International Commerce and Information Review
Volume 19, Number 4, December, 2017: pp. 29~50
통상정보연구 제19권 제4호 (2017년 12월 31일)

논문투고일자 : 2017. 11. 20
심사(수정)일 : 2017. 12. 12
게재확정일자 : 2017. 12. 16

# The government role in digital era innovation: the case of electronic authentication policy in Korea*

## 디지털 혁신시대의 정부역할: 한국의 전자 인증정책 사례

Wonbae Son
SUNY Korea, Ph.D. Student
Main Author

Mun-su Park
SUNY Korea, Research Professor
Corresponding Author

Contents

## ABSTRACT

In emerging technologies, innovation processes are dynamic in that the government needs to regularly review its policies to resonate with rapid technological advancements, changing public needs, and evolving global trends. In the 1990s, the Internet grew at an explosive rate, but many applications were constrained due to security concerns. Public Key Infrastructure (PKI) seemed to be the fundamental technology to address these concerns by providing security functions. As of 2017, PKI is still one of the best technologies for electronic authentication in an open network, but it is used only in limited areas: for user authentications in closed networks and for server authentications within network security infrastructure like SSL/TLS. The difference between expectation and reality of PKI usage is due to the evolution of the Internet along with the global adoption of new authentication policies under the Internet governance in the early 2000s. The new Internet governance based on the cooperation between multi-stakeholders is changing the way in which a government should act with regard to its technological policies. This paper analyzes different PKI policy approaches in the United States and Korea from the perspective of path-dependence theory. Their different policy results show evidence of the rise of the Internet governance, and may have important implications for policy-makers in the current global Internet society.

Key Words : Public policy, Electronic authentication, PKI, Path dependence, Governance

* This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ICT Consilience Creative program (IITP-2017-R0346-16-1007) supervised by the IITP (Institute for Information & communications Technology Promotion)

# Ⅰ. Introduction

For the last decades, electronic authentication technologies gained much more importance as the Internet grew at explosive rates. However, the most widely used electronic authentication method is still password even though it has many security problems. Public Key Infrastructure (PKI) has been a technological alternative, but it is not widely deployed despite its enthusiastic popularity in the 1990s on its advanced security features. Among the countries which tried PKI deployment, the US was the first country that established the legal framework for PKI, but Korea was the first and the only country that nation-wide PKI was deployed. PKI is not only a technology but a complex system which combines legal, economic, social and technological factors within a society. Therefore, comparing different countries where different PKI policies were implemented may give a clear view of how the government and technological stakeholders are interacting nowadays.

This research analyzes the Korean electronic authentication policy reform case applying a new public policy model of path dependence. By comparing the US and Korean policy approaches, the analysis will show the reasons for a decade-long policy continuity of Korea and the rise of the multi-stakeholder process as a new form of governance. To understand the path dependence of Korea, this research also covers other essential theories such as Developmental State, National System of Innovation (NSI), and the Internet Governance. It may give important implications for policy makers in modern hyper-connected Internet society.

# Ⅱ. Literature Review

## 1. Developmental State

The well-known seminal work on the developmental state is Johnson's study of Japan in 1982. In the study, Johnson presented a conceptual model of the developmental state which represented as an industrial policy with complex interaction of public-private partnership (Johnson, 1982). The dominant view on the developmental state is that since the late 1990s there has been an “end of the developmental state." Several works of literature discussing the developmental state of Korea, however, argue that the characteristic of the developmental state still be found in the early 2000s. Larson & Park assert that the Korean government showed its transition from developmental to networked state in the early 2000s, but they argued that the stakeholders in the country are still looking for government leadership (Larson & Park, 2014). Some authors reject the idea of the end of the developmental state of Korea. Kim analyzes Korea's telecommunication sector between the 1980s to 2000s and insists that the continued growth of Korean conglomerates, the chaebol, is still dependent on nation's transformative capacity despite the globalization of world economy (Kim, 2013). Moreover, an analysis of Wireless Internet Platform for Interoperability (WIPI) case of Korea in the early 2000s shows that the Korea government was still playing a developmental role with new forms of cooperation between the public and private (Kim, 2012). This long-lasting unique relation between the public and private sector of Korea characterized the structure and processes of its national systems of innovation.

## 2. National Systems of Innovation

Both National System of Innovation and National Innovation System describe the same idea. By OECD's definition, National Innovation System (NIS) is a systemic approach which explains the innovation process within the overall innovation system of a country. There is no single definition of a NIS, but the web of interaction or the system is one of the commonly accepted ideas of NIS (OECD, 1997). Below table summarizes key works on national systems of innovation comparing the definitions, factors, and unit of analysis:

