

Taking as an example the “Ambient” of Europe and the “Extra Internet” of the United States, their basic vision of a ubiquitous society is similar to those being established in Asia, but there is still a need for further exchange of strategies among the regions. Without this further exchange, a single basic common direction for a ubiquitous society cannot be identified. Intra-Asia work on such efforts is already well underway. At this point, further efforts are still necessary to aid both Europe and the United States in convergence with Asia. The GBDe will continue its advocacy mission in order to establish this common convergence.

Home Entertainment Networks

A great amount of investment in next-generation networks is needed in order to satisfy the bandwidth requirements necessary to implement the vision of home entertainment networks. National strategies oriented toward achieving a ubiquitous society should foster an adequate regulatory framework that stimulates network investment. (For further information see the specific reference provided by Telefónica.)

3.4. Negative Aspects of a Ubiquitous Network Society

It is an endless effort to overcome the negative sides of any new technology; Internet and/or ubiquitous societies are no exception. Yet these negative aspects must be overcome. The GBDe has made a few recommendations in the past, and they are all still valid. Today, however, there is a more urgent requirement to come up with new ingenuity

that can cope with such downsides. Spam was discussed in the GBDe's 2003 recommendations; spam is still affecting Internet users a year later. Other dangers spreading widely along the ubiquitous network include viruses, phishing, spyware, Trojan Horses, and denial-of-service (DoS) attacks.

Another weak point can be identified in the field of criminal tracking and the prosecution process. Anonymity is easily achieved on the Internet and ubiquitous network, and tracking down an offender is often very difficult. Once an incident occurs, the mass media will often lay the blame not on the attacker, but on those who did not adequately protect their system. While the ordinary user affected by the provided service may be a true victim, it is necessary for both the service provider and its users to realize the necessity of taking responsibility and protecting themselves to the best of their ability.

Each governing country must establish the enforcement of measures against Internet and ubiquitous society criminal acts both before and after individual responsibility on the use of a ubiquitous network has been established. All high-tech criminals must be caught and processed accordingly by the governing country, as well as by international authorities. The GBDe will act as the advocate in these areas with both governing countries and consumer protection advocacies. By realizing measures for all of these concerns, worries about negative aspects will be overcome, and the ubiquitous society can move on to the next stage with flying colors.

3.5. IPR and Copyrights

The use of a ubiquitous network for entertainment purposes continues to increase. This is true for most ubiquitous environments, such as "Out and About", "On the Move", and "In the Home" and even, sometimes, "In the Office". Entertainment applications such as online games, video, and music are delivered using the ubiquitous network. The delivery methods and technologies are being enhanced, and access capability and reliability are on the rise. However, there are significant problems with IPR and copyright that came into being when the Internet became more readily available to all in the early part of the 1990s.

Mobile (Portable Music Player): It is a common misconception that anything on the Internet is free. Given such a misconception, there have been several cases of illegal distribution of copyrighted content over content-sharing servers. These illegal content-sharing servers were especially targeted for litigation in the United States. An industry-born movement has taken place there in conjunction with the litigation efforts. However, despite this climate, an American computer manufacturer developed a portable storage device, designed to be a portable music player that can hold a great deal of audio content. When this device was created, the company did not stop at just manufacturing, but rather went on to develop a network-based music download and billing service. All content hosted by this music server is priced uniformly, and so far the music industry is going along with this method of collecting payments. It is yet to be seen whether this method could become the de-facto standard or a worldwide phenomenon, but it was certainly a good move toward a ubiquitous society. Perhaps the view is that, given a secure payment method and low content fees, the concept may prove acceptable to the consumer. The

current initial success could be credited to two reasons: (1) copyright and ownership are clearly defined, and (2) usage fees are inexpensive and the payment collection mechanism is standardized. The industry addressed the problem head-on, and it was a simple method from the consumer's perspective. The GBDe looks forward to the establishment of other successful industry-initiated mechanisms and controls.

Home Entertainment Networks

Strong copyright protection and enforcement are indispensable tools for exploring the full potential of online content. However, a balance between IPR and users' expectations must be achieved in order to eliminate any barriers to the development of new digital services.

