Journal of The Korea Society of Computer and Information
Vol. 17 No. 7 , July 2012

2012-17-7-3-5

i-PIN 서비스를 활용한 인증 서비스 구현

김 현 주*, 신 인 철**, 이 수 종***

Implementation of Personal Certification Using i-PIN Service

Hyun-Joo Kim*, In-Chul Shin**, Soo-Jung Lee***

요 약

기존 인터넷 웹 사이트에서는 개인을 식별하는 방법으로 주민등록번호를 사용해 왔다. 그러나 인터넷에서의 주민등록번호 사용은 개인정보 유출 위험을 증가시키는 주요인이 되고 있다. 현재 정부에서는 인터넷에서 주민등록번호 수집과 개인정보 유출을 방지하고자 다양한 정보 보호 서비스를 권장하고 있다. 이 중 인터넷상에서 주민등록번호 사용을 최소화를 위해 권장하는 서비스가 i-PIN 서비스이다. 그러나 i-PIN은 인터넷에서주민등록번호 수집을 대체 할 수는 있으나, 개인을 식별하는 유일한 키로 사용하기에는 한계점이 있다. 본 논문에서는 i-PIN을 개인인증서로 사용하여 인터넷 웹 시스템 접속 시 본인을 인증하는 웹 시스템 구성을 제안한다. 또한, i-PIN 서비스가 웹 시스템과 연계되어 개인인증서로 사용 시의 실용성과 안정성을 성능평가로 확인하였다. 그러나 i-PIN 서비스는 i-PIN 제공 본인확인기관에 장애가 발생되면 서비스 지원이 불가능해 진다. 이 불편을 해결하고자 i-PIN 본인확인기관의 장애 대처 방안도 제안한다.

▸ Keyword : i-PIN, 주민등록번호, 본인 인증

Abstract

Recently IT infrastructure plays a central role in the base of the society. However, use of personal registration number on internet sites has become a major factor increasing danger of leaking of personal information. Currently, the government is recommending various information protection services in order to prevent the collection of personal registration numbers and leaking of personal information on the internet. Among them, i-PIN service is the one recommended for

• 제1저자 : 김현주 • 교신저자 : 김현주
• 투고일 : 2012. 03. 09 심사일 : 2012. 04. 19, 게재확정일 : 2012. 05. 04.
* 단국대학교 전자전기공학부(Department of Electronics and Electrical Engineering, Dankook University)
** 단국대학교 전자전기공학부(Department of Electronics and Electrical Engineering, Dankook University)
*** 협성대학교 컴퓨터공학과(School of Computer Engineering, Hyupsung University)

minimal use of personal registration numbers on the internet. Although i-PIN can be used as a way to substitute personal registration numbers on the internet, there are certain limitations in using i-PIN as the only key to recognize individuals. This study proposes organization of web system in which self certification can be conducted using i-PIN as a tool for personal certification. Also its usability and stability have been verified through performance test when i-PIN service is linked with web service and used as personal certificate. But i-PIN service is unavailable if obstacles occur in providers of i-PIN self certification. To settle this inconvenience, the study also proposes how to cope with such obstacles.