<Table 1> The Key works on national systems of innovation (Lee & Yoo, 2007)

| Author | Definition | Key factors | Unit of analysis |
|---|---|---|---|
| Lundvall (1992) | Narrow definition: organizations involved in searching and exploring | Institutional set-up of a specific firm, a constellation of firms, or a nation | R&D departments, technological institutes, and universities |
| | Broad definition: institutional set-up affecting learning as well as searching and exploring | Open and flexible relationship | Production system, marketing system, and financing system |
| Nelson (1992) | Institutions and mechanisms supporting technical innovation | Institutions that function as supporting and uncertainty-avoiding organizations | Firm, domestic market customers, education systeam, and government polcy |

| Author | Definition | Key factors | Unit of analysis |
|---|---|---|---|
| Freeman (1995) | Network of institutions in the public and private sectors whose activities and interactions initiate, import, modify, and diffuse new technologies | Network of institutions<br>Role of the state | State level: government organization & policy, education system, technical and scientific institutions, and cultural traditions<br>Firm level: company's R&D and conglomerate structure |

NSI perspective premise that each country follows its own institutional structure and innovation trajectory. NSI's diverse institutional arrangements shape the relationships between technology and economic development of a nation. Empirical studies show diverged technological profiles and innovation capabilities among nations. Therefore, OECD (1997) stated that "It is believed that countries tend to develop along certain technological paths or"trajectories" determined by past and present patterns of knowledge accumulation“ (p. 13).

The Korean NSI has proved very successful in some industries by its logic of sectoral functioning, so there are several studies analyzing the Korean NSI in different industries. Kim asserts that the success of Korea's semiconductor industry is due to the complex interaction between public and private which evolved to changing interactions among state, world market conditions, and Chaebol governance from the national-political institutional arrangement like reciprocal subsidy (Kim, 1998). In the 2010s, the Korean public private partnership is focusing more on small and medium companes in the ICT sector. Moreover, the government's supporting measures include R&D funding and taxation supports (Park & Lee, 2012) and promoting technology transfer (Park, 2015)

## 3. Path dependence theory

There are several theories related to policy change: path dependence, advocacy coalition framework, policy learning, policy diffusion, punctuated equilibrium, etc. Among them, path dependence model argues that it is generally difficult to change policies. The strength of the theory is that it can explain why policy continuity is more likely than policy change. (Cerna, 2013). Simmie (2012) depicted basic path dependence model as below:

<Table 2> Basic economic model of path dependence (Simmie, 2012)

| Initial condition | Path creation processes | Path establish processes | Path dependence outcomes | Path dissolution |
|---|---|---|---|---|
| Not specified | Historical accidents,<br>Chance events<br>Serendipity | Contingent selection<br>Self-reinforcing effects | Lock-in of inefficient or sub-optimal technologies, institutions or organizational forms | External shocks |

Path dependence has its strength in explain the institutional durability and persistent difference between different institutions, but has weakness in institutional change and evolution (Son, 2006). Path dependence is frequently used in explaining cases which "history matters." Lim analyzes the rise and fall of the Korean economic development model based on path dependence (Lim, 2000). He insists that the early success of the Korean economic system made it difficult for policymakers to introduce fundamental changes, and made Korea stand on the brink of another debt crisis.

Several literatures are analyzing some structural problem of the ICT industry of Korea. Korea's conglomerates led hardware technology focused ICT sector R&D attributes path dependence of Korea's ICT industry and R&D experience (Ko &Kang, 2013). Some research find path dependence as a reason for different technological advancements among countries. Kubicek and Noack made a comparison of four national electronic Identity Management Systems (eIDMS) in Austria, Belgium, Spain, and Germany, and show a high degree of path dependency in each system. They concluded that each system's differences are just a continuation of differences between the previous systems (Kubicek & Noack, 2010).

In path dependence theory, a policy change is made at a critical juncture. Capoccia and Kelemen (2007: 348) define a critical juncture as 'relatively short periods of time during which there is a substantially heightened probability that agents' choices will affect the outcome of interest'. In this definition, relatively short period time means that the duration of the juncture is brief relative to the duration of path dependence establishment. The unique characteristic of the Korean NPKI policy reform lies this point. The critical juncture of Korean PKI case is made for over a decade while the path establishment process took approximately five years.

## 4. Electronic authentication technology and Public Key Infrastructure (PKI)

In 2011, the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-1 defined electronic authentication as “a process to establish confidence in user identities presented electronically to an information system” (Burr et al., 2011, vi). The latest publication NIST SP 800-63-3 changed its title as Digital Identity Guidelines. NIST SP 800-63-3 and its companion volumes provide technical guidelines for the digital authentication and define digital authentication as “the process of determining the validity of one or more authenticators used to claim a digital identity” (Grassi et al., 2017, p. 8). In the late 1990s, the technical classification of an authentication was somewhat dichotomous. International Telecoms Union Telecommunication Standardization Sector (ITU-T) recommended electronic authentication called X.509 describes two levels of authentication: simple authentication and strong authentication. Simple authentication uses a password to verify the claimed identity, and strong authentication involves credentials based on cryptographic techniques (ITU-T, 1997). ITU recommended solely to use strong authentication as the basis for providing secure services while simple authentication offers some limited protection against unauthorized access. The representative technology for the strong authentication was PKI. It is because PKI offers core security services such as authentication, integrity, and confidentiality. As seen the table below PKI technology was developed and standardized in the early 1990s, and security vendors including Entrust, VeriSign, and RSA Data Security developed packages for PKI in the enterprise environment.

