Volume: 4, Issue: 1
Page: 173-184
2020

ISSN 2520-4750 (Online) & ISSN 2521-3040 (Print)

International Journal of Science and Business

# A Case of A Government-Mandated Online Transaction Standard Acting As A Technical Barrier To Trade in South Korea

Nigel Callinan

## Abstract

Technical Barriers to Trade can form formidable hurdles for Organizations seeking to sell products and provide services to specific countries. These barriers are frequently erected based on government-mandated standards. This paper discusses the use of Online Transaction Standards in South Korea and explores the effect the Standards had on competition and diversity when it came to the availability of service providers for the country's domestic market. The paper concludes that a small number of companies benefitted from the unique business ecosystem set up within an effectively closed market and this reliance on this ecosystem may have been a problem for Korean companies when trying to expand overseas.

**IJSB**
Accepted 21 January 2020
Published 30 January 2020
DOI: 10.5281/zenodo.3631315

**Keywords**: Internet, Security, Encryption, Trade, Barrier, Technology, Korea.

About Author (s)

**Nigel Callinan,** Assistant Professor, Department of Global Business, Hannam University, South Korea.

Published By
IJSAB International

## 1. Introduction:

The volume of information, goods and services exchanged on the Internet has grown and diversified in recent decades. For example, consumers now buy a wide variety of goods using e-Commerce channels, citizens interact with e-Government websites to complete bureaucratic processes and people communicate through online social networks. However, as these transitions have taken place so quickly, security, safety and legal systems have ended up constantly playing catch up with the pace of technology change. This has resulted in the emergence and exploitation of regulations loopholes and challenges when it comes to developing adequate security solutions and standards. Sometimes, criminal groups try to identify weak points in the electronic transfer of information as a way to compromise data either for sale or for use in fraudulent transactions.

One way to try and mitigate the risks associated with online activity is though the use of Public Key Infrastructure (PKI) systems. PKI systems can be put in place to try and minimize the risks associated with data transfer on the Internet. PKI systems can either be mandated by Government regulations or implemented through industry standards and best practice. In this paper, we will explore the implementation and evolution of Government-Controlled PKI Systems in South Korea. This is an interesting instance of PKI development because Korea decided to diverge from global standards and create a standalone online security system.

When Korea was trying to increase its economic activity in the 1960s and 70s, Trade Barriers and Protectionist measures were put in place to protect and incubate domestic businesses against international competition. In some sectors this was a highly successful strategy and in others it cut Korea off from internationalization. Many of those barriers have recently been removed for certain markets as a part of Free Trade Agreements (FTAs). However, a growing trend in International Business is the use of Technical Barriers to Trade (TBT) as a more flexible substitute for traditional forms of trade protectionism (Yu, 2000). The study of the use of TBTs as substitutes for tariffs as a protectionist business strategy is an active and important research area.

## 2. Research Question

The aim of this paper is to explore how the Government-Controlled PKI systems created a TBT in South Korea either by accident or by design. Also, we will outline how this could cause problems in the future for businesses seeking to export their services or products.

## 3. Methodology

This research uses a qualitative narrative research synthesis approach. This involves organizing all of the sources into a timeline to trace the evolution of a story. This method is suitable for case-style research that has a natural beginning, middle and end with events happening at certain dates. It allows all the events to be tied together so the overall impact and context of a phenomenon can be explored. In this case, the development of the KPI business area in Korea will be explored and each of the stages can be traced to try and determine the key decision points and what significance each had. Each decision is a reaction to the previous set of possibilities and results, so the linear narrative research approach allows the events to be tied together for a deeper understanding while giving an overall context to the proceedings. Sometimes if a phenomenon is studied in isolation it may not seen like a logical step but, if it is studied in the context of the linear series of interrelated events, it may be more understandable and even rational. This can reduce the risk of making reductionist conclusions about how conditions arise and how problems emerge. It may be that things started off with good intentions but ended up with undesirable results. There are a lot of things that can be learned from studying these kinds of cases in depth. It can be the first step towards making sure that history does not repeat itself if the outcome was undesirable.