Public authorities, in cooperation with all industry players, should encourage the adoption of efficient and user-friendly DRM mechanisms through the support of open and interoperable solutions, as the most appropriate way of developing the market for consumers while protecting the interests of rights holders. (For further information see the specific reference provided by Telefónica.)

3.6. Introducing e-Commerce in the Developing World

The issue of introducing e-commerce in the developing world has been in discussion ever since the Internet spread into our everyday lives, beginning in the Western world in the 1990s and moving worldwide. Technologically advanced nations in Europe, North and South America, Asia, and elsewhere are fully advancing in the use of the Internet for e-commerce; it is merging into the ubiquitous society. However, there are many parts of the world that are still in need of development in these areas.

The GBDe could advocate some methodologies to help establish a strategy in working with the developing world. One of the major problems in these developing areas is the necessity to leapfrog into the Internet era. Currently, there are two types of network communication methods available for the ubiquitous network: fixed wired communication and wireless communication, with the fixed wired solution divided into several categories, such as ADSL over copper phone lines, fiber to the home, cable modems, and ordinary local area networks. In some countries, it is still difficult to readily obtain a fixed terrestrial communication line. In such cases, a mobile environment may be used to establish a ubiquitous network.

Developed nations already had fixed technologies by the time mobile technology was being introduced. With these developing worlds, however, both fixed technologies and mobile technology are now available. The use of mobile technology is understood to be cheaper than building a fixed environment, and it should be carefully considered and advocated to enhance the deployment of the ubiquitous network in the developing world.

A hybrid solution may also be considered in conjunction with a leapfrog approach of introducing mobile technology. A hybrid in general could be seen as using both fixed and mobile, but yet another technology may be considered for the developing world. Some developing nations are yet to have fully deployed fixed terrestrial communication

infrastructures; often electric power lines are deployed before fixed terrestrial communication lines can be provided to households. In this case, the usage of PLC—power line communication—will enhance the necessity of having a communication transport for the ubiquitous network.

PLC may be thought of as a technology to allow the developing world to leapfrog into the ubiquitous network, but its usage must be carefully examined. PLC will introduce line noise, which in some cases will affect other communication spectra. Judicious planning and examination is recommended. Still, it is a hopeful technology in a hybrid environment, and it should be advocated.

3.7. Spectrum Allocation, Interoperability, and Standardization

Most of the ubiquitous network-associated technologies and services are utilizing some form of the spectrum for their network communication. Although different parts of the world have different spectrum allocation-governing issues, efficient and low-cost spectrum allocation is a common issue and a shared goal. Allocated spectrum differences are the source of difficulties in interoperability and standardization.

The spectrum allocation issue was addressed before with previous GBDe recommendations in the last three years, specifically with the 2002 “Convergence” recommendation and the 2004 “Ubiquitous Society Framework” recommendation. This is still an ongoing concern. As was said in 2004, the ubiquitous network is utilizing a very large number of applications and devices, thus necessitating international cooperation on cross-border usage and spectrum licensing.

Applications affected include: (1) RFID, (2) mobile applications, (3) sensor networks, (4) networked appliances, and (5) PLC, or power line communication.

The interoperability issue is very similar to the spectrum allocation issue, and both are interdependent with each other. Domestic and international usage of ubiquitous devices and applications will continue to rise, and there is a need to operate them in a borderless environment. The true meaning of the word ubiquitous is achieved in four environments: “Out and Around”, “On the Move”, “In the Home”, and “In the Office”. Applications more greatly affected by this interoperability are: (1) RFID, (2) mobile applications, (3) sensor networks, and (4) networked appliances.

With many technologies where protocols and system are introduced continuously by the industry, the issue of standardization has always been very important to consumers. From a ubiquitous network prospective, networked appliances could cover a very broad range of devices; the following are only examples: (1) personal computer technology, (2) telephony, (3) audiovisual technology, (4) television, and (5) RON, or Real Object Networks. Currently, there is no single effort to bundle all of these five technologies under one harmonized standardization. They require ubiquitous interoperability and standardization.

More specifically, an example can be identified in the area of wireless technology usage in audio entertainment, household appliances, and personal computers. Currently, there are three types of WPAN (wireless personal area network) protocols being either used or consider for these consumer electronics. Consumer perspective should be incorporated into the decision-making process on the way to establishing standardization.