<Table 3> Technological development and standardization of PKI until the early 1990s

| Stages (year) | Theory Development (1976) | Technology Development (1978) | Standardization (1988) | Additional Standardization (1991) |
|---|---|---|---|---|
| Event | Introduction of Diffie-Hellman key exchange | Rivest-Shamir-Adleman (RSA) algorithm enabled digital signing and Diffie-Hellman key exchange came to be called PKI | The ITU-T Recommendation X.509 was approved. The identical text was also published as ISO/IEC International Standard 9594-8 | NIST proposed Digital Signature Algorithm (DSA) as a standard digital signature algorithm based on RSA algorithm. |

However, the PKI deployment in the open Internet is hardly found until now, and most literature argue that PKI is a failure. Literature on PKI failure are analyzing the PKI from multi-perspectives. Lopez et al. reviewed the technical, economic, legal, and social reasons for PKI failure and concluded the main reason is economic (Lopez et al., 2005). As PKI is related to the legal issue, some analyses were made based on its legal characteristic: Winn examined the role of law reform relates to PKI (Winn, 2006).

Unlike the global concerns on the legal and economic aspects of PKI, many of the literature which discuss Korean PKI argue technological problems of Korean national PKI (NPKI). It is because Korea is the only country where nation-wide PKI deployment was made, and the technological and operational problems of PKI can be found. Park argued the web accessibility problem due to the use of ActiveX in NPKI (Park, 2012). Choi makes recommendations for Korean NPKI use on smartphones (Choi, 2014). Lee argues the Korean NPKI's significant problems are accessibility and incompatibility issues which derived from its own standard (Lee, 2013).

## Ⅲ. Different PKI policy approaches of the US and Korea

In the 1990s, the Internet grew at explosive rates, and there was an idea that governments needed to establish legal and regulatory frameworks and support technological development including authentication to foster the required trust and security in the open networks (OECD, 2001). Moreover, it was believed that if the digital signature of PKI were given the legal force identical to a handwritten signature, it would address many questions in conducting online businesses (American Bar Association, 1996). Therefore, many countries prepared their own policies related to electronic authentication policies utilizing the PKI and digital signature. The US and the Korean policy approaches followed different paths. The U.S. left the market work, and Korea adopted strong regulatory approach by standardizing its national technology and mandating the use of the standard in online transactions.

<Table 4> PKI related issues at the International level, the US, and Korea from 1995 to 2005

| Region | 1995 ~ 1998 | 1999 ~ 2001 | 2002 ~ 2004 |
|---|---|---|---|
| International | 1995 PKIX Working Group established in IETF<br>1996 Model Law on Electronic Commerce | 1999 The year of PKI by InfoWorld<br>2001 Model Law in electronic signature | |
| U.S. | 1995 Utar Digital Signature Act | 2000 Electronic Signatures in Global and National Commerce Act | 2002 Government Accountability Office reported cost problem using PKI in the government<br>2003 E-Authentication Guidance for Federal Agencies |
| Korea | 1998 Draft bill of Digital Signature Act, Standard technology development | 1999 Digital Signature Act<br>1999 Established National PKI (NPKI)<br>- distribution via the Internet<br>- store the private key on users' hard disk drives<br>2000 The government issued software certificate for online banking<br>2001 Law revision enabling NPKI to use for personal identification | 2002 Mandated NPKI in online banking<br>2002 Certificate interoperability<br>2003 Mandated NPKI in online stock exchange<br>2003 Placed a ban on the use of private certificate for Internet banking<br>2004 Mandated NPKI in credit-card payment |

## 1. The U.S. policy approach: Laissez-faire policy

The first legal recognition of digital signature was made in the state of Utah, and several other states including Washington, Alabama, Colorado, Maine, Hawaii, California, Nevada, and Missouri followed. Moreover, some states including Georgia, West Virginia, Iowa, New Hampshire, Wisconsin, Kansas, Alaska, South Dakota, Minnesota, Nebraska, Kentucky, Oregon, and Illinois have decided to embrace digital signature as an authentication method (Lui-Kwan, 1999). The legislation of these states seemed to accelerate the PKI use in Electronic Commerce (e-commerce). However, disagreements over when digital signature should be enforced existed; a uniform framework for the digital signature was crucial. However, a significant event related to encryption technology called Crypto Wars occurred, and it affected the U.S. government's policy approach. The beginning of the Crypto War was the White House's introduction of the "Clipper Chip" in 1993. Clipper Chip was a microchip developed by National Security Agency (NSA) which provides the public with strong cryptographic tools to encrypt their communications. Moreover, it also provides government agencies with accesses for the unencrypted version of those communications. The technology was based on “key escrow” system, in which a copy of each chip’s unique encryption key would be stored by the government. Key escrow uses Diffie-Hellman key exchange-algorithm which is the foundation of PKI to distribute the crypto keys. In 1994, a flaw in the system was discovered and the chip was not embraced by consumers or manufacturers. As a consequence, the chip itself was no longer relevant. After the Clipper Chip initiative failed, the U.S. government proposed PKI include an escrowing of private key called “software key escrow” to preserve access to communications and storage applications, but the government’s trial proved unsuccessful due to the privacy, security, and economic concerns. By 1997, there were abundant pieces of evidence against any key escrow schemes (Kehl et al., 2015). After the resolution of Crypto War, with the rise of de facto standard SSL(Secure Socket Layer), companies like VeriSign and Comodo started to manage public key infrastructure, issuing digital certificates providing independent verification of the servers to consumers. This PKI usage was slightly different from the expected use of PKI in the 1990s. The old PKI proponents believed the resolution of the legal issue over digital signature was a critical obstacle to be addressed by the governments. However, the industry and market players started to their own PKI businesses without any resolution of the legal status of digital signature. Since then, the U.S. government has not intervened in the market. There were public policies related to electronic authentications, but it preserved technology neutrality even in the public area. For example, E-Authentication Guidance for Federal Agencies is applicable for remote authentication of human users of federal agency IT systems, but it does not identify which technologies should be implemented.

