韓國IT서비스學會誌
第16卷 第2號
2017年 6月, pp.97-110

Journal of Information Technology Services
https://doi.org/10.9716/KITS.2017.16.2.097

아이핀 기반 본인확인서비스의 안전성 강화 방안*

김 종 배**

Safety Improvement Methods of Personal Identification Services using the *i*-Pin*

Jongbae Kim**

■ Abstract ■

Due to development of IT, various Internet services via the non-face-to-face are increasing rapidly. In the past, the resident registration numbers (RRN) was used a mean of personal identification, but the use of RRN is prohibited by the relevant laws, and the personal identification services using alternative means are activated. According to the prohibition policy of RRN, i-PIN service appeared as an alternative means to identify a person. However, the user's knowledge-based i-PIN service continues to cause fraudulent issuance, account hijacking, and fraud attempts due to hacking accidents. Due to these problems, the usage rate of i-PIN service which performs a nationwide free personal identification service, is rapidly decreasing. Therefore, this paper proposes a technical safety enhancement method for security enhancement in the i-PIN-based personal identification service. In order to strengthen the security of i-PIN, this paper analyzes the encryption key exposure, key exchange and i-PIN authentication model problems of i-PIN and suggests countermeasures. Through the proposed paper, the i-PIN can be expected to be used more effectively as a substitution of RRN by suggesting measures to enhance the safety of personal identification information. Secured personal identification services will enable safer online non-face-to-face transactions. By securing the technical, institutional, and administrative safety of the i-PIN service, the usage rate will gradually increase.

Keyword : i-PIN, Personal Identification Service, Alternative Means of Resident Registration Number Service, Identification Means

Submitted : January 30, 2017 1st Revision : June 6, 2017 Accepted : June 14, 2017

* 본 연구는 「주민번호 대체수단 안전성 강화 방안」 연구의 성과물이며, 대한전자공학회(2015) 추계학술대회 논문을 수정하여 게재하였으며, 한국인터넷진흥원 연구용역과 교과부 일반연구자원사업의 지원을 받아서 수행되었음(NRF-2016R1D1A1B03931986).

** 서울디지털대학교 컴퓨터공학과 교수

1. 서 론

IT기술의 발전에 따라 전자상거래서비스가 급성장하면서 이용자의 개인정보를 불법적으로 수집·도용하는 피해사례가 빈번히 발생하고 있으며, 바이러스, 악성 봇 등 해킹기법이 지능화되고 있어 인터넷상의 주민등록번호 대체수단을 통한 본인확인 서비스의 안전성과 신뢰성이 요구되고 있다(Choi and Kim, 2015; Shin et al., 2015; Heo et al., 2013). 주민등록번호 대체수단이란 이용자가 자신의 신원정보를 신뢰할 수 있는 기관(본인확인기관)에게 제공하여 본인임을 확인한 뒤 한국인터넷진흥원(KISA)이 인정하는 기술을 이용하여 본인확인정보(연계정보(Connecting Information : CI), 중복가입확인정보(Duplicative Joining Verification Information: DI) 등)와 매핑 되어 있는 대체수단(아이핀, 공인인증서, 휴대전화)을 발급받아 인터넷 사이트 회원가입이나 성인인증 등을 위해 주민등록번호 대신 사용하는 것을 말한다(Jang and Shin, 2013; Jang and Youm, 2009; Choi et al., 2010; Choi et al., 2011; Im and Kim, 2015). 본인확인수단 중 아이핀은 대면확인이 어려운 인터넷상에서 명의도용이 쉬운 주민등록번호를 대신하여 본인확인을 할 수 있는 지식 기반(ID/PW)의 개인식별 수단으로 국민 보편타당한 서비스라는 관점에서 추가비용 없이 발급이 가능한 주민등록번호대체 대체수단이다. 아이핀 서비스의 특징으로는 주민등록번호 유출로 인한 개인정보 침해사고를 근본적으로 예방하고, 언제든지 재발급 및 사용중지 할 수 있어 도용의 위험감소, 이용자는 아이핀 인증이력을 확인할 수 있어 타인에 의한 도용을 추적이 가능하고, 발급 받은 본인확인기관에 상관없이 국내 공공, 민간 모든 웹사이트에서 이용이 가능하다(Choi et al., 2010; Shin, 2013; Kim, 2007). 2008년 6월에는 법제도상으로 주민등록번호 대체수단인 아이핀 서비스 이용활성화를 위해 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 개정되었다. 동법에서는 일일평균 이용자수가 일정 수 이상인 정보통신서비스 제공자에 대하여 주민등록번호 외에도 회원가입수단 제공을 의무화하였다. 또한 「개인정보보호법」에서도 일정한 기준에 해당하는 개인정보처리자는 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입할 경우, 주민등록번호를 사용하지 않고도 회원으로 가입할 수 있는 방법을 제공하도록 규정하고 있다. 이와 같이 인터넷상 전자상거래서비스 등에서 본인확인이 필요한 경우에 주민등록번호의 사용을 제한하고, 대체수단을 이용할 수 있는 법·제도의 정비 및 대체수단 이용을 활성화하기 위한 기술적 보완조치를 마련하였음에도 불구하고, 최근에도 주민등록번호의 도용 및 유출사고가 자주 발생하고 있다. <Table 1>과 감사원의 '국가사이버 안전관리 실태 보고서'(Audit and Inspection Report, 2016)와 같이 공공 아이핀 해킹으로 인한 부정발급으로 아이핀의 발급 신청 건수가 크게 감소하였으며 탈퇴율도 급격하게 증가하고 있는 추세에 있다. 특히 아이핀 기반의 본인확인서비스 이용도 예년에 비해 크게 감소하였음을 알 수 있다.

〈Table 1〉 Annual Trend of Public i-Pin

Year	Site	Issued	Withdraw	Used
2012	5,247	617,179	15,436	4,451,594
2013	793	892,771	8,404	12,030,884
2014	258	1,525,888	17,567	17,884,144
2015	158	1,744,279	23,258	21,323,336
2016.06	87	840,620	56,170	8,797,584

공공 아이핀 해킹사고를 통해 그동안 아이핀 서비스 기관들은 자체 점검과 자율적인 시정 노력에 의해 비교적 안전에게 본인확인서비스가 운영되고 있음을 피력하고 있었으나 실제 보안사고 발생을 대비한 유기적인 체계는 갖추고 있지 못한 상황임을 아이핀 이용자 탈퇴로 엿볼 수 있다(Kim et al., 2015; Lee et al., 2015). 더구나 감사원 보고서에 따르면 휴대폰을 통한 본인확인서비스 이용률이 급격히 증가하고 있어 아이핀을 통한 본인확인서비스의 폐지를 검토하고 있는 상황이다. 그러나 휴대폰

및 범용공인인증서의 경우 휴대폰 번호 유지비용, 범용 공인증서 발급 비용을 서비스 이용자가 자체적으로 부담하고 있으나, 아이핀의 경우 저소득층 및 사회취약 계층, 국내거주 외국인 등은 본인확인기관을 직접 방문을 통해 온라인상에서의 본인확인 수단인 아이핀을 발급 받을 수 있는 이점이 있어 국가적으로도 아이핀 서비스의 지속적인 유지가 필요한 상황이다.

