ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 8(23), DOI: 10.17485/ijst/2015/v8i23/79345 September 2015* ISSN (Online) : 0974-5645

An Empirical Study on a Tradeoff between Security and Convenience: The Case of i-PIN System

Hyuk Im[1], Seong Taek Park[1] and Mi Hyun Ko[2*]

[1]Deparment of Management Information Systems, Chungbuk National University, Cheongju, Chungcheongbuk - do - 362763, South Korea; imhyuk5054@gmail.com, solpherd@cbnu.ac.kr
[2]Deparment of Policy Research, Korea Institute of Science and Technology Information, Daejeon - 305806, South Korea; mihyungo@kisti.re.kr

Abstract

The resident registration numbers were used for administrative purposes including people's up-to-date residence information and vital statistics or provision of public services in Korea. In 2005, the government of Korea devised the i-PIN, a new online personal identification system replacing resident registration numbers. In the context of the i-PIN, the present study intended to shed light on the relationship between security and convenience. Also, we tried to explore the antecedents of adoption of the i-PIN. As a result, user support and perceived security had positive effects on the perceived ease of use, perceived usefulness respectively. The perceived ease of use also had significant effects on the perceived usefulness and satisfaction, whereas it did not exert direct effects on the use intention. Not surprisingly, the most significant variable influencing the use intention and satisfaction was perceived usefulness.

Keywords: Authentication, i-PIN; Resident Registration Numbers

1. Introduction

Recently, personal information is under dire threats of leakage by insiders, external hackers and unlawful marketers[1]. According to a civic group, no fewer than 374 million resident registration numbers in Korea were estimated to have been collected illegally for crimes from 1991 to 2014[2]. Concluding the on- and off-shore leakage of national resident registration numbers has reached to an uncontrollable level, the government is discussing overhauling the resident registration number system. The resident registration numbers were used for administrative purposes including people's up-to-date residence information and vital statistics or provision of public services[3]. Since the early 2000, web sites indiscreetly began to collect resident registration numbers for identification of their members, leading such numbers to be saved across the DBs of countless websites, which increased the risk of personal information leakage. According to a survey conducted in 2008, more than 62.2% of domestic internet web sites, and over 90% of top 200 online sites, were collecting, saving and using resident registration numbers for identification of subscribers[4].

The resident registration numbers contain personal information such as date of birth and gender, which is considered the most significant issue. Moreover, even when a number is found to have been leaked, one cannot change his or her number and may be exposed to crimes for life[5]. Thus, resident registration numbers are vulnerable to identify theft and financial loss once leaked[4,6]. In 2005, the government perceived the graveness of such issues, and devised the i-PIN, a new online personal identification system replacing resident registration numbers on local web sites[7]. The i-PIN is comprised of an ID and password

* *Author for correspondence*

for personal identification, designed to protect personal information, saving a user the trouble of using the resident registration number[8]. Unlike the permanently unchangeable resident registration numbers, i-PINs can be reissued or suspended once they are found to have been leaked. Furthermore, the i-PIN informs its user of a list of web sites where it is used for identification as well as the date and time, effectively serving to protect the user's personal information and to strengthen the person's control over such information[4].

In the context of the i-PIN, the present study intended to shed light on the relationship between security and convenience. Also, we tried to explore the antecedents of adoption of the i-PIN.

2. Literature Review

2.1 i-PIN

Identification refers to proving who you are. This is the process of determining who the person is when he or she tries to access an information system using a user name and ID. This is part of open information easily exposed externally. Authentication refers to proving the identification. That is, authentication is a process of seeing one's identity. Authentication often requires a password for an ID[9]. A person trying to access an information system proves who he or she is using a personal secret password. The i-PIN is an authentication system performing the identification and authentication simultaneously upon an ID and password being provided. The authentication system identifies a subject to be authenticated and provides relevant authentication services. i-PINs are usually used for personal identification of new subscribers. i-PINs replace the conventional approach of using real names and resident registration numbers for personal authentication. By providing an i-PIN ID with a password, one can join a website and use other services without having to present his resident registration number. Furthermore, should an i-PIN account be exposed, one can discard the compromised i-PIN and have a new pin issued, significantly lessening the potential risk of intrusion[4].