## 2. The Korean policy approach: regulatory policy

In the late 1990s, the Korean e-commerce industry was at its nascent stage, and it was one of the emerging markets that had a potential for rapid growth. However, technological gaps existed during the emergence of e-commerce in Korea. For the security reasons, strong encryption technology on web browsers was needed, but web browsers with 128-bit encryption technologies were not available outside the US due to the executive order for Export Controls on Encryption

Products (Clinton, 1996). In 1999, the Korean government developed a 128-bit block cipher named SEED and developed the National PKI (NPKI) by combining SEED and digital certificate based on Public Key Infrastructure (PKI) technology. The NPKI bridged the technological gap due to the low-security level of web browsers and provided an electronic authentication function. However, in the following year, the US government allowed the export and re-export of any encryption commodity or software (Department of Commerce, 2000) and countries worldwide, excluding terrorist supporting states, started to utilize the 128 bit SSL (Secured Socket Layer, which is now Transport Layer Security) protocol. In 2002 and 2003, the use of the NPKI was mandated in online banking and online stock trading respectively. Moreover, the NPKI is also used in credit card payment and in e-government. Therefore, more than 90% of the economically active population in Korea had no choice but to use the NPKI for the electronic authentication method (Park, 2010).

The Korean government seemed to have developed viable technology for electronic authentication and promoted it effectively. Moreover, it is obvious that the Korean government also understood the global nature of e-commerce: it included an article for reciprocal recognition of digital signatures (Article 27) between the governments.

## 3. The reason for Korean regulatory policy: The Korean National Systems of Innovation

According to Freeman, R&D is conducted by three different actors: government research centers, company laboratories, and university laboratories (Freeman, 1982). Among the actors, in the Korean NSI, the government research institutes and company laboratories are closely linked, and the government played essential roles in its technology innovation processes. Historically, after the Korean war ended in 1953, Korea’s economic growth started by state-led macroeconomic planning which is often referred as a developmental state (Johnson, 1982). Under this governance model, the Korean government had strong political power and control over the economy, and actively intervened in the market with extensive regulations. As Korea’s major industries shifted from heavy industry to electronics and ICT, the Korean government also started to intervene in the national innovation by establishing close Public Private Partnership (PPP). The development of digital electronic switching system (TDX) in 1982 is a well-known example of the Korean NSI. During the development of TDX, the government research institute and the Korean electronics companies cooperated, and the developed technologies were trasnferred to the companies for commercialization. TDX was the first huge success of the Korean PPP in ICT area followed by CDMA (Code Division Multiple Access), and this characterized the Korean NSI. Since the 1990s, the primary R&D focus of Korean NSI has been "expansion of public R&D (in the 1990s)" and "development of growth engine technologies (2000~2010)" (Oh, 2012). Moreover, the R&D expenditure for public R&D increased for 18 consecutive years as seen in the table below. This shows the Korean government tried to support its national innovation process proactively and wanted to utilize the results for its national economic growth.

<Table 5> Government R&D Budget (Statistics Korea, 2016)

(unit: trillion Korean won)

| | 1998 | 1999 | 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Expenditure | 3.3 | 3.7 | 4.2 | 5.7 | 6.1 | 6.5 | 7.1 | 7.8 | 8.9 | 9.8 | 11.1 | 12.3 | 13.7 | 14.9 | 16.0 | 16.9 | 17.8 | 18.9 |
| Growth rate,% | - | 11.6 | 13.2 | 36.6 | 7.1 | 6.6 | 9.2 | 9.9 | 14.1 | 10.1 | 13.3 | 10.8 | 11.4 | 8.7 | 7.6 | 5.3 | 5.3 | 6.4 |

Under the Korean NSI, it seemed to be appropriate for the government to intervene in the electronic authentication industry. The Korean government intervened in the technology planning, R&D, and commercialization of its NPKI. This uniqueness of NPKI policy later merged with its path dependence left a substantial impact on Korean society not only technological, but also economic and social.