▸ Keyword : i-PIN, Registration number, Self Certification

I. 서 론

국가 사회 기반의 중추적 역할을 담당하는 정보통신 인프라는 공유, 융합, 소통, 변화 등 국가 정책 패러다임과 더불어 웹 트랜드의 변화를 통해 사회 전반에 정보화의 확산을 이끌고 있다. 빠르게 발전하며 다양해지는 정보화는 우리에게 많은 편의성을 제공하지만 허위 정보의 급증과 개인정보의 훼손 등 불건전한 사이버문화의 위협이 계속적으로 확산되고 있다[1][2]. 최근 우리나라에서도 개인정보관리와 사이버 윤리 정책의 중요성을 법제화하여 2011년 9월 개인정보보호법을 발효하였다[3][4]. 인터넷에서의 실명 인증 방법은 공인인증서, 핸드폰, 아이핀 등 다양한 방법이 사용되고 있으나 지금도 많이 사용되는 방법 중의 하나가 주민등록번호를 이용한 개인 식별이라 할 수 있다. 대부분의 인터넷 이용자들은 웹 사이트에 주민등록번호를 등록하여 개인의 신분을 확인하고 ID(identifier)와 암호를 제공받아 다양한 웹 서비스를 이용하고 있다. 또 이용자의 대부분은 ID와 암호를 웹 사이트별로 동일하게 반복 사용하고 있다. 이것은 하나의 ID와 암호만 유출되더라도 주민등록번호를 포함하여 웹 사이트에 제공된 개인정보를 노출시키는 큰 부작용을 초래하게 된다[5]. 이에 주민등록번호 사용을 최소화하기 위해 정부를 중심으로 i-PIN(internet personal identification number) 식별 서비스를 권장하고 있다[6]. i-PIN이란 주민등록번호를 대체하여 개인의 식별하는 인터넷상의 가상식별 번호로 홈페이지에서 회원가입, 글쓰기에 주민등록번호를 사용하지 않고도 실명을 확인 할 수 있는 개인정보보호 서비스이다[2][7][8]. i-PIN 서비스를 이용하기 위해서는 i-PIN 등록기관에서 i-PIN 아이디와 암호를 발급 받아야 하고, i-PIN 등록기관은 이용자의 정보를 저장하고 인증 해주는 역할을 담당한다. 국내 i-PIN 서비스 등록기관으로는 민간기업 5개와 국가에서 운영하는 행정안전부 g-PIN(govement personal identification number)으로 총 6개의 서비스가 있다[9]. i-PIN 서비스는 제공기관 간 상호연동 기술과 중복가입확인 기술로 1개의 i-PIN ID로 인터넷 전체에서 개인 식별 지원이 가능하다. 그러나 i-PIN에서 제공하는 개인 식별 정보는 인터넷 웹 사이트에서 회원가입, 글쓰기 등에는 사용이 가능하나, 조직의 내부 시스템과 연계 시 본인을 식별 할 수 있는 유일한 정보는 제공하지 않아 그 사용이 제한적이다. 본 논문에서는 i-PIN 본인 인증 시스템을 제안한다. i-PIN을 이용한 본인 인증은 PKI 공인인증서와는 다른 형태의 인증으로 기존 웹 사이트 회원 가입 과정을 대신 할 수 있으며 i-PIN 실명인증을 확대하여 개인인증서로서의 본인 인증 과정을 연계하여 기존 PKI(public key infrastructure) 공인인증서와는 다른 형태의 본인 인증 서비스를 구현할 수 있다. 아울러 인터넷에서 남용되는 웹 사이트별 회원의 ID와 암호를 i-PIN ID 하나로 연계 사용하고 PKI 공인인증서에서 제공되지 않는 개인의 생년월일, 성별 등의 정보를 제공하므로 성인 인증의 어려움을 해결 할 수 있다.

본 논문에서 구현한 i-PIN 기본 기술은 국가에서 제공되는 i-PIN 표준 모델을 이용하였고, i-PIN 표준 모델은 TTA(Telecommunications Technology Association) 표준 서비스 규격에 준수되어 개발되었다. 또, i-PIN 본인 인증 후 웹 시스템과의 개인정보 데이터 전송은 128bit AES 암호화 알고리즘을 이용하였다. 그러나 i-PIN은 서비스 제공기관의 장애 발생되면 서비스 지원이 불가능해 장애 복구 시까지 웹 사이트에 접속 할 수 없는 단점이 있어 웹 시스템 사용자에게 불편을 초래한다. 이에 365일 지속적인 i-PIN 서비스 지원을 위해 2개의 i-PIN 서비스 프레임 워크를 운영하는 해결방안도 제안한다. 또, 제안시스템 검증을 위해 성능테스트 환경을 구축하여 시스템의 안정성을 확인하였다.