RFID: On the application side of standardization, an example can be drawn from the use of RFID. One of the simple merits of using IC tags is the ease of information and data exchange. The use of IC Tag in B2B is already well underway in Europe and the United States, along with portions of Asia. At the same time, there are many international discussions on the various data attributes. The initial proposal on GTIN (Global Trade Item Number) introduced by EPCglobal (Electronic Product Code) is now widely accepted in supply chain management. A similar effort called "Ubiquitous ID" is also in progress, and an ID platform standardization movement has begun. These efforts are necessary, and the issue of associated applications and their interoperability is likewise very important.

To enhance the use of RFID, the next step should be more robust standardization across common applications. An item for future consideration could be the incorporation of other specialized information into the RFID application such as different local customs and laws. All in all, RFID usage will enhance a ubiquitous society for the better, but there are still many issues to be resolved. The current standardization of RFID is a good start, but further continuous refinement is necessary.

Mobile Applications: The most commonly known issues of mobile applications—spectrum allocation, interoperability, and standardization—are all seen in mobile phones. Recently, mobile phone service abroad has begun to enjoy more services, extended coverage and availability, and increased ease of use. With the introduction of newer generations of mobile technologies such as 3G, including IMT200 and its family, and 4G, which will make its foray in the near future, continuing efforts should be made in all basic issues with spectrum allocation, interoperability, and standardization.

Many of these basic issues are specific to each country's governing communication industry laws. The GBDe will continue its advocacy with both telecommunication industries and governments toward the enhancement of mobile phone service. By advocating mobile phone efforts, similar approaches and movements could be undertaken for all other mobile-related issues, which are very alike in nature.

Networked Appliances: As many household appliances are becoming network-connectable and ubiquitous application-enabled, several issues are arising. Content and data movement among devices and external ubiquitous connectivity must be standardized, especially in the area of audio and visual appliances. It is also understood to be tied into the appliances' operability from a consumer perspective.

Historically, many different standards and interoperability styles have evolved throughout the world. Several different voltages (i.e., 100V, 120V, 200V, 220V) and two-major A/C

frequencies (50Hz and 60Hz) are being used to supply electrical power. In the same way, there are two-major television video formats (i.e., NTSC and PAL). When these specifications were introduced, the world was more regionally independent, but with the expansion of the ubiquitous society in the 21st century, consumers view worldwide interoperability is a "must".

WPAN: Although it is a wireless technology, its wireless coverage area is very small compared to mobile and wireless LAN technologies–usually within a few meters or feet. With the introduction of WPAN technologies, the proverbial "last one mile" problem is shrinking to one of the "last few feet", and network usability is said to increase as well. There will be a new market based on WPAN usage.

One of the commonly used and more mature WPAN technologies is Bluetooth, which has been deployed for the last few years. Others are still being developed and standardized, including UWB, or Ultra Wide Band, and ZigBee. All three fall within the IEEE 802.15 category. Although the GBDe is technology-neutral, the industry should consider the issue of standardizing technology use to avoid repeating history, namely the difficulties seen in videotape and disc format specifications.

The use of wireless technologies with networked appliances has led to a spectrum allocation discussion with the ZigBee protocol (IEEE 802.15.4). ZigBee is authorized to use the 915 MHz spectrums in the United States and the 868 MHz spectrums in Europe. Countries such as Japan have not yet authorized spectrum allocation to ZigBee technology, but Japan is planning to allocate 2.4 GHz soon. Interoperability and spectrum concerns do exist for the WPAN protocols.

In this ZigBee example, it is said that there were no successful worldwide efforts or movements in establishing a common worldwide spectrum. Because of this lack of discussion and advocacy, ZigBee was understood to use each country's open common spectrum band. This will lead to cross-border interoperability problems with soon-to-be-released ZigBee-enabled devices.

Another family of IEEE 802.15 network protocol with some prospects is UWB, or Universal Wide Band. UWB will cover a very small area of a few meters and will use very little power; some countries will not consider its use to be a spectrum allocation issue. However, if many UWB devices are to operate together at the same time, there will be enough transmission noise to affect other communications. A discussion on use among governments, industry, academia, and consumer advocacy should be pursued.