## 4. Literature Review

### 4.1 Seed creation

According to the International Guide to Combatting Cybercrime (Yoo, 2007), developing countries frequently assume digital or electronic signature laws require Government Mandated PKI encryption technologies along with Certification Authorities (CAs). The book continues by asserting that these legal frameworks provide a barrier that will deter foreign investment. Moreover, the author outlines how the UN, EU and U.S digital signature laws require technology neutrality, so countries that mandate locally developed PKI authentication schemes may not be aligned with most industrialized nations and global standards. In order to provide the infrastructure needed for electronic information to be exchanged safely, the Korean Government became heavily involved in the creation and management of Online Transaction Security Standards in the latter part of the 20th century. The South Korean Government and banks first started working together on Internet Security standards in 1998 (Kim and Cho, 2012). At that time, the most common form of cryptographic security system used to protect data around the world was called Security Socket Layer (SSL). However, during 1998, the 128-bit SSL protocol was still a work in progress. It was not finished and approved until January 1999 when the Internet Engineering Task Force (IETF) signed it off for use (Hankyoreh, 2010). The IETF is an International Standards Body that specializes in TCP / IP security.

This left the South Korean banks in a difficult situation because Korean National Legislation at the time would not allow the use of 40-bit encryption for online transactions. The scenario was further complicated because the U.S blocked the export of 128-bit encryption technologies until December 1999 due to National Security concerns (Chang, 2003). In order to circumnavigate the delays, the Korean Government instead funded a project by the Korean Information Security Agency (KISA) to create their own encryption standard using a block cipher approach. They named their resulting security algorithm SEED (KISA, 2009). In order to run SEED, users had to download a browser plugin. These plugins were bundled with a certificate issued by a Korean Government Certificate Authority. According to the Electronic Signature Law of Korea, only Financial Services Commission (FSC) accredited Certificate Authorities were allowed to provide user software for certificate handling (Microsoft, 2003). The user software needed to meet several regulations and technical conditions to achieve accreditation. The logic behind this system was that the Korean Government wanted to ensure approved user certificates were only handled by approved web browser certificate management and form-signing modules. The certificate issuing authority branched off into their own Government-controlled arm known as the Korea Financial Telecommunications and Clearings Institute (KFTC). This meant that only certain Internet browsers would be able to process electronic transactions (Kang et al, 2010). The rules were designed in the hope that the SEED encryption technique could eventually be something that South Korean firms could export and sell internationally as an alternative to the systems controlled and distributed by the U.S.

When SEED was launched, the main Internet browsers used in Korea for online transactions were Microsoft's Internet Explorer and Netscape (Globalsign, 2015). Internet Explorer plugins used Active-X technology whereas Netscape required an NSplugin. Therefore, most of the accredited Certificate Authorities in Korea decided to provide the user software for these two browsers only. In the early 2000s, Netscape use gradually dwindled and then disappeared, both in Korea and internationally, so that left Active-X for Internet Explorer as the sole standard for domestic Korean companies. Another development that happened during this time was that the security techniques used by the financial websites started to spread throughout the Korean website world. It also created a business opportunity for companies in Korea as they could exclusively provide the programs needed to support the system. As can be seen below in Table 1, the Korean Government accredited five Certification Authorities. All of the companies were domestic for profit Korean companies (KISA, 2012).

| | Accredited CA | Accredited Date |
|---|---|---|
| 1 | Signgate | 10th February 2000 |
| 2 | SignKorea | 10th February 2000 |
| 3 | Yessign | 12th April 2000 |
| 4 | Crosscert | 24th November 2001 |
| 5 | Tradesign | 11th March 2002 |

**Table 1: List of Accredited Certification Authorities (Source: KISA, 2009)**

These Korean companies emerged in this niche area (Kim, 2010). One big bonus for these companies is that they could bundle their anti-virus or even third party programs with the security installations to drive revenue growth. It quickly became a lucrative market. For example, the installation of keyboard security programs to prevent against keystroke logging and other security programs became a mandatory step or else the systems could not be used (Ramstad, 2012).