Previous local literature on i-PINs focused on technical application or implementation rather than users' behavior. Also, a few studies introduced policy aspects or simple service frameworks. Yet, to vitalize the i-PIN service, the behavioral analysis of user-side actual service experience should not be overlooked although it is important to pay attention to supplier-side technical and policy aspects. After all, it is the subjective perception of a potential user that decides on whether to use a newly adopted system or service[10]. Still, no previous studies viewed the intention to use i-PINs from the perspective of user behavior. The Korean government's initiative for developing and proceeding with an online ID management model is a rare case[11]. Recently, the EU including Germany is preparing to introduce the eID in connection with identification cards[12]. Also, some states including Japan and the US are benchmarking Korea's i-PIN system[13]. Meanwhile, lots of similar empirical studies in this field dealt with the intention to accept multiple authentication measures and relevant factors including OTPs[14], smart cards[15,16], email authentication services[17].

2.2 Authentication

Previous studies drew on significantly different models and variables leading to a paucity of consistency despite their commonality of investigating authentication approaches and of proposing alternatives to broaden the use of authentication methods. Thus, models and variables need to be generalized so that they can be used to develop a model for predicting the use of a new authentication approach. The present study reviewed previous studies to find out common factors that would facilitate the acceptance of authentication measures by potential users. Zviran and Erlich[18] proposed 4 factors that should be considered in choosing a means of authentication, i.e. effectiveness, ease of implementation, ease of use and user attitude and acceptance. Furnell et al.[19] stated effectiveness, cost and user acceptance are important in considering alternatives for authentication. Likewise, Yeom and Lee[11] suggested security, convenience and required legal level or economic feasibility should be considered extensively before choosing an option. From the previous literature, security and convenience were derived as the two factors affecting the user acceptance, as the ease of implementation and economic feasibility are supplier-side factors; they were excluded from this study focusing on the user-side factors.

2.3 Technology Acceptance Model

Davis et al[20] developed the TAM (Technology Acceptance Model), which has been one of the most widely used models by many studies for explaining and analyzing users'

acceptance behavior of information systems. The present study adopted the perceived usefulness, perceived ease of use and intention to use from TAM and included these in the model as important factors. The TAM stated attitude is an antecedent of the intention to use. Yet, we excluded the factor from the model. To maximize the simplicity of TAM and to prevent the model from getting too complicated, the present study skipped the measurement of attitude. Meanwhile, many authors extended TAM for their study objectives. Also, we added the satisfaction variable to scale up the dependent variables.

3. Proposed Model and Hypothesis

The present study identified the factors influencing the intention to accept i-PINs, and analyzed the effects of such factors on the intention to accept i-PINs. Figure 1 is the model proposed in this study.

The proposed model is based on TAM with the variables likely to affect the intention to accept i-PINs among other authentication methods being added. To be specific, the present study focused on the convenience dimension including user support and perceived ease of use, and the security dimension including security and perceived usefulness to find out their effects on users' satisfaction and intention to accept i-PINs.

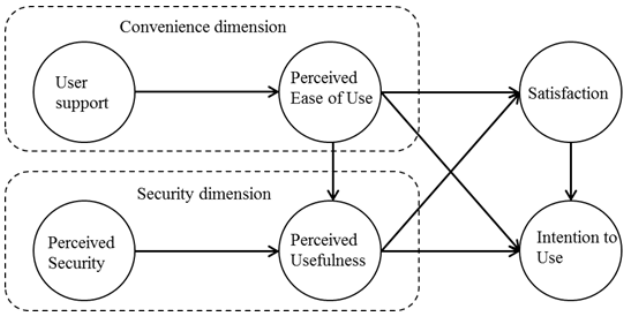

Figure 1. The proposed model.