4. Conclusion. For the Future of the Ubiquitous Network Society Vision

As written in the "National Strategies and Worldwide Activities" section above, there are many efforts throughout the world to accomplish the Ubiquitous Network Society Vision. Currently, this effort is stronger in Asia and Europe. Regardless of whether in Asia, Europe, the Americas, or elsewhere in the world, however, a ubiquitous network is meant to break through all barriers and be everywhere. To accomplish this, all visions must be

shared and understood by one other. With this understanding, a convergence will then take place to form a whole new direction called the "Ubiquitous Network Society Vision".

Looking at the GBDe's activity in each country, we see there are still several issues to be resolved and converged. Obstructions to convergence could occur at any level, but with the GBDe's efforts and cooperation, convergence will occur. To achieve this convergence, the GBDe has been very active in participating in many different advocacies this year.

As the next-generation information and communication technology (ICT) paradigm is emerging, a single unified Ubiquitous Network Society Vision is desired. With this new paradigm shift, we continue to look toward a joint effort initiated by the private sector and industry that will take the lead and obtain government-level support. Since the inception of the GBDe organization, the GBDe and its participating colleagues have worked closely together to achieve the goal of a Ubiquitous Network Society Vision.

At the time of its creation, the GBDe's purpose was to promote e-commerce on the Internet. The Internet then was mostly accessed by narrowband telecommunications, mainly with a dial-up modem line. Still, the GBDe anticipated e-commerce's wide growth and acceptance as the Internet continued to expand. Today, the Internet has expanded into the ubiquitous network, and in the 21st century, e-commerce will grow even further along with the Ubiquitous Network Society Vision.

Contributions from Issue Group Members were provided by: Chunghwa Telecom, Institute for Information Industry, Taiwan; Fujitsu, Ltd., Hitachi, Matsushita Electric, NTT DATA, TEPCO (The Tokyo Electric Power Company, Incorporated), Toshiba, Japan; Telefónica, Spain.

GBDe 2005 Issue Group

Ubiquitous Network Society Vision

October 11, 2005

Special References

Contributions by Issue Group Members

The Spectrum Allocation Issues – an example of Taiwan
Submitted by: Chunghwa Telecom, Taiwan

Introduction
In the early years, only telecommunications system like satellite or microwave systems and broadcasting services like TV or radio stations required frequency resources, however, due to the rapid development of wireless telecommunications technology, more frequency spectrum needs to be released to meet the new wireless services demand.

In Taiwan, the frequency spectrum resources are regulated by a governmental agency called DGT (Directorate General of Telecommunications). The DGT is responsible for assigning all frequency for government and commercial purposes, except for defense purposes. However, when the frequency is used for broadcasting services, such as TV or radio, there is another governmental agency called GIO (Government Information Office) which, jointly with DGT, reviews applicants' information and assigns frequency.

The Spectrum Regulators in Taiwan
The DGT
The DGT was established in 1943 as a government agency under the supervision of the Ministry of Transportation and Communications (MOTC). The DGT has dual roles of regulating telecommunications enterprises and providing telecommunications services.

In the early 1990s, for the purpose of restructuring the DGT to meet the telecom liberalization trend, the Taiwan government was engaged in amending the Telecommunications Act. After years of effort, legislation and enabling laws for an independent regulatory body, i.e. the Telecommunications Act and the Organizational

Statute of the DGT, were finally completed on January 16, 1996. Both of these laws were promulgated on February 5, 1996. According to the directive of the Executive Yuan, the DGT was designed to specialize in the telecom policy formation and market management from then on. With that milestone, the DGT's dual roles as both player and referee were formally terminated.

Pursuant to Article 3 of the 1996 Telecommunications Act, the DGT shall devise an integrated telecommunications development plan, supervise telecommunications enterprises and promote the development of an information society so as to enhance public welfare. To fulfill the\is duty, five departments in charge of general planning, public telecommunications, dedicated telecommunications, radio and TV broadcast technology, and radio wave regulation, respectively, and a Legal Office were established under the DGT.