Initially, this monopoly on Korean Internet browsing was a good business situation for Microsoft and they supported the system. In November 2003, Microsoft signed an MOU with KISA and on November 22nd 2004, both organizations marked a year of cooperation with a promise to persevere with their attempts to improve the computer security and data protection ecosystem in Korea (Lee at al, 2005). One serious ICT downside to being entirely reliant on one system is when that security wall is breached. This became apparent on 25th January 2003, when almost the entire Korean Internet environment, including banking and stock market systems, became completely paralysed for 9 hours in the wake of a worldwide virus that exploited certain Windows security loopholes (Kim at al, 2011). Other countries were also affected, but as the market share of Microsoft Windows for client PC's in Korea was 99.4% at the time, it temporarily brought the Internet in the country to a virtual technical standstill.

### 4.2 Opposition by the Open Web Group

The security problem prompted the new South Korean President at the time to pledge to diversify the computer ecosystem in the country by encouraging the use of Linux as an alternative operating system. Seven months after President Roh took office, he announced that by 2007, 20% of client PC's and 30% of servers in Korea would be Linux-based (MOLEG, 2013). However, this project met with limited success and the status quo continued. The Korean government also introduced statutes to encourage the use of neutral ICT infrastructure. The modified Electronic Signature Act required official certificate authorities to offer certification solutions for Linux and Mac users in addition to Windows users. It also imposed a legal obligation on the Government to ensure that e-commerce systems were inter-operable. This statute stipulated that the Korean Government must establish and implement platform-neutral Technology Standards for e-commerce. However despite these statutes, the Korean Government continued to grant licenses to Certification Authorities who did not service Linux or Mac users. Therefore, the vast majority of Korean websites, including 100% of Governmental websites, continued to rely on Active-X controls as of 2012 (Ramstad, 2012).

Some banks in Korea did try to branch out beyond Windows. In 2005, Shinhan Bank provided the EzPlus 2.0 for Apple systems, to enable Internet banking services for Mac OS users. Also, Nonghyup bank began to provide Internet banking services for Linux users in 2006. This was made possible by installing Active-X emulation middleware onto Linux PCs in order to access the banking website (Kim, 2010). However, these initiatives were only used by a tiny minority of users and did not influence the majority of consumers. A group of 83 Korean Internet users & academics, known as the Citizens Action Network at Open Web Korea, began a campaign to highlight website accessibility problems when using browsers other than Microsoft's Internet Explorer. Most of the group's members were open source programmers using Mozilla's Firefox or the Opera Internet browser. In late 2006, they decided to take legal action as Microsoft was embroiled in an antitrust case with the Korean Government based on their bundling of Windows Media Player with the Windows OS (Park, 2012). The group was led by Professor Kim Ki-Chang of Korea University, who was a well-known critic of the widespread use of Active-X in Korea. They sued the Korea Financial Telecommunications and Clearings Institute (KFTC) for KRW415,000,000 (approximately US$460,000). Professor Kim's accusation was that the Korean Government legislation on the usage of Active-X plugins for online banking and other public Internet services should be removed, as it was in opposition to fair trade and 'overly favored technology from a single company (i.e, Microsoft)'. Translated details of the accusation are shown below (Openweb, 2006):

1. 'That it is unlawful for a public body to operate browser-specific or OS-specific websites;
2. That the Government's decision to endorse MS optimized websites and web security applications is in violation of its treaty obligation under GATT/WTO as they create trade barriers to web browsers originating in other member countries of WTO, such as Norway; and
3. That, in view of the market condition and the prevalent web page designing practice in Korea, the government has a duty under Art. 3(1) of the Antitrust and Fair Trade Law and under Art. 4.1 of the Agreement on Technical Barriers to Trade (TBT) to adopt and implement appropriate measures to encourage private entities to comply with international standards in Internet engineering'.

The outcome of the case was that the Korean Government was found not guilty. The logic of the judgment was that as most Korean Internet users were already using Internet Explorer anyway, the fact that other browsers were not supported was not considered to have strongly affected Korean users' online experience (Baekdal, 2006). The Openweb group protested the judgment and continued to campaign but they didn't try legal approaches again to date.