II. 관련 연구

1. i-PIN(internet personal identification number)

1.1 i-PIN 개요

i-PIN은 인터넷상의 주민등록번호를 대체하는 개인식별번호이다. 2005년 정보통신부에서 시작된 i-PIN 서비스는 [표 1]과 같이 6개의 i-PIN으로 서비스된다. i-PIN 본인확인기관은 민간 기업에서 운영하는 나이스아이핀, 가상주민번호, Siren24아이핀, OnePass, 그린버트 서비스와 국가에서 운영하는 행정안전부 g-PIN 등 6개의 서비스로 구분된다[9]. 현재의 i-PIN 기술은 중복가입확인정보 , 본인확인기관 간 상호연동을 통해 이용자가 1개의 i-PIN 아이디와 암호로 다수의 인터넷 웹 사이트와 연계가 가능하도록 구성되어 있다[9][10][11]. 또한, i-PIN은 한번 부여 받으면 변경이 불가한 주민등록번호와는 달리 자신의 i-PIN이 노출되었다고 해도 언제든지 폐기가 가능하다. 분실 시에는 다른 i-PIN으로 재발급이 용이하여 주민등록번호 노출로 인한 개인정보 침해의 피해를 최소화 할 수 있는 특징이 있다[8][12]. 한국인터넷진흥원의 2009년 정보보호 실태조사 기업부문 결과에 의하면 인터넷 웹 사이트에서 i-PIN 서비스를 도입한 기업은 8.5%로 '08년도와 비교해 3배가량 증가되었고 i-PIN에 대해 알고 있는 사용자는 58.1%, 이 중 i-PIN 서비스의 인지 정도에 대해 전년 대비 19.7% 상승되어 i-PIN에 대한 인지도가 성장하고 있는 것으로 나타났다[13][14].

표 1. i-PIN 서비스 기관
Table 1. i-PIN Service Information Agencies

발급기관	서비스 명칭	인터넷사이트
한국정보인증	Onepass	op.singngate.com
한국전자인증	그린버튼	www.greenbutton.co.kr
한국신용정보	나이스아이핀	www.idcheck.co.kr
한국신용평가정보	가상주민번호	www.vno.co.kr
서울신용평가정보	Siren24아이핀	www.siren24.com
행정안전부	공공 g-Pin	www.g-pin.go.kr

2. i-PIN 기술

i-PIN은 이용자가 인터넷 웹 사이트에 주민등록번호를 기입 하는 대신 i-PIN으로 본인확인기관이 이용자의 신원을 확인하고 웹 사이트에 i-PIN을 제공하여 회원가입 또는 성인인증을 할 수 있도록 한 기술이다. i-PIN은 인터넷 웹 사이트에서 필요로 하는 주민등록번호의 수집 목적을 충족시키며, 그 문제점을 보완할 수 있다[12]. 또, 웹 사이트와 연계한 i-PIN 본인확인 기관은 이용자 회원관리를 위해 필요한 정보를 웹 사이트에 전달해준다. i-PIN 본인확인기관이 웹 사이트에 전달하는 정보로는 성명, i-PIN 13자리, 중복가입확인정보, 생년월일, 성별, 연령대, 내·외국민 정보를 제공하며 관련 내용 및 활용 가능 분야를 정리하면 [표 2]과 같다[9][12][15][16].

표 2. i-PIN 서비스 제공 정보
Table 2. i-PIN Service Information Available

구분	제공 정보	활용 정보
성명	신원확인 수단을 이용한 본인확인을 수행하여 검증한 사용자의 실명	사용자 식별 방법으로 활용
i-PIN (13자리)	사용자의 본인확인을 수행후 본인확인기관이 사용자에게 부여하는 13자리 정보	불량 사용자 추적 시 활용
중복가입 확인정보	회원가입 또는 글쓰기 권한을 얻고자 하는 인터넷 사이트 내에서만 유일하게 사용자를 식별 할 수 있는 64byte 정보	중복가관 확인 시 사용자 식별 시 활용
생년월일	신원확인수단을 통한 본인확인을 수행하여 검증한 주민번호에서 추출한 8자리정보(YYYYMMDD)	사용자 서비스 제공 시 활용 (예: 생일축하, 생일쿠폰 등)
성별	신원확인 수단을 통한 본인확인을 수행하여 검증한 주민번호에서 추출한 정보	사용자 마케팅 시 활용(예: 패션, 미용정보 등)
연령대	신원확인수단을 통한 본인확인을 수행하여 검증한 주민번호에서 추출한 정보를 분류하여 제공하는 8단계의 법적연령대 1자리 정보	연령대 별 제공 가능 서비스 식별에 활용 (예: 영화관람, 게임이용 등급 등)
내외국인	신원확인수단을 통한 본인확인을 수행하여 검증한 주민번호 또는 외국인 등록번호에서 추출한 정보	내·외국인 가능 서비스 구분 시 활용

