Knowledge Sharing Program

2016 Modularization of Korea's Development Experience:

Korea's E-Commerce Policy Experiences

2016

Ministry of Strategy and Finance

KDI Korea Development Institute

2016 Modularization of Korea's Development Experience:

Korea's E-Commerce Policy Experiences

2016 Modularization of Korea's Development Experience

Korea's E-Commerce Policy Experiences

Title	Korea's E-Commerce Policy Experiences
Supervised by	Ministry of Strategy and Finance (MOSF), Republic of Korea
Prepared by	Korea Development Institute
Author	Yeong-Kwan Song, Fellow, Korea Development Institute (KDI)
Advisory	Hong-Yol Kang, Senior Fellow, Korea Information Society Development Institute (KISDI) Il-Soon Shin, Professor, INHA University
Research Management	KDI School of Public Policy and Management
Supported by	Ministry of Strategy and Finance (MOSF), Republic of Korea

Government Publications Registration Number 11-1051000-000757-01

ISBN 979-11-5545-187-8 95320

ISBN 979-11-5545-179-3

Knowledge Sharing Program

Government Publications Registration Number
11-1051000-000757-01

Knowledge Sharing Program

2016 Modularization of Korea's Development Experience

Korea's E-Commerce Policy Experiences

Ministry of Strategy and Finance

KDI Korea Development Institute

Preface

The study of Korea's economic and social transformation offers a unique window of opportunity to better understand the factors that drive development. Within approximately a single generation, Korea transformed itself from an aid-recipient basket-case to a donor country undergoing fast-paced and sustained economic growth. What makes Korea's experience even more remarkable is that the fruits of Korea's rapid growth were relatively widely shared.

In 2004, the Korean Ministry of Strategy and Finance (MOSF) and the Korea Development Institute (KDI) launched the Knowledge Sharing Program (KSP) to assist partner countries in the developing world by sharing Korea's development experience. To provide a rigorous foundation for knowledge exchange engagements, KDI School has accumulated case studies through the KSP Modularization Program since 2010. Over the past six years, the Modularization Program has amassed 144 such case studies, carefully documenting noteworthy innovations in policy and implementation in a wide range of areas including economic policy, administration·ICT, agricultural policy, health policy, industrial development, human resources, land development, and the environment. Individually, the case studies convey practical knowhow and insights in an easily accessible format; collectively, they seek to share Korea's prosperity by illustrating how the country was able to kick-start and sustain its remarkable economic growth.

Building on the program's success over the past six years, we are pleased to present an additional installment of four new case studies and four e-content clips. The 2016 Modularization Program products were chosen based on the results of the careful analysis of topics in greatest demand in the KSP consultation program and comprehensive consultations with related ministries and specialists. The four new case studies discuss Korean experiences in the promotion of electronics industry, electronic commerce in advancing Korea's industrial structure, facilitation of resource management policies, and the developments in special economic zones.

In a further contribution to global knowledge sharing, the e-content topics feature Korean experiences in the development of Korea's major industries, including the automotive, electronic, shipbuilding, and cosmetics industries. Moreover, a total of 14 e-content modules have been uploaded to the World Bank's Open Learning Campus (OLC) in order to share Korea's knowledge with the international community.

I would like to express my gratitude to all those who were involved in the project this year. First and foremost, I would like to thank the Ministry of Strategy and Finance for its continued support for the Modularization Program. I would also like to express my heartfelt appreciation to the contributing researchers and their respective institutions for their dedication to research, to the former public officials and senior practitioners for the keen insight and wisdom they so graciously shared in their roles as advisors and reviewers, and also to the members of the KSP Executive Committee for their expert oversight of the program. Last but not least, I am thankful to each and every member of the Development Research Team for their sincere efforts to ensure the successful conclusion of the research project, as well as to Professor Taejong Kim for his supervision.

As always, the views and opinions expressed by the authors who have contributed to the body of work presented here do not necessarily represent those of the KDI School of Public Policy and Management.

December 2016

Joon-Kyung Kim

President

KDI School of Public Policy and Management

Contents | LIST OF CHAPTERS

Chapter 3

Contents | LIST OF CHAPTERS

Contents | LIST OF TABLES

Chapter 2

Chapter 3

Chapter 4

Contents | LIST OF FIGURES

Chapter 2

Chapter 3

Chapter 4

Summary

The exponential growth of Internet users has led to the emergence of a new Sale and Purchase structure known as "e-commerce." E-commerce refers to buying and selling carried out in virtual markets via the Internet. As there are no time constraints, spatial restrictions, or additional fixed costs incurred from the operation of physical stores, e-commerce expanded rapidly in major developed countries throughout the 1990s. In addition, the massive production of smartphones has enabled e-commerce to expand significantly in developing countries as well.

One of the many advantages of e-commerce is that buyers face no time constraints or spatial restrictions in making purchases. Additionally, in the process of making a purchase decision, a buyer can easily obtain information on alternative products and prices offered by various sellers. Sellers also face no time constraints on their sales activities, nor do they require any physical space for displaying their products, incurring lower distribution and advertising costs as a result. Such benefits of e-commerce have been highlighted in several studies. Brown and Goolsbee (2002) and Baye et al. (2005) state that by reducing the asymmetry in information and the cost of searching for information, e-commerce

increases the efficiency of the market, ultimately bringing prices down. Furthermore, Goldmanis et al. (2010) conclude that e-commerce not only reduces market prices but also encourages competition among firms in the market, thereby increasing economic efficiency and influencing the industrial structure.

To ensure the vitalization of the e-commerce industry, balanced development of infrastructure, social and institutional systems, and other infrastructures is necessary. Yet, the mass distribution of smartphones has dramatically decreased the need for new infrastructure and other infrastructure. With the advent of smartphones, the need for wired high-speed Internet networks in e-commerce has decreased drastically, and with the expansion of various mobile payment apps such as AliPay, it has become possible to build low-cost electronic payment systems. In this way, the distribution of smartphones has given developing countries greater opportunity to share in the benefits of e-commerce. In this respect, e-commerce vitalization policies in developing countries should prioritize the institutional systems that help build trust between buyers and sellers.

E-commerce is characterized by non-face-to-face transactions, making it difficult for consumers and sellers to establish trust early on. Due to this particular characteristic of e-commerce, it is of utmost importance to confirm the identities of the parties to transactions; thus, electronic authentication is a key factor in ensuring the reliability of e-commerce. In addition, consumers, who play a crucial role in vitalizing the e-commerce industry, face reliability issues that arise from purchasing products online, where the transactions are non-face-to-face, and security problems, such as leakages of personal information. In e-commerce, consumers make purchases without directly identifying the products they are buying. Therefore, e-commerce can never be vitalized unless the credibility of purchases is ensured. In order to establish an institutional system to accomplish this, developing countries should prioritize e-authentication and consumer protection measures so as to foster trust between consumers and sellers.

The e-commerce industry of the Republic of Korea (ROK) has expanded rapidly since the 2000s, growing to KRW 1.204 quadrillion annually by 2013. The purpose of this study is to provide a systematic summary of the policies of the Korean government, which have paved the way for the rapid vitalization of e-commerce in Korea since 2000, as a means of assisting policymakers in creating effective e-commerce vitalization policy measures. This paper focuses mainly on the ROK's policies on electronic authentication (e-authentication) and consumer protection.

In terms of e-authentication, the ROK has introduced policies, including certifications, i-PIN/My-PIN, and OTP, which require the government to certify e-authentication or enforce other specific measures. As the government of the ROK has ensured the credibility of e-authentication, the ROK's e-authentication policy, in particular, is believed to have played an important role in expanding e-commerce in the country in the early 2000s. However, under its e-authentication policy, the government made the use of specific technologies, such as PKI and OTP, mandatory, which created various problems. The consequences of making the use of such specific technologies mandatory were that it: disincentivized investment in technological development, thereby hindering the invention of new technologies; shifted the burden of responsibility for issues arising during e-commerce transactions to consumers; and, created security problems in e-authentication, as the Internet environment as a whole relies heavily on ActiveX technology. The biggest problem with the ROK's e-authentication policy is the mandatory use of specific technologies, which serves to hinder the development of new technologies and the growth of the industry in general. Therefore, to secure a foundation for their e-authentication policies, developing countries should maintain technology neutrality and the dynamicity of their private sectors, even when government intervention is necessary to establish trust between consumers and sellers early on. In addition, they should focus on customer convenience, as the failures of the i-PIN and My-PIN systems have demonstrated.

To promote consumer protection in the ROK's e-commerce industry, the government enacted Act on the Consumer Protection in Electronic Commerce, ETC. in 2002. Consumers who purchase goods online are becoming increasingly concerned with the preservation of relevant electronic records, misuse of electronic documents due to the lack of experience of those involved, and newly emerging issues in relation to advertising, shipping, prepayment, and so on. Regarding such issues, the Act on the Consumer Protection in Electronic Commerce, ETC. provides institutional tools to prevent potential harm to consumers. In order to promote consumers' trust in e-commerce, developing countries should also adopt a subscription withdrawal measure and an escrow system and establish organizations, such as an electronic trade dispute settlement committee, to mitigate consumer harm in e-commerce.

2016 Modularization of Korea's Development Experience
Korea's E-Commerce Policy Experiences

Chapter 1

Introduction

Introduction

The main driver of change in the 21st century has been digitalization. The digitalization of various types of information and knowledge has enabled the development and commercialization of diverse technologies, including artificial intelligence, big data, and 3D printing, triggering structural changes in industries around the world. The basis of digitalization is the evolution and spread of the Internet. Since the mid-1990s, several major developed countries have witnessed the vast expansion of the Internet through the spread of personal computers and broadband communications technology. This rapid increase in the number of Internet users has led to the emergence of a new type of Sale and Purchase industry, widely known as e-commerce. E-commerce refers to the act of buying and selling goods and services in virtual marketplaces. Due to the fact that there are no time constraints or spatial restrictions, and the fixed costs of producers are substantially lower, e-commerce made significant progress in the 1990s in major developed countries. With the subsequent rapid and massive distribution of smartphones, e-commerce has been rapidly expanding in developing countries as well.

The lack of time constraints and spatial restrictions is one of the many advantages of e-commerce. This allows buyers to purchase any products they like, no matter where they are or what time it may be. Also, in the process of making purchase decisions, buyers can easily obtain information on alternative products and prices from various sellers. Moreover, there are no time constraints on the sellers' sales activities and no need for physical distribution spaces, leading to lower distribution and advertising costs. These benefits of e-commerce have been outlined in numerous studies. Brown and Goolsbee (2002) and Baye et al. (2005) state that by reducing asymmetry in information and the cost of searching for information, e-commerce has increased the efficiency of the market, ultimately leading to lower prices. Furthermore, Goldmanis et al. (2010) conclude that e-commerce not only reduces market prices but also encourages competition among firms in the market, thereby raising economic efficiency and influencing the industrial structure.

In order to achieve the vitalization of the e-commerce industry, balanced development of infrastructure, social and institutional systems, and other infrastructure is necessary. Here, "infrastructure" refers to networks and the technologies that utilize them, while "other infrastructure" refers to general yet critical components that support e-commerce, including sales and purchasing support systems, electronic payment systems, security and verification software, and logistics systems. "Social and institutional systems" refers to a socially and institutionally provided array of laws and legislative provisions, along with measures to prevent potential leakages of personal information and punishments for deceitful conduct, such as fraud, which aim to vitalize e-commerce. Unlike in the physical world, face-to-face payment methods are not used in e-commerce, making the establishment of a well-functioning electronic payment system a crucial task. It is also necessary to build an efficient logistics and delivery system for transporting products to consumers.

The expansion of infrastructure and other infrastructure necessary for the vitalization of the e-commerce industry has been highly costly. For instance, from 1995 to 2002, the Korean government spent approximately KRW 680 billion to build a broadband communications network. If the government were to attempt to establish electronic payment and logistics systems, the costs would be astronomical. The distribution of smartphones, however, has substantially reduced the need for new infrastructure and other infrastructure in vitalizing the e-commerce industry. With the advent of smartphones, wired high-speed Internet networks for e-commerce are no longer a major necessity, and the expansion of various mobile payment apps, such as AliPay, has made it possible to build low-cost electronic payment systems. In this way, the distribution of smartphones has allowed developing countries to share in the benefits of e-commerce. As a result, the e-commerce vitalization policies of developing countries should prioritize the institutional systems that help build trust between buyers and sellers.

E-commerce is characterized by non-face-to-face transactions, making it difficult for consumers and sellers to establish trust early on. Due to this particular characteristic of e-commerce, the most important element in e-commerce is confirming the identities of the parties to electronic transactions, making electronic authentication a key factor in ensuring the reliability of e-commerce. In addition, consumers, who play a crucial role in vitalizing the e-commerce industry, face reliability issues, which arise from purchasing products online through non-face-to-face transactions, and security problems, such as leakages of personal information. In e-commerce, consumers make purchases without directly identifying the products they are buying. Therefore, e-commerce can never be vitalized unless the credibility of the sellers and their products is ensured. To accomplish this, developing countries should prioritize e-authentication and consumer protection measures in their policymaking efforts to promote e-commerce.

This paper seeks to systematically summarize the policies that the Korean government has implemented to vitalize the e-commerce industry, which has undergone rapid growth since 2000, with the aim of assisting policymakers in other countries in creating efficient policies to successfully vitalize their e-commerce industries. The e-commerce industry in the ROK has expanded rapidly since the 2000s, growing to KRW 1.204 quadrillion annually by 2013. This study focuses mainly on policies related to electronic authentication and consumer protection measures. As mentioned earlier, in order to vitalize the e-commerce industry, balanced development of infrastructure, social and institutional systems, and other infrastructure is crucial. In the ROK, investment in the broadband communications network has played an essential role in the establishment of e-commerce infrastructure. However, as e-commerce conducted via smartphone is growing in importance, wired Internet is losing its importance in modern society. Moreover, the emergence of diverse firms playing important roles in establishing sales and purchasing support systems, electronic payment systems, security and verification systems, and logistics and delivery systems is crucial in vitalizing the industry. Therefore, the government should develop policies that serve to lay the foundation for the growth of such companies. Due to numerous restrictions, however, this study focuses mainly on the ROK's e-authentication policy and consumer protection measures.

This paper comprises a total of five chapters. In Chapter 2, we provide a more in-depth introduction to e-commerce and summarize the current status of the e-commerce industry in the ROK and the efforts made by the ROK government to legalize e-commerce and establish e-commerce infrastructure, such as the construction of a broadband communications network and development of security policies. In Chapter 3, we explore and assess the ROK's electronic authentication policies. We explain how the Korean government has intervened to promote different methods of verification, such as official

electronic certificates, i-PIN, My-PIN, and OTP, and examine and assess the background of the promotion of e-authentication policies, the system established to enforce such policies, and the enforcement methods of those policies. In Chapter 4, we analyze the consumer protection measures in the ROK. To ensure a thorough analysis, we explore the background and main issues of the enactment of the Consumer Law, Act on the Regulation of Terms and conditions, Act on the Consumer Protection in Electronic Commerce, ETC. and introduce the ROK's consumer protection measures in the e-commerce industry. Finally, we assess those consumer protection measures by analyzing the types of disputes that have arisen frequently in the e-commerce industry. In Chapter 5, we conclude the study and speculate on the implications for the development of e-commerce policies by the governments of developing countries.

Chapter 2

E-Commerce in the Republic of Korea

1. Introduction to E-Commerce and Its Legalization in the Republic of Korea
2. Current State of E-Commerce in the ROK
3. Process of Establishing E-Commerce Infrastructure in the ROK

E-Commerce in the Republic of Korea

1. Introduction to E-Commerce and Its Legalization in the Republic of Korea

1.1. Definition

The main agents of e-commerce are firms, consumers, and the government. Normally, e-commerce transactions are categorized according to the parties involved in the transactions. First, B2C (Business-to-Consumer) refers to a business model in which firms sell goods or services to consumers, of which Amazon is a leading example. Second, B2B (Business-to-Business) refers to a business model in which firms sell and buy goods or services among themselves. Third, B2G (Business-to-Government) refers to a business model in which such transactions take place between firms and the government, with an example being the procurement duties of the Public Procurement Service. Lastly, C2C (Consumer-to-Consumer) is a business model where consumers sell goods or services to other consumers. Under this business model, the intermediaries between the sellers and consumers are online auction companies such as eBay.

In 1960, international shipping companies began using a standardized electronic format for the computer-to-computer exchange of electronic business documents called EDI, or Electronic Data Interchange, in order to ensure the prompt delivery of shipping documents. Initially developed for information exchange among firms, EDI has grown with the expansion of the Internet to become a general means of e-commerce. Along with the development of such information and communications and computer technologies, EDI has also been applied to B2B transactions. Finally, with the widespread availability of personal computers, this means of e-commerce has expanded to B2C as well.

Even now, there is no universally accepted concept of e-commerce. In general, however, e-commerce is thought of as all buying- and selling-related activities that take place online. And these activities have expanded to diverse sectors, including finance and education.[1] In the ROK, the legal definition of e-commerce is provided in the Consumer Protection Act in Industries Including E-Commerce. Article 2-1, of this Act describes e-commerce as all commercial activities conducted electronically via the Internet. In Article 2-5, of the Framework Act on Electronic Documents and Transactions, e-commerce is defined as "commercial activities that completely or partly involve the use of electronic documents in transactions of goods or services." In other words, under the laws of the ROK, e-commerce refers to transactions of goods or services conducted by electronic document, and if any step in the purchasing process, including placing an order, making a payment, and confirming the purchase, requires the use of an electronic document, the transaction can be classified

1. The OECD (2011) provides a definition for e-commerce: "An ecommerce transaction is the sale or purchase of goods or services, conducted over computer networks by methods specifically designed for the purpose of receiving or placing of orders. The goods or services are ordered by those methods, but the payment and the ultimate delivery of the goods or services do not have to be conducted online. An e-commerce transaction can be between enterprises, households, individuals, governments, and other public or private organisations. To be included are orders made over the web, extranet or electronic data interchange. The type is defined by the method of placing the order. To be excluded are orders made by telephone calls, facsimile or manually typed e-mail." In other words, in order for a transaction to be considered an e-commerce transaction, the purchase order must be placed via a network, yet payment and shipment may be carried out through offline channels.

as an e-commerce transaction. In this context, an electronic document is any information that is written, sent/received, or stored in electronic form by an information processing system, i.e. computer (Article 2-1, of the Framework Act on Electronic Documents and Transactions). In the ROK, non-face-to-face transactions conducted via such means as television, catalogue, or regular mail that provide information or offer subscriptions are classified as telemarketing, differentiating them from e-commerce. Moreover, the absence of a universally accepted concept of e-commerce makes it difficult to compare related statistics among different countries.

1.2. Impact and Issues

The impact of the vitalization of e-commerce can be analyzed from three different perspectives, those of the: 1) buyer, 2) seller, and 3) society in general. First, from the perspective of the buyer, buyers gain benefits from purchasing goods online, as there are no time or spatial constraints. This allows buyers to go online late at night after work and take their time to purchase products carefully. Second, when choosing which products to purchase, buyers benefit further from access to not only the same products offered at different prices but also information on alternative products and their prices. Finally, assuming that a buyer is purchasing a product from a credible source, the buyer can make purchases conveniently, without having to go to a store and look at the product directly. Trust is one of the most serious issues of e-commerce, and if solved, will bring significant benefits to consumers.

From the seller's perspective, sellers benefit from being able to operate their businesses at lower costs, as they have no need for a physical store in which to arrange their products in displays. This also allows sellers to lower their distribution costs. Second, sellers benefit from lower advertising costs. In terms of newspapers and television, the most commonly

used means of advertising, the cost of running an advertisement is high as the space in newspapers is limited and the times at which the advertisements can be presented to potential customers is somewhat predetermined. Such restrictions are less severe in e-commerce, driving down the cost of advertising. Third, selling products is possible under any circumstances. As there are no time constraints on sales, it is possible for sellers to reach out to their customers at any time of the day, no matter what their circumstances at the moment may be. Lastly, every transaction between buyers and sellers is stored in a database, allowing sellers to analyze the data and create marketing strategies accordingly. Furthermore, as the credentials of each buyer are stored in the database as well, sellers can create customized marketing strategies. In other words, sellers can analyze relevant data, including transaction times, products purchased, and consumers' identities, and create marketing strategies targeting specific customer types.

E-commerce vitalization policies serve to increase consumer welfare by reducing the opportunity cost of searching for product and pricing information and increasing the supply of various goods and services. From the perspective of producers, such policies reduce the costs of production and marketing for firms and increase production efficiency, thereby contributing to economic growth. Brown and Goolsbee (2002) and Baye et al. (2005) demonstrate that e-commerce reduces information asymmetry and increases efficiency in the market by reducing the search costs, ultimately leading to lower prices. In addition, Goldmanis et al. (2010) concludes that e-commerce not only decreases and sets online and offline prices but also encourages competition among firms, thereby influencing industries and increasing economic efficiency.

In order to vitalize e-commerce, balance needs to be achieved in infrastructure, social and institutional development, and other infrastructure. Infrastructure includes networks, multimedia technology, and the information superhighway. In other words, it refers to networks and all related technologies. Social and institutional development includes

the development of standards on leakages of personal information and the technologies that make up parts of the legal mechanisms or legislation that are needed to invigorate e-commerce. Since the Internet is an open network, it is susceptible to leakages of personal information. If consumers do not trust the Internet, however, the growth of e-commerce will be restricted, making it necessary to establish measures for the protection of consumer credentials. Furthermore, standards should be put in place concerning product quality as well as means for customers to express their demands. Other infrastructure refers to the general but core elements of e-commerce, including purchase and sales systems, electronic payment systems, and security and assurance systems, which allow e-commerce to function. As e-commerce is characterized by non-face-to-face transactions, the way in which the electronic payment system is constructed is of utmost importance. Finally, an efficient logistics system is necessary in order to efficiently deliver goods to consumers.

A few of the main issues concerning the government's policies on the vitalization of e-commerce are verification, establishment of firms, regulations for effective electronic contracts, protection of consumer privacy, payment systems and electronic currency, and consumer protection. The OECD (1997) explains some of these major issues in terms of the B2C model. First, the firm that supplies the goods should exist in cyberspace (Step 1). Second, the firm should be actively engaged in marketing activities in order to sell goods and services (Step 2). Third, the goods and services should be produced (Step 3). Fourth, the seller and buyer should make an agreement through negotiation concerning the product in which the buyer is interested (Step 4). Fifth, delivery should be completed upon payment (Step 6). Sixth, if the goods or services are not delivered as agreed, it must be possible to cancel the contract (Step 6). Seventh, the related tax is levied after a given period of time (Step 7).