Kim and Kankanhalli[22] argued that organizational supports in the form of training or resources in firms about to adopt new information systems reduced the time and effort required to learn the new business process and also difficulties in adjusting to the new systems. According to his study, the more the organizational supports are provided, the more the users' resistance decreased. Kim and Song[23] asserted that government's diverse supports for its portals would make it easier to use the information system, improving performance and promoting the acceptance of the system.

H1: User support will positively influence perceived ease of use.

The perception of security may have a considerable effect on raising the usefulness of systems[23]. As i-PINs operate in mobile environment, they do encompass the disadvantages of mobile devices and networks. Hacking attacks against smart phones are increasing. Mobile environment makes it easy to produce applications carrying malicious codes and uses limited OS, increasing the likelihood of migrating malicious applications, which is suggestive of a continuous growth of security risks[24]. Im et al.[25] studied on people's acceptance of technology regarding the internet electronic voting system and reported positive correlations between the perceived usefulness and the integrity of information delivered as well as personal information provided by users for the system, and between the perceived usefulness and the perceived security of authentication[25]. A study on mobile cloud service users' continuance use intention demonstrated the users' perceived security influenced their perceived usefulness[26].

H2: Perceived security will positively influence perceived usefulness.

Shin[13] surveyed i-PIN users on their satisfaction with the issuance and use of i-PINs. The linear regression analysis of the survey results illuminated the higher the satisfaction, the more intense the continuance intention. Taherdoost et al.[9] argued that the satisfaction with security had direct effects on the acceptance of smart cards. Limayem and Cheung[27] delved into the relationship between the perceived usefulness, satisfaction and continuance use intention, and argued the satisfaction with the experience of internet-based learning skills would bring a high level of continuance use intention. In short, it was found that the higher the perceived usefulness, the higher the satisfaction, which ultimately exerted effects on the continuance use intention for information systems. In a paper on e-government's trust models, TAM's core variables, viz. the perceived ease of use and the perceived usefulness were found to have effects on citizens' satisfaction with e-government systems[28].

H3: Perceived ease of use will positively influence satisfaction.

H4: Perceived usefulness will positively influence satisfaction.
H5: Satisfaction will positively influence intention to use i-PIN.

As aforementioned, the present paper is based on TAM. Studies adopting TAM as the underlying model in the specific contexts of interest took the perceived ease of use and the perceived usefulness as the most important antecedents of the acceptance intention, which has been proved by follow-up studies[29]. Moreover, the perceived ease of use can affect not just the acceptance intention but also the perceived usefulness. Kim and Song[23] reported when it was easier to use government portals, users found the technology more useful than any other element.

Bae[26] found a sequential relationship where the perceived ease of use led to the perceived usefulness, which in turn led to the continuance usage intention. Previous studies reported that the effects on the use intention mediated via the perceived usefulness were more significant than those of the perceived ease of use on the use intention[21,30]. Yet, under certain conditions in some cases, the perceived ease of use had greater effects on the use intention than the perceived usefulness[31,32]. The present study verified the following hypotheses with reference to the relationships between general variables suggested in TAM.

H6: Perceived ease of use will positively influence intention to use i-PIN.
H7: Perceived ease of use will positively influence Perceived usefulness.
H8: Perceived usefulness will positively influence intention to use i-PIN.

4. Data Analysis and Results

The present study verified the model using SmartPLS 2.0[33].

4.1 Data Collection

An online survey was administered by a research firm from December 15-17, 2014. The survey respondents were at least aware of i-PINs and recruited regardless of regions