### 4.3 Security issues with Active-X

Around this time, aside from its browser compatibility problems, Active-X controls also started to be flagged as a global Internet security problem. The controls became a widespread channel for viruses and malware because Microsoft initially designed Active-X to run by default as opposed to requiring user permission (Ellison and Schneier, 2000). Malicious programs from websites therefore had the ability to automatically install their malware on PCs when a user simply visited a website using Internet Explorer version 6 or 7. When these security problems became widespread, critics of Korea's system stressed that public-key certificates were also not very secure. One risk with this system was that keys were often stored on unprotected memory devices like hard disks or USBs, and that they could be transferred simply by using a copy and paste command from the NPKI folder to any other storage device. Another problem was that the security given by the Active-X plug-in was only temporarily available during that online session and it was effectively useless if the user's computer was compromised earlier (Burkholder, 2002). Usability was yet another complication. In a study by Huh Jun-ho of Oxford University, an Internet user logging on to the webpages of three Korean banks would have to install a minimum of nine Active-X plug-ins to proceed (Kim, 2015). Furthermore, to use more than one computer, a user would need to copy the private key each time and re-install all the plug-ins again and again.

Microsoft decided to address some of their browser security problems when they released their upgraded Operating System, Vista, in 2007. They re-designed Active-X controls to increase safety by requesting a user action before a control can run. This meant that the launch of Windows Vista in 2007 resulted in major disruption for Korea because the Active-X programs required by banks and online retail sites no longer functioned correctly after the upgrade. This prompted three South Korean Governmental ministries; the Ministry of Information and Communication, the Ministry of Government Administration and Home Affairs, and the Financial Supervisory Service to warn domestic users that a Vista upgrade would make it impossible for them to make any secure transactions online (Farrell, 2007). They also lobbied Microsoft to delay the launch of the Vista OS but their request was rejected. Microsoft announced 'We've been testing Vista with banks and other service providers since September, but we encountered more delays than we expected. We plan to release the product as scheduled'. The result was that many Korean companies and users opted not to upgrade and plenty of them still use Windows XP even today. Other large companies wishing to attract Korean users have been forced to try and accommodate the national reliance on Active-X controls. On November 26th, 2008, Google Korea announced that their Chrome Web browser would support Active-X only for the Korean market in order to allow for the use of digital certificate systems (Kang, 2010). This came at a time when Google held a 2% search engine share and a negligible slice of the browser market, so they were trying to find a way to make themselves attractive to Korean consumers.

The fact that almost every Korean website used the same security method meant that hackers had a unified point of attack. According to a study carried out at Cambridge University, close to 90% of Korean data breaches from 2008 to 2009 took place using only one attack method (Hiltgen, 2006). One example of this occurred in summer 2009, when a large Internet attack disabled over 80,000 Korean computers. This attack was blamed on Active-X providing a single channel for cyber criminals to spread malware to carry out Distributed Denial of Service (DDoS) attacks. Korea had issued almost 22 million public-key certificates by the end of 2009 (Kim et al, 2014). From January to August 2009, Korea reported 14 Internet banking security breaches leading the loss of KRW0.23 billion, while the US reported losses of approximately KRW135.2 billion in the 3rd quarter of 2009 alone. The UK had the losses of approximately KRW66.4 billion in the first half of 2009. However, some specialists asserted this could be down to the buffer provided by the Korean language as opposed to the protection offered by the nation's online security standards (Kim, 2010).

It was around this time that mobile devices became widespread in South Korea. Users expected to be able to access Korean websites and carry out transactions using these devices. However, the predominant browsers on these devices did not support Active-X. In February 2010, The Korean Financial Supervisory Service (FSS) introduced new standards for card transactions on smart devices (Kim, 2011). The standards stipulated that inputted card data must be protected using antivirus, anti-malware programs and encryption. Furthermore, the use of accredited certificates when making payments of KRW300,000 (approximately US$260) became mandatory. This caused many problems for online retailers that were targeting smartphone users. For example, the changes meant that the 'Alladin' and 'Yes24' Internet media stores had to stop using their new card payment system that confirmed user details via SMS messages for iPhone customers. Also, Samsung Electronics had an e-book reader for sale that allowed users to download e-book content using a wireless Internet connection but the new regulations meant that the service could not be used. As their e-book reader did not have a fully functional web browser, it was not possible for them to get an accredited certificate for their device. When these guidelines affected the business of high profile Korean companies, a strong lobby movement began. This resulted in a major change in legislation when in mid-2010, the Government opted to officially end mandatory usage of Active-X by introducing a procedure for e-commerce organizations to apply for exceptions. The Korea Communication Commission (KCC) announced they would permit alternative verification methods other than public-key certificates to protect encrypted transactions.