2.1 구성요소

i-PIN 서비스는 인터넷 이용자, 웹 사이트를 운영하는 인터넷 사업자 그리고 이용자의 신원 확인과 웹 사이트 이용자의 개인 정보를 제공하는 본인확인기관으로 구성된다[16]. [그림 1]은 이용자와 본인확인기관, 인터넷 웹 사이트에서의 i-PIN 정보서비스 관계를 설명한 것으로 i-PIN 서비스 프레임 워크 구성이라 할 수 있다. 이용자는 여러 개의 본인확인기관으로부터 i-PIN을 발급 받을 수 있으며, 자신이 이용하는 본인확인기관으로부터 i-PIN 발급받아 회원가입과 글쓰기 등의 권한을 부여받아 i-PIN 서비스를 이용할 수 있다[17].

이용자에게 i-PIN 서비스를 제공하기 위해서는 인터넷 웹 사이트는 본인확인기관 중 하나의 기관과 i-PIN 연계 서비스를 제공받아야 한다. i-PIN 연계 서비스 기술은 이용자가 발급받은 i-PIN 정보와 웹 사이트가 연계한 i-PIN 정보의 본인확인기관이 서로 같지 않아도 i-PIN 정보가 안전하게 전송되도록 본인확인기관 간 상호호환성을 제공하는 기술이다.[18][19].

2.2 i-PIN 본인확인기관 간 상호 연동

6개 i-PIN 본인확인기관은 상호연동 기술을 이용하여 i-PIN 하나로 모든 인터넷 웹 사이트에서 이용이 가능토록 하였다. i-PIN 본인확인기관 간 상호연동을 위해서는 송수신 메시지에 대한 전달 형식 표준을 준수해야하며, i-PIN 통신 서비스 규약은 하이퍼텍스트 통신 규약을 기본 통신 프로토콜로 사용한다. 전달메세지 형식 표준에는 WebsiteInfo(본인확인기관 정보 전달 메세지), PersonalInfo(개인정보 전달 메세지) 구조체를 사용하여 정보를 전달한다[12][19].

2.3 i-PIN 중복가입확인 정보

i-PIN에서 이용자를 유일하게 식별 할 수 있는 정보는 중보가입확인 정보로 본인확인기관은 이용자의 중복가입확인 정보를 웹 사이트에 제공한다. 웹 사이트에서는 이용자의 중복가입확인 정보를 본인확인기관으로부터 전달받아 보관하고 필요 시 이 정보를 비교하여 중복가입여부를 확인한다. 또한, 1인당 n개의 계정을 허용하는 웹 사이트는 중복가입정보 개수를 저장하여 n개의 계정보다 작으면 계정 생성을 허용하고 회원가입을 거절 할 수 있다[17]. 중복가입정보는 주민등록번호와 웹 사이트 식별 번호(SI: webSite Identification information)를 해시함수 SHA2로 압축하여 1차 결과 값을 생성하고 다시 1차 결과 값에 i-PIN 본인확인기관 공유 식별 번호를 더해 2차 해시함수 SHA2로 압축한 결과 값이다[2][12][17][20].