1.1 기존 연구

지금까지 아이핀 서비스의 문제점으로 불편한 UI, 사용자에 의한 추가 작업 부담, 인터넷사업자의 비용 부담 등 아이핀 서비스에 대한 기술적인 보안 방안 보다는 서비스 활성화 위주에 연구가 주류를 이루고 있는 상황이다(Jang and Youm, 2009). 기술적인 취약점과 대책 마련 연구로는 MITM (Man-In-The-Middle) 기반의 액티브 피싱 공격으로부터 아이핀 서비스의 안전성 강화를 위해 클라이언트 상에서 실행되는 아이핀 인증모듈의 보안성 강화와 대책 마련을 주문하고 있으나 실제 본인확인기관들이 마련할 수 있는 대책은 제시하지 못하고 있다(Kim and Choi, 2014; Jun and Kim, 2014). 그리고 본인확인수단에 대한 적합성 기준 제시, 신규 인증수단에 대한 방안 제시 연구는 진행되어 왔으나 실제 본인확인수단에 적용 가능한 기술적인 수단에 대한 안전성 검토 연구는 진행하지 못하고 있는 상황이다(Shin et al., 2015). 본인확인서비스에 대한 안전성 강화 방안을 위해 현재의 아이핀 서비스 문제점과 이에 대한 해결책을 제시한 기존 연구에서는 제도적인 대책 마련, 그리고 법적인 점검 기준 강화, 보안사고 발생 시 처벌에 대한 기준 마련 등을 제시하고 있어 실제 기술적인 보안 방안에 대해서는 제시하지 못하고 있다(Choi and Kim, 2015).

1.2 문제 정의

공공아이핀 해킹을 통한 75만 건의 부정발급사례와 같이 현행 아이핀 기반 본인확인서비스에 대한 기술적인 안전성 강화방안이 요구되고 있다. 특히 아이디와 패스워드를 통해 아이핀 본인확인서비스는 이용자의 주민등록번호를 검색하여 암호화 알고리즘을 통해 연계정보와 중복가입확인정보를 생성하여 인터넷서비스제공업체(ISP)에게 제공하는 과정에서 수많은 보안적인 이슈가 존재한다. 따라서 본 논문에서 아이핀 서비스 과정에서 발생 가능한 문제점을 나열하고 이들을 해결하기 위한 방안을 기술한다. 아이핀 기반 본인확인서비스에서 제기하는 문제들에는 첫 번째로 아이핀 서비스 설계 이후 암호화 알고리즘에 대한 보안성에 대한 검증이 이루어지고 있지 않으며 암호화 알고리즘 유출 시 대응 방안을 마련하지 못하고 있는 점이다. 두 번째로는 아이핀 본인확인기관 간의 이용자 개인정보 연동 시 암호화하는 암호화키 분배 프로토콜에 대한 안전성 강화 방안 마련이 미흡한 점이다. 세 번째로는 아이핀 서비스 이용자가 개인정보를 입력하는 아이핀 인증모듈에 대한 취약점으로 정보 노출의 위험성이 있는 점이다. 마지막으로 본인확인서비스의 제도적 관리방안 미흡으로 인해 아이핀 서비스 이용자 개인정보 유·노출에 대한 위험이 증가하여 아이핀 서비스 이용자의 감소로 귀결되는 문제가 발생한다.

1.3 제안 방안

본 논문에서는 공공 아이핀 부정발급에 대한 이용자의 인식 변화와 함께 강화된 아이핀 서비스를 위해 서비스 이용자 관점에서의 안전성 강화 방안을 제시하고자 한다. 아이핀 서비스의 안전성 강화 방안에는 첫째, 아이핀 서비스에서 주민등록번호의 암호화를 위한 암호화키에 대한 유출 가능성을 검토하고 유출 발생 시 대응하기 위해 키관리서버(HSM)의 도입, 강화된 사용자 인증, 2-factor 접근통제방안 등을 제시한다. 그리고 본인확인기관 간의 서비스 이용자 정보 연동 시 네트워크 구간 간 암호화키에 분배 알고리즘의 보안성 검토를 통해 전자여권에

적용하는 보안 메커니즘을 적용하는 방안을 제시한다. 아이핀 서비스 이용자들이 직접 이용자 정보를 입력하는 인증모듈에 대한 취약점 발생 원인을 분석하고 ISP 사업자들에게 설문조사를 통해 해당 원인을 감소시키기 위한 관리적·기술적·제도적 방안 제시한다. 마지막으로 아이핀 본인확인기관들을 제도적으로 관리·감독 이행을 위한 방안도 제안한다.

본 논문의 구성은 제 2장에서 아이핀 기반 본인확인서비스의 문제점과 대응방안들을 나열하고 최종적으로 아이핀 본인확인서비스의 기술적 안전성을 강화하기 위한 서비스 절차적인 방안을 제시한다. 제 3장에서는 아이핀 본인확인서비스의 안전성 강화를 위해 제도적인 정비 세 가지 방안을 제시하고, 마지막 제 4장에서는 결론을 맺는다.