Table 1. Measurement instrument

Construct	Item	Wording
User Support	USP1	I can get some clear explanation from issuing and operating organizations when I have to be issued and use i-PIN
	USP2	i-PIN issuing organizations provide me assistance when I wonder about i-PIN and have a trouble
	USP3	i-PIN issuing organizations provide me guide on how to get an i-PIN and log in
	USP4	i-PIN issuing organizations provide me assistance when I have to be issued and use i-PIN
Perceived Security	PSC1	I don't worry that my personal information will be exposed when I use i-PIN
	PSC2	i-PIN is a safe service protecting user's personal information
	PSC3	When I use i-PIN, I feel that i-PIN is protecting my personal information
Perceived Ease of Use	PEOU1	Learning to use and get i-PIN would be easy for me
	PEOU2	How to get an i-PIN is not difficult
	PEOU3	Learning to use and get i-PIN would be easy for me
Perceived Usefulness	PU1	Overall, i-PIN is useful
	PU2	i-PIN use is beneficial to user
	PU3	i-PIN is of utility value
	PU4	i-PIN use is advantageous
Satisfaction	SFC1	I'm satisfied with interface of i-PIN
	SFC2	I'm satisfied with processing speed of i-PIN
	SFC3	I'm satisfied with functions i-PIN has
	SFC4	I'm satisfied with procedure of i-PIN
	SFC5	Overall, I'm satisfied with i-PIN
Intention to Use	IU1	I will use i-PIN continuously
	IU2	I think I will use i-PIN if possible
	IU3	I plan to use i-PIN
	IU4	Maybe I will use i-PIN in the future

with equal distribution of gender and age. Of 396 people accessing the online survey window, 360 respondents completed the survey, which showed a very high response rate of 90.9%. Excluding 43 insincere copies, 317 copies were analyzed.

Regarding the demographics of respondents (Table 2), males and females were 48.9% and 51.1%, respectively. 34.7%, 32.2% and 33.1 of respondents were in their 20s, 30s and 40s and older, respectively. Those living in the capital area accounted for 65% in comparison to 35% living in other regions. The largest numbers of respondents (54.9%) were employees, followed by students (13.6%), other occupations (12.9%), professionals (12.9%), small business owners (3.2%) and public servants (2.5%) in the order named.

Table 2. Demographic characteristics

Classification		Frequency (unit:people)	Distribution (%)
Gender	Male	155	48.9
	Female	162	51.1
Age	20s	110	34.7
	30s	102	32.2
	More than 40s	105	33.1
Region	Capital area	206	65.0
	Other than capital area	111	35.0
Job	Public officials	8	2.5
	Salaried worker	174	54.9
	Professionals	41	12.9
	Self-employed	10	3.2
	Student	43	13.6
	Etc.	41	12.9

4.2 Reliability and Validity

The PLS analysis requires testing internal consistency, convergent validity, and discriminant validity of question items and constructs. To test the internal consistency, the user support, perceived security, perceived ease of use, perceived usefulness, satisfaction and use intention were analyzed in terms of Fornell and Larcker[34]'s composite reliability and internal consistency. Table 3 shows the analysis results. The composite reliability proved to be higher than 0.7, the reference standard suggested by Nunnally[35] and Thompson et al.[36]. The Cronbach's α, widely in use for testing the reliability, proved to be 0.7 and higher, indicating the internal consistency was good.

Table 3. Internal consistency analysis

Construct	Composite reliability	Cronbach's α
USP	0.916	0.924
PSC	0.941	0.906
PEOU	0.940	0.904
PU	0.938	0.911
SFC	0.943	0.924
IU	0.953	0.935

The convergent validity was tested with AVE and factor loadings of constructs. As in Table 4, the AVE proved to be higher than 0.5, the reference standard suggested by Fornell and Larcker[34] and Chin[37]. All factor loadings of constructs proved to be 0.7, the reference standard suggested by Fornell and Larcker[34].

Table 4. Internal consistency analysis

Construct	AVE	Item	Factor loading	t-value
USP	0.56	USP1	0.829	38.899
		USP2	0.847	45.313
		USP3	0.873	42.291
		USP4	0.874	48.123
PEOU	0.71	PEOU1	0.912	75.087
		PEOU2	0.919	61.936
		PEOU3	0.917	71.932
PU	0.81	PU1	0.915	85.001
		PU2	0.839	33.300
		PU3	0.926	99.021
		PU4	0.872	52.193
IU	0.88	IU1	0.919	79.500
		IU2	0.906	64.886
		IU3	0.940	118.570
		IU4	0.893	50.328
SFC	0.70	SFC1	0.839	33.650
		SFC2	0.833	30.860
		SFC3	0.897	73.162
		SFC4	0.900	73.357
		SFC5	0.909	79.423
PSC	0.70	PSC1	0.905	74.188
		PSC2	0.937	129.578
		PSC3	0.910	74.342

As in Table 5 the discriminant validity was tested based on whether the square root of every AVE marked on the diagonal axis of correlation coefficients was bigger than the coefficients of the other constructs. As a result, the smallest square root of AVE (0.856) was bigger than the largest coefficient (0.773), indicating the discriminant validity was good.