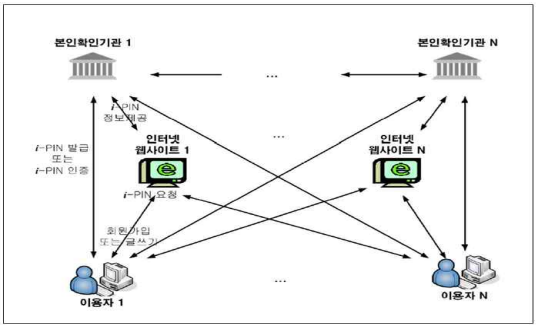

그림 1. i-PIN 서비스 프레임워크 구성
Fig. 1. i-PIN Service Framework Components

3. i-PIN 서비스의 문제

i-PIN은 인터넷에서의 주민등록번호를 대체하여 실명을 확인할 수 있는 개인정보보호 서비스이다. 그러나 i-PIN에서 제공하는 실명 인증은 인터넷에서 회원가입, 글쓰기 권한부여 수단으로는 사용이 가능하나 개인의 유일한 키를 수집하지 않아 개인인증서로서 조직의 내부시스템과는 연동 할 수 없는 한계점이 있다. 이 점을 해결하고자 i-PIN에서는 중복가입확인정보 기술이 사용된다. 그러나 웹 사이트에서는 암호화된 중복가입확인 정보를 복호화하여 해독 할 수 없기에 조직의 내부 시스템과 연계 시 개인의 유일성 식별이 불가능하다. 그러므로 i-PIN에서의 실명 인증은 개인인증서의 본인인증과는 다른 형태의 인증이다. 인터넷상에서 i-PIN을 이용하여 내부 시스템과의 접속하여 개인인증서로 사용되는 예는 아직까지는 드문 편이다. 현재, 인터넷에서의 개인정보 유출을 방지하고자 지난해 9월 개인정보보호법을 제정하여 개인정보의 중요성을 강조하고 있으며, 2012년 4월부터는 그에 따른 법적 제재 조치를 가하고 있다. 물론 i-PIN보다 사용의 융통성을 제공하는 PKI 공인인증서도 있지만, PKI 공인인증서는 서비스를 제공하는 기관이나 서비스를 제공받는 개인이 일정 비용을 지불해야 하며, 개인이 상시 소지해야 하는 불편함이 있다. 그러나 i-PIN은 국가를 중심으로 기관, 개인 모두에게 무상으로 제공되므로 비용 지불이 꺼리는 사용자 측면에서는 의미가 있다고 할 수 있다. 또, i-PIN 서비스에서만 제공되는 성인여부 식별 정보는 청소년 교육 지원에 도움이 될 것이다. i-PIN 서비스에서 지원되는 개인 정보는 철저히 본인확인기관에서만 제공된다. 그러므로 i-PIN 서비스 제공 기관에 장애가 발생되면 장애 복구 시까지 i-PIN 정보서비스 지원이 불가능해진다. 지난 2011년 3월 DDOS 공격이 발생되었을 때 공공 i-PIN 시스템 장애로 i-PIN 서비스 지원이 불가능하였고, 동년 5월에는 공공 i-PIN 보안인증서 교체 작업으로 장기간 i-PIN 지원이 불가능해 공공 i-PIN을 사용하는 웹 사이트와 사용자에게 큰 불편을 초래했다.

4. 국외 본인확인 동향

우리나라의 주민등록번호처럼 개인 식별이 가능한 번호를 부여하여 본인 확인을 하는 나라로는 프랑스, 독일, 벨기에 등이 있으며 우리와 동일하게 개인 신분증이 발급되면 일련번호를 부여한다. 발급된 일련번호를 등록하여 사용하고 분실이 발생하면 기존 일련번호는 폐기하고 재사용이 불가능토록 하고 있다. 또, 미국의 경우는 주마다 다른 번호를 부여하여 사용하는 사회보장번호(Social Security Number)가 있으

며, 개인 식별이 가능토록 하고 있다. 캐나다는 아직까지 온라인상에서 계좌개설 등의 서비스를 제공하지 않고 있어 온라인 신원 확인 절차는 사용하지 않고 있다[21]. 그러므로 우리나라를 제외한 대부분의 국가에서는 온라인에서 회원 가입 시 이메일을 개인 식별에 이용하고 주민등록번호과 같은 개인 식별번호는 입력받고 있지 않았다[22][23].