2. 기술적 안전성 강화 방안

2.1 아이핀 서비스 개요

주민등록번호를 대체하여 본인임을 확인하는 대체수단 중 아이핀 서비스는 인터넷 상에서 주민등록번호를 대신하여 아이핀 아이디와 패스워드를 이용하여 본인확인을 받는 대표적인 주민등록번호 대체수단이다. 아이핀 아이디와 패스워드를 이용하면 웹사이트에 더 이상 주민등록번호를 이용하지 않아도 회원가입 및 기타 서비스 이용이 가능하다. 더구나 아이핀 인증만으로 이용자의 성명, 생년월일, 성별, 연령대 정보, 내·외국인 정보 등을 제공하고 있다. 아이핀 서비스의 사용은 아이핀 발급 과정과 아이핀을 이용한 본인인증 과정의 두 가지로 구분된다. 사용자는 인터넷 웹사이트에 가입을 할 경우 아이핀을 발급받는 과정을 별도로 진행 한 후에 가입을 완료할 수 있으며, 이미 아이핀이 있는 경우 별도의 인증 필요시에는 아이핀 식별아이디와 암호만으로 간편하게 본인인증과정을 진행할 수 있다(Lee et al., 2007). 아이핀은 13자리로 구성된 임의의 변수로 본인확인기관 구별을 위한 2자리를 이용하여 본인확인기관을 구분할 수 있으며, 본인확인기관은 아이핀을 통하여 본인확인기관명, 이름, CI, DI, 성별, 나이, 국적, 생년월일 등의 정보를 인터넷 서비스 제공 사업자(ISP)에게 제공한다. 실제 이용자의 주민등록번호에 해당하는 연계정보는 이용자의 주민등록번호를 사용하여 이를 암호화 과정을 통해 생성한다. <Figure 1>(Choi et al., 2011)과 같이 CI는 사용자의 주민등록번호에 기반을 두어 해쉬(hash)를 적용한 연계정보를 생성하고 사업자간 다양한 제휴서비스를 위해 사용하거나 서로 다른 웹사이트 간에도 동일 이용자로 구분할 수 있다.

〈Figure 1〉 Connecting Information(CI) Creation Process

이용자가 본인확인기관 홈페이지에 접속하여 아이핀 서비스에 가입하면 본인확인기관에서는 이용자의 아이핀 아이디를 KISA에 전송하고, 본인확인기관이 이용자의 주민등록번호와 KISA로부터 전달받은 식별정보 생성 알고리즘에 따라 아이핀 번호 및 연계정보 등을 생성한다. 식 (1)은 CI와 DI 생성 과정에서 사용되는 암호화키로써 CI 생성에 사용되는 열쇠 2개(S_A, sk)와 중복가입확인정보에 사용되는 열쇠 1개(SK)이다. 즉, 본인확인기관이 CI와 DI 생성을 위해 안전하게 관리해야 할 키는 총 3개이다(Choi and Kim, 2015).

$$CI = HMAC_{sk}((RN \| Padding) \oplus S_A) \quad (1)$$

$$DI = HMAC_{SK}(H(RN \| SI))$$

여기서, $H()$: 512비트(64바이트) 이상의 출력을 갖는 암호학적으로 안전한 해쉬 함수, RN : Resident Number, 주민등록번호(13byte = 104bit), $Padding$: 입력 값을 512bit로 만들기 위해 주민번호 104bit를 제외한 408bit를 '0…0'으로 채워 넣음, S_A : Secret Information A, 본인확인기관과 KISA가 공유하는

비밀정보(64byte = 512bit), sk : Secret Key, 본인확인기관과 KISA가 공유하는 비밀키(64byte = 512bit), 그리고 || : concatenation, 기호의 앞뒤를 연접 기호이다.

DI는 인터넷사업자가 운영하는 웹사이트에 가입하고자 하는 이용자의 중복가입 여부를 확인하는데 사용되는 정보로서 본인확인기관이 이용자의 주민등록번호, 웹사이트 식별번호 및 본인확인기관 간 공유 비밀정보를 이용하여 생성한 정보이다. DI 생성을 위해서는 인터넷사업자는 본인확인기관으로부터 사이트 식별정보(SI)를 부여 받아야 한다. 사이트 식별정보는 아이핀 서비스 적용 시 최초 계약한 본인확인기관으로부터 발급받아 사용하고, 이후 계약한 모든 본인확인기관은 최초 계약에 의해 부여된 사이트 식별정보를 이용하여 중복가입확인정보를 생성한다. 또한, 본인확인기관은 DI를 생성하기 위하여 모든 본인확인기관에 동일한 비밀정보를 안전하게 공유 및 관리해야 한다. 인터넷사업자는 DI를 이용하여 중복가입 여부를 확인하기 위하여 본인확인기관에서 생성하여 전달받은 DI를 반드시 보관 및 관리해야 한다. 또한 본인확인기관에서 사용자 인증 시 확인된 사용자의 실명을 보관해야 한다. DI 생성 방법은 본인확인기관은 인터넷사업자로부터 본인확인정보 유효성 확인 요청을 받은 경우 또는 이용자의 본인확인정보를 인터넷사업자에게 전달하도록 요청하는 경우 DI를 생성하여 인터넷사업자에게 함께 제공한다. 위의 각각의 경우에 인터넷사업자의 사이트 식별번호는 반드시 본인확인기관에 전달되어야 한다. 본인확인기관은 DI를 아래의 생성절차에 따라 생성하여 인터넷사업자에게 제공해야 한다. 본인확인기관은 이용자의 주민등록번호(RN)와 요청 시 전달받은 웹사이트 식별정보(SI)를 연접하여 안전한 해쉬함수에 입력하여 해쉬값을 식 (2)와 같이 얻는다.

$$Temp = H(RN \| SI) \quad (2)$$

본인확인기관 간 공유된 비밀정보(SK)를 키 값으로 해쉬값($Temp$)를 안전한 해쉬함수에 입력하여 HMAC 값을 생성하여 DI를 식 (3)과 같이 얻는다.

$$DI = HMAC_{SK}(Temp) \quad (3)$$

본인확인기관은 위의 절차에 따라 생성된 CI, DI 정보 소유자의 실명(UN) 및 본인확인정보를 인터넷사업자에게 전달한다.

2.2 안전성 강화 방안

2.2.1 암호화키 유출 및 대응방안

아이핀 기반의 본인확인서비스는 서비스 이용자의 주민등록번호를 암호화 알고리즘을 통해 연계정보(CI)와 중복가입확인정보(DI)를 생성하여 ISP에게 전달하여 본인임을 확인한다.

① 문제점 : CI/DI 생성에 사용되는 키가 권한이 있는 내부자가 의도적으로 키값이 유출되는 경우 해당 키값이 획득한 자는 임의로 CI/DI를 생성할 수 있게 된다. 또한 소스코드에 키를 저장할 경우 개발자들이 실제 운용되고 있는 키에 접근할 수 있고 이로 인한 키 유출의 위험이 발생할 수 있으며 소스코드가 유출될 경우 이로 인해 암호화키까지 함께 유출되는 위험이 발생할 수 있다. 메모리에 키가 저장되어 있을 경우에도 악성코드 등으로 인한 키 유출의 위험이 발생할 수 있다. 앞 절에서 설명한 것과 같이 본인확인기관에서 안전하게 관리해야 할 키는 CI 생성에 사용되는 키 2개(S_A, sk)와 DI에 사용되는 키는 1개(SK)이다. <Table 2>는 각 키가 개별로 유출될 경우의 위험을 고려한 것이다. <Table 2>에서 알 수 있듯이 DI의 경우 한 개의 키(SK)를 알면 임의의 주민등록번호를 이용하여 임의의 사용자에 대한 DI 값을 생성할 수 있는 반면, CI는 두 개의 키(S_A와 sk)를 모두 알아야만 임의의 사용자에 대한 CI 값을 생성할 수 있다(Choi and Kim, 2015).