In implementing the telecommunications regulatory responsibility, three regional telecommunications regulatory stations, including the northern, central, and southern regions of Taiwan, have been founded. For administrative support there are four offices responsible for the secretariat and general affairs, personnel, accounting and government ethics. In order to ensure that the radio waves are maintained in order, the DGT coordinates with the National Police Administration of the Interior Ministry and has set up a telecommunications police unit.

The GIO

The GIO (Government Information Office) is under the Executive Yuan, and the Department of Broadcasting Affairs is the specific department under GIO in charge of all broadcasting services issues. The Department has the functions of:

- Enforcing legislation pertaining to the radio, television, and cable TV industry.
- Tabulating the activities of the radio, television, videotape and cable TV industries.
- Regulating radio and television broadcasting stations, cable television system operators, and radio and television program supply enterprises.

One major work of the Department of Broadcasting Affairs, which relates to the spectrum allocation issue, is assigning radio frequencies and allocating the quantity and distribution of radio, TV and cable TV operators.

<u>Spectrum Regulating Policies</u>

Radio frequency is a high-value and limited resource, therefore, spectrum allocation is well planned in every developed and developing country. In order to utilize the spectrum more efficiently in Taiwan, the DGT has fundamental rules to follow, which are:

1. Follow international technology trends and standards.
2. Enforce public benefits and safety, and protect the nation’s security.
3. Efficient use of the spectrum - frequency reuse, and avoid interference.
4. Implement market-oriented allocation, and meet domestic industry and commercial demand.
5. Make reservations for new developed technology.

License Types
According to the Article 11 of Telecommunications Act of DGT/MOTC, Telecommunications enterprises are classified into Type I telecommunications enterprises and Type II telecommunications enterprises.

A Type I telecommunications enterprise means an enterprise that installs telecommunications line facilities and equipment in order to provide telecommunications services. The aforementioned telecommunications line facilities and equipment refer to network transmission facilities connecting the sending and receiving terminals, the switching facilities installed to be integrated with the network transmission facilities, and the auxiliary facilities of both. Examples of Type-I enterprise wireless services are GSM, 3G, satellite and microwave. The Type-I enterprise wireless services providers are the major telecom carriers in Taiwan, such as Chunghwa Telecom Co. Ltd, Taiwan Cellular Corp. and Far EasTone Telecommunications Co., Ltd.

A Type-II telecommunications enterprise means a telecommunications enterprise other than Type I telecommunications enterprises. An example of Type-II enterprise wireless services is WLAN (Wireless Local Area Network), the WLAN service is classified in Type II Telecommunications Special Business. In other words, a Type II Telecommunications Special Business license is required for the WLAN service provider. According to the DGT web site information, all WLAN service providers are ISPs (Internet Service Providers). Currently there is a total of 182* ISPs in Taiwan. (*From http://www.dgt.gov.tw 2005/5/31)

Spectrum Allocation – Enterprise License Dependent
In the Telecommunications Act of Taiwan, spectrum resource can only be released on an enterprise license dependent basis, and once the spectrum is assigned to certain operator, it cannot be divided or transferred to the third party before the enterprise license has expired. The previous 3G-license auction in Taiwan is the typical example of the Type-I business license auction; it is not a spectrum auction. In contrast, the telecommunications legislation in developed countries like USA or UK, has defined a secondary market for spectrum resources. In this case, the authority allows spectrum owned operators to lease whole or a portion of the spectrum to the third party. This advanced approach can make the spectrum and the wireless communications market very efficient and for this reason the DGT may consider adding these secondary market approaches in the future Telecommunications Act amendment.

For efficient usage of the spectrum and minimize the interference, a technology called UMA (Unlicensed Mobile Access) features listen-before-transmit characteristics. The UMA provides access to GSM and GPRS mobile services over unlicensed spectrum technologies, including Bluetooth and 802.11.