### 4.4 Looking beyond a single operating system

In 2010, Wooribank began to expand its online banking service beyond Internet Explorer on computers when they began to support the Firefox, Chrome, Safari and Opera browsers. However, Wooribank's Mac OS customers still needed to install public-key certificates and keyboard encryption programs on their devices to access their accounts online (KISA, 2012).

In 2011, many computers by Samsung and LG in Korea were still on sale with Microsoft's Internet Explorer 6 and Windows XP as the default option. In 2011, the Korea Communications Commission and the nation's big Internet portals, Naver and Daum, began to encourage South Korean Web developers to stop using Active-X encryption and diversify the browsers they develop their sites for. In Oct 2011, the market share of Internet Explorer fell below 90% in the Korea as the campaign took hold (Kim at al, 2011). Meanwhile, Google Chrome tripled its share within a year to 7.27% of the market, partially attributable to its association with the successful Android Mobile Device Operating System. The figures in Korea were way out of sync with the global picture where Internet Explorer dropped to a 39.35% share as of 2013, nearly halving from 68.91% in August 2008

## 5. Analysis

Globally, the certificate authority business is fragmented due to regional legal framework variations. However, some international standards did emerge based on best practice standards in the industry. The most widely used Internet Browsers set forward criteria needed before websites can be "trusted". The requirements stipulate that CAs should be audited by third party organizations, such as WebTrust or ETSI. Browsers then exclude non-compliant CAs from their root store and provide warnings when users arrive at websites that cannot be trusted. These warnings frequently appear on Korean websites as the Korean Licensed CAs are not classified as being trusted because they did not undergo the audits (Kim. 2015). A report by the Korea Communications Commission (KCC) in 2012 gave a view of Active-X use in Korea. 168 sites of the Korea's 200 major Internet sites, 100 of them private and the other public, used Active X for payment settlements and security at that time. Within the 100 public Internet sites investigated, 82 of them were using an average of 3.7 Active-X applications, while 89 out of 100 private sites used an average of 3.9. On Governmental sites, the Financial Supervisory Service was using seven, followed by Korea Financial Telecommunications & Clearings Institute and Government Employees Pension Service with six each (Park 2012).

In late 2012, the Active-X situation in Korea even managed to become part of a Presidential Election Campaign. Ahn Cheol-Soo, the founder and major shareholder of AhnLab, the largest of the three big online security companies that offered Active-X solutions in Korea, announced his intention to run as an independent candidate for the National Presidential Elections. He stepped down from his post as Dean of the Graduate School of Convergence Science and Technology at Seoul National University in order to run his campaign. He announced that if he was elected, he would change the Governmental regulations that had been the cause of the country's dependence on Active-X and encourage the use of International Standards (Openweb, 2006). However, his Presidential campaign was not successful, so the calls lost some momentum. Moves to reform the regulations continued and in 2014, the Korean Electronic Financial Transactions Act was revised, coming into force in October 2015. The updated provision states that the FSC cannot mandate the used of any particular technology or service and the FSC must try to promote fair competition for security and authentication technologies. Moreover, another revision on the 3rd February 2015 removed the requirement to install additional software (Kim, 2015). This put responsibility into the hands of the Financial Service Providers. Also, a revision on the 18th March 2015, stipulated that the FSC could no longer promote the use of the NPKI digital certificates.