② 대응방안 : 암호화키 값 유출에 대한 대응방안으로는 내부 관리자에 대한 키관리시스템의 강화

〈Table 2〉 Encryption Key Risk Scenarios Used by the CI/DI Generation(Choi and Kim, 2015)

Keys used to generate CI/DI	Risk Scenario
S_A : key used for the RRN and XOR operation when generating CI	Even if you know S_A, you can not create CI because you do not know sk, $CI = HMAC_{sk}((RN\|Padding)\oplus S_A)$
sk : Secret key that is input to HMAC when generating CI	Even if you know sk, you can not create CI because you do not know S_A, $CI = HMAC_{sk}((RN\|Padding)\oplus S_A)$
SK : Key used to generate DI	If SK is exposed, DI generation is possible as follows $DI = HMAC_{SK}(H(RN\|SI))$

된 접근통제 방안이 필요하다. 그리고 키 유출에 대한 비상상황 대응 방안 마련도 필요하다. KISA 내부에서 운영 중인 아이핀 연계시스템의 접근통제 강화를 위해 2 factor 이상의 사용자 인증과 인가된 IP와 MAC에서의 접근 허용 등 인가된 단말기에서 접근, HSM과 같은 키관리시스템의 적용 등이 암호화키 유출에 대한 적절한 대응 방안이다.

2.2.2 본인확인기관 간 암호화키 분배 프로토콜 안전성 부재

본인확인서비스 이용자가 가입한 본인확인기관이 아닌 다른 본인확인기관에게 아이핀 인증을 받기 위해서는 본인확인기관 간 정보 연동이 필요하다. 즉, 아이핀 이용자가 가입한 본인확인기관과 ISP가 계약을 체결한 본인확인기관이 상이할 경우 이용자의 편의성 증대를 위해 이용자가 입력한 본인확인정보를 다른 본인확인기관에게 전달하여 이용자의 식별정보를 전달 받아야하기 때문이다. 이용자가 가입한 본인확인기관에만 이용자의 주민등록번호가 보관되어 있기 때문에 다른 본인확인기관에서는 이용자의 식별정보(CI, DI)를 생성할 수 없는데서 기인한다.

① 문제점 : 본인확인기관 간의 정보 연동을 위해서는 KISA로부터 전달받은 일일키와 분기키를 사용하여 암호화 한 후 통신을 수행한다. 일일키는 KISA가 매일 갱신하는 암호화키이며, 분기키는 분기마다 변경하는 암호화키이다. KISA와 각 본인확인기관은 분기별로 공유키(분기키)를 생성하여 교환하며, 공유키의 안전한 교환을 위한 전자서명에 공인인증서를 사용한다. 일반적으로 인증서를 통하여 암·복호화를 할 경우 상위인증기관(CA)에 접근하여 상대방의 공개키를 획득하지만 KISA와 본인확인기관은 각각의 시스템에 서로의 인증서를 공유하고 있다. 또한, KISA와 각 본인확인기관은 시각이 동기화하고 매일 동일한 시각에 일일키 생성 프로그램을 실행하여 해당 일 통신에 사용할 일일키를 생성한다. 이러한 본인확인기관 간 암호화 키 전달을 위해 사용하는 키분배 프로토콜 안전성 분석 부재에 따른 취약점 내재 가능성 검토가 요구된다. <Table 3>과 같이 KISA와 본인확인기관 간 분기키를 생성하는 알고리즘으로 대표적인 키분배 프로토콜인 Diffie-Hellman 알고리즘을 사용하고 있다. 아이핀 서비스에 적용되어 있는 키 분배 프로토콜은 비대칭키 기반의 키 합의 및 키 전송 방식이며 이는 ISO/IEC 11770-3에 정의되어 있다. ISO/IEC 11770-3은 다음과 같은 취약점이 발견되어 2015년에 개정되었다. 통신 상대방의 존재여부를 확인하지 않고 키 확인 과정이 없다. 즉 통신 상대방이 세션키를 정확하게 생성하여 같은 세션키를 가지고 있는지 확인하지 않고 암호통신을 개시한다. 암호화한 후 서명하기 때문에 서명자가 암호문의 평문을 알고 있다는 확인을 할 수 없다. 수신측 통신 개체는 세션키의 최신성을 확인할 수 없고 송신측 통신 개체가 세션키를 생성하였는지 확인할 수 없다. 아이핀 서비스 시스템에 구현된 세션키 공유를 위한 키분배 프로토콜이 ISO/IEC 11770-3을 만족하는지 검증을 하지 않았으며 정확하게 구현하였더라도 2008년에 구현하였으므로 최근 개정된 ISO/IEC 11770-3 (2015)을 반영하지 못하였기 때문에 위에서 언급한

〈Table 3〉 Encryption Algorithm between Personal Identification Agencies

Item	Update Time	Key Gen.	Length	Use
Certification	1year	SHA1RSA	1024	Digital signatures and data encryption/ decryption when branch key is shared
Branch key	3 mon	Diffie-Hellman	256	Mediation information for daily key generation
Daily key	1day	SHA256	128/128	Data encryption/decryption between KISA and the identity verification authority

문제점을 내재하고 있을 가능성이 있다(Kim and Lm, 2014). KISA와 본인확인기관 간 마스터키를 전송하는 과정에서 서버 인증서 공개키로 암호화하는데 서명용 인증서의 공개키와 구분하여 사용하고 있는지 확인이 불가능하고 본인확인기관에서 인증서 유효성 검증을 수행하는지 여부도 확인이 불가능하므로 인증서 기반의 키전송 프로토콜에 대한 안전성에 취약점이 존재할 수 있다.

② 대응방안 : 다양한 보안 공격에 안전하도록 키 분배 프로토콜이 구현되어 있는지 소스코드 검증 및 프로토콜 안전성 분석이 필요하다. 보안 공격에는 다음과 같다.