Single administrative process on licensing
One example of licensing of this year in Taiwan is DAB (Digital Audio Broadcasting). As previously mentioned, the GIO works with the DGT when the license is broadcasting

service related. This is one of the examples a two-track overlapped process (GIO and DGT) to issue a license in Taiwan. Both agencies has to review all applicants (or candidates). Therefore, in order to simplify the process in similar cases, the Taiwan government plans to establish a NCC (National Communications Commission) to take the GIO's and DGT's places in future. The NCC law is still under construction in the Legislative Yuan but the Commission is expected to be established in two or three years. Once the NCC is formed, Taiwan will have the ability to efficiently meet the issues raised by increasing digital convergence.

Future of the Ubiquitous and Society - Home Entertainment Networks
Submitted by Telefónica of Spain

Introduction
When analysing in detail the different dimensions of a Ubiquitous Society, the home environment sticks out as a centrepiece of interaction for both professional and leisure activities.

Increasing technological convergence between telecommunications, IT, consumer electronics and content industries and the advent of broadband access as a mass market technology provided through multiple and competing open platforms are creating opportunities for new multimedia and content revenue-generating services based on a consistent offer of voice, data and video services to the end user. Consumers' ability to build up their home networks (based in these two factors together with an increasing supply of home net equipment at affordable prices) is a crucial step forward towards the consolidation of these new business models based on cooperation between the different actors in the value chain.

A home network could be simply defined as a set of connected household devices (set-top-boxes, TVs, PCs, portable devices, etc.) that may share content in a predictable and consistent way. When used for the transfer of data and audiovisual content related to leisure activities (music, video, games, gambling) we might define them by using the term home entertainment networks.

HEN: increasing demand for leisure content
Forecasts for the global entertainment and media industry predict an increase from $1.2 trillion in 2003 to $1.7 trillion in 2008, growing at a compound annual rate of 6.3 percent[1]. New distribution channels based on information technologies will contribute to increase demand for the on-line provision of legitimate leisure content. Home networks will play a crucial role as facilitators for consuming content and for the implementation of new business models (VOD, download & play, interactive services etc).

Challenges and barriers for HEN
However, there are a few regulatory challenges and barriers that need to be overcome to achieve this vision of home entertainment networks: the need for investment friendly

[1] PWC: Global Entertainment and Media Outlook 2004-2008

regulatory environments, interoperability and content protection and availability are the main knots that public authorities have to untie to allow home entertainment networks to achieve their full potential as a source both of customer satisfaction and business revenues.

Investment friendly regulatory environments

The potential of home entertainment networks as a demand aggregator for online content and new business models relies upon the existence of high-speed networks able to provide high quality services. Further pressure on bandwidth requirements is put into the networks used to offer higher-speed Internet access, demanding a great bulk of investments from the private sector in upgrading them or deploying new infrastructure. Public Authorities should avoid the application of a regulatory approach purely focused on service-based competition as this could distort economic incentives for investments in infrastructure putting at risk customer benefits derived from technological improvements and innovation. Next generation networks require and adequate regulatory approach that stimulates investment, focusing strictly in areas where competition is not anticipated to emerge.

Interoperability

Affordable home net equipment and the consumer's desire to access any content, anywhere, anytime are crucial drivers for the demand of home networking. However, in order to reach the stage of plug and play, where content becomes accessible on any home networking device, several levels of interoperability need to be accomplished.

At the transport level, devices must utilize the same communication protocol; to ensure proper decompression, devices must share a common compression standard and if content is protected against piracy, devices must use the same protection scheme or agree to a common protection scheme. At the user level, devices should manage content and function in a consistent and predictable way, referring to similar functions in the same way and using similar symbols. This interoperability framework should rely upon an industry led development of open standards and their voluntary adoption, without any regulatory constraints.

Content protection and content availability

As the GBDe Working Group on New Business Models stated in 2004, strong copyright protection and enforcement are indispensable tools for exploiting the full potential of online content. However, a balance between IPR and users' expectations must be achieved in order to eliminate any barrier to the development of new digital services.

In this context, the use of Digital Rights Management systems is still considered the best solution to benefit all stakeholders, by facilitating the licensing, acquisition and protection of copyright and other neighbouring rights through technical means, without interfering with normal consumption by the end user[2].

[2] Neighbouring rights concern other categories of rights and owners of rights i.e. rights that belong to the performers, the producers of phonograms (CDs and records) and broadcasting organizations in relation to their performances, CDs and broadcasts respectively.