The following is an explanation of each of these steps. First, Step 1 deals with the establishment of firms. In this regard, brand names can pose a major problem. There are only few regulations concerning the protection of brand names on certain websites. This means that a website in one country can use exactly the same registered company and brand names from on a website in another country. Although this might not be controversial for offline commercial activities, due to geographical limitations, it can cause serious disputes among e-commerce firms. Specifically, as Internet search engines are designed to find all websites that contain the same keywords, disputes may emerge among firms that use the same names. In broad terms, the regulations on the establishment of online companies can themselves be an issue.

Step 2 deals with sales. Along with the development of the IT industry, the majority of marketing activities have moved to cyberspace. This has made it possible to collect information on the demographics, payment types, and preferences of consumers, as well as other types of information, from the Internet. For example, servers provide information on the websites visited by users and records of related information. Based on such data, sellers can utilize network tools such as email to engage in so-called "one-to-one" marketing. Such marketing strategies provide more convenience to the consumers, thereby contributing to the efficiency of the market. However, excessive use of consumer credentials can also become a social issue in terms of invasion of privacy.

Step 3 is production. The most serious issue in electronic publication is copyright infringement. From a technological perspective, servers create numerous copies of digital references when sending such references to the computers of the final users. In this context, various intermediary servers create copies of files, and the final users search websites and acquire information. In order to receive digital content, users usually copy information to their computer hard disks. However, it is doubtful whether the author has authorized the

copying of such files. At the same time, it is difficult to enforce legislation related to property rights on the Internet, as content on the Internet can be accessed by anyone. Empirically, each country operates under different property rights systems, which can lead to serious property rights issues. For example, a document that is considered illegal in one country may be considered legal in another. Therefore, managing the content of the websites, which can be accessed by anyone, by country will become an important issue.

Step 4 deals with negotiations and contracts. In business, it is important to clearly identify the person with whom one is making a contract. However, this is extremely difficult to do for online transactions, especially considering how people sometimes pretend to be someone else online. Unlike the offline market, the online market does not provide a system that allows users to identify with whom they are dealing. From the perspectives of consumers and producers, the process of identifying the legal consumers and suppliers, i.e. transaction certification, is highly important. Concurrently, some question the legal force of electronic contracts, as it might be difficult to complete the signing of contracts through email. In addition, it is questionable that all the countries that allow e-commerce will acknowledge electronic documents.

Step 5 is payment. Online payments are convenient for consumers and facilitate the development of e-commerce. Nonetheless, there are several technological difficulties and flaws that need to be overcome at the institutional level. Electronic payment systems should be utilized widely, since the use of such systems is warranted from the perspective of the economy. However, technologies related to security are important as well. Electronic payment systems require payment means that can be conducted in cyberspace. Currently, several projects are being carried out in an attempt to create online currencies for such a purpose. However, in a theoretical framework, the use of online currency has an impact on monetary policies. Furthermore, the development of new online currencies could lead to new forms of money laundering and other negative impacts.

Step 6 is transaction cancellation and contract nullification. In e-commerce, where consumer protection measures have not yet been properly established, this gives rise to numerous issues. Dissatisfied consumers who return goods to sellers may not always be able to receive full refunds. Also, the ways in which offline refund policies are applied to the online market are obscure. Individual firms might have the ability to refund the full amounts of purchases, and the firms have the incentive to do so. Nevertheless, there should be legal obligations for firms related to such issues, including the resolution of related disputes. This would promote the development of the market as well as consumer trust. There should also be regulations that assign legal obligations to the parties engaged in online transactions.

Step 7 is tax payment. It is difficult to compute value-added tax, or VAT, for online transaction schemes. For example, if a European customer makes a contract with a company registered in the United States, but the product is currently in the custody of another European country, and the server through which the contract was made is located in Asia, it is difficult to say who should levy and pay VAT and which regulation should be applied to the collection of income tax. Regulations on taxes for online transactions have not yet been clearly defined. For instance, the firm may have locations in several countries, enabling it to change its location frequently without informing consumers. Considering the constant debates on issues related to the application of tax policies to online markets, it is clear that a decisive regulation is needed to resolve this issue.

B2C transactions give rise to other problems as well, including invasion of privacy and security, which are major issues. During a transaction, a customer's personal information is created and handled electronically, requiring measures to protect such information. In this respect, users need to be given the power to manage and protect the security of their personal information. Furthermore, systems must be able to maintain their credibility, and the structure of networks should be able to support e-commerce while protecting personal information from fraud and theft. Moreover, the legal obligations assigned to the parties of buyer-seller transactions should be established in advance.

1.3. International Discussion and Legalization in Korea[2]

Since e-commerce began expanding in the 1980s, numerous issues have arisen in relation to trustworthiness, taxes, personal information protection, data transfer among countries, and consumer protection, among others. These issues have been debated even more fervently since 1990. The United Nations Commission on International Trade Law (UNCITRAL) and the World Trade Organization (WTO) have also officially addressed these issues. Through diverse forums, the OECD has spread international standards and policy recommendations to OECD member and non-member states.

UNCITRAL adopted the Model Law on Electronic Commerce and the Model Law on Electronic Signatures in 1996 and 2001, respectively. UNCITRAL is an organization that, among its other duties, establishes international e-commerce policy guidelines for all countries to use as a reference.

The purpose of UNCITRAL's Model Law on Electronic Commerce, enacted in 1996, was to provide an internationally accepted law capable of removing legal obstacles and enhancing predictability. The basic principles of said law are nondiscrimination, technology neutrality, and functional equivalence. Nondiscrimination assures users regarding the legal force of electronic documents, while technology neutrality prevents the forced use of specific technologies so as to ensure neutrality in the selection of e-commerce technologies. In a world where technological development is accelerating, this principle aims to facilitate the adoption of new technologies by removing legal obstacles. Finally, functional equivalence provides a level playing field for electronic communication compared to its counterpart, paper communication. These three principles were applied to the Electronic Model Law on Electronic Signatures, enacted in 2001 by UNCITRAL.

2. Refer to Song (2014), pp. 27-31.

The basic laws governing e-commerce in the ROK are: the Framework Act on Electronic Documents and Transactions, Digital Signature Act, Act on the Consumer Protection in Electronic Commerce, Etc., and Electronic Financial Transactions Act. There are other relevant regulations as well, such as the Basic Information and Communication Protection Law, Promotion of Information and Communication and Information Protection Laws, Consumer Basic Law, and so on.

The first laws in the ROK related to e-commerce were the Digital Signature Act, enacted on February 5, 1999 and implemented on July 1, 1999, and the Basic Electronic Transaction Law, enacted on February 8, 1999 and implemented on July 1, 1999. The Basic Electronic Transaction Law states its purpose as "promoting e-commerce by granting electronic documents legal force equal to that of paper documents and defining basic terms in relation to credibility, consumer protection, promotion of e-commerce, etc. so as to protect citizens from harm in the advent of the Information Age." Clause 19 of this law prescribes that, along with the spirit of the Model Law on Electronic Commerce, "the government should create legislation to allow citizens to transact freely in the market, minimize government regulation, ensure the credibility of e-commerce, reinforce international cooperation in e-commerce, etc." According to Clause 16 of the same law, the government can designate the certifying institution, which then identifies the parties of e-commerce transactions.

The Basic E-Commerce Transaction Law, which was partially revised on June 1, 2012, and implemented on September 2, 2012, was renamed the Electronic Document and Basic E-Commerce Transaction Law, which has been in force since March 23, 2013. Clause 19 of the Electronic Document and Basic E-Commerce Transaction Law, which is subject to the Ministry of Science, ICT and Future Planning and Ministry of Justice, states the basic policy principles and obligations of the government in terms of electronic documents and e-commerce as: (1) ensuring a citizen-driven market; (2) minimizing regulation; (3) ensuring the security and credibility of electronic documents and e-commerce; (4) reinforcing international cooperation.

Clause 1 of the Digital Signature Act, which is subject to the Ministry of Science, ICT and Future Planning, states, "The purpose of this law is to provide for the security and credibility of electronic documents and promote the use of electronic documents, to which end it defines the basic terms regarding digital signatures, thereby stimulating the national information sector and enhancing the welfare of citizens." Concerning the effect of digital signatures, Article 3, Clause 2, of the Digital Signature Act elucidates the integrity of digital signatures by stating, "The content of an electronic document that is officially electronically signed with specific dates is presumed to have not changed." On the other hand, Article 3, Clause 3, states, "Other types of unofficial digital signatures are valid from the specific date that is agreed by the people engaged in the transaction," which clearly illustrates that the Act does not attribute integrity to any other types of unofficial digital signatures.

Articles 3 and 8 of the original Digital Signature Act, enacted in 1999, restrict technologies for digital signatures to specific technologies including "digital signature keys."[3] However, including the Digital Signature Act, revised on December 31, 2001 and implemented on April 1, 2002, all laws incorporate the principle of technology neutrality of UNCITRAL's Model Law on Electronic Signatures. The reason for the amendment of this Act was stated as, "As the current law restricts the technology used for digital signatures to specific technologies such as 'digital signature keys,' the concept of digital signatures

3. Articles 3 and 8 of the original Digital Signature Act are as below:

Article 3 (The effect of electronic signature)

① An electronic signature generated by an electronic signature generation key conforming to an electronic signature verification key included in a certificate issued by an accredited certification body pursuant to Section 15 shall be deemed to be a signature or signature signed by a decree.

② If there is an electronic signature pursuant to Clause 1 above, it shall be presumed that the electronic signature is the signature or seal of the name of the electronic document concerned, and that the electronic document has not been altered after it has been digitally signed.

Article 8 (Obligation of an authorized certification body)

① An authorized certification body shall obtain a digital signature verification key from the Korea Information Security Center (hereinafter referred to as "Protection Center") pursuant to Section 14-2 of the Informatization Promotion Basic Act before commencing the certification work.

② The accredited certification body shall perform the certification work by using the digital signature generation key that matches the digital signature verification key that is certified according to the provision of Clause 1 above.

should be newly defined through a clear regulation pertaining to the verification of digital signatures so as to accommodate more diverse technologies in preparation for future trends in digital signature and authentication technologies, cope with the growing number of international transactions, and improve upon and compensate for the defects of the current legislation system." As a result, the concept of the digital signature, which was once limited to the technology specified in Articles 2 and 3 of the revised legislation, was broadened to incorporate all applicable technologies.[4]

The Consumer Protection Act in Industries Including E-Commerce, subject to the supervision of the Fair Trade Commission, was enacted on March 30, 2002, and implemented on July 1, 2002. Article 1 of this Act reveals its purpose by stating, "The purpose of this law is to protect the interests of consumers and improve market confidence by contributing to the sound development of the national economy by stipulating matters concerning the fair trade of goods and services through e-commerce and telesales." This law enabled the adoption of an escrow system in which payments made by consumers are deposited into an account with a third party so as to prevent consumer harm in non-face-to-face transactions and helped

4. Articles 3 and 8 of the current Digital Signature Law are as follows:

Section 3 (The effect of digital signatures, etc.)

① If another act requires a document or written signature, signature seal or signature, the electronic signature shall be deemed to have met the official electronic signature.

② If there is an authorized electronic signature, it is assumed that the electronic signature is a signature of the signer, a signature seal or a registered seal, and that the content of the electronic document has not been changed after it has been electronically signed.

③ An electronic signature other than an authorized electronic signature shall have the effect of signing, signing, or signature under the agreement between the parties.

Section 8 (the duty of an authorized certification body)

① In order to secure the safety and reliability of the certification work, the Minister of the Ministry of Science, ICT and Future Planning may designate specific details that the accredited certification body should observe in the execution of the certification work as a guideline for the digital signature certification work.

② The Electronic Signature Certification Practice Guidelines under Clause 1 shall include the following:

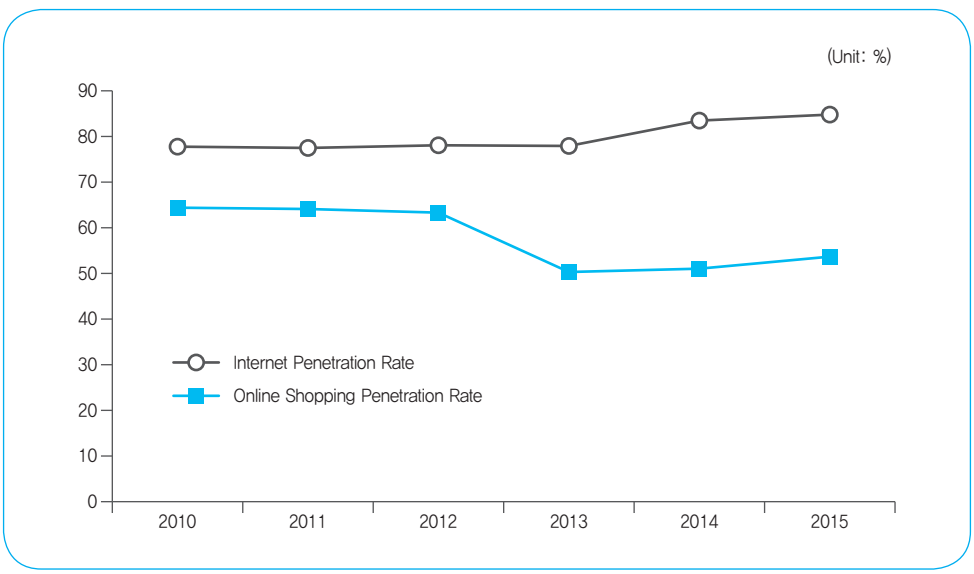
1. Management of official certificate
2. Management of the information on the production of electronic signatures
3. Protection of the facilities of the authorized certification body
4. Other matters concerning certification and operation management

avoid inconveniences caused by indiscriminate advertising by sellers through the operation of a system that allows consumers to choose whether Internet-based advertisements will be displayed on their screens. In the 2007 amendment of this Act, specific criteria are provided for delayed interest rates, which form the standard for calculating delayed compensation, while the 2010 amendment of the same Act adopts the principle of culpability in the joint penal provision by granting exemptions from punishments to employers who have fulfilled their duties in terms of the management and supervision of their employees. The Consumer Protection Act in Industries Including E-Commerce was partially revised in 2012 and 2013 and is now in effect.

2. Current State of E-Commerce in the ROK

The growth of the ROK's e-commerce industry since 2000 is closely related to the rapidly increasing rate of Internet use. In 2015, there were 419.4 million Internet users in Korea. Of those above the age of 12, 53.6 percent have tried online shopping, representing a 2.3-percentage-point increase over the 51.3 percent of last year.

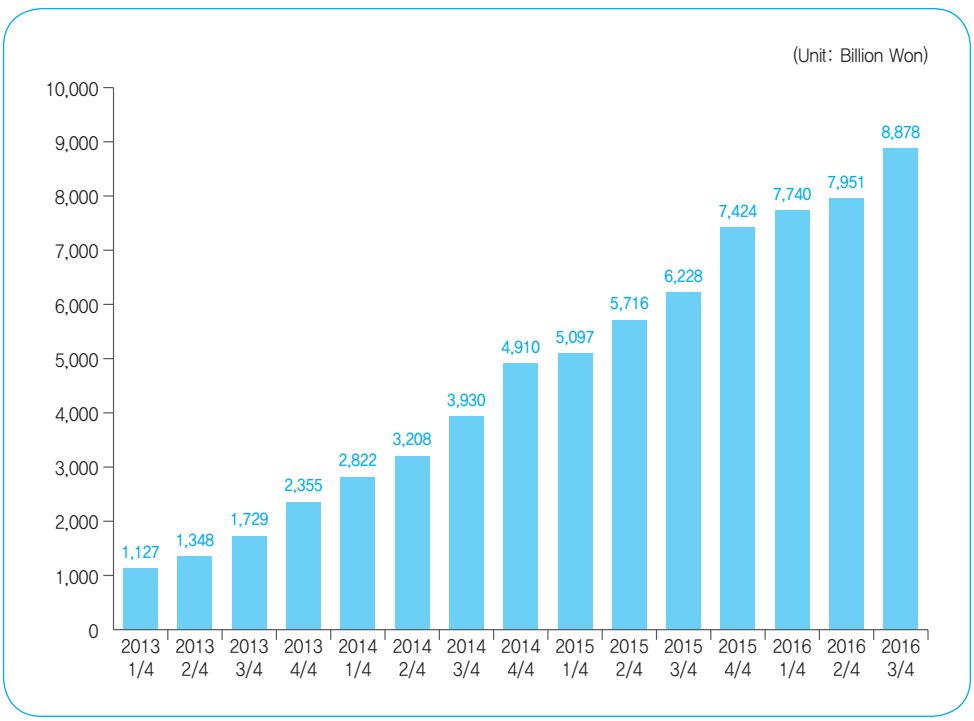
Figure 2-1 | Internet users and online shopping



Source: Korea Internet and Security Agency (date accessed: Nov. 2, 2016).

The decline of the online shopping user rate since 2012 is related to the expanded use of smartphones. With the increase in Internet use and massive distribution of smartphones, the growth of the domestic e-commerce industry has been accelerating. Smartphones offer the advantage of not having time and space restrictions. Therefore, the size of mobile shopping, which has emerged as a new distribution channel for e-commerce, is expected to increase continuously.

Figure 2-2 | The Size of Domestic Mobile Shopping Market



Source: Korea Internet Agency, (Date accessed: Nov. 2, 2016.)

If B2B and B2G are included, the total size of the e-commerce industry in Korea is estimated to be KRW 1.204 quadrillion annually, as of 2013.[5] Even during the global economic crisis in the late 2000s, Korea's e-commerce transactions grew by approximately 20 percent year-on-year, expanding by five percent year-on-year in 2013 alone. B2B transactions account for about 90 percent of all e-commerce transactions, with B2G, B2C, and C2C transactions accounting for the remaining 10 percent. However, B2C transactions are growing steadily at around 10 percent annually, reaching a total market value of KRW 24.3 trillion by 2013.

Table 2-1 | Domestic E-Commerce Market Size and YoY Growth Rate

(Unit: billion won)

	Total Market Size of E-Commerce	B2B	B2G	B2C	C2C
2009	672,478 (6.7%)	592,965 (5.8%)	59,455 (13.8%)	12,045 (6.0%)	8,012 (29.1%)
2010	824,392 (22.6%)	747,090 (26.0%)	52,772 (-11.2%)	16,005 (32.9%)	8,524 (6.4%)
2011	999,582 (21.3%)	912,883 (22.2%)	58,378 (10.6%)	18,533 (15.8%)	9,788 (14.8%)
2012	1,146,806 (14.7%)	1,051,162 (15.1%)	62,478 (7.0%)	21,160 (14.2%)	12,006 (22.7%)
2013	1,204,091 (5.0%)	1,095,696 (4.2%)	70,649 (13.1%)	24,331 (15.0%)	13,414 (11.7%)

Source: Korea Internet and Security Agency (Date accessed: Nov. 2, 2016).

5. The definition of e-commerce differs by country, as there is no internationally agreed-upon concept of e-commerce. The Korea National Statistical Institute (KNSO) defines e-commerce as "the exchange of goods and services through electronic media such as computers and networks." In other words, if at least one of the various processes of a transaction, including bidding, contracting, or ordering, is carried out on a computer network, the transaction is classified as an electronic commerce transaction, while transactions involving the provision of information or subscriptions via such means as TV, catalog, and regular mail are put in a different category from e-commerce. The KNSO has not published e-commerce statistics, including statistics on B2B and B2G transactions, since 2013; instead, it publishes statistics on online shopping malls.

About two-thirds of B2B transactions take place in the manufacturing sector, with a large majority of the remaining transactions taking place in the wholesale and retail trade sector and construction sector. More specifically, 70 percent of B2B transactions occur in the manufacturing sector and 15 percent in the wholesale and retail trade sector. The growth trend of these two sectors, therefore, closely follows that of the B2B market. Since 2010, the manufacturing sector and wholesale and retail trade sector have steadily increased in size, but the growth rates of these two sectors have been decreasing gradually, which is reflected in the growth rate of the B2B market.

Table 2-2 | Domestic E-Commerce Transactions by Industry and YoY Growth Rate

(Unit: billion won)

	Total B2B Market Size	Manufacture	Retail	Construction	Others
2009	592,965 (5.8%)	275,246 (-23.5%)	105,073 (9.2%)	56,978 (-10.0%)	155,668 (279.2%)
2010	747,090 (26.0%)	508,520 (84.8%)	126,543 (20.4%)	61,711 (8.3%)	50,316 (-67.7%)
2011	912,883 (22.2%)	635,965 (25.1%)	146,174 (15.5%)	71,264 (15.5%)	59,480 (18.2%)
2012	1,051,162 (15.1%)	751,007 (18.1%)	159,549 (9.2%)	83,813 (17.6%)	56,793 (-4.5%)
2013	1,095,696 (4.2%)	787,003 (4.8%)	164,496 (3.1%)	74,706 (-10.9%)	69,491 (22.4%)

Source: Korea Statistical Information Center (Date accessed: 2014.09.28).

As of 2015, online shopping transactions amounted to KRW 53.8 trillion, increasing by 19 percent from the previous year.[6] Looking at the transaction value by product category, it can be easily seen that travel and reservation services have the highest transaction value, at KRW 9.9 trillion, followed by clothing and fashion products, living and automotive products, and home appliances and electronic communication devices. As of 2015, the transaction values in cosmetics, food and beverages, living and automotive products, and children's and infants' products have increased significantly.

Table 2-3 | Online Shopping Mall Transactions by Item and YoY Growth Rate

(Unit: billion won)

	Total	Computers/ Relevant Machinery	SW	Telephones and Relevant Telecommunication Products	Books	Music CDs/ Videos/ Instruments	Travel/ Reservation Services	Baby Products	Food and Beverages
09'	20,643	2,035	130	2,683	1,030	136	2,670	1,247	1,352
	(14%)	(24%)	(0%)	(9%)	(18%)	(23%)	(-7%)	(21%)	(34%)
10'	25,203	2,388	132	3,117	1,169	154	3,445	1,512	1,642
	(22%)	(17%)	(2%)	(16%)	(14%)	(13%)	(29%)	(21%)	(21%)
11'	29,072	2,808	93	3,238	1,274	152	4,066	1,539	2,142
	(15%)	(18%)	(-30%)	(4%)	(9%)	(-1%)	(18%)	(2%)	(31%)
12'	34,068	3,063	81	3,751	1,273	142	5,577	1,658	2,892
	(17%)	(9%)	(-13%)	(16%)	(-0%)	(-7%)	(37%)	(8%)	(35%)
13'	38,494	3,074	82	4,078	1,196	152	6,447	2,017	3,246
	(13%)	(0%)	(1%)	(9%)	(-6%)	(7%)	(16%)	(22%)	(12%)
14'	45,302	3,414	58	4,962	1,280	163	8,383	2,227	3,611
	(18%)	(11%)	(-29%)	(22%)	(7%)	(14%)	(30%)	(10%)	(11%)
15'	53,888	3,543	57	5,880	1,151	169	9,982	2,711	4,857
	(19%)	(4%)	(-2%)	(18%)	(-10%)	(4%)	(19%)	(22%)	(35%)

6. This refers to B2C and C2C transactions, including B2B and B2G transactions, which form part of the online shopping mall business.