## Ⅳ. The results of PKI policy approaches of the US and Korea

Since the late 2000s, the public interest of PKI sharply dropped. PKI was not widely used on the Internet as an electronic authentication method, but only used in closed networks or server authentication in SSL/TLS. In 2013, PKIX, the working group for PKI in IETF concluded, and it seems that the standardization processes for PKI are mostly finished. There would be little room for further technological innovation, and little possibility of its use in the electronic authentication process for identifying the users.

<Table 6> PKI related issues at the international level, the US, and Korea since 2006

| Region | 2005 ~ 2009 | 2010 ~ 2013 | 2014 ~ 2017 |
|---|---|---|---|
| International | | 2013 PKIX the working group in IETF concluded | |
| U.S. | | 2011 Electronic Authentication Guideline. NIST Special Publication (800-63-1)<br>2013 Electronic Authentication Guideline. special publication (800-63-2) | 2017 Digital Identity Guidelines. NIST Special Publication (800-63-3) |
| Korea | 2005 First Internet banking hacking incident | 2010 Trial of law revisions to increase the web browser compatibility failed<br>2013 Trial of law revision to remove mandatory use of NPKI failed | 2014 Presidential recommendation to remove ActiveX to encourage foreigners' purchase on the Korean online marketplace<br>2015 Policy Reform |

## 1. The result of the US policy: incremental innovation under the Internet governance

The resolution of Crypto War was not only about policy responses to new technology but simultaneously an experiment of a new governing system. It was a coordinated effort among industry groups, privacy advocates, and technology experts to make a shift from old governance to the new Internet governance. Until now, U.S. has maintained its free-market policy in electronic authentication industry. However, as the importance of electronic authentication grows the U.S. government started to give basic directions to the market by detailing its guidelines and adjusting the factors for Multi-Factor Authentication (MFA). In the US, most widely used electronic authentication method is passwords. There have been concerns about the use of passwords as an electronic authentication method in important information transactions because 62% of data breaches resulted from passwords even in 2016 (Verizon, 2016). However, the global market trend still adopts password and other innovations like fraud detection/ prevention services are improving the securities. The market does not show abrupt change as it needs a consensus among the multi-stakeholders under the Internet governance. The U.S. government's policy approach has been following this trend, and the U.S electronic authentication industry is making incremental innovations in line with the global market trend.

## 2. The result of the Korean policy: nation-wide problems posed by NPKI use

On the contrary, Korean had experienced several negative impacts on society made by its electronic authentication policies. As described above, the Korean government standardized NPKI and mandated its use in online transactions and e-government services. The government's standardization required the unavoidable use of plugin applications. The mandatory use of a specific technology and plugins posed several problems: such as falling behind in using the latest online security technologies and remaining locked in the Internet Explorer (IE) monoculture of Korea. The policy mandates tend to have multiple adverse impacts on Innovation, Security, and Internet Environment:

### 1) Problem 1: Policy mandate negatively impacted innovation

Because of the policy mandate, Korea's online security industry lags. The financial services companies only followed the guidelines set by the Korean government. Where there is a government mandated technology, there is no incentive for companies to develop new technologies or make investments. This negatively impacted innovation. The problem is evident from the financial services companies' lack of investment in online security.

### 2) Problem 2: Policy mandate created vulnerabilities

The security level of citizens' Personal Computers (PCs) weakened due to the policy mandate. There were about 100 million personal information leakage cases in Korea between 2008 and 2013 (Yoon, 2013). PCs in Korea have about 400 to 700 plugin applications (National Cyber Security Center; National Security Research Institute, 2008). Malicious plugins can easily pass thru without notice, which led to hackers worldwide using PCs in Korea to hack other countries (Mundy, 2014). Numerous personal computers still have many plugin applications installed; so, there is a high probability of similar incidents occurring in the near future.

### 3) Problem 3: Policy mandate distorted the Internet environment

Due to the monopoly of IE in the late 1990s and the early 2000s and ActiveX, a plugin application compatible only with IE, Korea continued to show a very high usage rate (87.64%) of IE (Baek, 2015) compared to the world average of 13.3% in 2015 (Statcounter.com, 2015)

This monoculture limited the user experience and discouraged software developers from developing software or websites based on other web browsers. This again decreased the diversity of Internet services and weakened the software industry's competitiveness in the world market (Kim, 2009). During the presidential election in 2012, the presidential candidate Park Geunhye and the Saenuri Party stated in the book of public commitment that various authentication services compatible with global standards would be allowed (Saenuri Party, 2012). After she was elected, the mandatory use of the Authorized Certificate was abolished in 2015. Since the first online banking hacking incident in 2005, the need for the electronic authentication policy change had been continuously rising, which means the problems related to electronic authentication policy has been an important issue all along. But this policy change took over a decade to implement is because this is not only a technological but also a political, economic and social issue.