III. i-PIN 환경의 본인 인증시스템 설계 및 구현

1. 제안시스템 개요

본 논문에서는 웹 사이트 접속 시 i-PIN을 이용하여 본인을 인증하는 시스템을 제안한다. 본 논문에서 구현한 i-PIN 본인 인증은 기존 웹 사이트 회원 가입과정을 대신하고 인터넷 웹 사이트에서 사용되는 다수의 개인 ID와 암호를 i-PIN ID, 암호 하나로 사용할 수 있다. 무엇보다 i-PIN은 한번 부여받으면 평생 바꿀 수 없는 주민등록번호와 달리 자신의 i-PIN이 노출되었다고 해도 언제든지 폐기가 가능하다. 또, 사용자는 언제든 새로운 i-PIN발급이 용이하며 이미 노출된 기존 i-PIN은 해독이 불가능해 개인정보 침해로 인한 피해를 최소화 할 수 있다. i-PIN 본인 인증에서 사용된 i-PIN은 국가에서 제공하는 i-PIN 표준 모델로 TTA(Telecommunications Technology Association) 표준 서비스 규격에 준수하여 개발하였다. i-PIN TTA 표준 서비스 규격은 i-PIN 서비스 프레임워크, 전달메세지형식, 중복가입확인정보로 구성되어 있다. 웹 정보시스템과 i-PIN 본인확인기관은 1:1 구성으로 연결되어 있어 i-PIN 서비스 제공기관에 장애가 발생되면 본인 인증이 불가능하여 웹 정보시스템에 접속 할 수 없는 단점이 있다. 이를 개선하여 365일 중단 없는 서비스를 지원하고자 2개의 i-PIN 서비스 프레임워크를 설계하여 구현하였다. 또, i-PIN 본인 인증 후 웹 시스템과의 데이터 전송은 128bit AES(Advanced Encryption Standard) 암호화 알고리즘을 이용하여 안전한 자료 전송이 가능토록 하였다. AES 알고리즘은 1987년 NIST에서 DES(Data Encryption Standard)를 대신할 새로운 암호화 알고리즘으로 우수한 안전성으로 인해 차세대 암호 표준로 채택된 알고리즘이다[24].

2. 제안시스템 설계

2.1 개발도구 및 환경

i-PIN을 이용한 본인 인증 시스템은 i-PIN 본인확인기관 장애 시 이용자의 불편을 개선하고자 2개의 i-PIN 프레임워크를 구성했다. 2개의 i-PIN 프레임워크는 Active, Standby 서비스 구조로 설계되었으며, 대량 접속자 발생 시는 접속자 제어를 위해 시스템 SLB(Server Load Balancing)를 사용하였다. [표 3]은 2개의 i-PIN 프레임워크 제안시스템 개발 환경이다.

표 3. 제안시스템 개발 환경
Table 3. The Proposed System Development Environment

구분	세부사항
서버 #1	IBM P-570 AIX 5.6 CPU : 4.2GHz PowerPC_POWER6* 2cpu MEM : 8960 Mbytes HDD : 146.8GB SAS Disk Drive*2EA 운영체제 : AIX 5300-08-08-0943 Kernel : 64bit
서버 #2	
개발언어	JAVA, JDK 1.6
DB 및 WAS	Oracle 10g , WebSphere 6.1
부가장비	IBM HACMP, L4 Switch(SLB)
서비스	공공 g-PIN, 민간 i-PIN
	RS232, RS422 Asynchronous Adaptor

2.2 시스템 설계

i-PIN을 이용한 본인 인증 웹 정보시스템 접속의 기본 조건은 다음의 4가지 형태로 분류된다. 아래의 ①~④의 분류는 조직 내 서비스를 기준으로 권한이 결정된다.

① User 분류: 사용 권한 구분 요소로 일반인, 내부인, 관리자로 구분된다.

② User 사용권한: 접근 권한은 User 분류에 따라 사용권한이 서로 다르다.

③ 동작의 일원화: 각 단위 별 정보시스템은 하나로 동작하는 형태, 즉, 하나의 계정으로 연계되어 전체 시스템의 사용이 가능, 접속이 일원화 되어 운영한다.

④ 시스템 안정화: 접속 속도 및 트래픽, 연속 서비스로 구분 된다.

≒ 접속속도 및 트래픽: 모든 웹 서비스는 인터넷을 통해 사용되며, 이용자 불편을 최소화하기 위해 인터넷 접속 속도와 웹 트래픽의 안정화가 보장되어야 한다.