Table 5. Correlation between latent variables

Construct	SFC	IU	USP	PSC	PEOU	PU
SFC	0.876					
IU	0.725	0.915				
USP	0.658	0.560	0.856			
PSC	0.569	0.638	0.574	0.917		
PEOU	0.560	0.460	0.469	0.246	0.916	
PU	0.764	0.773	0.630	0.638	0.483	0.889

The present study performed the confirmatory factor analysis as in Table 6. In the confirmatory factor analysis, the factor loading of a construct should be higher than those of the other constructs. As a result, every question item met the requirement.

Table 6. Confirmatory factor analysis

Construct	USP	PEOU	PU	IU	SFC	PSC
USP1	0.829	0.403	0.564	0.492	0.562	0.520
USP2	0.847	0.376	0.579	0.521	0.582	0.558
USP3	0.873	0.415	0.482	0.455	0.533	0.448
USP4	0.874	0.410	0.536	0.454	0.575	0.447
PEOU1	0.441	0.912	0.489	0.464	0.554	0.224
PEOU2	0.444	0.919	0.432	0.391	0.499	0.244
PEOU3	0.401	0.917	0.400	0.404	0.479	0.209
PU1	0.588	0.509	0.915	0.740	0.740	0.589
PU2	0.528	0.357	0.839	0.587	0.608	0.501
PU3	0.595	0.431	0.926	0.708	0.690	0.605
PU4	0.524	0.408	0.872	0.699	0.669	0.564
IU1	0.482	0.461	0.694	0.919	0.687	0.554
IU2	0.526	0.427	0.732	0.906	0.663	0.591
IU3	0.521	0.444	0.726	0.940	0.676	0.588
IU4	0.522	0.349	0.673	0.894	0.627	0.602
SFC1	0.530	0.439	0.596	0.570	0.839	0.449
SFC2	0.552	0.477	0.597	0.526	0.833	0.413
SFC3	0.591	0.482	0.718	0.687	0.897	0.552
SFC4	0.613	0.576	0.633	0.606	0.900	0.451
SFC5	0.593	0.482	0.775	0.755	0.909	0.600
PSC1	0.515	0.263	0.603	0.612	0.520	0.905
PSC2	0.551	0.186	0.602	0.594	0.543	0.937
PSC3	0.514	0.229	0.547	0.546	0.502	0.909

As above mentioned, the constructs and question items used here were found to be fit for the structural model analysis as their internal consistency, convergent validity and discriminant validity met the reference requirements.

4.3 Structural Model Analysis

In the PLS analysis, the explanatory power of the path model is expressed as the explained variance, R^2[38]. The PLS analysis of R^2 showed the perceived ease of use, perceived usefulness and satisfaction explained 64.2% of the use intention, whilst the perceived ease of use and perceived usefulness explained 63.1% of satisfaction, which exceeded Falk and Miller[39]'s power (10%). Next, in GoF (goodness-of-fit) testing, the impact of GoF was 0.635, which was higher than Wetzels et al.[40]'s reference standard, indicating a very high goodness of fit of the model.

With the PLS analysis, path coefficients and their significance were tested. For this, the full sample was used to find out the path coefficients of the structural model. The bootstrapping provided in PLS was used to calculate the t-value for the path coefficient. Table 7 summarizes the analysis results. The results of the analysis are as follows in the order of hypotheses. In brief, 7 out of 8 hypotheses set up in the present study except the hypothesis 6 were found significant and adopted.