However, although the mandate abolished in 2015, citizens still need the Korean NPKI for electronic financial transactions and electronic government services to this date. Even the number of issuances for the Korean NPKI increased in both 2015 and 2016. Moon Jae-in, the new president elected in 2017, mentioned that he would remove the Korean NPKI; the electronic authentication problem in Korea is still ongoing.

## 3. The barrier to policy reform of Korea: path dependence

Even though there have been several problems posed by its electronic authentication policy, the Korean government did not change its policy until 2015. This research finds the reasons by applying path dependence theory on Korean NPKI policies. Below shows a Korean NPKI model of path dependence based on basic economic model of path dependence by Simmie (Simmie, 2012)

<Table 7> The Korean NPKI model of path dependence

| Initial Conditions | Path Creation Process | Path establishment process | Path dependence outcome | Following innovation process |
|---|---|---|---|---|
| Korea as a Developmental state | Success cases of TDX, CDMA development under Korea's National System of Innovation | NPKI mandates in online banking, credit card payment, online stock exchange, and e-government<br>Other follow up measures to encourage NPKI use<br>Even the first online banking hacking revealed NPKI's weakness, the NPKI policy reinforced by mandating more complex passwords | Problems in Korea's online environment: Low investment in online security, Increased vulnerability, and IE monoculture | Block chain use in banks for the first time in the world. |
| | | | Path dissolution<br>Policy reform in 2015 by accumulated political, economic, social and technological needs for policy changes | |

The Korean NPKI policy is in the extension of its developmental state and national systems of innovation. The Korean government, public institutions, and private companies operate NPKI for the use of it in online transactions. As discussed before, this kind of government-led R&D is a typical approach of the Korean government under its national systems of innovation. Once the NPKI was developed, the Korean government made two choices: the first one is the NPKI's distribution via the Internet using plugin application (ActiveX) and the second one is allowing users to store their certificates on the unprotected medium such as hard disk drive and Universal Serial Bus (USB) memories. Those two choices substantially lowered NKPI deployment cost. However, the former cause Microsoft monoculture in Korea and the latter exposed the users for hacking. After the technology development and deployment, the Korean government set the goal of 10 million NPKI users which was approximately 1/5 of the total population by the end of 2002. However, the number of NPKI users was not reached such a huge number, and the Korean government introduced follow-up measures. Law revision, usage mandates in several online transactions, certificate's inter-operability mandate, and ban of private certificate use are the examples. In addition to these regulatory approaches, Ministry of Information and Communication introduced an information security plan which contains pilot projects for widespread use of NPKI. During this period of time, Korea's NPKI policy path was established and imprinted in its national electronic authentication systems. In addition to the policy path, network effect, positive feedback, and technological lock-in of NPKI have established over a decade. Then, the NPKI policy path combined with NPKI's technological lock-in effect developed strong path dependence. Consequently, this path dependence worked as a barrier to policy reform, and the policy reform took over a decade since there have been several problems since the early 2000s.

## Ⅴ. The reason for Korean policy reform: failure to resonate with the evolving global trends

In the path dependence theory, a critical juncture can initiate policy change. There are several reasons for the Korean policy change, but one critical juncture for policy reform was made by web browser companies' end of plugin application supports. PKI was not widely used for online user authentication worldwide, and web browsers do not carry this function. Therefore, to enable user authentication process, plugin applications should be installed on user's PC. However, as the hacking technics advances, the vulnerability caused by plugin applications grew. Since 2006, security vulnerability issues related to ActiveX plugin use began to arise, and even the Microsoft (MS) started to discourage the ActiveX use. However, MS had to support ActiveX for backward compatibility of its previous IEs. Critical juncture was started by Google which is a developer of Chrome web browser. In 2013, Google announced that Netscape Plug-in Application Programming Interface (NPAPI) support would be completely removed from Chrome before the end of 2014 (Chromium 2013). In 2015, MS finally announced its next generation web browser Edge, which does not support ActiveX anymore. For NPKI, this was a critical issue for its use because NPKI cannot operate without ActiveX or NPAPI on PCs. Before its end of plugin support, MS and Google warned several times for their ends of plugin support.

The MS's failure in smartphones' Operating System (OS) was another critical factor for the critical juncture. Since the introduction of iPhone in 2008, Apple's iOS, Google's Android, and

MS's Window Mobile have competed in the smartphones' OS market. These three tech-giants competed each other in the smartphones' OS market, but simultaneously they competed in the web browser market. As described before, most of Korean NPKI operated only on Internet Explorer, but Internet Explorer was not available in the iOS and Android. As the MS failed to penetrate the smartphone market, the Korean NPKI could not be used on smartphones. The service providers which utilize Korean NPKI had to develop and operate its own mobile application. Additional application means additional costs for the service providers. The users also had to install additional applications for each service provider on their smartphones. This is an inconvenient experience for the users, and made the NPKI's standard incompatibility issues recognized by citizens.