- known-key attack에 대응하기 위해 매 세션마다 공유 비밀 값이 달라지도록 구현하였는지 여부
- small subgroup attack에 대응하기 위해 공개정보의 유효성 검증 절차를 구현하였는지 여부
- forward secrecy에 대응하기 위해 공유 비밀 값 안에 통신 개체가 랜덤하게 생성한 임시 값(ephermeral 키 생성정보)을 조합하여 입력 값으로 사용하였는지 여부
- key compromise impersonation attack에 대응하기 위해 세션키에 B의 long-term 비밀키를 포함한 B의 공개키와 A가 랜덤하게 생성한 ephermeral 값을 조합하여 만든 값을 사용하였는지 여부
- unknown key-share attack에 대응하기 위해 인증기관의 루트 인증서 검증절차가 포함되어 있는지 여부
- 서명 후 암호화한 경우 서명함수의 입력 값에 수신자의 ID 포함 여부
- 암호화한 후 서명한 경우 암호화 함수 입력 값에 수신자 ID 포함여부

특히 키분배 프로토콜 및 보안채널 프로토콜을 구현하여 실생활에 적용되고 있는 분야는 전자여권 분야이다. 전자여권에 구현할 목적으로 설계한 암호프로토콜은 위에서 언급한 공격에 대응할 수 있도록 설계되어 있다. 그러므로 전자여권에 구현할 목적으로 설계한 암호 프로토콜 활용을 고려해 볼 만하다.

2.2.3 아이핀 인증모듈의 취약점 및 대응방안

인터넷서비스 제공사업자는 이용자의 본인확인을 위해 아이핀 본인확인기관 중 하나의 기관을 채택하고 해당 본인확인기관과 서비스 이용계약을 체결한다. 서비스 이용계약을 체결한 본인확인기관은 아이핀 이용자의 정보 수집하고 인증할 수 있는 아이핀 인증 모듈을 제공하며, ISP는 설치매뉴얼에 따라 서비스용 웹서버에 아이핀 인증 모듈을 설치한다. 아이핀 인증 모듈은 본인확인기관과 사업자간 이용자 정보를 암호화하여 송·수신하기 위한 목적으로 사용되는데 보안 취약점이 발견된 경우 아이핀 본인확인기관에서 관련 아이핀 인증 모듈을 업데이트하여 새로 배포하고 있다.

① 문제점 : 일부 ISP들은 아이핀 인증 모듈 설치 후 최신 모듈로 업데이트를 하지 않고 있어(업데이트를 강제할 수 있는 방안도 마련되어 있지 않아) 취약한 인증 모듈 사용에 따른 보안사고 발생 가능성이 높은 상태이다. 2015년 7~8월간 설문조사(Kim et al., 2015)를 통해 ISP가 최신 인증모듈

버전으로 패치하지 못하는 주요 이유를 파악한 결과, 최초 설치 이후 관리·운영 인력의 부재, 개발 비용 소요, 최신버전 인지 부족, 신규 모듈에 대한 안전성 검증을 보장하지 않음(이미 안정적으로 사용 중인 운영 시스템을 업그레이드하지 않음), 그리고 변경 내용(패치)이 크게 문제되지 않는다고 판단 등의 이유로 신규 패치를 적용하지 않는 것으로 조사되었다. 이러한 상황에서 본인확인기관들은 서비스를 제공하는 을의 입장으로 인증모듈의 패치를 강제화하지 못하는 한계가 존재한다.

② 대응방안 : 최신 아이핀 인증모듈의 배포와 적용을 위해 법적, 제도적, 기술적 대응 방안 마련이 요구된다. 기술적 방안에는 취약한 아이핀 인증모듈 사용 현황을 확인하기 위한 체계 구축, 아이핀 인증 모듈 자동 또는 주기적 업데이트 체계 구축, 그리고 아이핀 인증 모듈 배포 시 디지털 전자서명 도입 등이 있다. 관리적 방안에는 아이핀 인증 모듈의 취약점 발견 및 업데이트 시 표준화되고 공식적인 사업자 통보 절차 수립, 그리고 아이핀 인증 모듈에서 중요 취약점 발견 시 사업자의 이행 조치 여부 확인 강제화 또는 본인확인기관을 통한 사업자 점검 강화가 있다. 그리고 제도적 방안에는 일정 기한 내 취약한 아이핀 인증 모듈을 업데이트하지 않을 경우 서비스 이용 제한, 그리고 본인확인기관 지정 및 점검과 관련된 제도의 개선 등이 있다. 기술적 방안으로 기존 아이핀 인증 모듈에서 취약점이 발견될 경우 본인확인기관은 관련 모듈을 업데이트하여 새로 배포하고 있으나, 사업자가 영세하거나 이미 안정적으로 운영중인 시스템을 변경하지 않으려고 하는 등의 이유로 인증 모듈 업데이트가 어려운 것이 현실이다. 그런데, 더 큰 문제는 현재의 본인확인기관과 사업자간의 데이터 송수신 체계를 보면 사업자가 사용하고 있는 모듈이 취약한 모듈인지를 확인할 방법이 없다는 것이다. 이에 따라 사업자가 취약점이 패치 되지 않은 구 인증모듈로 본인확인 정보를 암호화하여 송·수신하는 경우 보안사고의 위험성이 높은 상태이다. 이러한 문제점을 개선하기 위해서는 기술적인 인증모듈 검증 절차 도입이 필요하다. 따라서 본인확인기관과 사업자간 데이터 송수신 시 현재 사용 중인 아이핀 인증 모듈의 버전 정보를 제공하도록 하는 것이다(데이터 프로토콜 설계 반영 등). 또한, 아이핀 인증 모듈 자동 또는 주기적 업데이트 체계 구축도 필요하다. ISP들에게 아이핀 인증모듈 업데이트에 관한 설문조사 결과(Kim et al., 2015)를 통해 사업자들은 안정적인 시스템에 변경을 하지 않으려는 성향과 신규 인증모듈에 대한 안전성을 검증하지 못하는 상황에서 서비스 연속성에 대한 부담이 크고, 업데이트된 내용(패치)이 크게 문제 되지 않는다는 판단하여 최신 버전으로 패치 하는데 소극적인 것으로 판단하고 있었다. 앞서 설명한 두 가지 기술적 방안(인증모듈의 버전 정보 제공과 자동/주기적 업데이트 체계 구축)을 연계할 경우 보다 큰 시너지 효과가 있을 것으로 생각된다. 이러한 기술적 방안은 사업자가 영세하거나 외주 개발하는 등의 경우 취약점이 패치된 최신 인증모듈을 배포하여도 실질적으로 사업자가 적용할 수 없는 것이 현실이다. 또한, 기술적인 방안을 적용하기 위해서는 현재 본인확인기관과 사업자간에 송·수신되는 데이터에 버전 정보를 추가하고 본인확인기관에서는 이를 확인해야 하는 등 현재의 프로세스를 수정하여야 하는 문제점과 함께 비용이 발생한다. 또한 사업자의 고의 또는 실수로 인증모듈이 최신으로 업데이트되지 않아 본인확인서비스가 제공되지 않는 경우, 실제 그 피해는 해당 서비스를 이용하는 이용자들에게 돌아가게 되는 문제점도 있다. 이를 해결하기 위한 관리적 방안으로 아이핀 인증모듈에서 중요 취약점 발견 시 사업자의 이행 조치 확인 강제화 또는 본인확인기관을 통한 사업자 점검 방안을 도입할 필요가 있다. 이전에 기술한 기술적 방안이나 관리적 방안 모두 본인확인기관과 사업자의 자율에 맡기는 방식으로 본인확인기관이나 사업자가 해당 방식을 적용하지 않을 때 강제화하거나 제제를 가할 수 있는 방법이 없다는 문제점