	Flower	Sports/ Leisure	Living/ Automobile Products	Attire/ Fashion	Cosmetic	Stationary	Agricultural	Other Services	Others
09'	60 (18%)	844 (38%)	1,959 (15%)	3,524 (18%)	1,104 (20%)	298 (14%)	588 (19%)	69 (23%)	915 (-4%)
10'	54 (-10%)	1,076 (28%)	2,572 (31%)	4,248 (21%)	1,414 (28%)	340 (14%)	681 (16%)	81 (17%)	1,179 (29%)
11'	49 (9%)	1,215 (13%)	3,044 (18%)	4,869 (15%)	1,605 (14%)	357 (5%)	821 (21%)	135 (67%)	1,663 (41%)
12'	45 (-8%)	1,334 (10%)	3,655 (20%)	5,550 (14%)	1,946 (21%)	415 (16%)	956 (16%)	523 (287%)	1,207 (-27%)
13'	46 (2%)	1,797 (28%)	4,256 (16%)	6,256 (12%)	2,092 (8%)	470 (13%)	1,130 (18%)	640 (22%)	1,606 (33%)
14'	44 (-5%)	1,899 (11%)	5,175 (22%)	7,346 (17%)	2,669 (28%)	471 (0%)	1,171 (4%)	960 (50%)	1,469 (-9%)
15'	32 (-27%)	2,089 (10%)	6,672 (29%)	8,467 (15%)	3,520 (32%)	459 (-3%)	1,434 (22%)	1,157 (20%)	1,708 (16%)

Source: Korea Statistical Information Center (Date accessed: 2016.11.02).

With the growth of the e-commerce industry, the importance of e-commerce in the Korean retail industry has been increasing. From 2010 to 2015, the Korean retail industry grew at an average annual rate of 3.79 percent, reaching KRW 369.2 trillion in 2015. In particular, the average annual growth rate of the online shopping sector, including TV home shopping, Internet/mobile shopping, and catalog shopping, increased by 16.41 percent over the same period, far exceeding the 4.63 percent of the offline shopping sector. In 2015, following this remarkable growth, e-commerce accounted for KRW 53.8 trillion, or 14.5 percent of the entire retail sales industry, making it the largest type of retail business in the industry as of the previous year.

Table 2-4 | Market Size of Retail Services by Categories

(Unit: trillion won, %)

Categories	2010	2011	2012	2013	2014	2015	Average Yearly Growth Rate
Retail	306.5	335.5	349.5	353.5	361.2	369.2	3.79
Offline							
Department Store	24.8	27.6	29.1	29.8	29.0	28.9	3.15
Big Mart	38.1	42.2	44.3	45.1	47.4	48.6	5.02
Supermarket	29.9	32.5	34.0	35.8	35.8	36.7	4.18
Convenience Store	7.8	9.2	10.9	11.7	12.7	16.5	16.17
Online							
Online Shopping	25.2	29.0	34.0	38.4	45.3	53.8	16.41

Note: 1) This excludes professional retailers and car & fuel retailers.
2) This uses geometric mean.

Source: Korea Statistical Information Center (Date accessed: 2015.11.02).

Since e-commerce statistics first began to be collected in 2004, e-commerce revenue has been growing steadily, in terms of both the number and amounts of transactions. In 2015, however, the growth rate declined significantly, but from 2010, the growth rate had remained at over 40 percent. The lowering of language and institutional barriers, expansion of procurement services, strengthening of security in the e-commerce industry, and proliferation of active importers purchasing directly from overseas are believed to be driving the high growth rate of e-commerce. The average annual growth rate of imports through electronic commerce was 5.57 percent, and the average annual growth rate of the amount reached 15.56 percent.

Table 2-5 | The Number of Imports via E-Commerce, YOY Growth Rate

(Unit: thousands, million USD)

	2010	2011	2012	2013	2014	2015
The Number f Transactions	3,579 (43%)	5,602 (57%)	7,944 (42%)	11,159 (40%)	15,530 (39%)	15,842 (2%)
The Amount	274 (64%)	472 (72%)	707 (50%)	1,040 (47%)	1,545 (49%)	1,521 (-2%)

Source: Korea Customs Service (Date accessed: 2016.11.02).

A little over 70 percent of e-commerce goods imported from overseas come from the United States, followed by China and Germany. Three-fourths of foreign e-commerce goods flowing into the country are imported from the United States. By 2011, Chinese goods had come to account for about five percent of all e-commerce transactions. Since 2012, however, sales of Chinese goods have surged, now accounting for more than 10 percent of the total. Imports from New Zealand accounted for 4.4 percent of all imported e-commerce goods in 2009, but has steadily declined since then, falling to only 0.7 percent in 2015.

Table 2-6 | The Number of Imports via E-Commerce, Amount (Share in %)

(Unit: thousands, million USD)

		2009	2010	2011	2012	2013	2014	2015
United States of America	The Number of Transactions	1,863 (74.2%)	2,967 (82.9%)	4,392 (78.4%)	6,318 (79.5%)	8,405 (75.3%)	11,413 (73.5%)	11,395 (71.9%)
	The Amount	128 (76.7%)	225 (82.1%)	358 (75.9%)	557 (78.7%)	780 (75.0%)	1,122 (72.6%)	1,083 (71.2%)
China (Hong Kong)	The Number f Transactions	209 (8.3%)	177 (5.0%)	304 (5.4%)	797 (10.0%)	1,590 (14.3%)	2,265 (14.6%)	1,691 (10.7%)
	The Amount	9 (5.3%)	10 (3.8%)	23 (4.9%)	69 (9.7%)	136 (13.0%)	210 (13.6%)	135 (8.9%)
Germany	The Number of Transactions	9 (0.4%)	40 (1.1%)	156 (2.8%)	323 (4.1%)	490 (4.4%)	839 (5.4%)	1,202 (7.6%)
	The Amount	1 (0.5%)	4 (1.4%)	14 (2.9%)	28 (3.9%)	41 (3.9%)	80 (5.2%)	110 (7.3%)
New Zealand	The Number of Transactions	110 (4.4%)	124 (3.5%)	110 (2.0%)	95 (1.2%)	90 (0.8%)	109 (0.7%)	110 (0.7%)
	The Amount	5 (3.0%)	6 (2.1%)	5 (1.1%)	4 (0.6%)	4 (0.4%)	5 (0.3%)	6 (0.4%)
Others	The Number of Transactions	318 (12.7%)	270 (7.6%)	641 (11.4%)	411 (5.2%)	584 (5.2%)	904 (5.8%)	1,443 (9.1%)
	The Amount	24 (14.5%)	29 (10.6%)	72 (15.2%)	49 (7.0%)	80 (7.7%)	128 (8.3%)	187 (12.3%)
Total	The Number of Transactions	2,510 (100.0%)	3,579 (100.0%)	5,602 (100.0%)	7,945 (100.0%)	11,160 (100.0%)	15,531 (100.0%)	15,842 (100.0%)
	The Amount	167 (100.0%)	274 (100.0%)	472 (100.0%)	707 (100.0%)	1,040 (100.0%)	1,545 (100.0%)	1,521 (100.0%)

Source: Korea Customs Service (Date accessed: 2016.11.02).

3. Process of Establishing E-Commerce Infrastructure in the ROK

3.1. Broadband Networks[7]

The expansion of e-commerce requires the development of different types of infrastructure, including personal computers, broadband Internet networks, and smartphones. In 1998, the number of Internet users per 100 people and computer ownership among households in the ROK were seven and 18 percent, respectively, putting the country in 20th place among the 31 OECD member states (Ko, 2011). In 1994, however, the Korean government established the "Comprehensive Plan for Establishment of Broadband Information and Communication Infrastructure" and began focusing on building and upgrading the country's high-speed information and communications networks. In 1999, the Korean government also began promoting the use of the Internet, starting with the "Comprehensive Plan for National Information Education." Thanks to such policy efforts, the number of Internet users in Korea, which had stood at only 1.9 million in 1997, expanded rapidly to 31.58 million in 2004 (Ko, 2011).

Since the 1990s, the ROK has focused on formulating and implementing development and investment strategies for the information and communications sector, in line with the sector's emergence as an integral factor of national competitiveness. As part of its effort to secure national competitiveness, the ROK developed a strategy to build a broadband network, with the goal of securing infrastructure capable of transmitting voice, data, video, and other multimedia information at high speeds. Toward this end, the government launched the KII-G, KII-P, and KOREN projects. The KII-G, in which public resources were invested, is a network designed to enable public institutions, such as federal and local governments,

7. Refer to Yoon (2011) and Ko (2011).

national universities and research institutes, to use high-speed services at low costs by connecting major cities, small cities, and metropolitan areas via ATM (Asynchronous Transfer Mode) exchange networks. The KII-P, on the other hand, is a network in which private operators invested their own resources in order to provide high-speed Internet services in the private sector, including privately owned businesses and households, and enable the high-speed, high-capacity transmission of information nationwide. The purpose of the KOREN network is to verify the feasibility and suitability of high-speed information and communications technologies and carry out testing of advanced communications services in advance.

In order to create an environment in which policies may be implemented in relation to such high-speed information and communication network construction projects, the government has taken measures to raise public awareness of the necessity of such networks, foster the education and training of experts in the information and communications industry, improve relevant legislation and institutional systems, and strengthen international cooperation activities. To achieve these goals, the government designated the Korea Culture Information Service Agency as a public relations agency and established a strategy for promoting public relations in stages. In order to foster experts in government communication, the government improved facilities and subsidized research studies at universities and continued supplying computers for student use to elementary, middle, and high schools. In addition, to resolve the quantitative and qualitative disparities in demand and supply, the government supported experts with actual experience in the information and communications industry, raising the quality of education to a level on par with the international standard, cultivated researchers in the information and communications industry by providing subsidies, established infrastructure for human resources statistics, and increased access to market information by promoting and strengthening relevant policies. In 1995, the government

promulgated the Basic Law for Promotion of Informatization in order to promote national informatization, build infrastructure for the information and communications industry, and establish broadband networks. This law is said to be the parent law of all the ROK's other laws related to informatization as well as a cornerstone for the systematic promotion of policies for state society information. To effectively promote informatization, the ROK actively participated in international cooperation activities in which the member states of international organizations, such as the OECD and G7, shared relevant information and their prior experiences in relation to the promotion of informatization.

From 1995 to 2002, the ROK government invested approximately KRW 680 billion in the construction of broadband networks, gaining benefits valued at roughly KRW 17.7 trillion in return. Explicitly, the economic effects induced by the construction of the broadband networks are estimated to be KRW 22 trillion in terms of production, KRW 16 trillion in value added, and 230,000 in job creation, as well as a 0.45-percent increase in the GDP. The broadband network infrastructure has promoted innovation in the public sector and government while enhancing the productivity of and creating new businesses in existing industries. It has also led to the enhancement of informatization at the national level. In particular, the implementation of e-government has increased management efficiency in relation to human resources, finance, education, administration, and other relevant tasks in and among government organizations, central agencies, and central and local governments. The distribution of e-settlement and e-documents has also enhanced the productivity and transparency of administrative processes. The contribution of the IT industry to total GDP growth more than doubled from 1.1 percentage points in 1998 to 2.5 percentage points in 2004, while production grew from KRW 51.4453 trillion in 1995 to KRW 229.2322 trillion in 2004, expanding at a rate of 346 percent.

3.2. Security[8]

In the ROK, the National Intelligence Service (or NIS) is responsible for information security at the national level. In accordance with the National Intelligence Service Act, the NIS is responsible for coordinating tasks related to information security and assisting information investigation agencies and administrative agencies with tasks and projects related to national security based on the Security Regulations. Each administrative department executes relevant tasks in the areas of national defense, public and private sectors, industry, finance, and so on. The Ministry of National Defense (or MND), for example, carries out national-defense-related cyber security activities in accordance with the national cyber security management regulations. Toward this end, the Defense Information Warfare Center was established under the jurisdiction of the MND to handle cyber security tasks at the national-defense level. The Ministry of Government Administration and Home Affairs (MOGAHA) conducts tasks related to information security and privacy policy in the public sector, in accordance with the National Informatization Basic Law, E-Government Act, Information and Communications Infrastructure Protection Act, and Public Information Protection Act. Under the Act on Promotion of Information and Communications Network Utilization and Information Protection, the Korea Communications Commission (KCC) promulgates the guidelines on information protection, manages and supervises the agency that assesses information security, and verifies the information security management system, while the Ministry of Science, ICT and Future Planning nurtures experts and assigns relevant tasks with the aim of fostering the information security industry.

Since the 1980s, the rapid development and expansion of informatization, along with its related side effects, has led to numerous amendments of information security legislation. The Act on the Expansion and Use of Network, enacted in 1986, was the first law related to informatization. Since then, information protection has only grown in importance,

8. Refer to Yoon (2012).

leading to the enactment of the Basic Act on Promotion of Informatization in 1995. This Act provides for the promotion of informatization and lays out the basic regulations on information protection. Furthermore, the criminal law of the ROK has been amended to address infringements of electronic records and criminal offenses and confidentiality related to electronic records. The Digital Signature Act was enacted in 1999 to ensure the security and safe distribution of the private information of individuals and companies. In addition, the Act on the Expansion and Use of Network was amended and renamed the Act on Promotion of Utilization of Information and Communication Network, which provides measures designed to address the negative impacts of informatization at the institutional level.

In the 2000s, as the both the state and society in general became increasingly dependent on information and communications systems, the information protection laws were amended in the interests of national security. In 2001, the Information and Communication Infrastructure Protection Act was enacted and promulgated in order to protect core infrastructures, such as those for finance, telecommunications, and energy, in the information and communications industry. In addition, the Act on Promotion of Utilization of Information and Communication Network was reformed and renamed as the Act on Promotion of Utilization of Information and Communication Network as well as Protection in Private Information, further reinforcing information protection measures. In 2004 and 2005, the penalties for invasions of privacy and indiscriminate circulation of advertisements were strengthened to prevent user harm. In 2005, the National Cyber Safety Management Regulations were put into effect, by Presidential Order, in order to protect the national information network from cyber-attacks with the potential to threaten national security. In addition, with the enactment of the Effective Adoption and Operation of Information Systems Legislation, the supervisory structure for information systems was established to promote the development of a foundation for the efficient adoption and operation of information systems.

Since the late 2000s, numerous laws related to informatizaiton and information protection have been enacted, including the E-Government Act, National Informatization Basic Law, Information and Communications Industry Promotion Act, National Informatization Foundation and Defense Information Resource Management Act, and Personal Information Protection Act. In 2007, the Act on the Promotion of Electronization of Administrative Affairs for Implementation of E-Government was revised and renamed as the E-Government Act, facilitating the procedure for the realization of e-government. In addition, the Information Communication Infrastructure Protection Act was revised, leading to a reorganization of the verification system concerning the implementation of protective measures for major communications facilities. In 2009, the Basic Law for Promotion of Informatization was combined with the Effective Adoption and Operation of Information Systems Legislation and revised and renamed as the National Informatization Basic Law. In addition, the Information Communication Industry Promotion Act was enacted, providing the institutional foundation for the promotion of the vitalization of the information protection industry. In 2010, the Formation of National Informatization Foundation and National Defense Information Resource Management Legislation was enacted, and the E-Government Act was revised to improve the system for the development of information protection. In 2011, the Act on Private Information Protection was enacted, the public and private sectors were made subject to the regulations on the management of private information, and the measures prohibiting invasions of privacy were strengthened. Through such actions, the government sought to ensure people's rights in relation to personal information and strengthen personal information protection measures.

Korea's information protection laws and systems can be classified under different categories depending on the purpose and function of the law or system, such as laws and regulations related to: the protection of state secrets, the prevention of the outflow of important information, digital signatures and verification procedures, promotion of information systems and information and communications networks, punitive measures for invasions of privacy, and protection of private information. The status of these legal systems, according to the purposes of each, is as follows. For the protection of state secrets, there are regulations such as the Security Regulation, National Informatization Basic Law, and E-Commerce Basic Law, while for the misuse of passcodes, there is the Military Criminal Act. Concerning the prevention of the outflow of important information, there is the Act on the Prevention and Protection of Industrial Technology Spill, the Act on Transfer of Technology and Promotion of Commercialization, and the Act on Promotion of Technology in Public and Private Sectors, which prevent leakages of secret information held by public research institutes and private companies that participated in technological transfer and commercialization promotion projects. In relation to the legal system governing digital signatures and verification procedures, there are the Digital Signature Act and laws such as the Electronic Information Law, which regulate administrative digital signatures and verification processes. In terms of laws related to the protection of information systems and information and communications networks, we have the National Informatization Basic Law, Information Communication Infrastructure Protection Act, and Promotion of Information and Communication and Information Protection Laws. For invasions of privacy, there are the Basic Information and Communication Protection Law and Promotion of Information and Communication and Information Protection Laws. Moreover, we have the Personal Information Protection Law, which ensures people's rights in relation to and strengthens the protection of personal credentials. Finally, regarding personal information protection in the public sector, there are such laws as the E-Government Act, Residency Registration Law, and Passport Law, among others.

2016 Modularization of Korea's Development Experience
Korea's E-Commerce Policy Experiences

Chapter 3

Electronic Authentication Policy in the ROK

1. Public Authentication
2. Other Policies on Authentication
3. Evaluation

Electronic Authentication Policy in the ROK

Electronic authentication has become crucial in ensuring security and reliability in the rapidly expanding e-commerce industry. As e-commerce involves non-face-to-face transactions, in which it is hard to confirm the identities and intentions of the parties involved, establishing trust between the parties of e-commerce transactions is difficult. Moreover, in consideration of the difficulty of maintaining the confidentiality of e-documents and the ease with which electronic documents can be falsified or altered and used illegally, e-authentication is a necessary means of ensuring security and reliability. There needs to be a "mutual safety device" in e-commerce, serving as an institutional and technological tool for establishing trust between buyers and sellers. Examples of mutual trust devices include the right to withdraw contracts to protect consumers' rights and means of personal information protection, such as e-authentication.

1. Public Authentication

1.1. Background

Official digital certificates are the seals of the cyber era. Just as we have national ID cards, seals, and signatures to verify our identities and confirm transactions in everyday life, we also need a means of authentication to verify the identities of the parties of e-commerce transactions. E-authentications have the same power online as seals and national ID cards do in the offline world, and are similar to existing authentication systems in that there is an authorized institution to confirm that corresponding digital signatures belong to particular parties of transactions. An e-authentication is a government-approved digital certificate that is used as a type of seal for self-identification in e-commerce transactions. According to Article 2, Clause 8, of the Digital Signature Act, an e-authentication is a digital certificate certified by a certification authority. In this context, a certificate refers to "an electronic document that confirms and verifies that the information generated by a digital signature belongs solely to the subscriber."

Currently, e-authentication has a public key infrastructure (or PKI). PKI is a security infrastructure that uses an asymmetric encryption algorithm to protect personal information and prevent the falsification and tampering of information by unauthorized persons in e-commerce by electronically distributing, delivering, and providing legally valid digital certificates to and among users on the Internet. Under this infrastructure, there are two types of keys: private keys, such as a seal, which are held by individuals, and public keys, which are assigned by a trusted authority. By checking whether two keys are in agreement, any forgery or alteration of transmitted and received messages can be detected. PKI was established to maintain the security of e-commerce and enable anyone to acquire and use public keys securely and conveniently.

Article 25-1 of the revised Digital Signature Act (January 16, 2001) specifically states that the highest certification authority, the Korea Information Security Center (currently the Korea Internet and Security Agency), is responsible for all tasks related to the management of digital signatures. Article 25, Clause 1, of the Act states, "In order to create an environment in which digital signatures can be used safely and reliably and to efficiently manage accredited certification authorities, the Korea Information Security Center should be responsible for the verification of the certification of digital signature verification keys of the certification authorities, the development and distribution of digital signature verification technology, and other relevant tasks related to the verification of digital signatures."

1.2. Means of Promoting Public Authentication[9]

The e-authentication system based on the Digital Signature Act, implemented in July 1999, was established in the early 2000s and began spreading rapidly as the use of e-authentication became mandatory. In January 2003, a mutual cooperation agreement regarding e-authentication entered into by six major certification authorities enabled all digital signatures to be validated under one single authentication system. In September 2002 and March 2003, the government made the use of e-authentication mandatory for Internet banking and e-commerce, accelerating the expansion of e-authentication nationwide. Even today, e-authentication is widely used in areas such as Internet banking, e-commerce, government subsidies, e-bidding, online stock exchanges, e-trade, and customs clearance, among others.

E-authentication is particularly prevalent in the finance sector. In 2002, with its announcement of the interoperability agreement, the Financial Supervisory Service (FSS) integrated all e-authentication systems, leading to the expanded use of e-authentication in the finance sector. The FSS stated, "As all private certificates issued and used individually

9. Refer to Song (2015).

by banks have been integrated under a single system, all electronic financial transactions, such as Internet banking and securities, as well as civil affairs, such as electronic complaints, procurement, and bidding, can now be carried out under one e-authentication system, and not only have such transactions become more convenient, but they are also protected under law" (FSS, 2002). In particular, as Article 25-3 of the Digital Signature Act, implemented in April 2002, states, it is now prohibited to request official authentication without any justifiable reason.[10]

E-authentication in the ROK is a digital signature certified by the government. It is a kind of electronic seal that verifies one's identity in electronic transactions. After adopting e-authentication, the government made the use of e-authentication in Internet banking and online stock exchanges mandatory in September 2002 and March 2003, respectively.[11] In April 2004, the use of e-authentication became obligatory for credit card transactions exceeding KRW 300,000, with that limit being reduced to KRW 100,000 in October 2004. However, the government gave credit card companies the freedom to decide whether to use e-authentication, if the method of payment in the transaction was credit card, and obligated the use of e-authentication for bank wire transfers exceeding KRW 300,000 in November 2005. As the above shows, although the government began making the use of e-authentication in financial transactions mandatory in 2002, it wasn't until the Electronic Financial Transactions Act was first implemented in 2007 that the measures became law.

The Financial Services Commission was authorized to decide the specific technologies to be used for e-authentication, as stated in Article 21, Clause 3, of the first version of the Electronic Financial Transactions Act: "In order to ensure the safety and reliability of electronic financial transactions, the Financial Services Commission may establish necessary standards for the certification methods mentioned in Article 2, Clause 8, of the Digital

10. Enforcement of Digital Signature Act, April 2002, Article 25, Clause 3 (Ban on Request for Particular E-Authentication) "Anyone who verifies an electronic signature using e-authentication should not only accept e-authentication certified by a specific certification authority without justifiable grounds."