The critical juncture which broke the strong path dependence of Korean NPKI and invited policy reform shows the importance of multi-stakeholder process under the Internet governance. Internet technology companies and Standard Developing Organizations (SDOs) are important actors in the multi-stakeholder process, and it is essential for a government to participate in the process if a country plans to initiate any Internet related standards. However, the Korean government established its NPKI system and focused only on its operation within the nation. Electronic authentication technology is inherently global because its core usage, e-commerce is inherently transborder. The Korean government did not closely look at the global trend surrounding the technological trajectory of web browsers and online security trends. Consequently, the Korean government's disconnected choice from other stakeholders in the Internet governance made its abrupt policy reform and left substantial disadvantages to Korea.

# Ⅵ. Conclusion

In the early 2000s, the U.S lagged Korea in electronic authentication technologies as Korea established nationwide infrastructure for advanced authentication technology for the first time in the world. The Korean PKI's infancy was primarily fostered by government, and it seemed to be an appropriate approach for its national innovation. However, the global electronic authentication technology development encountered a rise of Internet governance based on a consensus among multi-stakeholders. Under the new Internet governance, a government cannot manage even its domestic industries without keeping in line with global trends. The Korean government overweighted the benefit of PKI and poured continuous efforts to utilize the technology believing the country could lead the global market. These significant investments based on regulatory policy formed a policy path and lock its domestic electronic authentication industry in the PKI. On the contrary, the multi-stakeholders' consensus drove the global PKI usages to a different use of applications from what the Korean government expected. Then, the Korean government could have chosen to integrate this technological change into their policies, but the government decided to take a different path from the rest of the world due to the path dependence it created. Under the Internet governance, a government's policy should resonate with or utilize other stakeholders including SDOs and international organizations. Government-led innovation which achieved huge successes in the Korean history is not effective anymore under the new governance. Policy-makers should understand that government's role is not leading a certain technological or industrial development, but an efficient distribution of the national resources closely observing the global trends as one of the participants in the whole governance.

## Ⅶ. Limitations

This paper is based on historical case studies and empirical analyses. Additional reasoning based on both qualitative and quantitative analyses may make this paper more concrete and reliable one. For example, hierarchical clustering may show whether the Korean security industry is in the different status from other technologically advanced countries. Moreover, additional explanations of technological lock-in caused by mandatory use of Korean NPKI and its interactions with policy path may help explain the unique characteristics of Korean NPKI path dependence model better.

# References

American Bar Association, *Digital Signature Guidelines*, 1996

Baek, Bongsam., *Korean Internet Environment, 'PC=MS'·'Mobile=Google'.* Retrieved September 10, 2015.

Burr, William E., Dodson, Donna F., Newton, Elaine M., Perlner, Ray A., Polk, W. Timothy., Gupta, Sarbari, & Nabbus, Emad. A., *Electronic Authentication Guideline*. National Institute of Standards and Technology, 2011.

Cerna, Lucie, *The Nature of Policy Change and Implementation: A Review of Different Theoretical Approaches*, Organization for Economic Co-operation and Development, 2013.

Clinton, J. William., Administration of Export Controls on Encryption Products. *Executive Order,* 13026, 1996.

Chromium Blog (2013) *Saying Goodbye to Our Old Friend NPAPI*, Retrived from https://blog.chromium.org/2013/09/saying-goodbye-to-our-old-friend-npapi.html

Danielle, Kehl, Wilson, Andi, & Bankston, Kevin. (2015). *Doomed To Repeat History?* Retrieved from https://static.newamerica.org/attachments/3407-125/Lessons From the Crypto Wars of the 1990s.882d6156dc194187a5fa51b14d55234f.pdf

Department of Commerce. (2000, January 10). *Revised U.S. Encryption Export Control Regulations.*

Grassi, Paul A., Garcia, Michael. E., & Fenton, James. L., *NIST 800-63-3: Digital Identity Guidelines*. National Institute of Standards and Technology, 2017.

International Telecoms Union Telecommunication Standardization Sector. (1997). *International TeleX 509 : Information technology-Open Systems Interconnection-The Directory: Public-key and at tribute certificate frameworks* Retreved from: https://www.itu.int/rec/T-REC-X.509

Johnson, Chalmers., *MITI and the Japanese miracle: the growth of industrial policy, 1925-1975*, Stanford University Press, 1982.

Kim, Tong-hyung. (2009, September 23). *Korea Paying Price for Microsoft Monoculture*. Retrieved from the Korean Times,: http://www.koreatimes.co.kr/www/news/biz/2010/05/123_52401.html

Lee, Junghyun, The usage and problem of the authorized certificate in smart environment, *Internet & Security Focus,* Korea Internet Security Agency, 2013.

Lee, Soo Hee, & Yoo, Taeyoung, "Government Policy and Trajectories of Radical Innovation in

Dirigiste States: A Comparative Analysis of National Innovation Systems in France and Korea", *Technology Analysis and Strategic Management,* Vol. 19, No. 4, 2007, pp. 451-470.

Lopez, Javier, Oppliger, Rolf, & Pernul, Günther, "Why have public key infrastructures failed so far?" *Internet Research,* Vol. 15, No. 5, 2005, pp.544-556.