Table 7. The results of the hypotheses

Hypothesis		Path coefficient	t-value	Result
H1	USP → PEOU	0.469	9.657	Supported
H2	PSC → PU	0.552	11.983	Supported
H3	PEOU → SFC	0.249	5.152	Supported
H4	PU → SFC	0.664	16.354	Supported
H5	SFC → IU	0.308	5.168	Supported
H6	PEOU → IU	0.037	0.776	Not supported
H7	PEOU → PU	0.347	8.448	Supported
H8	PU → IU	0.520	9.984	Supported

5. Discussion

The user support was found to have positive effects on the perceived ease of use (β=0.469). Those who used to draw on their resident registration numbers or mobile authentication would not find it easy to use i-PINs including their issuance process. Particularly, the senior citizens are not accustomed to computer and Internet and are likely to find it difficult to understand the technology and thus become unwilling to learn how to use i-PINs. Therefore, the entities operating i-PINs need to develop creative and efficient ways to increase their user supports so that users will perceive using i-PINs is not difficult.

The perceived security was found to have positive effects on the perceived usefulness (β=0.552). As a service for protecting personal information, the i-PIN system prevents personal information from being leaked on the internet, in which sense security is the overriding component. All systems that are potentially connected to external networks have vulnerabilities to security issues. So does the i-PIN system. The servers managed by the i-PIN operators might be attacked by hackers. The information delivered to the i-PIN servers from personal computers of users might suffer sniffing and spoofing. As such, the i-PIN system in its entirety is exposed to severe potential risks. Despite the possibility of i-PIN data being exposed on networks, technical encryption measures should be taken so that hackers cannot read the plain texts of data unlawfully acquired.

The perceived ease of use had significant effects on the perceived usefulness (β=0.347) and satisfaction (β=0.249), whereas it did not exert direct effects on the use intention. Those who are unwilling to use i-PINs pointed to the complexity of the issuance procedures, the installation of Active X or multiple other security programs and the requirement to enter the illegible security characters, all of which should be improved to raise the perceived ease of use of i-PINs. If using i-PINs remains challenging, users will get back to the conventional authentication methods. Such challenging aspects hinder further penetration of i-PINs, which has significant implications for i-PIN-related policy makers.

The perceived usefulness proved to be the variable having the most significant effects on the use intention (β=0.520) and satisfaction (β=0.664). To increase the perceived usefulness, its antecedent, that is, the perceived security should be considered. It is important to guide potential users to become aware of the advantages of i-PINs over certificates or mobile authentication. To that end, in addition to the aforementioned technical security measures, i-PIN-related campaigns or advertisements should strategically emphasize the privacy protection and the prevention of personal information from any leakage gained by using i-PINs.

Satisfaction as a variable was found to have positive effects (β=0.552) on the intention to use i-PINs. When users are forced into using the system, they feel dissatisfied because they have to use it without resistance. The present study empirically demonstrated the satisfaction with i-PINs instead of the attitude variable had mediating effects on TAM's core elements. Furthermore, the present survey findings suggested that the attitude variable in the conventional TAM should possibly be replaced in the sense that the perceived usefulness affected the use intention not directly but indirectly via the satisfaction. Thus, the present study proposes that the satisfaction variable should be considered in the environment where a certain means of authentication is enforced by the government or other organizations.

6. Conclusion

This study built on previous studies on authentication methods to propose a model with additional variables likely to exert effects on the intention to accept i-PINs. To verify empirically the proposed model, those who were aware of i-PINs were surveyed online with the help of a research firm. The selection of variables from the features of authentication methods will give a fresh insight into developing a model for generalization. Also, the academic value of this study lies in the fact that previous studies hardly investigated the psychological perception and behavioral attributes of i-PIN users excluding a few simple questionnaire surveys. The present findings will be conducive to further studies on psychological aspects of i-PIN users.

i-PINs are not used prevalently given the fact that it has been adopted for a decade. The present findings will help policy-makers understand how people think of i-PINs and what they value. Especially, the government should give priority to understanding the complexity of the issuance procedures of i-PINs, the settings of many security programs and the inconvenience of entering security characters. The present findings will facilitate the government's understanding of budget priorities in addition to the i-PIN PR campaign.