The wording of the revisions suggest that the FSC is stepping back and loosening control instead of trying to actively solve the problems that were created. The problem now is that a very strong business relationship has been built up between the transaction security providers and the banks based on these systems and there is no strong incentive for them to change their technology approaches yet as the market has already been established. Now, consumer demand will be the driving force for change but it may be a slow process because it will take time to dismantle the previous monopoly and retrain the developers to take different security approaches. Until the transition takes place, International users will continue to be blocked or face restrictions and inconveniences when using Korean websites, and this may limit business opportunities for Korean e-Commerce companies seeking to internationalize their services.

## 5. Conclusion

This study illustrated how Government-mandated TBTs can lead to a protected business environment. Initially, the reasoning behind creating a National transaction security standard in Korea was understandable considering the delay in the distribution of emerging technology from the U.S. The strategy in Korea also may have opened a business opportunity to create an alternative that could have been exported around the world. However, as can now be seen that opportunity never materialized. A number of technical mistakes were made during the implementation of the technology. One was that the project was closed. Other countries such as Denmark took the same path as Korea but as an Open Source Project meaning that they did not create a TBT. Another problem was that the technology used plugins in a way that they were not designed for, which eventually led to major security problems. In addition, the certification companies did not try or were not encouraged to get international accreditation or audits, as the Korean websites were mostly initially aimed at domestic consumers only. Moreover, legislation was created to ensure the Government had to approve any company who sought to create the software needed to support this new encryption system. This had a twofold effect. The first was that it ensured the Korean Government had a certain amount of quality control over the services offered. The second was that it created a barrier to any other company intending to enter the business area. A small group of domestic Korean companies then managed to gain approval and build successful and profitable business in this new niche.

When Netscape left the browser business, leaving Internet Explorer as the only available browser that could support the plugins needed, it created a monopoly for Microsoft. At a quick glance, it may have seemed to observers that the Korean Government had created a technical trade barrier that benefitted a large Multinational Corporation (MNC). However, behind the scenes, the Korean companies providing the certificates and security software needed for Internet Explorer were also benefitting, and were thus protected from competition. This TBT was contested in court by a group of Korean academics and Netizens using the argument that it was in breach of laws restricting the use of technical trade barriers. They based their opposition on the fact that the Mozilla Firefox browser was unusable with many Korean websites because it could not support the Active-X plugin needed. The court ruled against them explaining that as Firefox and other minority browsers had such a small market share, the barrier did not affect Korean users much. Then, another complication emerged when Active-X controls were identified as a major security problem. They provided a channel to bypass user confirmation and install things without consent by malware developers. This led to Microsoft seeking ways to reduce their own reliance on Active-X and trying to boost the security of their operating systems. This was problematic for the Korean encryption standards, as the added security included with Microsoft's upgraded operating system rendered it unusable until it could be adapted. The situation got even more complicated when devices started to converge. Smartphones, tablets and e-book readers all had new types of browsers and none of them were compatible with the Korean transaction security standards. The Korean Government moved to try and create new legislation to support transactions on these devices but it was a difficult process. However, as the use of these convergent devices grew exponentially, concessions had to be made to allow for their use. It showed how the Korean Government's attempts to micromanage the online security system resulted in a situation where consumers were effectively locked into a monopoly that restricted them from being able to keep up to date with technology changes. The irony here is that Korea ended up isolated from international standards by using an approach that entirely depended upon a single foreign Internet browser. This is example of a situation where a Technical Barrier to Trade was raised through Governmental regulation. This allowed the Korean transaction security companies to safely develop their businesses while only competing for customers against each other. However, it also had another side affect as it effectively locked out International customers from Korean websites too unless they were able to navigate their way through the platform requirements and layers of installed programs. As Korea is aiming at becoming a Knowledge Economy this was a major problem. The learning opportunity here is to try not to diverge from global standards too much in case there may be an opportunity to export products and services later.

**Acknowledgement**
*This research is supported by the Hannam University research fund*.

## References

Baekdal, T. ( 2006 ). Microsoft IE ActiveX Update, *Baekdal Website*, 18 January, available: http://www.baekdal.com/insights/microsoft-ie-activex-update ( 16 Nov 2018 ).