11. Refer to Song (2015).

Signature Act, including the use of e-authentication." In addition, Article 7 of the Electronic Finance Supervision Act, amended on December 28, 2006, specifies that "e-authentication, in accordance with the Digital Signature Act, should be used in every electronic financial transaction," except for those for which it is difficult to adopt e-authentication, either for technological or institutional reasons. The same Act delegates the responsibility for such exceptional cases to the head of the FSS. In accordance with Article 31, Clause 4, of the Enforcement Regulations of the Electronic Financial Supervision Regulations, which was also amended on December 26, 2006, the FSS declared the "exemption from the use of e-authentication" for credit card payments and online account transfers of less than KRW 300,000.

The policy mandating the use of accredited digital certificates in electronic financial transactions generated significant controversy. On May 31, 2010, the Korea Chamber of Industry and Commerce, under the Office of the Prime Minister, finalized the "Safety Guidelines for Electronic Financial Transaction Authentication Method." Based on these guidelines, the Electronic Financial Supervision Regulations, enforced on June 30, 2010, have been amended to relax the standards for the use of accredited certificates. The new regulations stipulate that the use of e-authentication shall not be obligatory for financial transactions to which it is difficult to apply e-authentication. The most significant change to this amendment is in Article 7, which allows the use of authentication methods of equivalent security levels as well as e-authentication and stipulates that the evaluation of security levels should be carried out by the Evaluation Method Committee for Authentication Method, which is to be established under the Financial Supervisory Service.

In May 2013, the National Assembly initiated revisions of the Electronic Financial Transactions Act and Digital Signature Act to abolish the public certificate regulations and introduce various authentication methods. In March 2014, there was a problem with the regulation on official digital certificates at the Regulatory Reform Ministerial Conference

and Private Joint Regulatory Reform Review Conference. In April of that year, the Ministry of Science, ICT and Future Planning announced the establishment of the "2014 Future Regulatory Reform Implementation Plan," which was created to promote the development of e-authentication technology that does not require ActiveX, and stated its intention to launch full-scale regulatory reform. As of May 20, 2014, the FSS revised Article 4 of the Enforcement Regulations of the Electronic Financial Supervision Regulations and removed "credit and debit card payments and wire transfers of less than KRW 300,000" from the list of online transactions requiring e-authentication. As a consequence, the use of e-authentication became obligatory for only wire transfers involving amounts in excess of KRW 300,000. In July 2014, the government announced a strategy called the "Alternative Authentication Method for Payments of over KRW 300,000" and gave permission to the Payment Gateway (PG) company to save the card information of its users. On September 23 of the same year, the Financial Supervisory Service announced that it would simplify e-commerce settlement, develop e-authentication technology that does not require ActiveX, and adopt a simple payment service. The once controversial regulatory framework enforcing the use of e-authentication in electronic finance was abolished in March 2015. With its revision of the Electronic Financial Supervision Regulation on March 18, 2015, the FSS completely abolished mandatory e-authentication. Article 21 of the Electronic Financial Transactions Act, implemented on October 16, 2015, states, "The Financial Supervisory Service…shall not enforce the use of specific technologies or services and shall endeavor to promote fair competition between security and authentication technologies."

The designation of certification authorities was provided for in Article 4 of the Digital Signature Act. In 1999, when the law was enacted, the Ministry of Information and Communication was granted the authority to approve certification authorities, as it was deemed to be capable of certifying digital signatures securely and reliably. In the 2008 amendment of the same Act, the institution responsible for designating certification

authorities was changed from the Ministry of Information and Communication to the Ministry of the Interior (MOI). In the 2013 amendment, it was changed again to the Ministry of Science, ICT and Future Planning. Currently, the top executive organization is the Korea Internet and Security Agency (KISA), a quasi-government agency under the Ministry of Science, ICT and Future Planning. According to Article 8 of the Digital Signature Act, implemented on July 1, 1999, certification authorities should have their digital signature verification keys verified by KISA.[12] Article 8 of the Implementation Plan of the same Act, implemented July 1, 2001, states, "The designated certification authority shall have its digital signature verification key verified by KISA, pursuant to Article 52 of the Act on the Promotion of Information and Communication Network Utilization and Information Protection (abbreviation: Information and Communication Network Act)."[13] In accordance with the policy for the advancement of public institutions that was implemented in 2009, the Korea Information Security Agency (KISA), National Internet Development Agency of Korea (NIDA), and Korea ICT International Cooperation Agency (KIICA) were combined to form the Korea Internet and Security Agency (KISA), once again changing the top executive organization responsible for designating certification authorities.[14]

KISA Electronic Signature Verification Management Center is a nationally designated top executive organization of a certification authority. Article 25, Clause 1, of the Digital Signature Act, amended in 2001, states, "In order to create an environment in which

12. Article 8 of the Enforcement of the Digital Signature Act, July 1, 1999, states, "An authorized certification authority shall certify the electronic signature verification key from Korea Information Security Agency under Section 14-2 of the Informatization Promotion Basic Act before commencing the work on certification."

13. Article 52, Clause 1, of the Information and Communication Network Act, July 1, 2001, reads, "The government establishes the Korea Information Security Agency to efficiently implement the measures necessary for information security for the secure distribution of information."

14. Article 52, Clause 1, of the Information and Communication Network Act (revised on April 22, 2009, by the Korea Internet Promotion Agency): ① The Government shall take necessary measures to enhance the information communication network (excluding matters related to the construction, improvement and management of the information communication network) and establish Korea Internet and Security Agency (hereinafter referred to as "Internet Security Agency") to promote secure utilization of information communication network and facilitate globalization."

electronic signatures can be used safely and reliably, and to efficiently manage accredited certification authorities, the Management Center performs tasks related to the verification of the electronic signature verification key of certification authorities, the development and dissemination of electronic signature authentication technology, and other relevant tasks." The specific tasks of KISA are stipulated in Article 25, Clause 1, of the same Act.[15]

In 2000, the Korea Information Certificate Authority and KOSCOM were designated as the first two accredited certification authorities. By December 2008, six institutions had been designated as accredited certification authorities, but due to Article 9 (Transfer of Certification Services), Clause 2, of the Digital Signature Act, the National Information Society Agency (or NIA)'s responsibility for certification in the public sector was transferred to the Korea Information Certificate Authority on June 30, 2008. As a consequence, the Korea Information Certificate Authority, KOSCOM, Korea Fair Trade Commission (KFTC), Korea Electronic Certificate Authority, and Korea Trade Information Telecommunication Company were designated as the five authorized certification authorities (NIA, 2011). Under the authority of KISA, the top executive organization responsible for the designation of certification authorities, five accredited certification authorities are designated for each area of business, and each accredited certification authority receives authorization from KISA and provides authentication services to subscribers.

15. Article 25 of the Digital Signature Act (revised on Mar. 23, 2013) specifies the tasks of KISA as:

1. Under the designation of an accredited certification authority in accordance with the provisions of Article 4, KISA should assist in the examination of facilities and equipment of the accredited certification authority

2. Inspection support for accredited certification authorities under Article14, Clause 1

3. Examination of protection measures under Article 18, Clause 3, and technical support

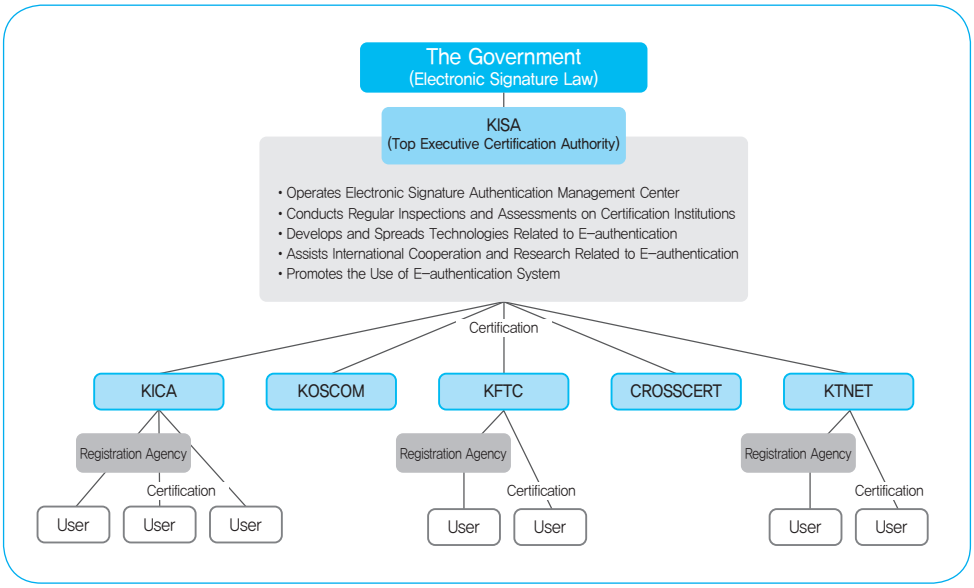
4. Inspection of safe operation of facilities and equipment under Article 19, Clause 2

5. Tasks related to certification such as issuing and managing official authentication for the accredited certification authorities

6. The research in the development, dissemination and standardization of technology related to electronic signature authentication

7. Research in electronic signature verification system and assistance in global cooperation, which includes mutual recognition of electronic signatures

Figure 3-1 | The Process of E-Authentication



Source: KISA (Date accessed: 2016.06).

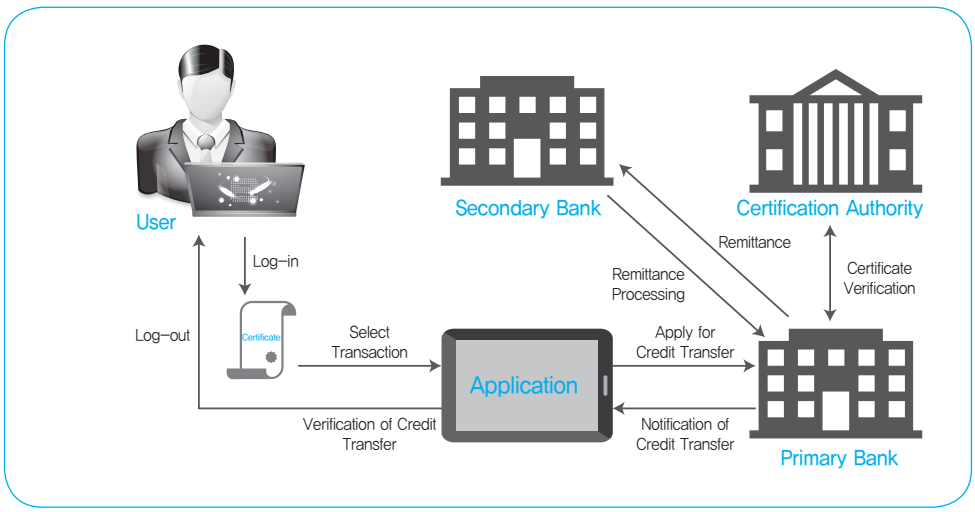
Table 3-1 | The Designation Date of Institutions

Institution	Date	Main Area	Category
KICA	February 2002	E-Commerce	Corporation
KOSCOM	February 2002	Online Securities	Corporation
KFTC	April 2000	Internet Banking	Non-profit Organization
CROSSCERT	November 2001	E-Commerce	Corporation
KTNET	March 2002	Online Trade	Corporation

1.3. Details

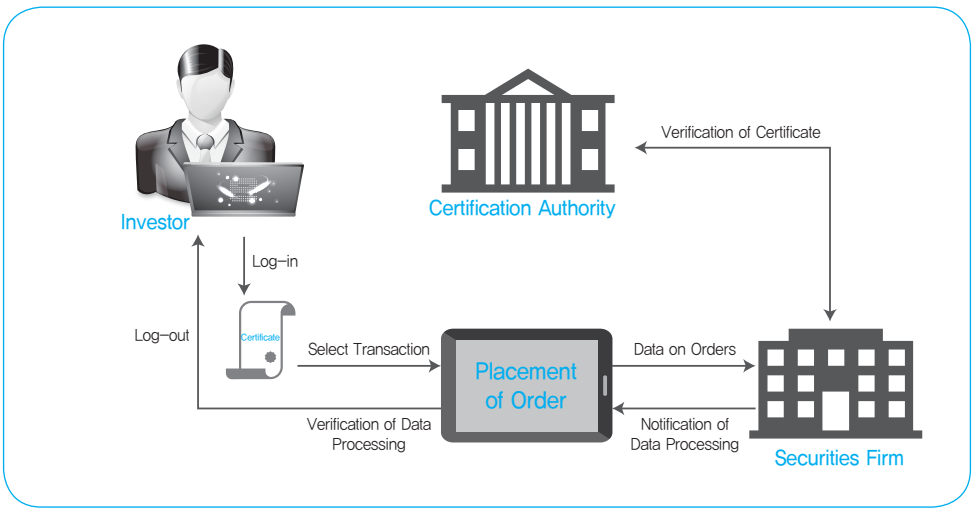
By using official digital certificates, users can safely manage various tasks, such as bank transfers, remittances, and issuances of loans through Internet banking without visiting a bank in person. Regarding online securities trading, it is possible for securities companies to use e-authentication to securely confirm the identities of investors even without receiving any calls or visits from said investors directly.

Figure 3-2 | The Flow of E-Authentication Using Banks



Source: KISA.

Figure 3-3 | The Flow of E-Authentication Using Securities Firms



Source: KISA.

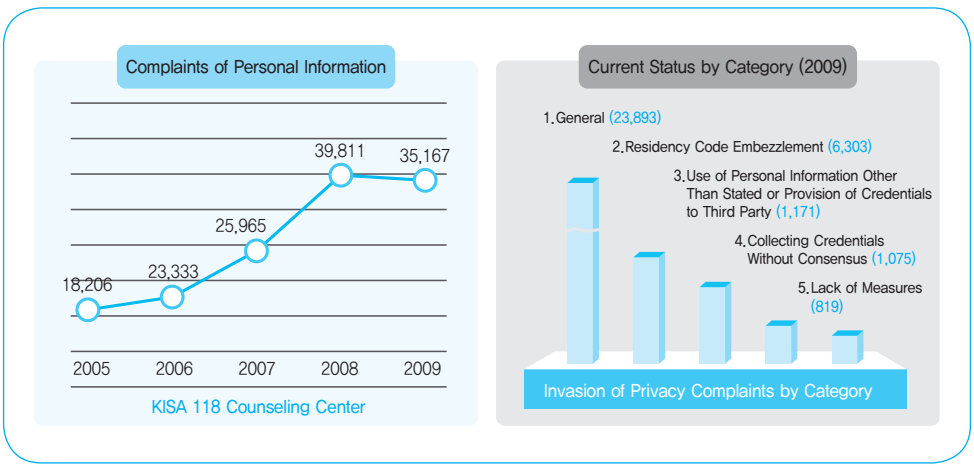
2. Other Policies on Authentication

2.1. I-Pin and My-Pin

As it contains personal information, such as age, sex, and place of birth, the resident registration number on the national ID card uniquely identifies individuals. However, it is difficult to change this number, for reasons such as identity theft, because it remains the same throughout an individual's lifetime (KISA, 2010). In fact, the number of cases of invasion of privacy has increased due to the inherent weakness of the resident registration number system. According to the number of complaints received by the Korea Information Security Agency (KISA), the number of cases of illegal use of residency registration numbers rose from 9,810 in 2005 to 10,835 in 2006 (KCC, 2007). In addition, complaints regarding the misuse of personal information have increased steadily since 2005, reaching a total of

39,000 complaints in 2008. By complaint type, those concerning infringements of personal information and invasions of privacy were the highest, at 23,893 cases, followed by 6,303 cases of identity theft (KISA, 2010). Under such circumstance, the call for plausible means to replace the resident registration number was reinforced.

Figure 3-4 | The Increase in Complaints of Personal Information



Source: KISA 2010.

In 2008, the ROK government passed legislation designed to provide a means for e-commerce companies to become members without using a resident registration number. In Article 23-2 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc., the KCC stipulates, "A provider of any type of information and communications service that satisfies the criteria regarding the daily average number of users prescribed by Presidential Decree should be allowed to register as a member, even if said provider does not use the resident registration number," thereby making it legal for providers to become members without using the resident registration

number.[16] As a result, the Internet Personal Identification Number (or i-PIN), a personal verification code designed to replace the use of the resident registration number for online transactions so as to prevent infringements of personal information, was adopted. In other words, the i-PIN is "an Internet-based personal verification number with which users may identify themselves online in lieu of a resident registration number, which is vulnerable to fraudulent use as face-to-face confirmation is impossible" (KCC, 2007).

The i-PIN is a 13-digit number issued to a user after the identity verification organization has confirmed said user's identity. It consists of two numbers that contain information on the i-PIN issuer along with other random numbers. The i-PIN is classified into two categories: private and public. The private i-PIN is under the jurisdiction of the KCC, while the public i-PIN is under that of the MOI. In 2007, the i-PIN issuers were: NICE (Nice i-PIN), NICE Information Service (virtual residency code), Seoul Credit Rating & Information Inc. (Siren24 i-PIN), Korea Information Certificate Authority (OnePass), and Korea Electronic Certificate Authority (Green Button). In 2010, the i-PIN issuers were: NICE (Nice i-PIN), NICE Information Service (virtual residency code), Seoul Credit Rating & Information Inc.

16. According to Article 23-2, Clause 1, of the amended Enforcement Decree of the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc., "a person who meets the criteria prescribed by the Presidential Decree" is a person who falls under any of the following categories:

1. A provider of information and communications services as part of an Internet portal service (which provides services such as searches for other Internet addresses, information, email, online communities, etc.) that had an average of 50,000 or more users per day for three months immediately preceding the end of the previous year

2. A provider of information and communications services as part of an online game service (which provides game and gambling game services according to Article 2, Clause 1, and Clause 1, Subordinate Clause 2, of the Act on the Promotion of the Game Industry through information and communications networks) with average daily users of 10,000 or more

3. A provider of information and communications services as part of an e-commerce service (which provides electronic commerce and mail order services using information and communications networks pursuant to Article 2 (1) and (2) of the Consumer Protection Act in Industries Including E-Commerce) with average daily users of 10,000 or more.

4. A provider of information and communications services as part of any other services not mentioned above with an average daily number of users of 10,000 or more for the three months immediately preceding the end of the previous year.

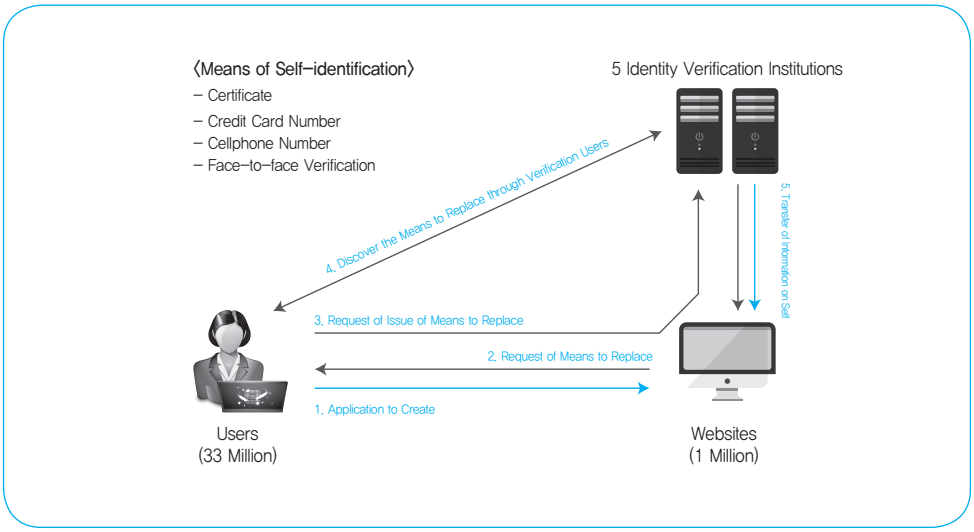
② The KCC must post on its website all relevant information, including the preparation period, period of application, and individuals who fall under each category of Clause 1, pursuant to Article 23-2 of the Act.

(Siren24 i-PIN), Korea Information Certificate Authority Inc. (SG i-PIN), and Korea Credit Bureau (KCB i-PIN). In 2015, the private i-PIN issuers were reduced to NICE Information Service, Seoul Credit Rating & Information Inc., and Korea Credit Bureau, while the public i-PIN was issued by public i-PIN centers.

Table 3-2 | The Comparison Between Existing Identity Verification Process and i-PIN

		Existing Identity Verification	i-PIN
User	The Process	• Input of residency registration code and name	• Input of residency registration code → identity verification → issue of id/pw
	Aspects on Convenience and Security	• Convenient as only the input of residency registration code is required; however, the concern is in the leak of personal information ('05 Survey illustrates such fact that 78% of internet users are concerned with providing residency registration code)	• The initial process of issuing i-PIN might be inconvenient due to its complexity; however, user can verify his or her identity only with id/pw • Strengthens protection of personal information as residency registration code cannot be retrieved
Business Operator	Identity Verification	• Verifies residency registration code provided by the user through verification institutions (3 institutions for credit evaluation)	• Verifies user through verification institutions (3 institutions for credit evaluation and 2 certification authorities)
	Contained Information	• Residency registration code of user	• Information on user consists of 13 random numbers, information on duplicate account, the age of user

Figure 3-5 | Verification of i-PIN



Source: KCC 2006.

However, i-PINs issued through such issuance procedures have caused problems for users due to the different procedures used by each issuer. To address this, the government adopted iPIN 2.0 in an effort to unify the i-PIN issuance procedures and resolve any inconveniences experienced by users. i-PIN 2.0 contains "Connecting Information" (CI; a verification code issued by personal verification institutions for service connection) that allows the uniform use of online services, such as reward points and cyber money. In this way, users can use the reward points they accumulate online in the physical world, and vice versa (KISA, 2010).

In response to the illegal issuance and use of 750 million public i-PINs in March 2015, the government implemented i-PIN safety measures (KCC, 2015). In addition, the government adopted a secondary authentication process, and made its use mandatory, to complement the primary authentication process, which involves entering a password. This authentication method allows each issuer to decide the security means they will use, while mandating

that each issuer provide various means of authentication, such as OTPs, QR codes, and secondary passwords, to prevent the exclusion of any user. Furthermore, the government obligated issuers to reinforce password management by having them issue suggestions to their users to change their passwords every three months and make it mandatory for users to change their passwords every year. The government also forced issuers to separately manage i-PINs that have been in disuse for more than one year and assist users in conducting a self-identification process to reactivate such i-PINs. In addition, the government made it mandatory for issuers to have regular pop-ups that contain a list of steps for users to follow to prevent any of the problems related to i-PINs mentioned above.