DRM systems may ensure a fair collection of revenues and appropriate remuneration schemes for all players in the value-chain, thereby promoting wider availability of high-quality digital content.

Public Authorities in cooperation with all industry players should encourage the adoption of efficient and user-friendly DRM mechanisms through the support of open and interoperable solutions, as the most appropriate way of developing the market for consumers while protecting the interest of the right holders.

On the other hand, availability of premium content in the different multimedia platforms (ADSL, cable, mobile, satellite) is of critical importance to attract consumers and hence for the success of home networking. Consumers should not have to make a technology decision when purchasing content, but so far it has been difficult for some of these platforms to gain access to premium movies, sports or even TV channels.

A proper balance should be sought between the interests of content and service providers in light of the common objective of meeting consumers' interests and maximising the benefits of the new value chains for all stakeholders. Contract clauses that discriminate against particular platforms hampering competition should not be allowed by Public Authorities to avoid possible market foreclosures.

It may be concluded that the wide availability of content through the development of legal offers attractive to the consumer, technically effective and user friendly if in fact the best solution in the fight against piracy.

Trends in Power Line Communication (PLC)

Submitted by the Tokyo Electric Power Company, Incorporated (TEPCO)

Introduction

A. Overview of PLC

Power Line Communication (PLC), also called Broadband Over Powerline (BPL), is a technology to transmit information over the existing electric cables. Power utilities have used PLC for many years for the management of their electric grid. In recent years high-speed PLC technology has advanced and become available for communication network, thus it can provide a wide array of services such as broadband Internet access, VoIP services, in-home services, audiovisual and multimedia services, energy applications, etc.

B. Advantages and disadvantages

The main advantage of PLC is that it is available in almost every room and house in the world because power outlets are almost ubiquitous. PLC has the great potential to reduce the digital divide between rural and urban areas. Another advantage of PLC is Plug and

Play, so that it does not require any extra rewiring work when starting a broadband subscription, which means it is cost-effective.

However there are some issues surrounding PLC. The first is the electromagnetic compatibility issue. Because the 2-to-30MHz band, which is to be used for PLC, is assigned to shortwave radio broadcasting, amateur radio stations and so on, there have been concerns about the unwanted radiation from high-speed PLC which might influence radio use. Another issue is the competition from other network technologies. PLC is used mainly for broadband access and home network. Existing network technologies such as DSL, cable, fiber, wireless network are also available for this purpose and are used more widely than PLC at present but PLC can complement other existing networks e.g., a mixed solution that uses PLC for in-home networking and DSL for broadband access.

World Trends in PLC

To date, many trials and tests in more than 40 countries have been conducted, and some of them are being deployed commercially. At the same time, there are different regulations for PLC by countries because Electrical power systems vary in configuration from country to country depending on the state of the power sources and loads. Table 1 shows the status of regulations and trials of PLC in representative countries.

Table 1 Worldwide PLC status of regulations and trials

Country	Availability (Regulation)	Status of PLC services	Comments
US	○ □Yes□	Commercial	Regulations are clearly determined. Outdoor use of special frequencies is prohibited. Many of power lines are aerial.
Germany	○ □Yes□	Commercial	Uniform standards in EU are under discussion. Many of power lines are underground.
Spain	○ □No□	Commercial	
UK	○ (Yes)	Experimental	
France	○ □No□	Experimental	
China	○ □No□	Experimental	
Singapore	○ □No□	Experimental	
Korea	○ (Yes)	Experimental	Radio Law is going to be deregulated in 2005. Many of power lines are aerial.
Japan	× (Yes)	Experimental	MIC established a study group on PLC. Regulations are under discussion. Many of power lines are aerial.

PLC in Europe

Broadband penetration in Europe is low compared to Asia and the USA and PLC is expected to help to overcome the existing digital divide. PLC pilot projects have reached the commercialization stages in Spain, Germany and other countries. In Spain, one of the largest power companies Endesa began commercial service in Zaragoza and Barcelona in

2003.Power Plus Communication in Germany is made available commercially to approximately 5,000 houses in Mannheim.

PLC can be already deployed with current regulation in Europe but a more stable and nondiscriminatory regulatory framework is under discussion to take full advantages of PLC. The European Commission is also developing a recommendation applicable to PLC.