The present study lacked in considering demographic variables. The intention to use information systems may vary with gender or age, which could be proved by analyzing the moderating effects of demographic variables. In addition to such demographic variables as gender, occupation, education and income levels, the moderating effects of personal experience of authentication methods and of leakage of personal information should be considered. Future studies need to establish the variables comparable to the perceived security such as the perceived

risk, perceived privacy and perceived trust. Finally, it is worth investigating whether any significant difference arises when the resistance to authentication methods, not the intention to accept those, is included as a dependent variable in a model.

7. References

1. Choi GH, Ahn JC, Lee GS, Ahn SH. The i-PIN 2.0 Service Framework Replacing the Use of Resident Registration Number over Internet. Journal of Korea Institute of Information Security & Cryptology. 2010; 20(6):88–95.
2. Kim DH. The Resident Registration Number has been collected about 370 million times. OhmyNews. 2014 Feb 9 [cited 2015 August 24]. Available from: http://www.ohmynews.com/NWS_Web/View/at_pg.aspx?CNTN_CD=A0001959786
3. National Intelligent Service (NIS), Ministry of Science, ICT and Future Planning, Korea Communications Commission, Ministry of Security and Public Administration. National Information Security White Paper. Korea; 2014.
4. Jung CJ, Kim YJ, Kim JW, Park GJ. The i-PIN Standard and Service Framework for the Development of Alternative of the Resident Registration Number. Journal of Korea Institute of Information Security & Cryptology. 2008; 18(6):20–7.
5. Han MJ, Choi GH, Hong SH, Lim JI. A Study on reforming the national personal identification number system: The unconnected random personal identification number system. Journal of the Korea Institute of Information & Cryptology. 2014; 24(4):721–37.
6. Kim HJ, Shin IC, Lee SJ. Implementation of personal certification using i-PIN Service. Journal of the Korea Society of Computer and Information. 2012; 17(7):117–28.
7. Choi GH, Jung SW, Lee GS, Ahn SH. i-PIN Development Strategy for National ID Management. Journal of Korea Institute of Information Security & Cryptology. 2011; 21(4):40–6.
8. Yoo JH. People are reluctant to use i-PIN because the procedure for joining and issuance is inconvenient. JoongAng Sunday. 2014 Feb 9 [cited 2015 August 24]. Available from: http://sunday.joins.com/archives/7511
9. Taherdoost H, Sahibuddin S, Jalaliyoon N. Smart Card Security; Technology and Adoption. International Journal of Security. 2011; 5(2):74–84.
10. Dimitrova DV, Chen YC. Profiling the Adopters of E-Government Information and Services, the Influence of Psychological Characteristics, Civic Mindedness, and Information Channels. Social Science Computer Review. 2006; 24(2):172–88.
11. Yeom HY, Lee DT. The development direction of alternative means of the resident registration number on the internet. The Magazine of IEEE. 2005; 32(11):61–73.
12. Harbach M, Fahl S, Rieger M, Smith M. On the acceptance of privacy-preserving authentication technology: The curious case of national identity cards. Privacy Enhancing Technologies. 2013; 7981:245–64.
13. Shin YJ. A Study on the Improvement through Diffusion and Application of i-PIN. The Korea Association for Policy Studies. 2013; 22(3):171–99.
14. Yun HJ, Jang JB, Lee CC. Drivers for trust and continuous usage intention on OTP: Perceived security, security awareness, and user experience. Journal of the Korea Society of Computer and Information. 2010; 15(12):163–73.
15. Aubert BA, Hamel G. Adoption of smart cards on the medical sector: The canadian experience. Social Science & Medicine. 2001; 53(7):879–94.
16. Loo WH, Yeow PHP, Chong SC. User acceptance of malaysian government multipurpose smartcard applications. Government Information Quarterly. 2009; 26(2):358–67.
17. Herath T, Chen R, Wang J, Banjara K, Rao JWHR. Security services as coping mechanisms: An investigation into user intention to adopt an Email Authentication Service. Information Systems Journal. 2014; 24(1):61–84.
18. Zviran M, Erlich Z. Identification and Authentication: Technology and Implementation. Communication of the Association for Information Systems. 2006; 17(4):90–105.
19. Furnell SM, Dowland AS, Illingworth HM, Reynolds PL. Authentication and Supervision: A Survey of User Attitudes. Computer & Security. 2000; 19(6):529–39.
20. Davis FD, Bagozzi RP, Warshaw PR. User acceptance of computer technology: A comparison of two theoretical models. Management Science. 1989; 35(8):982–1003.
21. Fu JR, Fam CK, Chao WP. Acceptance of Electronic Tax Filing: A Study of Taxpayer Intentions. Information & Management. 2006; 43(1):109–26.
22. Kim HW, Kankanhalli A. Investigating User Resistance to Information Systems Implementation: A Status Quo Bias Perspective. MIS Quarterly. 2009; 33(3):567–82.
23. Kim SH, Song YM. An empirical study on user's intention to use government portal sites: moderating effects of ambiguity & government supports. The Journal of Information Systems. 2009; 18(1):117–44.
24. Gu SH, Kim DW, Park CM, Kim KH. Influence of LTE characteristic and personal innovativeness on LTE smart phone acceptance. Journal of Digital Contents Society. 2013; 14(3):291–301.
25. Im DB, Jaegal D, Park TJ. A study on the information technology acceptance for electronic policy participation: Internet electronic voting. Korean Public Administration Quarterly. 2009; 21(2):375–406.
26. Bae JK. An Empirical Study on the Effects of Perceived Privacy, Perceived Security Perceived Enjoyment, on Continuance Usage Intention in Mobile Cloud Computing. The E-Business Studies. 2014; 15(3):3–27.
27. Limayem M, Cheung CMK. Understanding Information Systems Continuance: The Case of Internet-based Learning Technologies. Information & Management. 2008; 45(4):227–32.
28. Liu Y, Zhou C. A Citizen Trust Model for E-government. 2010 IEEE International Conference on Software Engineer-