In 2016, the KCC announced the Measures to Improve the Security and Utilization of Private i-PIN. In April of the same year, i-PIN security enhancement measures were implemented in the aftermath of public i-PIN scandals, including the illegal trade and use of i-PINs, which occurred in March of the previous year. However, public i-PINs were still vulnerable to illegal transactions and theft. As i-PIN uses an ID/PW method that relies heavily on users' memory, it is vulnerable to leakages of personal information or malicious use due to user carelessness. Since 2013, private i-PIN issuance has been increasing at a steady rate of 10.8 percent, but the number of i-PINs in use decreased from 3.1 million in the first quarter of 2015 to 1.6 million in the second quarter, marking a 50-percent decrease. Three stages have been improved in relation to the i-PIN system: issuance, utilization, and management. In the issuance stage, identification was strengthened to prevent the illegal issuance of private i-PINs. In addition, persons under the age of 14 were obligated to be accompanied by a guardian to the identity verification agency and required a guardian's consent when acquiring a private i-PIN. If this procedure was done online, the public i-PIN issuance website would have protocols to follow. In the utilization stage, the government adopted diverse additional means of verification, such as mobile-app-based verification. In

addition, in order to diversify the means of verification, the government made it mandatory for issuers to develop and disseminate additional means of authentication besides IDs and passwords, such as biometric information and pattern locks. In the management stage, the government adopted measures to prevent the illegal trade and use of private i-PINs. It also implemented i-PIN expiration dates, created the "e-privacy clean service" (www.eprivacy.go.kr), through which users could see their i-PIN transaction histories, and reinforced i-PIN issuer supervision.

Moreover, the issuance of i-PINs by the NICE Information Service, Seoul Credit Rating & Information Inc., and Korea Credit Bureau based on the resident registration number became a controversial issue among security experts, prompting the government to seek out solutions (MOI, 2014). Also, in January 2014, the government decided to use other means of identity verification besides the resident registration number in order to mitigate anxiety over the use of resident registration numbers.[17] First, the collection of resident registration numbers was banned under Article 24-2 of the Personal Information Protection Law, enacted on August 7, 2014.[18] To resolve the issues arising due to the implementation of this measure, the government adopted My-PIN as an offline means of identity verification. A means of identity verification designed for everyday use, My-PIN consists of 13 random numbers that do not incorporate any personal identification information and is under the jurisdiction of the MOI.

17. On January 18, 2014, it was revealed that the KB Kookmin Card, NH Nonghyup Card, and Lotte Card companies had suffered leakages of customers' personal information. The story broke on January 18, but the leakages had occurred from October 2012 to December 2013, and the number of outflows was the highest ever (104 million).

18. The Act on Promotion of Information and Communication Network Utilization and Information Protection, Etc. states the following:

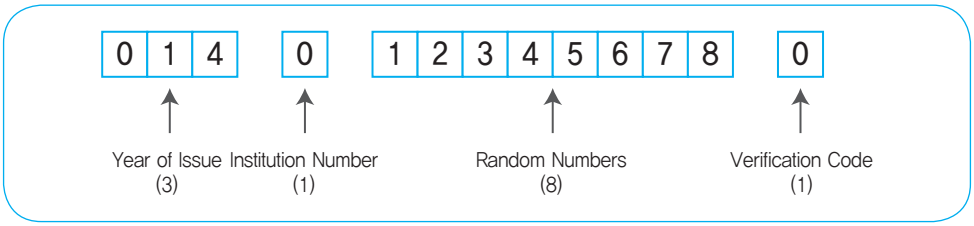
Article 23-2, Clause 1 (The Limited Use of Residency Registration Code) A provider of information communication service cannot collect user's residency registration code unless he or she falls in the categories listed below:

① designated as identity verification authority pursuant to Section23-3

② legally allowed to collect and use the resident registration code of the user

③ classified by KCC as the provider of information and communication service who cannot help but to collect and use the residency registration code of the user for business purposes

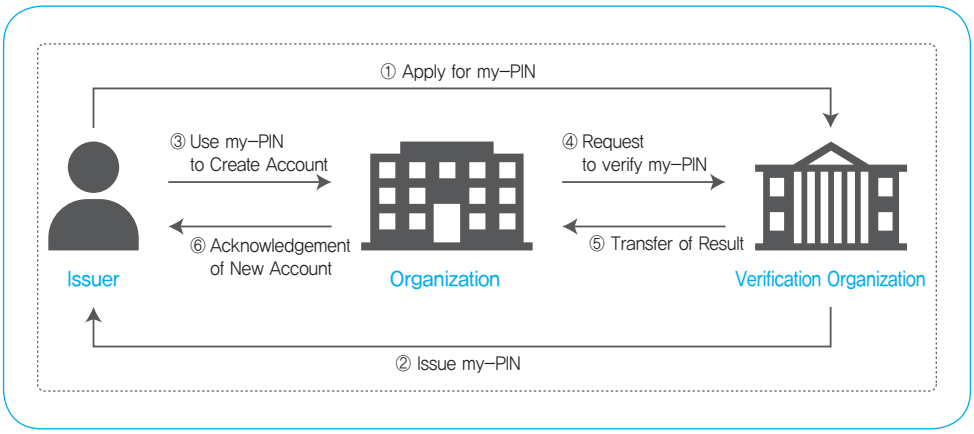
Figure 3-6 | The Pattern of my-PIN



Source: http://www.privacy.go.kr/.

Anyone who wishes to have a My-PIN number can apply for one on the website of the identity verification agency. As an individual inputs the 13 random numbers of their issued My-PIN to register for membership with the My-Pin issuer, the My-PIN issuer submits a request for a My-Pin number with the identity verification agency. The issuer then receives a My-PIN number from the agency and completes the identify verification process. When the resident registration numbers were used, the numbers were stored on individual systems, increasing the risks of loss and theft. My-PIN, however, reduces such risk, as it does not involve the use of resident registration numbers and can be changed when needed. Moreover, the identity verification agency encodes the My-PIN information to prevent redundancy in registration. Decoding My-PIN is extremely difficult, which makes it a highly secure means of protecting personal information.

Figure 3-7 | My-PIN Verification



Source: KCB.

Table 3-3 | The Comparison Among Residency Registration Code, i-PIN, and my-PIN

Classification	Residency Registration Code	i-PIN	My-PIN
Pattern in Numbers	Date of birth, gender, region of birth, application number, verification code	Institution number, random numbers (including letters)	Year of issuance, institution number, random numbers, verification code
Possibility of Change	Very difficult	At disposal	Possible
Issuance Method	Through registering at the Community Center	i-PIN homepage, Community Center	i-PIN homepage, Community Center
Areas of Use	Online & Offline	Online	Offline
Method of Use	Residency Registration Code (or the actual residency card)	User ID, password	My-PIN
Mandatory vs. Voluntary	Mandatory	Voluntary	Voluntary

Source: http://www.privacy.go.kr/.

2.2. OTP

The proportion of the population using Internet banking services rose from 8.8 percent in 2001 to 31.6 percent in 2005, a four-fold increase over a five-year period. By the end of 2005, the number of registered customers had increased to 27 million, recording a 50-percent increase. This growth, however, came with an increased risk of hacking targeting Internet banking services (Paik, 2006). The several cyber-attacks that occurred, targeting domestic Internet banks, despite security measures such as security cards and certificates, were a wake-up call for Koreans, showing that anyone could be a victim of such cybercrimes. Since then, the banks and supervisory office have developed measures to strengthen the security of electronic financial transactions. Since 2004, the majority of domestic electronic financial accidents have been the result largely of leakages of personal information through Internet banking and telebanking services, as shown in <Table 3-4>.

Table 3-4 | The Current Status of Accidents in Domestic Electronic Finance

(Unit: number of cases, million won)

Classification	2002	2003	2004	2005
Internet Banking	1(71)	-	1(3)	2(67)
Telebanking	-	1(10)	5(162)	5(186)
Duplicate Card	4(452)	6(66)	6(26)	-
Total	5(523)	7(76)	12(191)	7(253)

Note: 1. 2005 data shows up to July.
2. () refers to the amount.

Source: FSS.

The FSS introduced the One-Time Password (or OTP) in Internet banking and telebanking in 2005 to strengthen security. OTP is an authentication technology that increases the security of electronic transactions by creating a unique password for each transaction that can be used only once (Kim, 2014). To introduce OTP, the OTP Integrated Certification Center was established at the Financial Security Research Institute in June 2007, and the OTP service was transferred to the KFTC upon the launch of the Financial Security Service in April 2015.

General passwords are unreliable, as they remain fixed until the user changes them, making them vulnerable to the risk of exposure over time. OTP overcomes this drawback of general passwords. Once an OTP is created and used, it cannot be used again, making OTPs highly secure. However, the application of OTPs to transactions is a burden that users and banks must manage. As OTP is applied via a two-factor authentication method, users must use more than two authentication factors for every financial transaction. The FSS sought to minimize the damage caused by electronic financial accidents due to security flaws in authentication means by setting users' security levels differently depending on which authentication means is used and differentiating the transaction amount.

Table 3-5 | The Transaction Amounts for Each Security Rating

(Unit: ten million won)

Security Rating	The Means of Verification	The Limit of Amount per Transaction	
		Internet Banking	Telebanking
1st	- OTP or E-Authentication (HSM method) + Security Card	10(50)	5(25)
2nd	- Security Card + Notification of Transaction via Cellphone (3M3)	5(25)	2(10)
3rd	- Security Card	1(5)	1(5)

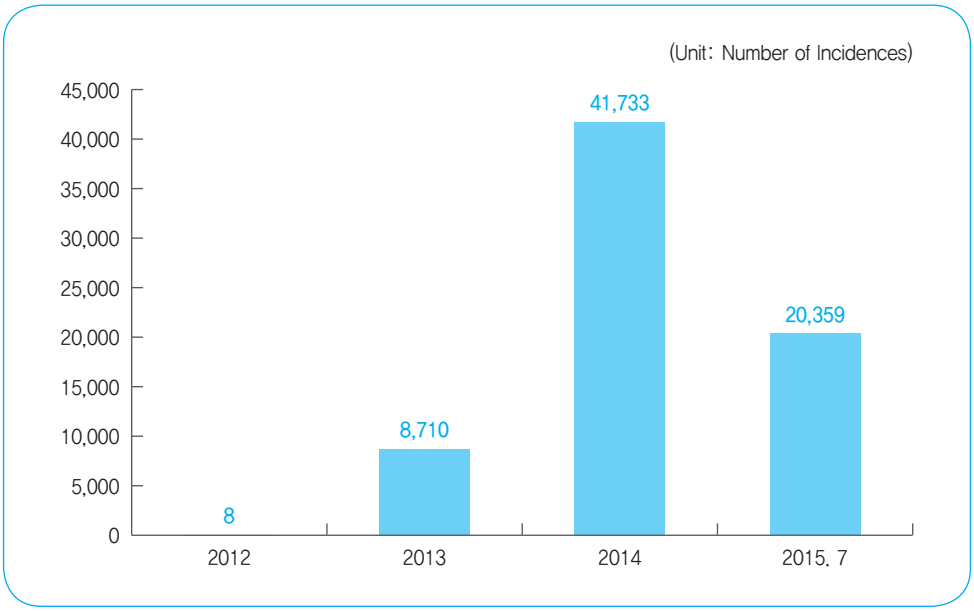
Note: ( ) refers to the limited amounts of transaction per day.

3. Evaluation

In March 2015, the highly controversial system that forced the use of e-authentication in electronic finance was abolished with the FSS' complete elimination of the mandatory certification from the Electronic Financial Supervision Regulation, revised on March 18, 2015. E-authentication, which was introduced with the enactment of the Digital Signature Act in July 1999, was instituted rapidly in the early 2000s with the establishment of the accredited certification system and introduction of a decree that made the use of accredited digital certificates for electronic financial transactions mandatory. In January 2003, six certification authorities agreed to integrate all electronic signatures under one single authentication system. In September 2002 and March 2003, e-authentication was applied to Internet banking and online stock exchanges, accelerating the spread of e-authentication. Currently, e-authentication is widely used in domestic Internet banking, e-commerce transactions, government procurement, e-bidding, online securities trading, and electronic trade and customs clearance.

The reason the FSS abolished the regulation requiring the use of e-authentication for electronic financial transactions was the intense criticism of the policy resulting from the protracted controversy over the convenience and safety of e-authentication over the previous 10 years. During that time, e-authentication technology relied heavily on ActiveX, which is highly vulnerable to security risks and widely believed to be hindering efforts to increase the compatibility of Web browsers. The ActiveX software is stored in a specific folder on users' hard disks, making it highly vulnerable to hacking and cyber-attacks. Although e-authentication technology is not based on ActiveX, most domestic financial institutions use ActiveX to provide e-authentication services. Once ActiveX is installed on a user's PC, it can run on arbitrary websites, allowing others to access the user's system resources without any security restrictions. Although KISA has not made any official announcements on this issue, the number of authorized certificate outflows increased from 8 in 2012 to 8,710 in 2013, and further to 41,733 in 2014. The total number of outflows from January to July of 2015 was 20,359.

Figure 3-8 | The Leak in E-Authentication Certificates



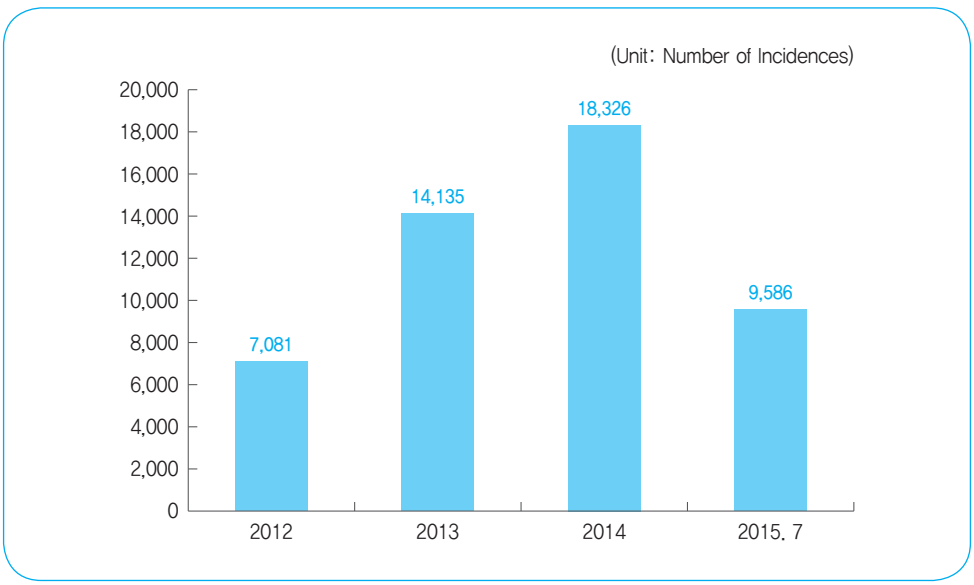
Note: 2015 data goes up to July only.

Source: Moon 2015.

The FSS acknowledged the inconvenience of the certificate but insisted on its use, arguing that there was no reasonable alternative. It claimed that, although the other authentication schemes that had been suggested as alternatives to public certificates offered security measures, such as confidentiality, integrity, and authentication, they were ineffective at preventing non-repudiation. However, some have questioned the strength of the anti-repudiation function of the current system. In other words, if certificates are never lost, the anti-repudiation function of the system is said to be strong, but if certificates are leaked or lost through cyber-attacks such as hacking or pharming, then the function is said to be weak, giving rise to problems. Although KISA does not collect such statistics, according to websites on the issue of pharming, the number of pharming victims has been increasing annually, from 7,018 cases in 2012 to 14,135 cases in 2013, 18,326 cases in 2014, and 9,586 cases as of July 2015. Like a seal, an official certificate is a powerful means of identifying a person, for which consumers bear the responsibility of custody. A public

certificate, therefore, provides strong security for a service provider, such as a financial company or e-commerce company. However, as the consumer is responsible for the custody of the certificate, there is still a risk of the certificate being hacked or lost due to consumer negligence.

Figure 3-9 | The Number of Incidences in Pharming

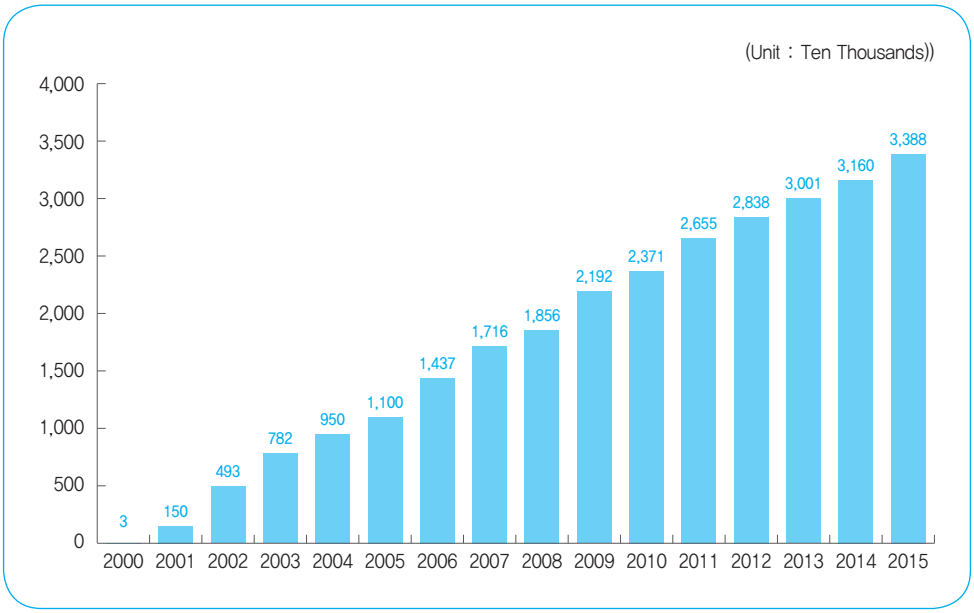


Note: 2015 data goes up to July only.

Source: Lee 2015.

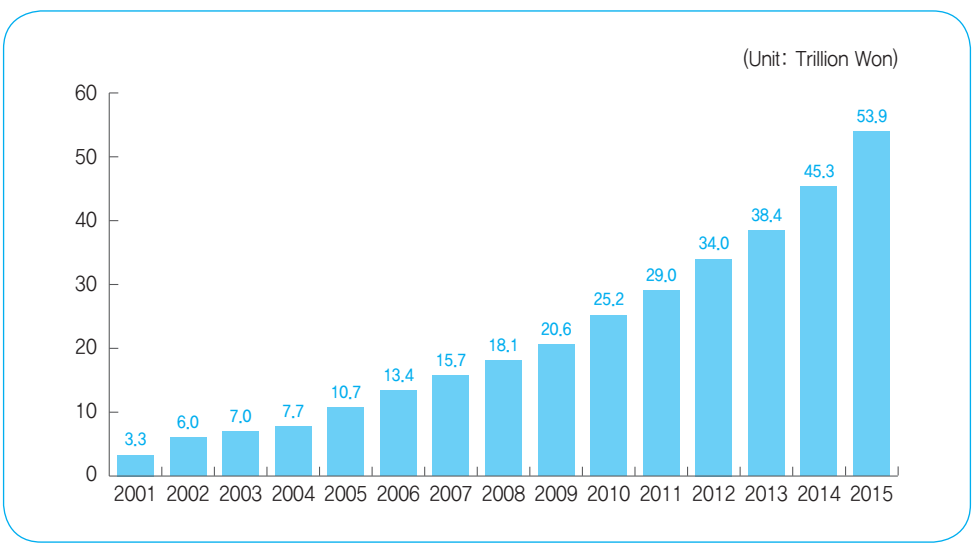
Certified authentication has contributed to the growth and development of e-commerce in the ROK. However, considering prior experiences with the enforcement of the use of accredited certificates in electronic finance, it is widely believed that the accredited certificate system should be removed completely from the Digital Signature Act. The e-authentication system, which was created to ensure the security and reliability of digital signatures, was based on the Digital Signature Act, implemented in July 1999, and has played a major role in expanding e-commerce in the ROK.

Figure 3-10 | The Trend of E-Authentication Users



Source: NIS Korea 2015.

Figure 3-11 | The Trend of Online Shopping Transactions



Source: KOSIS (Date accessed: 2016.08.26).

However, as the leakage of accredited certificates is increasing rapidly, consumer harm is expected to increase accordingly, and the security and reliability of such certificates will become increasingly difficult to guarantee. Moreover, very few advanced countries today have a nationally recognized electronic certification system. If the certification authority system were to remain, it is highly possible to encounter the violation of "technology neutrality" by giving the exclusive rights to the authentication technology issued by these organizations. Technology neutrality excludes the forced use of a specific technology so as to prevent the expansion of e-commerce from being dependent on a specific technology. This principle also aims to eliminate the need for additional legislative work in the implementation of new, advanced technologies, especially considering the rapid development of e-commerce technologies today.

The effectiveness of the i-PIN and My-PIN systems is also questionable. The problem is the inconveniences caused by the complex authentication procedures involved in the issuance of i-PIN and My-PIN numbers. i-PIN has been largely neglected by users due to its complicated authentication procedure, and the penetration rate of My-PIN is quite low. In order to receive a My-PIN number, users must first acquire an i-PIN number and go through the difficult process of installing additional software in order to verify their identity. As a result, i-PIN and My-PIN are not frequently used. The penetration rate of public i-PIN decreased consistently from just before 2011 to May 2015. As smartphone-based verification processes are capable of replacing i-PIN and other more convenient verification technologies exist as well, the penetration rates of i-PIN and My-PIN are expected to continue falling.

Table 3-6 | The Current Status of Use of i-PIN

Types	Total	Before 2011	2012	2013	2014	May 2015
The Number of Propagation	13,474	7,108	5,247	793	258	68
The Number of Issuance	5,049,990	1,061,173	617,179	892,771	1,525,888	952,979
The Number of Use	21,706,339	3,405,252	2,861,372	4,074,570	6,339,545	5,025,600

Source: BAI of Korea (2015).

There are also some problems with OTPs in terms of security, and more advanced technologies are currently being developed. OTPs have been assessed as secure against voice phishing and pharming, since the password is constantly changing; however, a case of pharming was reported recently. The potential exists for criminals to target OTPs, because they can be used to access banking, securities, insurance, and other financial institutions as well as game sites. There is also some doubt concerning the efficiency of the OTP Integrated Certification Center in terms of information processing. Through the Integrated Authentication Center, OTP integrated authentication requires user information to determine whether the OTP user is a legitimate customer of the bank, giving rise to a debate over whether the Center should possess such information (Paik, 2006). In the event of a failure of the Integrated Authentication Center, OTP authentication is prohibited at all banks, which carries more risk than OTP authentication offered by individual banks. There is also the problem of responsibility. In the event of a problem in an OTP-based electronic financial transaction, it is very difficult to determine where the problem originated if the institution that originally issued the OTP token is different from the bank at which the actual electronic financial transaction occurred.