PLC in USA

The Federal Communications Commission (FCC) regards PLC as a potential "third wire" that may help increase the availability of broadband service and be an alternative to existing DSL and cable. The FCC has declared the policy for promoting Internet access over power lines and is completing the regulatory framework for PLC in the US.

To date, several dozen experiments or trials of PLC have been conducted. The first commercial PLC deployments have occurred in the city of Manassas. The service has been fully provided to 12,500 homes. Cinergy in Ohio has also deployed the commercial services and is creating a network that it expects to serve over 250,000 customers within three years. In addition, a PLC modem called "HomePlug" is sold for the purpose of home networking in the US.

PLC in Asia

PLC demonstrative experiments and trials have been conducted in China, Singapore, Malaysia, Korea and other countries. In Hong Kong, commercial service is being provided to a few thousand locations at hotels and housings complexes.

In Japan, the use of hi-speed PLC is restricted by the Radio Law and its work-execution regulations. Still, field trials are being carried out to reduce the emission of electrical fields.

The Ministry of Internal Affairs and Communications (MIC) established a "Study Group on High-Speed Power Line Communications" in January 2005. The study group consists of stakeholders from electric power companies, equipment manufactures, broadcasters, amateur radio development association, etc. They are deliberating upon the conditions for coexistence between radio use and high-speed PLC.

Challenges for the Age of Ubiquitous Connectivity
Exemplified by the Home Robot
Submitted by Toshiba

In advanced ubiquitous networks, robots will provide an interface between the cyber world and the real world. There is an emerging demand for artificial intelligence but it is difficult to achieve.

Stages on the Road to Ubiquitous Connectivity

1. The real world is connected to the cyber world
2. Real world information is processed in the cyber world, but people only can use that information.
3. Real world information is processed in the cyber world, which uses its judgment to achieve autonomy and control the real world.
4. The cyber world perceives and recognizes the real world autonomously and proactively, and controls the real world.
    a. Ubiquitous connectivity allows the cyber world to realize autonomy
    b. A comfortable world without burdens for users is realized, as the cyber world assesses situations and makes arrangements. There are problems that need to be solved.

Conventional appliances: independently provide convenience. However, networked appliances: provide users with much better "entertainment, safety and comfort"

Challenges for Ubiquitous Connectivity with Robots
Robots can be seen as active sensors, with the capability to become the ultimate components for sensor nets.

Consider the example of robots connected to the network:

- Why? The robot differs from a conventional home appliance. The robot is a new home appliance that had autonomous mobility and is able to independently carry out tasks.
- Robots are a promising technology, a potential next generation growth engine for Japan, which is adept at maximizing and integrating advanced technologies.

Challenges for robotics in an age of ubiquitous connectivity

1. How to make sure that the potentially infinite variety of robots (countless variations in robot specifications and how they operate) can be recognized by the network.
2. How to develop robots that can minimize problems when the network gives contradictory or too many orders.
3. How to realize truly autonomous robots.

Difficulties in realizing home robots

The "home" is the place where the robot moves around: an extreme environment. Nevertheless, in all circumstances, the robot must behave autonomously and carry out ordered tasks.

- shape and conditions differ from house to house
- the movement of objects in the home constantly changes the landscape
- things are always changing: the number of people at home; guests; kids; pets. The robot must be able to handle this.

Obstacles for robots when moving around

How is the robot to behave if there are obstacles or if there is a change in the environment while the robot is trying to carry out orders from the owner or the network?

- wait until the situation gets better
- find a way around, a detour
- give up the action
- bulldoze its way through

Items Indispensable for Development of Home Robots

- Recognition of family structures
- Automatic mapping of the home interior
- Identifying optimized self-positioning
- Sensing and image recognition function required
- Learning function
- Autonomous judging function

Contributions from Issue Group Members were provided by: Chunghwa Telecom, Institute for Information Industry, Taiwan; Fujitsu, Ltd., Hitachi, Matsushita Electric, NTT DATA, TEPCO (The Tokyo Electric Power Company, Incorporated,, Toshiba, Japan; Telefónica, Spain.