Burkholder, P. ( 2002 ). SSL Man-In-The-Middle Attacks. *SANS Reading Room Website*, available: http://www.sans.org/reading-room/whitepapers/threats/ssl-man-in-the-middle-attacks-480 ( 14th Nov 2018 ).

Chang, Y. T. ( 2003 ). Dynamics of Banking Technology Adoption: An Application to Internet Banking, *Royal Economic Society Annual Conference*, n. 41, 2003. available: http://ideas.repec.org/p/ecj/ac2003/41.html. ( 14th Nov, 2018 ).

Ellison, C. and Schneier, B. ( 2000 ). Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure. *Computer Security Journal*, 16(1) pp. 1–7.

Farrell, N. ( 2007 ) Korean government warns against Vista upgrade. *The Inquirer*. 24 Jan, available: http://www.theinquirer.net/inquirer/news/1011686/korean-government-warns-against-vista-upgrade ( 20 Nov 2018 ).

Globalsign ( 2015 ) 9 common myths about CAs, *Globalsign Homepage*. Available: https://www.globalsign.com/en/ssl-information-center/myths-about-cas/ ( 20th June 2016 )

Hankyoreh. (2010). S.Korea's global online market becoming increasingly isolated. *Hankyoreh Website*, 20 Feb, available: http://english.hani.co.kr/arti/english_edition/e_business/405748.html ( 22nd Nov 2018 ).

Hiltgen, A. Kramp, T. and Weigold. T. ( 2006 ). Secure Internet Banking Authentication. *IEEE Security and Privacy*, 4(2) pp. 21–29.

Kang, S. K., Yoon, H. S., Park, Y. W., Kim, M. H., Kwon, H. Y., Kim, D. S., Kim, G. B. ( 2010 ). A Study on the Construction of Efficient System for Safe Cyber space, *Korean Institute of Criminology*. Seoul: Korean Institute of Criminology.

Kang, K. ( 2007 ). Google Chrome will support ActiveX for Korea. *Cnet Asia*. 20 June. available: http://asia.cnet.com/blogs/google-chrome-will-support-activex-for-korea-62114316.htm ( 8 Nov 2018 ).

Kang, S. K., Yoon, H. S., Park, Y. W., Kim, M. H., Kwon, H. Y., Kim, D. S., Kim, G. B. ( 2010 ). A Study on the Construction of Efficient System for Safe Cyber space, *Korean Institute of Criminology*. Seoul: Korean Institute of Criminology.

KFTC ( 2012 ). Statistics and Finance Report. *Korea Financial Telecommunications and Clearings Institute*. Available: http://www.kftc.or.kr/ ( 13th Nov 2018 ).

Kim K.C ( 2015 ). Recent Changes in the Regulatory Landscape for E-Commerce in South Korea , *The Asian Business Lawyer* [Vol.16:87]

Kim, H. K. ( 2011 ). Criminal Laws & Policies of Korea for Promoting International Cooperation in Cybercrime Control. *Supreme Prosecutors' Office, International Criminal Justice Forum*, 1 December 2011.

Kim, H., Huh, J. H., Anderson, R. ( 2011 ). On the Security of Internet Banking in South Korea: a lesson in how not to regulate security. *Cambridge University Press*.

available: http://www.cl.cam.ac.uk/~hk331/Publications/sp10KoreanBanking_v3.pdf ( 19 Nov 2018 ).

Kim, H. K. ( 2011 ). Criminal Laws & Policies of Korea for Promoting International Cooperation in Cybercrime Control. *Supreme Prosecutors' Office, International Criminal Justice Forum*, 1 December 2011.

Kim, T. H. ( 2010 ). Experts Say Specific Tech Mandates Make Internet Banking Vulnerable, *The Korea Times*, 29 April.

available: http://www.koreatimes.co.kr/www/news/biz/2010/05/123_65102.html ( 22 Nov 2018 ).

Kim, T. H. ( 2010 ). Is AhnLab to blame for online banking mess?, *The Korea Times*, 12 May.

Available: http://www.koreatimes.co.kr/www/news/biz/2010/05/123_65650.html ( 25th Nov 2018 ).