The government of the ROK has implemented policies to certify e-authentication through certification policies. These policies are believed to have played a crucial role in the expansion of e-commerce in the early 2000s, when the government began ensuring the credibility of e-authentication. Nevertheless, the Korean government has enforced the use of specific technologies, such as PKI and OTP, through its e-authentication policy. There have been several negative impacts of this policy: it discouraged the development of new technologies, transferred the risks of financial accidents to consumers, and created a weak security environment by establishing an e-authentication system heavily reliant on ActiveX. If they were not forced to use e-authentication, finance companies would be able to choose from among various other verification methods, and consumers would choose other finance companies if they found e-authentication to be inconvenient. The major problem with the e-authentication policy of the ROK is the enforcement of specific technologies, which has the potential to impede the development of technology and the industry in general. If the standardization of a specific technology is carried out by a state, the benefits of standardization can be increased through the network effect. Nonetheless, the development of rapidly advancing technology might not be commercialized and become inferior, hindering economic development and technological advancement. Therefore, the governments of developing countries should limit their interference in e-commerce, and have the private sector lead the expansion of their e-commerce industries instead. Moreover, as the cases of i-PIN and My-PIN have shown, the government will also need to focus on consumer convenience.

Chapter 4

Consumer Protection Policy in the Republic of Korea

1. Importance of Consumer Protection in E-Commerce
2. Consumer Protection Laws in the Republic of Korea
3. Act on the Consumer Protection in Electronic Commerce, ETC.

Consumer Protection Policy in the Republic of Korea

1. Importance of Consumer Protection in E-Commerce

E-commerce, which emerged along with the development of the information and technology industry in the late 20th century, has rapidly expanded to become a major mode of transactions between buyers and sellers. As e-commerce uses the Internet as a buyer-seller transaction platform, it is free of both temporal and spatial constraints and has promoted the emergence of new markets and business opportunities, facilitating its expansion throughout diverse industries. However, this incredible advancement of e-commerce has given rise to various issues concerning consumer protection, due to the fact that it involves only non-face-to-face transactions between consumers and producers. Therefore, it will be impossible to maintain the growth of the e-commerce industry if no appropriate consumer protection measures are put in place. From the perspective of consumers, non-face-to-face transactions and the automatic purchase order system make it difficult to identify reliable suppliers, prevent buyers from verifying the merchandise before making purchases, and force consumers to make purchase decisions based solely on the advertisements and/or

commercials posted by sellers. In addition, the leakages of consumers' personal information, incompetency, limitations of programming languages, nascent legislation, complex contract procedures, inconvenient modes of payment, and various disputes and resolutions have manifested the importance of consumer protection measures. Furthermore, as e-commerce is expanding into the realms of mobile phones and television, violations of consumer rights have been occurring with greater frequency.[19]

Within e-commerce, consumer protection measures can be adopted in various ways; however, such measures can only be implemented through regulations. In 1999, the ROK government enacted the Electronic Commerce Act, and in 2002, it enacted the Act on the Consumer Protection in Electronic Commerce, ETC. to promote consumer protection. The Electronic Commerce Act regulates specific aspects of consumer protection in e-commerce. It was first enacted as a means of addressing basic legal issues related to e-commerce, but was revised several times to incorporate measures on consumer protection.[20] Today, despite the ROK government's attempts to protect consumers and stimulate the industry through the establishment of a well-functioning legal system, constant legislative revisions are required to enforce consumer protection measures.

19. According to the Korea Consumer Agency (2010), consumer damages are comprised of livelihood, physical, property, and mental damages caused by flaws or defects in goods or defaults or illegal acts faced by consumers in the process of using goods or services purchased from a business operator. These consumer damages, comprising livelihood, physical, property, and mental damages incurred in the process of using goods or services purchased from a business operator, are clearly distinguished from consumer complaints. Consumer complaints arise after the use of purchased goods and concern the utility of purchased goods or services or after-sales services provided by the business operator not meeting the reasonable expectations of consumers.

20. The Electronic Commerce Act aims to resolve general legal issues associated with e-commerce, while the E-Commerce Consumer Protection Law serves to protect consumers engaging in e-commerce or mail order transactions. The clauses related to consumer protection in the Electronic Commerce Act when it was first enacted were extended through subsequent revisions. The provisions of the Electronic Commerce Act in relation to consumer protection concern e-commerce in general, but the Electronic Commerce Consumer Protection Act specifically addresses consumer protection. The Electronic Commerce Act focuses mainly on e-commerce and online vendors, while the Electronic Commerce Consumer Protection Act addresses e-commerce and mail order transactions as well as sellers operating online and through mail order.

2. Consumer Protection Laws in the Republic of Korea

2.1. Consumer Basic Law

2.1.1. Background

In the Republic of Korea, laws concerning consumer protection have developed in line with the emergence of various issues and economic growth. The first law related to consumer protection in the ROK was the Quality Management Act for Manufactured Goods, enacted in 1967. The purpose of this law was to protect consumers and increase the quality of manufactured goods in line with the expanded production of manufactured goods with economic growth. In the mid-1970s, the negative externalities of monopoly and inflation became social issues. As a result, the government enacted the Stabilization of Inflation and Fair Trade Regulations in 1975, followed by the Act on Stabilization of Agricultural Prices in 1976, which aimed to promote the stabilization of the prices of agricultural goods, thereby protecting consumers' interests.

First enacted in 1980, the Act on Consumer Protection sought, first and foremost, to protect consumers. Furthermore, the legislation, which was revised on August 27, 1980, incorporated the Consumer Protection Clause (Clause 125) to provide a legal foundation for the protection of consumers.[21] In order to build the foundation for an efficient regulatory consumer protection system, the government established the Korea Consumer Agency in 1987, following an amendment to the Act on Consumer Protection in 1986.[22] As a consequence, consumer protection policies were created by the Consumer Policy

21. Although this provision ensures the "consumer protection movement," it is significant in that it could be seen as forming the constitutional basis for basic consumer rights. In the 1987 amendment, Article 124 of the Act was revised to stipulate that "the State shall guarantee the consumer protection movement to promote sound consumer behavior and improve the quality of its products by law."

22. The Consumer Protection Law (1986) consists of seven chapters: Chapter 1, General Provisions; Chapter 2: Obligations of State and Local Governments; Chapter 3: Obligations of Business Operators; Chapter 4: Consumer Protection Agencies; Chapter 5: Consumer Policy Deliberation Committee; Chapter 6: Korea Consumer Agency (Section 1: Establishment, Section 2: Officers and Board of Directors, Section 3: Consumer Dispute Resolution Committee, Section 4: Damage Relief, Section 5: Accounting, Audit, Etc.), and Chapter 7: Penalties.

Promotion Agency under the Economic Planning Agency, but the enforcement of those policies was the responsibility of the Korea Consumer Agency, which is not only a policy research institute but an organization that seeks to reduce consumer harm (Seo, 2010). Act on Consumer Protection Law, which was revised in 1986, provides for basic consumer rights, the establishment of regulations for the foundation of consumer agencies, and so on. In addition, measures for consumer loss compensation and the formation of a dispute resolution committee, governed by the Korea Consumer Agency, were adopted. As a result, a three-step system—comprising consultations, compensation for consumers' losses, and dispute resolution—was established. In essence, the Act on Consumer Protection, enacted in 1986, and the Korea Consumer Agency, which was established to enforce the Act, facilitated the installation of the Consumer Basic Law of the ROK and related legal administrative procedures.

The Act on Consumer Protection underwent a comprehensive revision in 2006 and was renamed the Consumer Basic Law. The main purpose of the revision was to clearly define the purpose of the law and make changes to policy administration agencies. In the Consumer Basic Law, the purpose of the law was changed from "the protection of basic consumer rights" to "the increment of consumer welfare" (Article 1 of the Consumer Basic Law);[23] the governing organization, the Economic Planning Agency (or Finance Economy Department), was renamed as the Free Trade Committee (Article 21 of the Consumer Basic Law); and the Korea Consumer Protection Agency was renamed as the Korea Consumer Agency. Through this revision, "the obligation of the consumer," which responds to consumers' basic rights, was newly appended. Although the regulation related to "the role of the consumer" (Article 4) already existed in the original version of the Act on Consumer Protection, it was amended by including a clause related to the increment of consumer welfare in the purpose of the legislation, thereby clearly stating that consumers themselves

23. Article 1 of the Consumer Basic Law states, "To promote the interests of consumers, it is necessary to define the relationship between consumers and sellers in terms of consumer rights and obligations, the obligations of state and local governments and sellers, and the role of consumer agencies in order to contribute to the improvement of consumers' quality of life and the development of the national economy by stipulating the basic matters for comprehensive promotion of the policy."

also bear some responsibility. There was also was a transition in the policy system for the promotion of consumer protection. The Consumer Policy Committee (Clause 23), which assesses consumer policies, was established and tasked with proposing consumer policy plans every three years and submitting plans for the implementation of such policies annually. The central and local governments put the Korea Consumer Agency and other consumer protection agencies under the jurisdiction of the Fair Trade Commission to reinforce the Commission's consumer policies; established protective measures for children, the elderly, and people with disabilities to strengthen consumer safety (Article 45); and mandated the Ministry of Strategy and Finance to establish basic regulations granting the Ministry the right to take measures concerning relevant central administrative agencies (Article 46) as well as the Consumer Safety Center, under the Korea Consumer Agency, to collect and analyze relevant information (Articles 51 and 52). In addition, it adopted new measures, including a collective dispute resolution system (alternative dispute resolution system) and collective consumer action, to mitigate consumer harm.[24]

2.1.2. Main Contents

Article 4 of the Consumer Basic Law stipulates that the basic rights of consumers are: the right to be protected from risks to livelihood, body, or property posed by goods or services (hereinafter referred to as "goods, etc.") (Clause 1); the right to receive essential information on goods, etc. (Clause 2); the right to choose the transaction counterparty, place of purchase, and price and terms of the transaction (Clause 3); the right to reflect one's opinion on the consumer policies of the central and local governments and business activities of business

24. The collective dispute resolution system (alternative dispute resolution system) aims to create an exception to the existing dispute resolution system (Section 68), which enables small-scale disputes involving minor damages to be settled in the same or a similar way as disputes involving more than 50 consumers. On the other hand, the consumer collective action system allows consumer or business groups that meet certain requirements to file collective lawsuits concerning damages inflicted by business operators on consumers' livelihoods, bodies, or properties. This is one of the most notable provisions of the Consumer Basic Law enacted in 2006. For more details, refer to Ko (2010).

operators (Clause 4); and the right to receive prompt and fair compensation for damages caused by the use of goods, etc. (Clause 5). Other rights include the right to receive proper education for satisfactory consumption (Clause 6), the right to organize and be an active participant of organizations that serve to increase consumer welfare (Clause 7), and the right to consume under a secure and pleasant environment for consumption (Clause 8).

The Consumer Basic Law defines the role of the state in protecting consumers and preventing consumer harm. Article 8 states that the state should set standards concerning the composition, content, and structure of goods and services by which business operators should abide in order to prevent consumer harm. Article 46 grants jurisdiction over consumer safety affairs to the chairman of the Fair Trade Committee.[25] Article 12, Clause 1, of the Consumer Basic Law imposes on the state the obligation to implement necessary measures for preventing unfair transactions causing consumer harm, while Article 12, Clause 2, bestows on the state the responsibility to define and declare the actions of vendors that are believed to inflict harm on consumers. Article 12, Clause 3, of the Consumer Basic Law also imposes on the state the obligation to take all measures necessary to protect the interests of consumers in special types of transactions, such as transactions following provisions, door-to-door sales, sales on installment, mail order transactions, and electronic transactions.

The Consumer Basic Law also includes a regulation that holds the state responsible for addressing the issue of illegal advertising. The state must provide standards for labels so as to prevent consumers from choosing the wrong products or misusing products due to the obscurity of the labels or packaging (Article 10), firmly request that business entities abide by the standards (Article 20), and permit consumer agencies to file collective lawsuits against

25. In cases where business operators violate the safety measures set forth in other laws and regulations, causing potential harm to consumers, the Fair Trade Commission may request that the head of the relevant central administrative agency take measures pursuant to other laws and regulations (Clause 1). In cases where such other laws and regulations have not established safety standards or criteria, however, the Fair Trade Commission may request that or directly order the head of the relevant central administrative agency institute a recall (Clause 2).

business entities in cases of violations of the standards.[26] In order to ensure that consumers are able to make purchase decisions objectively, the central and local governments should take necessary measures to make sure consumers have access to such information as transaction terms and methods and product quality, safety, and environmental performance (Article 13, Clause 1). In cases where the degree of consumer harm is deemed to be severe, the head of the central administrative agency may order the business operators involved to take all actions necessary to ensure the safety of consumers through various measures, such as requesting information on said damages from the Consumer Safety Center (Article 50, Clause 1).

The Consumer Basic Law also specifies the provisions that concern the role of the state in the provision of relief for consumer damages, including counseling services for consumers and dispute resolution services. The central and local governments should devise necessary measures, such as the establishment of relevant organizations tasked with ensuring that consumer complaints and damages are promptly and fairly mediated (Article 16, Clause 1). In addition, to ensure that disputes among consumers and business operators are resolved smoothly, the state should establish "consumer dispute resolution standards" (Article 16, Clause 2), which will play a crucial role in resolving disputes among consumers and business operators unless any of the parties indicate otherwise (Article 16, Clause 3).

Article 19 of the Consumer Basic Law makes it mandatory for business operators to: take necessary measures to prevent harm to the livelihoods, bodies, or properties of consumers (Clause 1); not provide any terms or means of transaction for goods, etc. that could potentially harm consumers' choice or welfare (Clause 2); provide consumers with accurate and honest information on all goods, etc. (Clause 3); handle the personal credentials of consumers

26. There is a separate law that provides provisions for labels and advertisements called the Fairness in Labels and Advertisement Act. This Act prohibits business operators from using unauthorized labels and carrying out advertising activities that may provide misleading information to consumers (Article 3), commands the Fair Trade Commission to take appropriate measures, such as suspensions of the harmful activities related to unfair labeling or advertising by business operators (see Article 7 below), and imposes penalties of up to two years of imprisonment or fines of up to KRW 150 million on business operators (Article 17).

faithfully so as to prevent such credentials from being lost, stolen, leaked, altered, or damaged (Clause 4); and compensate consumers for any dissatisfaction or damages caused by defects in the goods, etc. provided as well as for any damages inflicted on consumers through actions such as default (Clause 5). However, the Consumer Basic Law does not regulate failures of duty on the part of business operators. It obligates business operators to collect products and provide information. When a business operator discovers a serious defect in the system, design, or label that could cause harm to the livelihood, body, or property of a consumer, the operator should report the details of the defect to the head of the central administrative agency under which it operates (Article 47) and take all necessary measures, including the collection, destruction, repair, exchange, or refund of the relevant goods, etc., or ban the production, import, sale, or provision of the relevant goods, etc. (Article 48).

2.2. Act on the Regulation of Terms and Conditions

2.2.1. Background

The terms of transaction is a contract prepared in advance by a party in a certain form in order to conclude a contract with multiple parties. The Act on the Regulation of Terms and Conditions prevents business operators from abusing their authority by writing and utilizing unfair terms of transaction, thereby protecting consumers and improving the lives of the people through the regulation of unfair transactions. Act on the Regulation of Terms and Conditions are provided by business operators before concluding a contract, although they are in a position superior to that of consumers in terms of professional knowledge and organizational and economic power. Therefore, due to the asymmetry of information, it is highly likely that the terms and conditions of transactions will be unfair to consumers. However, contracts with specific terms and conditions cannot be revised. As this type of

contract is often carried out in large quantities, the government should implement stricter measures to regulate it.Although regulating terms and conditions leads to restrictions of liberty, it is necessary for the government to do so in order to ensure that the potential side effects of such terms and conditions cause no harm to consumers.

Since the 1970s, the use of contracts has become standardized, in line with the country's economic growth. As a result, the regulation of contracts became the subject of intense discussions in the late 1970s, as corporations were frequently abusing their power to take advantage of consumers who lacked legal knowledge. In November 1985, the Terms and Conditions Regulation Committee was established, and in July 1986, new measures governing the regulation of the terms of transactions were submitted to the Economic Planning Board.[27] Written by the Terms and Conditions Regulation Committee, this legislation provided a framework for the current laws governing the terms and conditions of contracts. Act on the Regulation of Terms and Conditions Act was enacted on December 31, 1986, and implemented on July 1, 1987. The legal provisions of Act on the Regulation of Terms and Conditions Act at the time of its enactment were almost the same as those of the current law. Those that differ from the current law (Chang, 2006) are: the provision allowing the head of the Economic Planning Board to request business operators to alter their inoperative terms of contracts (Article 17), the provision granting the head of the Economic Planning Board the authority to request an examination of terms (Article 19), and the provision commanding the Economic Planning Board to establish a committee responsible for examining terms of contracts (between Articles 24 and 29). With Act on the Regulation of Terms and Conditions, business operators are now prevented from using their advantage in terms of knowledge when creating contracts to inflict damage on consumers and potential consumers (Chang, 2006).

27. According to Chang (2006), this constitution benchmarks the old Terms and Conditions Regulation Act of Germany and Unfair Contract Provision Act of the UK and draws from the Unfair Provision Committee of France and Market Court of Sweden.

2.2.2. Main Contents

Act on the Regulation of Terms and Conditions focuses on the fairness of contractual arrangements between business operators and customers by presenting the criteria for the inclusion, interpretation, and invalidation of the terms of contracts. The law prohibits the use of unfair contract clauses by business operators and requires the Fair Trade Commission, the supervising authority, to take corrective actions, such as recommending or ordering corrective actions, in cases where business operators use such clauses. In order to prevent the use of unfair terms and conditions, business operators may ask the Fair Trade Commission to examine whether the contents of their contracts are in violation of the law (Article 19-3, Clause 1). Consumer agencies and the Korea Consumer Agency, registered in accordance with the Consumer Basic Law, may request that the Fair Trade Commission enact or amend terms to serve as a standard for types of transactions in which consumer damages occur frequently (Article 19-3, Clause 2). In addition, the Fair Trade Commission may, if necessary, establish provisions for the amendment or revision of such standards and advise business operators and business agencies regarding legal violations (Article 19, Clause 3).

If, upon examination of the terms of a contract, the Fair Trade Commission finds that the provisions of the terms used by the business operator are unfair, it may invalidate the relevant terms and take appropriate actions. Such actions may comprise a corrective order issued to the business operator, a recommendation for correction issued to the relevant business operator or the Financial Supervisory Service, or a request for correction issued to the relevant administrative office. At the time this law was enacted, the public and judicial officers advocated that the validity of contracts falls under civil litigation; therefore, only non-legally binding measures were adopted. However, with the first amendment on December 8, 1992, entrusting the Fair Trade Commission with abstract content control,

some legally binding measures of corrective action were incorporated in order to enhance the effectiveness of the regulation. Since the call for changes in the conduct of business operators that are in violation of the law is only a recommendation, the regulation mandates the elimination and revision of unfair terms and conditions of contracts and is not legally binding (Article 17-2, Clause 1).

When the Fair Trade Commission recommends or orders a specific business operator to change unfair terms in a contract, it may also issue a recommendation for all other business operators in the same industry to change their terms and conditions as well (Article 17-2, Clause 3). In addition, the Fair Trade Commission may notify the Financial Supervisory Service in the event a financial institution uses the unfair termination clause (Article 18, Clause 2). The order issued to a business operator to revise the terms and conditions of its contract includes both the elimination and revision of unfair terms (Article 17-2, Clause 2), which indicates that it is legally binding. If a business operator fails to comply with such an order, a penalty of up to two years imprisonment or a fine of up to KRW 100 million could be applied (Article 32). Of the measures implemented by the Fair Trade Commission related to unfair terms and conditions, corrective action is the most powerful. Nevertheless, if a business operator objects to the corrective action, and the Fair Trade Commission finds sufficient evidence that such correction could cause irreparable harm to the operator, then the order for corrective action may be suspended (Articles 30-2 and 53-1, Clause 1, of the Fair Trade Act: Suspension of Execution). As the request for alternation involves informing the relevant administrative office of unfair terms discovered in a contract, pursuant to the regulations or other laws imposed by the administrative office, and calling for corrective action (Article 18, Clause 1), it is legally unbinding.

2.3. Act on the Consumer Protection in Electronic Commerce, ETC.

a. Background

Consumer damage can reduce the credibility of e-commerce from the perspective of users and ultimately hamper the development of the e-commerce industry. In countries around the world, including OECD member states, the legislative efforts to protect consumers in e-commerce are focusing on the enactment and revision of regulations at the institutional level. As consumer damages have been increasing in line with the rapid growth of e-commerce, countries need to take preventive measures at the legal and institutional levels so as to promote user confidence in e-commerce and promote the development and health of the e-commerce industry. Toward this end, in 2002, the ROK enacted the Act on the Consumer Protection in Electronic Commerce, which aims to protect consumers in areas such as e-commerce and mail order transactions.

There are already some existing regulations on various commercial transactions and consumer protection that also apply to e-commerce, such as the Consumer Basic Law, Act on the Regulation of Terms and Conditions, Act on Mail Order, Etc., and the Act on the Fairness of Label and Advertisements. However, the expansion of e-commerce has given rise to new types of consumer damages related to the signing of electronic contracts upon the purchase of goods or services. These unprecedented problems include issues involving e-document preservation, consumer misunderstanding in relation to the use of e-documents, display of unwanted advertisements, accidents in the delivery process, and problems with prepaid transactions. In light of these issues, the Act on the Regulation of Terms and Conditions was enacted with the aim of establishing a fair environment for trade and protecting consumers by eliminating legal uncertainty through the designation of consumer and producer liability in e-commerce transactions.