ing and Service Sciences; 2010. p. 751–54.
29. Wang BR, Park JY, Chung KY, Choi IY. Influential factors of smart health users according to usage experience and intention to use. Wireless Personal Communications. 2014; 76(4):2671–83.
30. Ma WWK, Andersson R, Streith KO. Examining user acceptance of computer technology: An empirical study of student teachers. Journal of Computer Assisted Learning. 2005; 21(6):387–95.
31. Wang YS. The Adoption of Electronic Tax Filing Systems: An Empirical Study. Government Information Quarterly. 2003; 20(4):333–52.
32. Carter L, Bélanger F. The utilization of E-Government services: Citizen trust, innovation and acceptance factors. Information Systems Journal. 2005; 15(1):5–25.
33. Ringle CM, Wende S, Will A. SmartPLS 2.0. Hamburg: University of Hamburg; 2005.
34. Fornell C, Larcker D. Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research. 1981; 18(1):39–50.
35. Nunnally JC, Psychometric Theory. NY: McGrow-Hill; 1987.
36. Thompson R, Barclay DW, Higgins CA. The Partial Least Squares (PLS) Approach to Causal Modeling: Personal Computer Adoption and Use as an Illustration. Technology Studies: Special Issue on Research Methodology. 1995; 2(2):284–324.
37. Chin WW. The Partial Least Squares Approach to Structural Equation Modeling. Modern Methods for Business Research. 1998; 295–336.
38. Chin WW, Gopal A. Adoption Intention in GSS: Importance of Beliefs. ACM SIGMIS Database. 1995; 26(2-3):42–64.
39. Falk RF, Miller NB. A Primer for Soft Modeling. Ohio: University of Akron Press; 1992.
40. Wetzels M, Odekerken-Schröder G, Oppen CV. Using PLS Path Modeling for Assessing Hierarchical Construct Models: Guidelines and Empirical Illustration. MIS Quarterly. 2009; 33(1):177–95.