Kim, T. H. ( 2010 ). Online banking wiggles out of Microsoft chokehold. *The Korea Times*. 27 Sept,

available: http://www.koreatimes.co.kr/www/news/tech/2010/09/133_73601.html

( 28th Nov 2018 ).

Kim, T. H., Cho M. H. ( 2012 ). Tech industry people's mixed feelings on Ahn. *The Korea Times, 16 Nov.*

Available: http://www.koreatimes.co.kr/www/news/nation/2012/11/608_124848.html ( 11th Feb 2018 ).

Kim, D. J., Kang, J. J., Cho B. Y. ( 2014 ). An Analysis on Using ActiveX Plug-in Controls and Public Key Certificates for On-line Transactions, with Policy Implications of Plausible Regulatory Reform Strategies. *Journal of e-Commerce Research* (2014): pp. 133-159.

KISA ( 2009 ). Current Situation of Hacking and Virus Attacks on Information Systems and Responses, *Korea Internet & Security Agency*. ( May 2009 ).

KISA ( 2012 ). KISA SEED. *Korea Internet & Security Agency*. Available: http://seed.kisa.or.kr/eng/about/about.jsp. ( 12 Mar 2018 ).

KISA ( 2011 ). 2010 Hacking Virus Status and Responses. *Korea Internet & Security Agency*. Feb 2011.

Lee, H. Lee, S. Yoon, J. Cheon, D. and Lee, J. ( 2005 ). The SEED Encryption

Algorithm. *RFC 4269 (Informational),* December 2005.

Microsoft ( 2003 ). Korea Information Security Agency and Microsoft Announce Plans to Work Together to Improve Computer Security Awareness. *Microsoft Homepage*. Available: http://www.microsoft.com/en-us/news/press/2003/nov03/11 04koreainfosecuritypr.aspx ( 16th Nov 2018 ).

MOLEG ( 2013 ). Korean Laws in English. *South Korean Ministry of Government Legislation.* Available: http://www.moleg.go.kr/english/korLawEng ( June 2018 ).

Openweb ( 2006 ). Korean Approach to Web Accessibility. *Openweb Homepage*. 16th Oct, available: http://openweb.or.kr/?page_id=61 (22th Nov 2018 ).

Openweb ( 2006 ) Korean Saga. *Openweb Homepage*, 16th Oct, available: http://openweb.or.kr/?page_id=60 ( 22 Nov 2018 ).

Openweb ( 2006 ). Quirks and bugs are not only for geeks. *Openweb Homepage*, 16th Oct, available: http://openweb.or.kr/?page_id=59 ( 22 Nov 2018 ).

Park, H. M ( 2012 ). 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*, available:

https://www.computer.org/csdl/proceedings/hicss/2012/4525/00/4525c319.pdf

Ramstad, E. ( 2012 ). Ahn Pledges To End Outdated Encryption Standard, *Wall Street Journal Asia*. ( 13th Nov, 2012).

Westby, R. W ( 2003 ). International Guide to Combating Cybercrime

*American Bar Association- Business & Economics.*

Yoo, Y. ( 2007 ) .Web Security Certificate Issuer Preps $10mil Lawsuit with Korean Administration. *ZDNet Korea*. 31 Jan 2007.

Available: http://www.zdnet.co.kr/news/news_view.asp?artice_id=00000039155029&type=det ( 8 Nov 2018 ).

Yoon, J. Y. ( 2012 ). Korea Stuck in Active X. *Korea Times*. Available: http://www.koreatimes.co.kr/www/news/biz/2015/01/326_108495.html (6th April 2012 )

Yu, Z. ( 2000 ). A model of Substitution of Non-Tariff Barriers for Tariffs. *The Canadian Journal of Economics*, Vol. 33, No. 4

**Cite this article:**

**Nigel Callinan (2020).** A Case of A Government-Mandated Online Transaction Standard Acting As A Technical Barrier To Trade in South Korea. *International Journal of Science and Business,* 4(1), 173-184. doi: 10.5281/zenodo.3631315

Retrieved from http://ijsab.com/wp-content/uploads/454.pdf

**Published by**

IJSAB International