2.3.2. Main Contents

a. Utilization of e-documents and preservation of records

The Electronic Transactions Act is in effect as it is considered as an electronic copy of a document. Therefore, business operators can express themselves through e-documents sent via e-mail. However, consumers who do not check their e-mail frequently or are not notified by business operators regarding email address changes may suffer unexpected losses. Thus, the Act on the Regulation of Terms and Conditions mandates business operators to ask for agreement from consumers in advance concerning the conversion of documents that may affect, in any way, the rights or obligations of consumers into e-documents (Article 5, Clause 1). The same law assigns to business operators the responsibility of preserving the original form of all types of documents while ensuring that consumers have easy access to such documents (Article 6).

b. Prevention of accidents in the use of technology

In e-commerce, the contracting process is carried out rapidly based on procedures established by each company, thus giving rise to the possibility of consumers making unwanted orders or making multiple payments for the same order. To address these issues, Article 7 of the Act on the Consumer Protection in Electronic Commerce instructs business operators to confirm and correct the contents of orders before receiving payment so as to prevent consumer damages caused by consumers' unfamiliarity with the technologies used. In addition, to confirm the true intention of the consumer upon the issuance of an electronic payment, Article 8, Clause 2, states that the business operator and e-payment provider are required to provide a process through which the consumer may confirm the price of the goods, period of the service, and other relevant details.

c. Issues Related to Labeling and Advertising

Article 10 of the Act on the Consumer Protection in Electronic Commerce defines the legal obligations of online shopping mall vendors. Such vendors are required to clearly indicate on their websites the name of the company's owner, location of the company's office, telephone number, email address, company registration number, contract terms and conditions, and name of their service provider. In addition, vendors must put a link on their websites to the page of the Fair Trade Commission's website containing the information of the business operator. Article 13, Clause 3, of the same law allows the Fair Trade Commission to provide any relevant information to consumers. According to the Guidelines on E-Commerce Consumer Protection, provided by the Fair Trade Commission concerning issues related to labeling and advertising, it is required to display more specific information about the companies participating in electronic transactions. Under the same guidelines, vendors are required to provide information on themselves, their products, and the terms and conditions of transactions. In recognition of the non-face-to-face nature of e-commerce, the FTC also requires vendors to provide detailed information on themselves to consumers with which they make transactions as a means of preventing fraud. Addressing the issue of vendors sending advertisements to consumer indiscriminately via such means as SMS, text message, and email, causing inconvenience to some, Article 24, Clause 2, of the Act on the Consumer Protection in Electronic Commerce regulates the advertising activities of vendors.

d. Termination of Contract

Article 17 of the Act on the Consumer Protection in Electronic Commerce the cancellation of contracts. In accordance with this provision, consumers may terminate contracts without any conditions, provided that they do so within seven days from the day on which the written terms and conditions of the contract were received or within seven days from the day the product was delivered. This provision serves to protect consumers in cases where the product information provided was misleading, the appearance of the product is substantially different from that advertisement, or the product is damaged at no fault of the consumer. If the appearance of a product is significantly different from that used in the advertisement or the terms of the contract are differently performed, the consumer may terminate the contract within three months from the day he or she received the product or within 30 days from the day he or she was informed or could have been informed (Article 17, Clause 3).

e. Adoption of Escrow Account

Considering the non-face-to-face nature of e-commerce, the adoption of an escrow system is a necessity. E-commerce transactions are vulnerable in terms of security and reliability due to the non-face-to-face nature of the transactions, absence of physical stores, and processes of prepayment transactions. To address these issues, the escrow system was adopted with the 2005 amendment of the Act on the Consumer Protection in Electronic Commerce (Article 24, Clause 2). Escrow service providers require consumers to make deposits with them until receipt of the commodity in question or conclusion of a consumer damage compensation insurance contract, at which time the funds are released. However, transactions involving credit cards, non-delivery of goods, or payment amounts within the boundary prescribed by Presidential Decree that do not exceed KRW 100,000 are excluded from this system.[28] The escrow system was first adopted in the United States in 1997. In the ROK, this service was first introduced by domestic banks and payment companies. The

28. The amount that exceeds 100,000 won was reinforced as it was rewritten as more than 50,000 won in 2011, and since May 2013, all small payments below KRW 50,000 have had to be made through secure payment systems.

Korean government also took measures to promote this system. In August 2012, the FTC made it mandatory for online shopping malls to create escrow accounts, pursuant to the Electronic Transaction Law.

f. Compensation for Consumer Damages and Corrective Actions

The Act on the Consumer Protection in Electronic Commerce provides a basis for the Fair Trade Commission to encourage related companies to conclude insurance contracts or payment guarantee contracts with financial institutions regarding the payment of compensation for consumer damages, thereby protecting consumers in e-commerce or telesales (Article 24, Clause 1). In the event a business operator refuses to comply with an order to take corrective action issued by the Fair Trade Commission, the FTC has the authority to suspend the operation of said business for a period of not more than one year. It can also impose a fine up to the amount of revenue the business earned by violating the law (Article 32, Clause 4, and Article 34).

3. Act on the Consumer Protection in Electronic Commerce

3.1. Purchase Safety Service

Purchase Safety Service refers to a service that protects a consumer from fraud upon making a purchase, when the consumer chooses to make a contract with the escrow system or a vendor concerning compensation for damages. If none of the subordinate clauses of Article 24, Clause 3, apply to the transaction, the telecommunications distributor is legally required to make a contract with a financial institution that provides such Purchase Safety Service for consumers, thereby ensuring that the consumer is free to choose to use the Purchase Safety Service. Vendors should display, advertise, or notify their consumers regarding such Purchase Safety Service on the website of the online shopping mall and the payment webpage.

The types of Purchase Safety Service include escrow accounts, consumer damage compensation insurances, escrow transfer services, and debt payment guarantee contracts. First, in the escrow system, a third party registered with the Financial Services Commission pursuant to Article 28 of the Electronic Financial Transactions Act holds a deposit paid by the customer in an amount equal to the purchase amount and, upon the delivery of the goods purchased, releases the funds to the vender, thereby completing the purchase. The provider of this service is a private entity registered with commercial banks or the Financial Services Commission. Second, consumer damage compensation insurance is insurance that pays compensation to consumers for damages incurred through transactions with online shopping malls. Such payment of compensation occurs through the issuance of the consumer damage compensation insurance certificate that the vendor concluded with Seoul Guarantee Insurance upon the receipt of payment for goods purchased by the customer from the online shopping mall. The service provider is the Seoul Guarantee Insurance Company. Third, the escrow transfer service is an escrow system that features no interconnection between the operation of the escrow system and the online shopping mall, instead linking the online shopping mall of the vendor with an escrow system established with online banks. The service providers include IBK, KB, Woori Bank, and NH Bank, among others. Lastly, a debt payment guarantee contract is a guarantee provided by a financial institution concerning the obligations to be fulfilled by the vendors in the course of the transaction with consumers. This service is provided by commercial banks.

3.2. Guidelines for Online Vendors on the Provision of Product Information

By presenting detailed information on goods in various categories, these guidelines are intended to help consumers make rational purchasing decisions and prevent consumer damage caused by lack of information. The basic principles are as follows. First, the information on goods provided to consumers must be written in terms that the consumers can understand. Second, product information provided to consumers should be clearly presented using methods such as color differentiation, borders, and large font sizes. Third, product information should be provided in as much detail as possible. Fourth, even if the product does not correspond exactly to the main product provided in the guidelines, the distributor should consider the ways in which the product is similar to that in the guidelines, as well as its functions and utility, and provide product information as presented in the guidelines.

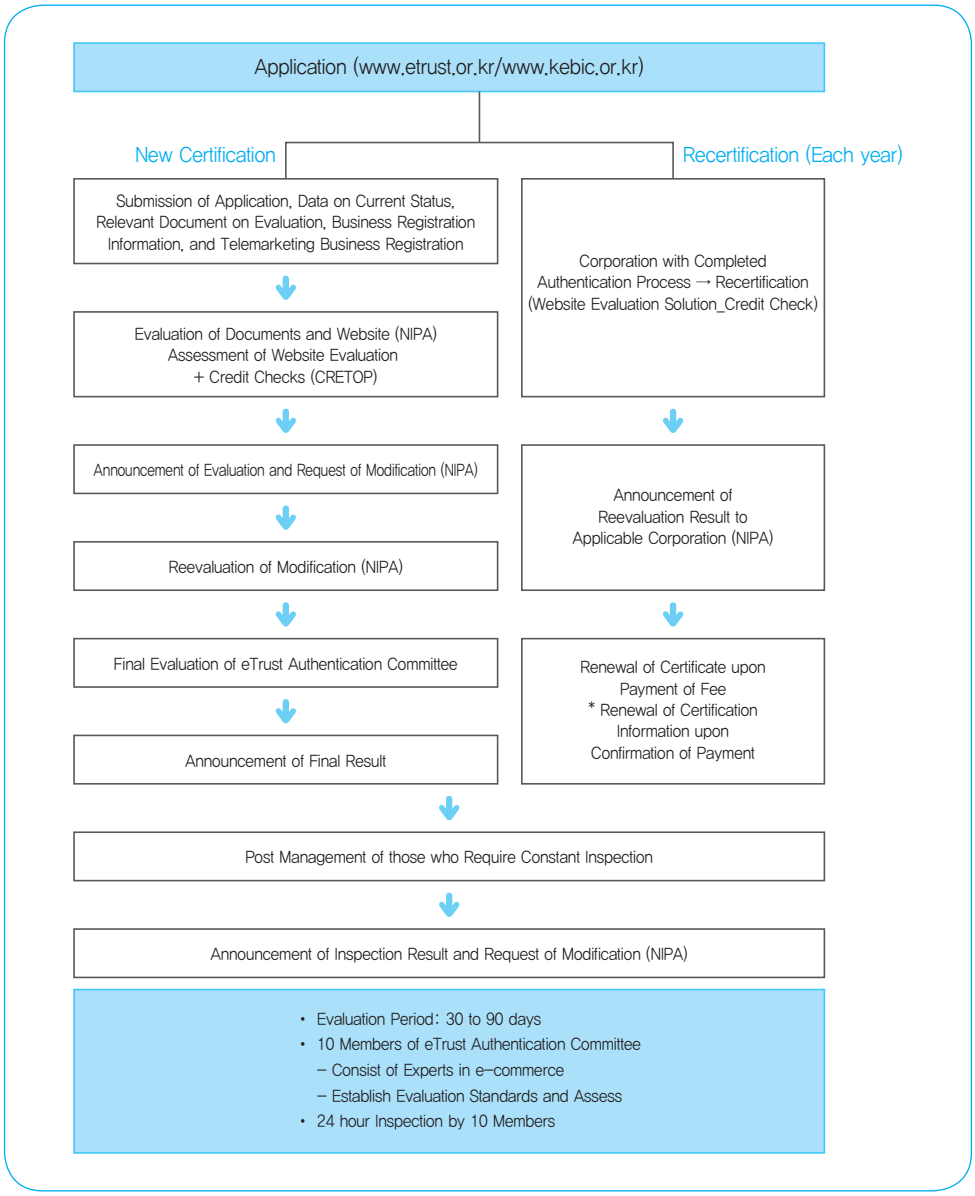
Regarding the provision of information, vendors should adhere to the following guidelines. First, telemarketing vendors should display detailed information on each major product in the designated space for such information under the price of the product and place an order. Second, vendors should regularly check to ensure that the information provided is of sufficient detail. Third, mail-order brokers should make every effort to confirm that the vendors who ordered telemarketing service provide customers with satisfactory and sufficient product information through the brokerage system. In the event an error in the product information is discovered and confirmed, the telemarketing intermediary shall promptly issue a request to the vendor to correct the information. If the vendor fails to fulfill the request, the intermediary should take appropriate measures promptly and in accordance with the relevant law.

3.3. eTrust Certification System

The eTrust certification system was introduced as a means of contributing to the establishment of a secure e-commerce environment by ensuring the reliability of online shopping malls and the security of users by certifying excellent e-commerce providers with healthy and rapidly growing businesses and customer bases. This system aims to help ensure consumer confidence, establish a safe e-commerce environment through the rigorous operation of a certification mark system for excellent electronic transaction providers, provide business development opportunities by assigning e-trust marks to online shopping mall operators, and ensure the safety and convenience of consumers in online transactions through the operation of an eTrust certification mark.

eTrust certification is granted to electronic transaction providers who are deemed to be trustworthy, deal with consumers fairly, and review the entire purchase process rigorously, including the consumer protection and privacy policies of related websites. The eTrust certification system is operated by the Ministry of Science, ICT and Future Planning, and eTrust certifications are registered under the authority of the National IT Industry Promotion Agency. eTrust certification is a comprehensive evaluation of online shopping mall operators who have been in operation for three months or longer, including their consumer protection measures, privacy policies, and overall e-commerce purchase process and business model suitability. The certification criteria include the convenience and safety of the website (order/payment process, product delivery, and exchange/return), company and product information (compliance with the product labeling guidelines of the Fair Trade Commission), system security, privacy protection, web accessibility, after-sales service, and business model and website suitability. The eTrust certification assessment process is outlined in [Figure 4-1].

Figure 4-1 | eTrust Authentication Process



Source: MSIP 2016.

eTrust-certified companies receive several benefits. First, they see increased sales of products and services resulting from greater customer confidence fostered in an environment of trust created through the expanded use of eTrust logos and certificates. Second, they enjoy more effective dispute resolution as, with the cooperation of the Cyber Terror Response Center and Fair Trade Commission of the National Police Agency, the Dispute Settlement Committee reviews and handles complaints concerning eTrust-certified companies first. Third, they can expect increased revenue through the formation of a council of eTrust-certified vendors and co-promotion opportunities through mass media, including business cooperation and information sharing through councils of certified vendors, websites, and KISA publications.

Through eTrust certification, the members of the World Trustmark Alliance (WTA), which includes major countries around the world, cooperate with each other to mutually recognize the online trustmark system operated by each member country.[29] Also, as part of the effort to address the increasing necessity of consumer protection due to the increase in cross-border e-commerce transactions, WTA members promote mutual cooperation with alternative dispute resolution (ADR) organizations, such as the Electronic Commerce Mediation Committee (ECMC). Since the signing of an MOU with the trustmark agencies in Korea, Japan, Singapore, and Taiwan in 2004, the WTA has expanded to 25 organizations in 16 countries, as of 2013.

3.4. Consumer Damage Relief System

The consumer damage relief system is operated by the Korea Consumer Agency. Although Article 12 (Fairness of Transactions), Clause 1, of the Consumer Basic Law stipulates, "The state should establish and implement necessary measures to prevent unfair damage to consumers due to unfair trade conditions or transaction methods of businesses," Article 35 of the same law requires the KCA to handle all cases of consumer complaints and

29. WTA member states include the ROK, U.S., Japan, Singapore, Taiwan, ROC, Mexico, Vietnam, Philippines, Malaysia, Spain, and EU.

damages. Article 55 (Request for Damage Remedy), Clause 1, of the same law states that consumers may submit requests to the Korea Consumer Protection Board to relieve damages caused by the use of goods or services. In addition, Article 55, Clause 2, of the same law provides that the central and local governments and consumer organizations may call on the Korea Consumer Agency to assist consumers in cases where consumers are requesting compensation from sellers. Under this provision, the Korea Consumer Agency is to serve as a damage relief agency for consumer disputes. Furthermore, the head of the Korean Consumer Agency may recommend the parties to the claimant's settlement of consent for damage compensation under Article 57 (Consensus Recommendation) of the law.

3.5. E-Commerce Mediation Committee

The Electronic Commerce Transaction Act requires the establishment of an electronic trade dispute settlement committee tasked with relieving damages caused by electronic transactions and establishing fair electronic trading practices (Article 32 of the E-Commerce Act). Accordingly, the E-Commerce Discussion Committee has been established and is currently being operated under the Korea Institute for Electronic Commerce. The deliberation or adjustment of disputes concerning electronic transactions, as well as the dispute adjustment, are conducted both online and offline.[30] The E-Commerce Mediation Committee was established to resolve disputes arising in relation to electronic documents and electronic transactions, realize a healthy online environment for e-commerce through fair trade practices, facilitate the use of electronic documents and execution of electronic transactions, and protect the rights of business operators and consumers. The Committee also operates under the National IT Industry Promotion Agency.

30. Online coordination can resolve conflicts efficiently and quickly and is advantageous in that it is free from geographical or time constraints. However, because it is done over the Internet, there is a risk of third party intervention or interference, such as through hacking (Kwon, 2009).

The E-Commerce Mediation Committee consists of 39 mediation committees comprising experts in fields related to electronic documents and electronic transactions, including experts from the legal profession, academia, industry, consumer organizations, and the MSIP. The main functions of the Committee are to: carry out dispute prevention activities, such as education promotion activities and activities to prevent business disputes related to electronic documents and transactions; provide follow-up dispute resolution services, such as consultations and service coordination for electronic document and transaction dispute resolution; and establish a cooperative system among related institutions for the realization of the world.

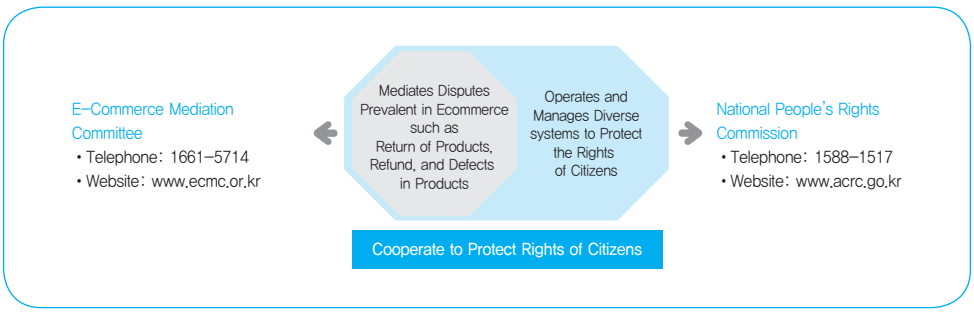
Dispute settlement spans all kinds of disputes, including those concerning B2C, C2C, and B2B transactions. Prime examples are disputes related to contracts; delivery issues, such as delayed deliveries or losses of goods; burden of shipping, such as refusal of withdrawal of subscription; non-fulfillment of contract terms and conditions; changes of contract terms and conditions; misrepresentation of product information or prices; and electronic documents. Dispute resolution methods can be categorized into face-to-face, online, written, and phone call methods. Face-to-face coordination, where disputes are resolved with a mediator, the disputing parties, and an investigator all present in one meeting place, is more appropriate for complex dispute cases. For onilne coordination, one can simply access the online coordination center (chatting.ecmc.or.kr) to resolve a dispute. Written coordination is another means available to disputing parties who are unable to engage in a face-to-face dispute resolution process. As this process involves resolution, it is more appropriate for cases involving specific details. Phone call coordination involves phone calls between a mediator, the disputing parties, and an investigator.

In order to increase the efficiency of the dispute counseling service and consultations, the cooperation of the government and organizations related to the dispute settlement process has become crucial, especially considering the continuous expansion and use of e-commerce and the growing number of disputes. Recognizing this, the E-Commerce Mediation Committee is working hard with other organizations to develop measures for improving dispute resolution efficiency.

Figure 4-2 | Business Cooperation with Faire Trade Commission

Looking at the business cooperation with the National Human Rights Commission of Korea, complaints related to electronic transactions received by the National People's Journal are confiscated and processed by dispute resolution committees related to electronic documents and electronic trade. On November 5, 2002, Cheong Wa Dae's "Internet Newspaper" was also designated as a civil complaints handling agency. In December 2007, the complaints handling system of the National People's Journal and Electronic Document and Electronic Transaction Dispute Arbitration Committee were integrated and linked. This has made it possible to carry out online, real-time complaint forwarding and duplication processes through the e-government communication network.

Figure 4-3 | Business Cooperation with Anti-Corruption and Civil Rights Commission



Source: Ministry of Science, ICT and Future Planning (2016).

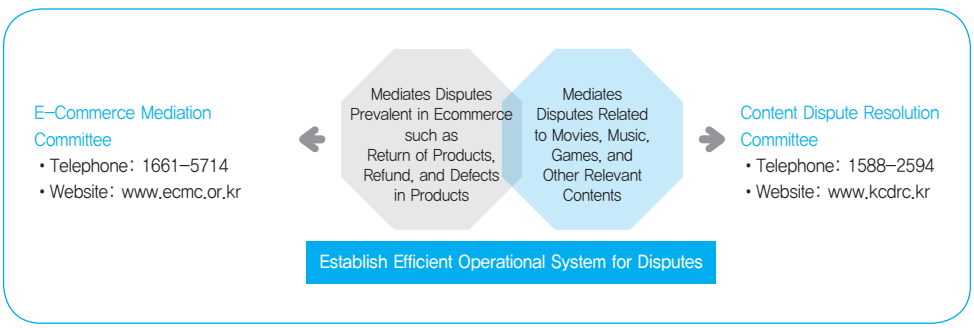
Regarding business cooperation with the Cyber Security Bureau (formerly Cyber Terror Response Center) of the National Police Agency, a business agreement was concluded to promote mutual cooperation in anti-counterfeiting activities related to electronic transactions (October 12, 2006). This cooperation involves mutual guidance and information exchange regarding suspected crimes during the application of dispute received at Cyber Terror Response Center, simple bonsai issues, electronic documents, and electronic trade dispute mediation committees. Joint responses to the spread of public awareness of electronic transaction security and other matters deemed necessary for improving the nation's public services are also included in business cooperation.

Figure 4-4 | Business Cooperation with Korean National Police Agency Cyber Bureau

Source: Ministry of Science, ICT and Future Planning (2016).

Concerning the status of business cooperation with the Content Dispute Mediation Committee, we concluded a business agreement regarding the establishment of cooperative relations in relation to electronic transaction and content disputes (Oct. 4, 2011). This cooperation involves: mutual guidance and handling of consultation and coordination applications related to administrative affairs, exchange of information on dispute settlement support projects and coordination of applications, identification of dispute trends, and mutual cooperation in response to disputes.

Figure 4-5 | Business Cooperation with Content Dispute Resolution Committee



Source: Ministry of Science, ICT and Future Planning (2016).

In relation to business cooperation with the Dispute Settlement Organization, an agreement regarding e-commerce dispute settlement agencies was made (Dec. 20, 2012) to promote e-commerce consumer protection and e-commerce market restoration. This cooperation involves: business cooperation, such as the reinforcement of e-commerce consumer protection and joint policy research for the creation of a consumer-oriented e-commerce market; mutual support and information exchange and sharing for the promotion of e-commerce consumer information protection and consumer rights; counseling for e-commerce consumers concerning damage relief; and mutual aid for damage relief and dispute settlement services.

Figure 4-6 | Business Cooperation with Dispute Settlement Organization

Source: Ministry of Science, ICT and Future Planning (2016).

3.6. Evaluation

In 2014, the total value of online shopping transactions was KRW 45.24 trillion, increasing by 17.5 percent from the previous year (KRW 38.489 trillion). Mobile shopping transactions increased by 125.8 percent to KRW 14.8 trillion.