Lui-Kwan, M. Kalama, "Recent Developments in Digital Signature Legislation and Electronic Commerce", *Berkeley Technology Law Journal,* Vol. 14, Iss. 1, 1999.

Mundy, Simon. (2014, June). *South Korea suffers poor cyber security controls.* Retrieved from https://www.ft.com/content/7ae2b288-e29a-11e3-a829-00144feabdc0

Muller, Milton, *Rulling the root: Internet governance and the taming of cyberspace,* The MIT Press, Cambridge, Massachusets London, England, 2002.

National Cyber Security Center; National Security Research Institute, *ActiveX Control Development Security Guideline,* 2008.

Organization for Economic Co-operation and Development, *National Innovation System,* 1997.

Organization for Economic Co-operation and Development, Electronic Commerce. *Policy Brief,* 2001.

Oh, Se-Jung, *Networking between Academia, Public Research Institutes and Industry-Korean Experiences* [PowerPoint slides], 2012.

Park, Hun Myoung, "The Web Accessibility Crisis of the Korea's Electronic Government: Fatal Consequences of the Digital Signature Law and Public Key Certificate", *45th Hawaii International Conference on System Sciences,* 2012.

Park, Jihyun, *Major issues and status on deregulation of the Authorized Certificate mandate in online transactions.* Korea Financial Telecommunications & Clearings Institute. Korea Financial Telecommunications & Clearings Institute, 2010.

Park, Mun Su, "An Exploratory Study for Convergence-type Technology Transfer", *International Commerce and Information Review,* Vol. 17 No. 1, 2015, pp.165-191.

Park, Mun Su, & Lee, Ho-hyung, "A Study of Technical Support Policy for Innovative SMEs", *International Commerce and Information Review,* 14(1), 2012, pp.197-218.

Saenuri Party, *Public commitment of Saenuri party for 18th presidential election,* 2012.

Simmie, James, "Path Dependence and New Technological Path Creation in the Danish Wind Power Industry", *European Planning Studies,* Vol. 20, No. 5, 2012.

Son, Yeol, “Technolgy, Institutions, Path Dependence: A compartive Study of Venture Nurturing Policies in Korea and Japan”, *Korean Political Science Review,* Vol. 40, No. 3, 2006, pp.237-261.

Statcounter.com. (2015). *StatCounter Global Stats - Browser Market Share.* Retrieved from Statcounter.: http://gs.statcounter.com/browser-market-share#monthly- 201501-201501-map

Statistics Korea. (2016). *The government Research and Development Budget,* Retrieved from http://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=1330

United Nations Commission on International Trade Law, *Model Law on Electronic Commerce with Guide to Enactment,* 1996.

United States General Accounting Office, *Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology,* 2001.

Verizon, *2016 Data Breach Investigations Report.* Verizon

Yoon, Min-sik. (2013, July). Korea grapples with massive personal data theft, regulatory mess. Ret rieved from *The Korea Harald*: http://www.koreaherald.com/view.php?ud=20130719000708

Winn, Jane K., *US and EU Regulatory Competition and Authentication Standards in Electronic Commerce,* 2006.

## 국문초록

# 디지털 혁신시대의 정부역할: 한국의 전자 인증정책 사례

손원배* · 박문수**

신기술의 혁신과정은 매우 역동적이어서 정부는 빠른 기술발전, 대중의 필요 및 변화하는 글로벌 트렌드에 맞춰 주기적인 정책 검토를 할 필요가 있다. 1990년대 인터넷은 폭발적인 성장을 하였지만 다양한 응용프로그램들의 활용이 보안 문제로 인해 제한되었고, 공개 키 기반구조 (PKI)는 이러한 문제들을 해결할 수 있는 근본적인 기술로 인식되었다. 2017년 현재에도 PKI는 개방형 네트워크에서의 전자인증에 있어 최고 기술의 하나이지만 그 사용처는 폐쇄 네트워크 내에서의 사용자 확인 및 SSL/TLS와 같은 네트워크 보안 인프라 내에서의 서버 인증과 같이 한정된 부문에 한한다. PKI에 대한 기대와 현실의 차이는 2000년대 초반 인터넷 거버넌스 하에서의 새로운 인증정책의 글로벌한 도입과 함께한 인터넷의 진화에 기인한다. 새로운 인터넷 거버넌스는 다수 이해관계자간의 협력에 기반하고, 이는 기술정책과 관련한 정부의 행동방식에 변화를 가져왔다. 이 연구는 미국과 한국의 PKI 정책을 경로의존성 이론 (Path Dependence Theory)의 관점에서 분석한다. 두 국가의 다른 정책 결과는 인터넷 거버넌스의 부상을 증명하고, 또한 현재의 글로벌 인터넷 사회의 정책결정자들에게 중요한 함의를 줄 수 있을 것이다.

주제어 : 공공 정책, 전자 인증, PKI, 경로의존성, 거버넌스

* 한국 뉴욕 주립대학교 박사과정, 주저자

** 한국 뉴욕 주립대학교 전임연구교수, 교신저자