이 존재한다. 이를 해결하기 위해서 서비스 이용제한 조치 도입과 본인확인기관 지정 및 적합성 심사와 관련된 제도의 개선이 필요하다. 서비스 이용제한 조치는 본인확인기관이 사업자와 데이터 송·수신 시 현재 사용 중인 인증모듈의 버전을 확인하여 최신 버전이 아닌 경우 인증실패에 해당하는 에러정보를 전송하고 최신 버전으로 업데이트되기 전까지 사용을 중지시키는 방안이다(사전 예고를 통해 유예 기간을 주고 일정 기한 후 서비스 이용제한 조치 적용). 또한, 본인확인기관과 사업자간에 본인확인 인증모듈의 버전을 확인하는 등 인증모듈의 취약점과 관련된 내용은 없는 상황이다. 따라서 이러한 문제점을 보완하기 위하여 고시의 개정과 같은 제도 개선을 통하여 대책을 강제화 하는 것이 필요하다. 즉, 이해 당사자 간 협의를 통해 『본인확인기관 지정 등에 관한 기준』 등을 개정하여 근거기준을 마련해야 한다. 제도의 개선을 통하여 강제화 할 내용으로는 먼저 앞에서 언급한 본인확인 기관과 사업자간의 인증모듈 버전 확인을 위한 점검 프로세스 적용과 필요 시 인증모듈 강제 업데이트 방식의 도입이 될 수 있다. 또한, 본인확인기관이 사업자를 정기적으로 점검할 수 있는 기준을 마련하고 이행하지 않을 시 불이익을 줌으로써 본인확인기관과 사업자가 동시에 노력할 수 있는 기반을 마련할 수 있다. 추가적으로 현재 본인확인기관에 대한 점검 대상을 확대하여 본인확인서비스와 관련된 인증대행사 및 사업자들에게도 적용하여 실제 보안상 점검의 사각지대에 놓여있는 본인인증 대행사 및 사업자들의 보안수준 점검 및 보안수준 향상을 도모할 필요가 있다.

3. 제도적 안전성 강화 방안

아이핀 기반의 본인확인서비스의 제도적으로 개선할 사항과 대응방안에 대해 기술한다.

첫째, 현재의 아이핀 본인확인서비스는 본인확인을 요청하는 인터넷서비스 제공 사업자에게 이용자의 과도한 개인정보를 제공하고 있다. 즉, 이용자를 명확하게 식별할 수 있는 정보 혹은 성인인증 등과 같은 업무에 필요한 정보만을 제공하는 것이 필요하다. 본인확인기관이 이용자로부터 아이핀 ID와 패스워드를 통해 인증을 성공하게 되면 인터넷서비스 사업자에게 이용자의 성명, 생년월일, 성별, 내·외국인정보, CI, DI, 연령대 정보 등을 제공한다. 실제 이용자들은 본인확인서비스 약관을 통해 아이핀 서비스 사용을 통해 인터넷서비스 사업자들에게 연계정보와 중복가입확인정보, 성인인증을 위한 연령대 정보만을 제공함을 안내하고 있다. 하지만, 실제는 이용자의 이름, 생년월일, 내·외국인 정보 등을 인터넷서비스 사업자들에게 제공하고 있는 것이다. 이는 결국, 인터넷서비스 사업자들은 회원가입 혹은 결제 과정 등을 통해 본인확인서비스 이용자들의 개인정보를 본인확인기관으로부터 제공받아 저장하고 있다는 사실에 대한 고지를 하고 있지 않는데 문제가 있다. 물론 모든 인터넷서비스 사업자들이 본인확인서비스를 이용한 이용자의 개인정보를 보관하는 것은 아닐 것이다. 필요에 따라 선별적으로 저장하거나 혹은 주기적으로 개인정보를 삭제하는 등 기술적·관리적 보호조치를 취하고 있는 사업자들이 존재한다. 하지만, 근본적으로 현재의 본인확인서비스 제도에서 이용자가 대체수단 발급을 위해 입력한 개인정보(이름, 생년월일, 성별, 내·외국인 등)를 본인확인을 요청 인터넷서비스 사업자들에게 제공하는 것은 다시금 제고할 필요가 있다. 즉, 현재의 본인확인기관이 이용자 본인을 확인해 주는 서비스가 오히려 국가가 이용자의 진성 개인정보를 확인 및 과다 제공해 주는 서비스로 비춰질 여지가 있기 때문이다. 더구나 인터넷서비스 사업자들은 본인확인기관으로부터 제공받은 이용자의 본인확인정보들 중 어떤 개인정보를 얼마만큼 보관하고 있는지 고지를 해야 하며, 또한 적절한 정보보호 활동을 이행하고 있는지 관리·감독 기관으로부터의 점검을 통해 현황을 파악할 필요가 있다. 만약 인터넷서비스 사업자가 이용자의 성명 혹은 내·외국

인정보, 생년월일 등이 필요하다면 별도의 개인정보 수집과 동의를 받아야만 할 것이다. 초창기 아이핀 서비스 태동 시는 분명 이용자와 사업자 입장에서는 편리한 수단이었을 것이다. 이용자는 단순히 아이핀 ID와 패스워드를 입력하면 부가적인 정보(이름, 생년월일 등) 입력 없이 본인인증이 되는 결과를 가져다주고, 사업자 입장에서는 이용자가 입력한 개인정보가 진성 정보인지 확인이 가능한 이점이 있었을 것이다. 하지만, 근래 개인정보 보호에 대한 인식과 함께 관련 법·제도에 의거하여 최소한의 수집원칙, 과도한 수집 금지, 수집 시 동의 징구 및 고지 등 항목에서 위배될 수 있는 소지가 다분히 존재한다. 따라서 이러한 부분의 개선을 위해 본인확인서비스의 재검토를 통해 최소한의 개인정보 제공을 의무화할 수 있는 제도 마련이 필요하다.