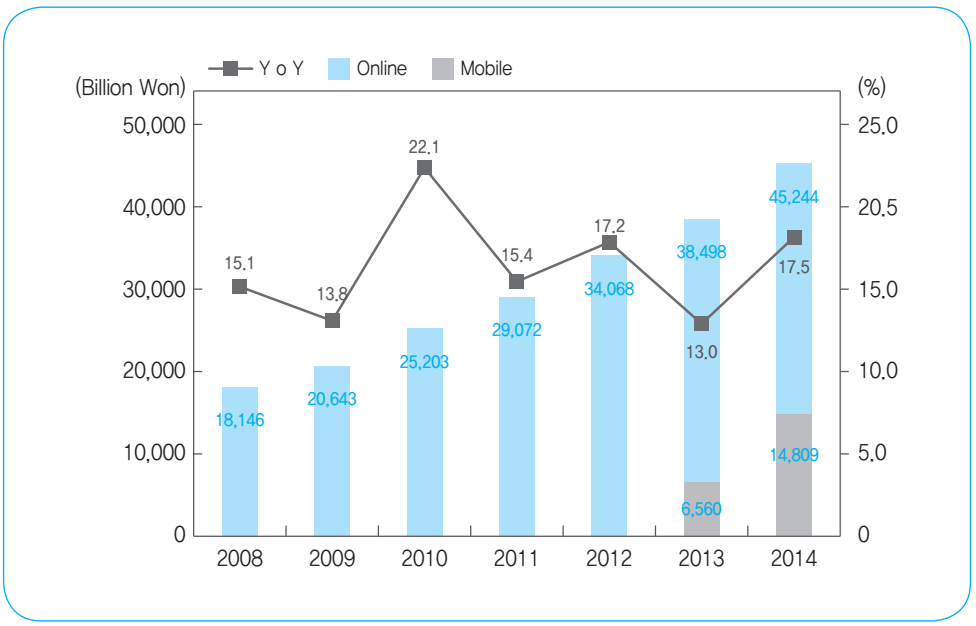
Table 4-1 | The Status of Turnover of On-Line Shopping

(Unit: billion won, %)

Type of Transaction	2008	2009	2010	2011	2012	2013	2014
Total Transaction	18,146	20,643	25,203	29,072	34,068	38,498	45,244
Mobile Transaction	-	-	-	-	-	6,560	14,809
YoY	15.1	13.8	22.1	15.4	17.2	13.0	17.5

Source: Statistics Korea.

Figure 4-7 | A turnover and Growth Rate of On-Line Shopping



Source: Ministry of Science, ICT and Future Planning (2016).

The trend of consumer disputes differs from that of the continuous expansion of electronic commerce. In 2014, a total of 2,165 cases of consensus recommendation and reconciliation among electronic dispute settlement committees received on electronic documents and electronic trade dispute settlement committees, decreasing by 50.1 percent from the previous year. These statistics have led to speculation that Korea's consumer protection policy is having a positive effect. Of course, consumer dispute statistics are only one of the indicators of the effectiveness of the consumer protection policy. However, considering that there is a large variation in the yearly consumer dispute statistics, it is too soon to make any definitive assessment. Of the 2,165 dispute cases, 2,134 (98.6 percent) disputes were concluded by Secretariat Recommendation, while 31 cases (1.4 percent) were concluded through the Coordination Department. At the Secretariat Recommendation stage, 1,787 disputes were

concluded with the agreement of all parties, with the remaining 347 cases being rejected by the parties. The number of cases in which the disputing parties accepted the amendment was 27, along with four cases in which the parties did not accept the amendment.

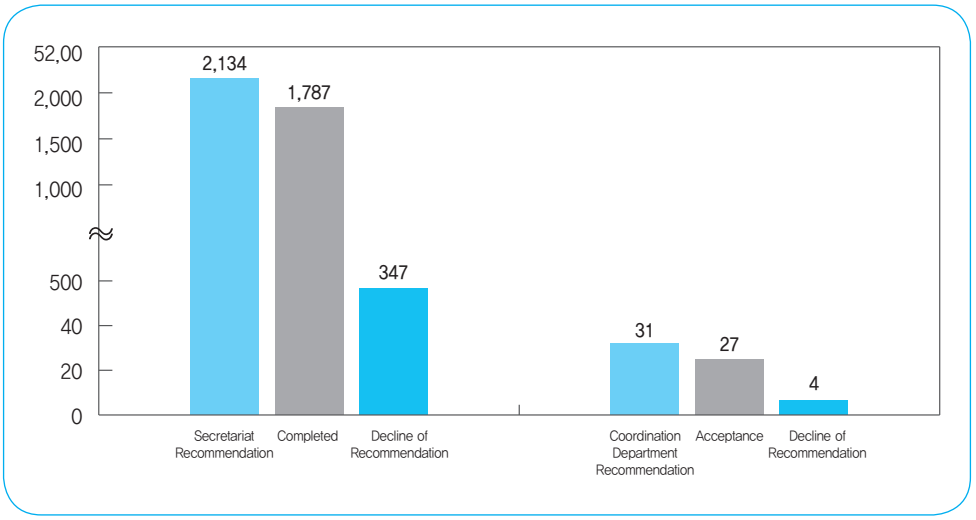
Table 4-2 | Recommendation to Coordinate Per Year and the Status of Coordination

(Unit: number of incidences, %)

Classification		2010		2011		2012		2013		2014		YoY Growth Rate
			Proportion		Proportion		Proportion		Proportion		Proportion	
Secretariat Level	Completed	2,586	82.1	2,527	84.1	3,029	85.4	3,729	85.9	1,787	82.5	△52.1
	Decline of Recommendation	519	16.5	448	14.9	491	13.8	575	13.2	347	16.0	△39.7
	Sub Total	3,105	98.6	2,975	99.0	3,520	99	4,304	99.1	2,134	98.6	△49.6
Department Level	Acceptance of Coordination Plan	24	0.8	20	0.7	21	0.6	29	0.7	27	1.2	△6.8
	Decline of Coordination Plan	19	0.6	9	0.3	7	0.2	8	0.2	4	0.2	△50.0
	Sub Total	43	1.4	29	1.0	28	0.8	37	0.9	31	1.4	△16.2
Total		3,148	100	3,004	100	3,548	100	4,341	100	2,165	100	△50.1

Source: MSIP 2016.

Figure 4-8 | 2014 Recommendation to Coordinate and Status of Coordination



Source: MSIP 2016.

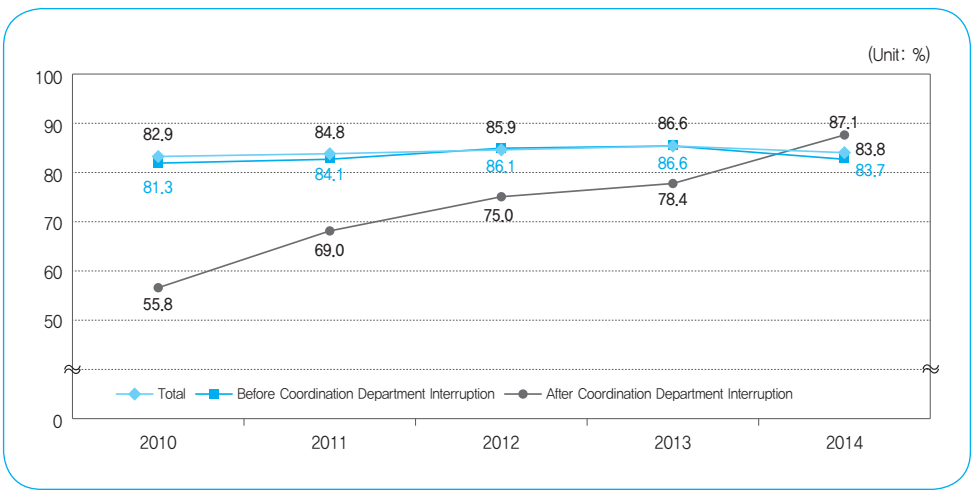
The dispute settlement rate in 2014 was 83.8 percent, down by 2.8 percentage points from 86.6 percent in the previous year. The dispute resolution rate by the Secretariat was 83.7 percent, while the dispute resolution rate of the Arbitration Department was 87.1 percent. The rate of dispute resolution via Secretariat Recommendation decreased by 2.9 percentage points from the previous year, while the rate of dispute settlement via adjustment of the coordinator increased by 8.7 percentage points from the previous year. The rate of dispute settlement by the Arbitration Department has been increasing gradually every year since 2010, seemingly due to the Arbitration Department's success in establishing a reasonable level of reconciliation that can be accepted by the parties.

Table 4-3 | Dispute Resolution Trends

Classification	2010	2011	2012	2013	2014	YoY
Total Resolution (%)	82.9	84.8	85.9	86.6	83.8	△2.8
Secretariat Resolution (%)	81.3	84.1	86.1	86.6	83.7	△2.9
Coordination Department Resolution (%)	55.8	69.0	75.0	78.4	87.1	8.7

Source: MSIP 2016.

Figure 4-9 | The Trends of Dispute Resolution per Year



Source: MSIP 2016.

Looking at the status of dispute counseling by type in 2014, contract cancellations, returns, and refund consultations, including contract terminations due to simple remorse, return refusals, and delayed refunds accounted for 19,850 cases, or 44.3 percent of the total. A total of 6,731 (15.0 percent) consumer complaints were related to delivery, 5,588 (12.5 percent) to product defects, 2,308 (5.2 percent) to changes to or failures to fulfill contract terms, 1,882 (4.2 percent) to false or exaggerated advertising, and 1,710 (3.8 percent) to misleading product information. In 2015, the number of cases related to contract cancellations, returns or refunds, and delivery, which amounted to 60 percent of all dispute

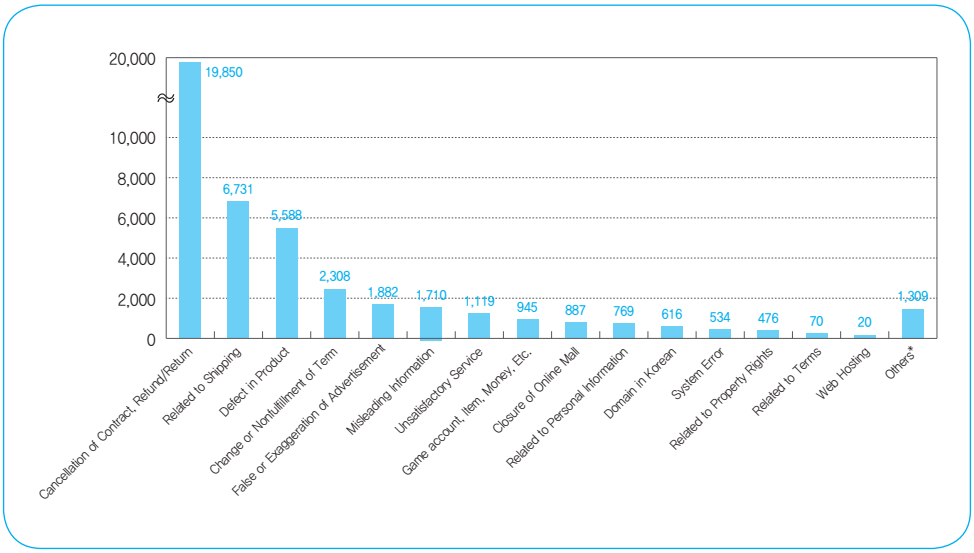
counseling cases, increased by about 10 percent from the previous year. Notably, although the number of dispute counseling cases related to personal information, Korean Internet addresses/domains, contract terms, and web hosting was small compared to other types, these categories recorded an enormous increase from the previous year. Also, dispute counseling cases related to product defects, system errors, and property rights decreased by more than 40 percent.

Table 4-4 | The Trends of Dispute Counselling per Category

Classification	2010		2011		2012		2013		2014		YoY Growth Rate
		Proportion		Proportion		Proportion		Proportion		Proportion	
Cancellation of Contract, refund/return	6,460	35.9	9,284	40.7	12,364	49.6	18,993	39.2	19,850	44.3	4.5
Related to Shipping	3,050	17.0	4,750	20.8	3,211	12.9	5,893	12.2	6,731	15.0	14.2
Defect in Product	1,842	10.2	2,344	10.3	2,208	8.9	9,600	19.8	5,588	12.5	Ð41.8
Change or nonfulfillment of terms	884	4.9	1,098	4.8	1,366	5.5	2,166	4.5	2,308	5.2	6.6
False or Exaggeration of Advertisement	890	4.9	937	4.1	1,324	5.3	2,296	4.7	1,882	4.2	Ð18.0
Misleading information	1,176	6.5	1,393	6.1	1,138	4.6	1,647	3.4	1,710	3.8	3.8
Unsatisfactory Service	432	2.4	507	2.2	751	3.0	1,402	2.9	1,119	2.5	Ð20.2
Game account, item, money, etc.	2,044	11.4	1,410	6.2	424	1.7	886	1.8	945	2.1	6.7
Closure of Online Mall	592	3.3	486	2.1	593	2.4	934	1.9	887	2.0	Ð5.0
Related to personal information	319	1.8	498	2.2	254	1.0	416	0.9	769	1.7	84.9
Domain in Korean	15	0.1	5	0.0	142	0.6	320	0.7	616	1.4	92.5
System error	58	0.3	37	0.2	468	1.9	1,555	3.2	534	1.2	Ð65.2
Related to Property Rights	4	0.0	12	0.1	107	0.4	893	1.8	476	1.1	Ð46.7
Related to Terms	5	0.0	12	0.1	49	0.2	24	0.1	70	0.2	191.7
Web Hosting	2	0.0	5	0.0	15	0.1	5	0.0	20	0.0	300.0
Others	20	0.1	51	0.2	501	2.0	1,445	3.0	1,309	2.9	Ð9.4
Total	17,993	100	22,829	100	24,915	100	48,415	100	44,814	100	Ð7.4

Source: MSIP 2016.

Figure 4-10 | The Status of Dispute Counselling by Category in 2014



Source: MSIP 2016.

In an effort to relieve the damages caused to consumers, arising due to the unprecedented issues emerging in the e-commerce industry and the major differences between e-commerce and offline commerce, the Korean government enacted Act on the Consumer Protection in Electronic Commerce in 2002. This Act established institutional measures for addressing these new issues. The most notable provision of the Act is Article 17, which addresses the issue of contract termination. This provision enables consumers to terminate contracts with vendors within seven days of purchasing goods or services. It also allows for the adoption of an escrow system and establishment of the E-Commerce Mediation Committee, tasked with protecting consumers from the potential harms inherent in e-commerce. Developing countries should also consider implementing the measures outlined above.

Chapter 5

Conclusion

Conclusion

The constant expansion of the Internet since the 1980s has brought about numerous changes in various sectors and industries. In commerce, the development of the e-commerce industry has generated unprecedented changes and innovations, leading, in turn, to major transformations in consumption and the business operations of firms. The e-commerce industry has grown particularly rapidly since the 1990s, expanding from major developed countries to the rest of the world, facilitated by the spread of smartphones. The Republic of Korea has been no exception. Since 2000, the size of the ROK's e-commerce industry has grown to the extent that it now easily surpasses the country's GDP. With the rapid expansion of e-commerce, countries around the world, including OECD member states, have experienced problems related to online transactions, involving such issues as trust, taxation, invasion of privacy, transfer of information among countries, and consumer protection measures. With the ongoing debates on these issues having become more fervent since the 1980s, UNCITRAL and the WTO have taken steps to intervene.

In order to vitalize e-commerce, balanced development of new infrastructure, social and institutional systems, and other infrastructure is required. However, the broad and rapid distribution of smartphones has substantially reduced the need for building new infrastructure and other infrastructure for e-commerce, offering incredible opportunities for developing countries to enjoy the benefits of the recent expansion of the e-commerce industry. In order for developing countries to take advantage of this opportunity, however, they must prioritize the establishment of institutional systems that foster trust between buyers and sellers over the building of infrastructure. In this sense, developing countries should consider the non-face-to-face nature of e-commerce and prioritize e-authentication and consumer protection measures accordingly, thereby facilitating the growth of trust between buyers and sellers. This study aims to systematically summarize the policies implemented by the Korean government to vitalize the e-commerce industry, which has seen significant growth since the 2000s, in the hope of assisting other countries around the world seeking to create efficient policies and successfully vitalize their e-commerce industries.

In terms of e-authentication, the ROK has introduced numerous policies, including those on electronic certifications, i-PIN/My-PIN, and OTP, which require government-certified e-authentication or the enforcement of other specific measures. As the ROK government has successfully ensured the credibility of e-authentication, the country's e-authentication policy, in particular, is considered to have played a crucial role in the expansion of e-commerce in the early 2000s. However, the Korean government made the use of specific technologies, such as PKI and OTP, a mandatory part of its e-authentication policy, a move that has given rise to various problems. The negative impacts of the mandatory use of specific technologies were: the disincentivization of investment in technology development, thereby

hindering the invention of new technologies; the shift of responsibility to the consumer in relation to problems arising during e-commerce transactions; and the emergence of e-authentication security problems, resulting from an Internet environment that relies heavily on ActiveX. The mandatory use of specific technologies is the biggest problem in the ROK's e-authentication policy, as it serves to restrain the invention of new technologies and the growth of the industry as a whole. In light of this, developing countries should strive to maintain technology neutrality and foster the dynamicity of their private sectors as core principles of their e-authentication policies, even when government intervention is necessary, so as to promote trust between consumers and sellers early on. In addition, they should focus on customer convenience, the importance of which has been clearly demonstrated by the failures of the i-PIN and My-PIN systems in the ROK.

Regarding consumer protection in the ROK, the government enacted the Act on the Consumer Protection in Electronic Commercee in 2002 to promote consumer protection in e-commerce. Today's e-commerce customers are becoming increasingly concerned about the preservation of electronic records of relevant documents, misuse of electronic documents due to the lack of experience of those involved, and newly emerging issues in advertising, shipping, and prepayment, among others. In relation to such issues, the Act on the Consumer Protection in Electronic Commerce provides institutional tools designed to prevent any potential harm to consumers. In order to foster consumers' trust in e-commerce, developing countries should also adopt subscription withdrawal measures and escrow systems and establish organizations such as the E-commerce Mediation Committee to mitigate consumer harm in the e-commerce industry.

This paper focuses on the B2C model. Universally, however, e-commerce follows the B2B model. Therefore, more studies need to be conducted on feasible government policies for invigorating the B2B and B2G models. Considering the growing proportion of e-commerce in cross-border trade, a research study on e-commerce policy in relation to customs clearance should also be done. Lastly, as stated in the introduction, the emergence of diverse firms to lead the establishment of sales and purchasing support systems, electronic payment systems, security and verification systems, and logistics and delivery systems is crucial in vitalizing the industry; hence, government policies capable of laying the foundation for the growth of such companies should be studied as well.

(In Korean)

Beak, MiYeon, "Security enhancement plan of Electronic financial transaction and use of OTP", Payment and Information Technology, 2006

Board of Audit and Inspection of Korea, "National Cyber Security Management Actual Condition", 2015

Chang, KyungHwan, "The Meanings and Successes of the Korean GTC Law", Kyung Hee Law Journal, 2006

Financial Supervisory Service, "Expansion of Using Electronic Signature in Financial Sector", Press Release, 2002.7

Kim, GunWook, "One-time Password Integrated Authentication Service Framework", ITA Journal Vol. 153, 2014

Ko, Sang-Won, "Internet Education for All Citizens", 2010 Knowledge Sharing Program, IT Fostering Policy, Chapter 2, KDI School of Public Policy and Management, 2011

Korea Communications Commission, 'Implementing Measures to Strengthen The Safety of Using I-PIN During This Month' Press Release, 2015

Korea Consumer Agency, "Consumer Damage Remedies Annual Report and Casebook", 2010

Korea Internet and Security agency, "The Guide for Introduction of I-PIN 2.0" 2010

_____, "National Internet White Paper", 2011.

Kwon, Sang-Ro, "Legal and Systematic Study on Consumer Protection In Electronic Commerce", The Korean Contents Association, Vol.9, No. 12, 2009

Ministry of Information and Communication, “Introduction of Alternative Means of Resident Registration on the Internet”, Press Release, 2006.10

_____, “Understanding I-Pin through Case Studies”, Press release, 2007, pp.6

Ministry of Security and Public Administration, “Use My-Pin Instead of Resident Registration Number From Now Onwards”, Press Release, June 2014.

Ministry of Science, ICT and Future Planning, National IT Industry Promotion Agency, E-Commerce Mediation Committee, “2014 Electronic Transaction Dispute Resolution Case Book”, 2016

National Intelligence Service, National Information Security White Paper, 2016

Song, Yeongkwan , “Lessons from the Dispute over Korea’s Digital Certification Regulation and Policy Suggestions for Electronic Commerce”, KDI FOCUS, No.51, 2015

_____, “Past, Present and Future of Public Key Certificate Policy in Korea’s Electronic Commerce”, Policy Study, 2014-07, Korea Development Institute, 2014

Yoon, SeokHwon “Hyper Internet Network Build and Fund for Informatization.” 2010 Knowledge Sharing Program, IT Fostering Policy, chapter 3, KDI School of Public Policy and Management, 2011

Yoon, JeaSeok, “2011 Knowledge Sharing Program: Korea’s Information Security Activity and its implications”, KDI School of Public Policy and Management, 2012

(In English)

Michael R. Baye, John Morgan, and Patrick Scholten, "Price Dispersion in the Small and in the Large: Evidence from an Internet Price Comparison Site," Economic Theory 26(2), 2005, pp.445-469.

Jeffrey R. Brown and Austan Goolsbee, "Does the Internet Make Markets More Competitive? Evidence from the Life Insurance Industry," Journal of Political Economy 110(3), 2002, pp.481-507.

Maris Goldmanis, Ali Hortacsu, Chad Syverson, and Onsel Emre, "E-Commerce and the Market Structure of Retail Industries," The Economic Journal 120(545), 2010, pp. 651-682.

OECD, "OECD Guide to Measuring the Information Society 2011," OECD, 2011.

_____, "Business-To-Consumer Electronic Commerce Survey of Status and Issues," OECD, 1997.

www.ksp.go.kr

Ministry of Strategy and Finance, Republic of Korea

30109, Sejong Government Complex, 477, Galmae-ro, Sejong Special Self-Governing City, Korea Tel. 82-44-215-2114 www.mosf.go.kr

KDI School of Public Policy and Management

30149, 263 (Bangok-dong, Korea Development Institute), Namsejong-ro, Sejong-si, Korea Tel. 82-44-550-1114 www.kdischool.ac.kr

9 791155 451878 95320

ISBN 979-11-5545-187-8

Knowledge Sharing Program
Development Research and Learning Network

- 30149, 263 (Bangok-dong, Korea Development Institute), Namsejong-ro, Sejong-si, Korea
- Tel. 82-44-550-1172
- www.kdischool.ac.kr