



Office of the President of the Philippines
COMMISSION ON INFORMATION AND COMMUNICATIONS TECHNOLOGY

First Public Key Infrastructure (PKI) Seminar

Thursday, 10:00 AM, 6 November 2008

Sampaguita Hall, Manila Hotel

Opening Remarks

SECRETARY RAY ANTHONY ROXAS-CHUA III

Chairman, Commission on Information and Communications Technology

To be read by

COMMISSIONER ANGELO TIMOTEO M. DIAZ DE RIVERA

His Excellency Ambassador Choi Joong-Kyung of the Republic of Korea, Department of Trade and Industry Undersecretary Thomas Aquino, Mr. Kim In, Resident Representative of the Korea International Cooperation Agency, our partners in government, the academe, and the private sector, distinguished guests, ladies and gentlemen, good morning.

On behalf of the Commission on Information and Communications Technology, or CICT, allow me to welcome you to this First Public Key Infrastructure, or PKI, Seminar, which is part of a series of capacity-building activities towards developing a Master Plan and Pilot System of a National PKI in the Philippines. I would like to acknowledge the Korea International Cooperation Agency, or KOICA, for funding yet another landmark project in support of Philippine e-commerce—the establishment of a national system for electronic signatures to ensure the security and integrity of online transactions in the country. KOICA, and its project management arm POSDATA, will be providing us with expert knowledge on the development of a PKI for the Philippines. I also wish to commend the Department of Trade and Industry, the CICT's partner in this important initiative, for organizing this First PKI Seminar, which has convened an impressive representation from government and the private sector.

When the Philippine Electronic Commerce Act was signed into law in 2000, the Philippines became the third country in Southeast Asia to enact legislation to promote, as well as secure, the integrity of electronic transactions. Among the law's important provisions were the recognition of electronic documents, electronic signatures and electronic transactions, and their admission as evidence in court adjudications. Through its identification of cybercrimes, such as hacking, introduction of viruses, and piracy, the E-Commerce Act is able to penalize the unauthorized access to information, as well as the disruption of networked systems. Since its enactment, the Law has enabled the Philippines to position itself as a key player in the global e-commerce community, and has made us one of the world's fastest growing e-economies. It has also been a driver for the transformation of government towards e-government by encouraging the widespread adoption of e-commerce models and strategies in government processes.

The importance of the E-Commerce Act is even more evident eight years after its enactment. It has provided the foundation for current drafts of cyber security and data privacy laws, having already identified cyber crimes such as hacking and piracy. It should be noted that piracy alone accounts for losses of approximately 147 million US dollars for the software industry in 2007, according to the Business Software Alliance, and casts a shadow on the country's efforts to achieve international competitiveness in the global ICT marketplace.

The widespread use of e-commerce in the global marketplace has made PKI a critical element in network and online security. PKI authentication has strengthened privacy levels in the exchange of data, and made online transactions using digital certificates more reliable and secure. We believe that building consumer and user trust in the integrity of online transactions is integral to the growth of the Philippines' e-commerce industry, as well as our e-government services.

In recent years, we have observed with concern the increasing threat of cybercrime, ironically enabled by the same technologies that bring digital and economic opportunity. In order to thwart these growing threats, the CICT has endorsed to Congress a landmark Anti-Cybercrime Bill, entitled the "Cybercrime Prevention Act of 2008", which defines various forms of cybercrime offenses and prescribes corresponding punishments. These offenses include hacking, identity theft, phishing, spamming, website defacement, denial-of-service (DoS) attacks, malware and viruses, child pornography and cyber prostitution.

The Bill has staunch supporters from the ICT industry, as well as the country's law enforcement agencies, who have been calling for a more defined and effective anti-cybercrime framework to secure the integrity of computer and communications systems, as well as to protect the citizenry from rising incidents of illegal, malicious and life-threatening acts committed through the use of computers, mobile phones, or other networked devices.

Network and online security should never be taken for granted. I am heartened by the bilateral efforts of the Republic of Korea and the Philippines, as well as the participation of agencies and institutions represented here today, on the exchange of knowledge on the establishment of a PKI. This project is especially critical in light of the CICT's current advocacy for the passage of the anti-cybercrime bill pending in Congress, because we believe that a country's PKI plan will be more effective if it is implemented as part of a national cyber security strategy. We fully support the efforts of the Inter-Agency Working Group on PKI, co-chaired by the DTI and the CICT's National Computer Center, and all their adjunct activities that will hopefully develop the most appropriate PKI strategy for the Philippines. This program demonstrates government's commitment to providing our citizens with a secure online environment.

Once again, I would like to welcome all of you to this First Public Key Infrastructure Seminar and I enjoin all the stakeholders to work together in ensuring a secure Philippine e-commerce community.

Thank you and mabuhay!