둘째, 아이핀 본인확인서비스를 통한 본인인증 실패 시에 대한 실패 정보 제공 범위를 명확히 할 필요가 있다. 일부 인터넷서비스 제공사업자들은 고객의 응대를 위해 본인인증 실패 사유에 대한 실패 정보를 본인확인기관들에게 요구하고 있다. 물론 신속한 고객 응대도 중요하지만, 한 이용자의 본인인증 실패정보를 수집하게 되면 일부 수집된 실패 정보들의 조합으로 이용자의 개인정보를 식별할 수 있게 되는 문제가 발생한다. 예를 들어 휴대전화 인증을 통한 본인확인서비스 시 일반적으로 이용자는 가입한 이동통신사의 지정 오류로 본인확인 실패가 발생한 가능성이 존재한다. 이러한 입력 오류의 경우 실제 인터넷서비스 제공사업자들은 휴대전화 인증이 실패하였기 때문에 이동통신사업자들에게 본인확인서비스 요금을 납부하지 않아도 되는 점을 이용할 수 있다. 즉, 이러한 점을 악용하여 인터넷서비스 사업자들은 본인확인기관에게 일부 이용자의 개인정보를 활용하여 본인확인서비스를 시도하고 본인인증이 실패 이용자들의 개인정보 클리닝 작업에 이용할 가능이 존재한다. 즉, 이용자들은 해당 인터넷 서비스를 이용하지 않는 이상 본인의 개인정보를 잘 수정하지 않는 경향이 있다. 이러한 점을 개선하고자 인터넷서비스 사업자들은 본인확인기관을 통해 이용자의 개인정보가 현행화되어 있는 정보인지를 주기적으로 확인할 개연성이 다분하다. 특히, 이용자 휴대전화의 이동통신사명, 전화번호 등이 그 대표적인 예일 것이다. 따라서 본인확인서비스 실패 시 단순한 실패 정보만을 인터넷서비스 사업자들에게 제공하고 본인확인기관만이 인증실패 정보를 보관하여 향후 과금 등의 분쟁 발생 시에만 열람 및 보호할 수 있도록 하는 조치가 요구된다.

셋째, 아이핀 본인확인서비스의 부정발급 및 부정인증 시도에 대한 체계적이고 통합적인 관리가 미흡한 상황이다. 민간 및 공공 아이핀 발급 기관 간의 정보 공유 채널이 존재하지 않아 각각의 서비스 영역에서만 부정인정 및 발급시도를 탑지하고 있으며 이들의 정보를 한곳에 집중하여 체계적으로 분석하는 시스템에 존재하지 않는다. 물론, 각 아이핀 발급기관들마다 다양한 공공기관 및 정보통신사업자들과의 계약을 통해 획일화된 부정사례 모니터링 체계 마련을 쉽지 않을 것이다. 특히, 해당 아이핀 발급 기관에서 부정사례 모니터링을 위해 서비스 이용자들의 IP 정보 등을 저장하거나 타 기관과의 공유 시 관련 법령에 저촉되는지에 대한 부분도 고려해야 할 것이다. 이를 방지하지 위해서는 최소한으로 규제기관에서 아이핀 부정발급 및 인증 시도에 대한 상시 모니터링 체계 마련을 위한 창구 역할은 필요할 것이다. 예를 들어, 각 아이핀 발급기관들의 부정시도에 대한 체계 공유, 부정시도 IP 등에 대한 차단 조치 이행 등에 대한 가이드라인 마련도 한 대안이 될 것이다. 그러나 무엇보다도 규제기관이 관련 모니터링 체계에 대해 가이드를 마련하는 것보다는 각 아이핀 발급기관들이 자발적으로 마련된 부정시도탐지체계에 대한 정보 교류와 상호 연동 방안을 제시하고 이를 KISA가 공동으로 관리하여 상황을 전파하고 차단조치 등 이행할 수 있는 중계자 역할을 하는 것이 바람직한 대안으로 고려해 볼 수 있을 것이다. 또한, 부정행위가 지속적으로 발생하는 ISP에 대해서는 1차적으로 계

약된 본인확인기관에서 시정조치를 요구하고 이에 대한 사항을 KISA에 전달하여 각 아이핀 발급 기관들 간에도 상호간에 인지함으로써 해당 ISP가 다른 본인확인기관과 계약을 변경 시에도 이전에 시정 사항이 반영할 수 있도록 유도할 필요가 있을 것이다.

4. 결 론

본 연구를 통해 아이핀 기반의 본인확인서비스의 안전한 제공을 위한 다양한 방안 제시로 서비스 이용자들이 편리하고 안전하게 이용이 가능하게 함으로써 아이핀 서비스의 확산을 기대할 수 있으며, 아이핀 기반 본인확인서비스에서 아이핀 기관 간 정보 송수신 시 통신 체계 검토를 통한 취약점 분석 및 해결 방안 모색, 본인인증 결과 값, 키 교환, 사용자인증정보 연계 등을 검토하여 통신체계의 개선 방안 제시, 해킹 방지를 위한 인증모듈의 정기 업데이트 방안 제시와 같이 아이핀 기반의 본인확인서비스 안전성 강화를 통해 서비스의 신뢰성을 제고할 수 있다. 실제 아이핀 본인확인기관과 인터넷서비스 제공사업자들 간의 본인확인서비스 이용자들의 개인정보를 효과적으로 관리할 수 있는 계기를 마련할 수 있을 것이다. 향후 연구에서는 신규 대체수단의 적용과 활성화 방안에 대해 연구를 수행하고자 한다.

References

Audit and Inspection Report, “National Cyber Safety Management Status”, The Board o Audit and Inspection of Korea, 2016.

(감사보고서, “국가 사이버안전 관리실태”, 감사원, 2016.)

Choi, J.S. and J.B. Kim, “Study of Enhancing Safety of Personal Authorization Methods”, *Proceedings of IEEK*, Vol.1, 2015, 298-301.

(최중석, 김종배, “주민번호 대체수단의 안전성 강화 방안 연구”, *대한전자공학회 추계학술대회*, 제1권, 2015, 298-301.)

Choi, J.S. and J.B. Kim, “A Study of Improving user Authentication Procedures for Enhanced Safety of Personal Authorization Methods”, *Proceedings of KIPS*, Vol.22, No.2, 2015, 668-671.

(최중석, 김종배, “본인확인서비스 안전성 개선을 위한 본인인증수단 및 절차 개선 방안 연구”, *한국정보처리학회 추계학술대회*, 제22권, 제2호, 2015, 668-671.)

Choi, K.H., S.W. Jung, G.S. Lee, and S.H. Ahn, “i-Pin Development Plan for National IDM”, *Journal of The Korea Institute of Information Security and Cryptology*, Vol.21, No.4, 2011, 40-46.

(최광희, 정승욱, 이강신, 안승호, “국가 IDM을 위한 아이핀 발전 전략”, *한국정보보호학회지,* 제21권, 제4호, 2011, 40-46.)

Choi, K.H., J.C. Ahn, G.S. Lee, and S.H. Ahn, “i-Pin 2.0 Service Frameworks for Alternative Means of Resident Registration Number”, *Journal of The Korea Institute of Information Security and Cryptology*, Vol.20, No.6, 2010, 88-95.

(최광희, 안종찬, 이강신, 안승호, “인터넷상 주민번호 이용을 대체하기 위한 아이핀 2.0 서비스 프레임워크”, *정보보호학회지*, 제20권, 제6호, 2010, 88-95.)

Heo, G.I., J.W. Kang, and W.H. Park, “Countermeasures of Privacy Disclosure Vulnerability in Data Transfer Section”, *Journal of the Korea Society of IT Service,* Vol.12, No.1, 2013, 163-171.

(허건일, 강지원, 박원형, “데이터 전송 구간에서 개인정보노출 취약점과 대응방안”, *한국IT서비스학회지*, 제12권, 제1호, 2013, 163-171.)

Im, H. and T.S. Kim, “An Empirical Study on

the Factors that Affect the Continuous use Intention of i-PIN", *Journal of Information Technology Applications & Management*, Vol.22, No.4, 2015, 159-179.

(임 혁, 김태성, "아이핀(i-PIN)의 지속적 사용의도에 영향을 미치는 요인에 관한 실증적 연구", *한국데이터베이스학회*, 제22권, 제4호, 2015, 159-179.)

Jun, Y.E. and J.Y. Kim, "The Study on the Present Condition of Personal Information Security in Accordance with Cyber Security Threat in Financial Firms", *Journal of the Korea Society of IT Service,* Vol.13, No.1, 2014, 79-89.

(전영은, 김정연, "금융회사의 사이버 보안 위협에 따른 개인정보보호 실태에 관한 연구", *한국IT서비스학회지*, 제13권, 제1호, 2014, 79-89.)

Jang, W.C. and L.S. Shin, "Estimating Value Creation Effects of i-PIN", *Journal of the Korea Society of IT Service*, Vol.12, No.2, 2013, 185-193.

(장원창, 신일순, "아이핀(i-PIN)의 가치창출효과 추정", *한국IT서비스학회지*, 제12권, 제2호, 2013, 185-193.)

Jang. I.Y. and H.Y. Youm, "A Research of i-Pin of Personal Identification Method on the Internet", *Journal of The Korea Institute of Information Security and Cryptology*, Vol.19, No.5, 2009. 81-94.

(장인용, 염흥열, "인터넷상의 본인확인수단인 아이핀의 활성화 방안 연구", *정보보호학회논문지*, 제19권, 제5호, 2009, 81-94.)

Kim, J.H. and J.S. Lm, "Recent Information Security Issue and Cryptology Research Trends", *KISA Internet & Security Focus*, 2014.

(김주혁, 임진수, "최신 정보보호 이슈 및 국외 암호기술 연구 동향", 한국인터넷진흥원, Internet & Security Focus, 2014.)

Kim, J.B., S.T. Kim, J.H. Kim, J.H. Jun, H.Y. Han, D.H. Jun, and J.S. Choi, "A Research on The Improvement for Securing Safety of An Alternative Resident Registration Number on The Internet", KISA Research Report, KISA-WP-0027, 2015.

(김종배, 김성태, 김지연, 전진환, 한홍렬, 전동호, 최중석, "주민번호 대체수단 안전성 강화 방안", 한국인터넷진흥원, KISA-WP-0027, 2015.)

Kim, S.H. and H.S. Choi, "Active Phishing Attack Against the i-PIN Service", *Proceedings of IEEK.*, 2014, 587-590.

(김승현, 최대선, "아이핀(i-PIN) 서비스에 대한 액티브피싱 공격", *대한전자공학회 학술대회*, 2014, 587-590.)

Kim, S.J., "A Study on Improvement of i-PIN Service", Ph.D Thesis, Sungkyunkwan University, 2007.

(김승주, "주민번호 대체수단 서비스 개선 방안 연구", 학위논문, 성균관대학교, 2007.)

Lee, H.K., H.H. Lee, and J.H. Myung, "A Survey on Privacy Level : Part Personal", KISA Report, 2015.

(이현규, 이훈행, 명준형, "개인정보보호수준 실태조사 : 개인부분", *한국인터넷진흥원*, KISA-WP-2014-0051, 2015.)

Lee, J.S., B.K. Son, and J.H. Gu, "Electronic ID Wallet based i-PIN Technology Development", KISA Research Report, 2007.

(이재신, 손병록, 구자현, "전자 ID지갑 시스템 기반의 i-PIN 고도화 기술 개발 및 구현", 한국정보보호진흥원 최종보고서, 55, 2007.)

Shin, Y.J., S.H. Shin, J.S. Lee, and W.G. Han, "A Study on Improvement of Identification Means in R.O.K", *Journal of Korean Association for Regional Information Society,* Vol.18, No.4, 2015. 59-88.

(신영진, 신승호, 이자성, 한웅기, "한국에서의 본인

확인수단 개선방안에 관한 연구", *한국지역정보화학회지*, 제18권, 제4호, 2015, 59-88.)

Shin, Y.J., "A Study of Enhance Method of Internet Personal Identification(i-PIN)", *Korean Policy Studies Review*, Vol.22, No.3, 2013, 171-199.

(신영진, "인터넷 본인확인수단(i-PIN)의 보급 및 적용에 따른 개선방안 연구-개인정보보호법 제정 전, 후 이용자의 인식변화를 중심으로", *한국정책학회보*, 제22권, 제3호, 2013, 171-199.

About the Authors

Jongbae Kim (jbkim@sdu.ac.kr)

Dr. Jong Bae Kim is currently working a full professor at the Department of Computer Engineering in the Seoul Digital University. He received the M.S. and Ph.D degrees in computer engineering from Kyungpook National University in 2002 and 2004. His current research interests include the personal identification service strategy, pattern recognition and artificial intelligent.