≒ 중단 없는 연속 서비스: 인터넷을 이용한 웹 시스템은 365일 24시간 무정지가 보장되어야 한다.

i-PIN 서비스는 본인확인기관에 장애가 발생되면 본인인증 서비스 지원이 불가능 웹 시스템에 접속 할 수 없는 불편

을 초래한다. 이 단점을 해결하고자 i-PIN 서비스 프레임워크를 이중화로 설계하여 이용자 불편을 개선하였다. [그림 2]는 웹 사이트 접속 과정으로 이용자, 웹 시스템, 2개의 i-PIN 프레임워크 절차도이며 i-PIN 센터 장애를 고려하여 2개의 i-PIN은 Active, Standby 형태로 설계하였다. [그림 3]은 i-PIN 발급에서 i-PIN을 이용한 본인 인증 등 웹 시스템 접속 절차이다. [그림 2][그림 3]의 Active, Standby는 i-PIN 서비스센터 장애를 대비한 구성으로 Active는 공공 i-PIN 서비스를 이용한 구성이며 Standby는 민간 i-PIN 서비스를 이용한 구성이다. Active, Standby에 사용된 Application은 동일한 구조이다.

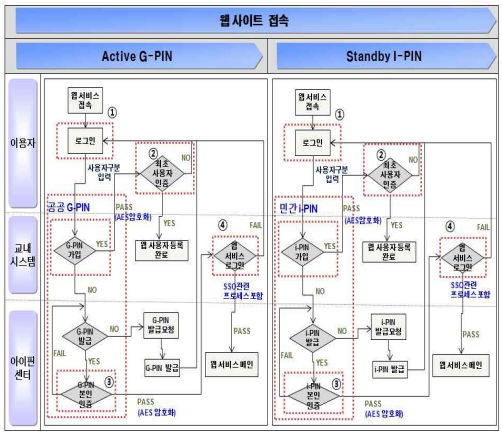

그림 2. i-PIN 이용 웹 사이트 접속 flower
Fig. 2. Web Site Access Flow Using i-PIN

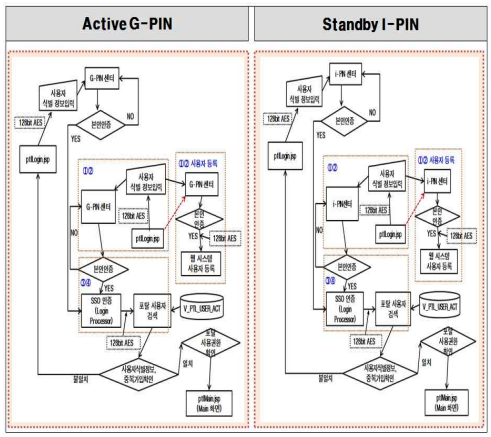

그림 3. 웹 사이트 사용자 등록과정 및 웹 서비스 절차도
Fig. 3. Web Site Registration Process and Prodedures Web Service

2.3 i-PIN 본인 인증 절차

i-PIN 본인 인증을 통한 웹 시스템에 접속하는 과정은 [그림 2][그림 3]의 ①②③④는 다음의 4가지로 설명한다.

① 웹 시스템에 접속하기 위해서는 사용자 식별 정보를 입력 한다. 이 때 i-PIN 모듈이 구동되어 i-PIN 아이디와 암호를 입력받는다. i-PIN 아이디와 암호가 없으면 i-PIN 본인확인기관에서 i-PIN 아이디와 암호를 발급받는다.

② 웹 시스템에 발급받은 i-PIN 아이디와 암호를 제공하고 웹 시스템은 i-PIN 본인확인기관과 통신하여 사용자 i-PIN 아이디와 암호 유효성 검사를 요청한다. i-PIN 본인확인기관에서 유효성 검사가 승인되면 웹 시스템에 사용자 등록 과정이 수행된다. ①② 사용자 등록은 웹 시스템에서 사용자를 확인하는 과정으로 인터넷 웹 사이트의 회원가입 대신 사용되는 사용자 인증 과정이다. ③④ i-PIN 본인확인 인증 값이 정상적으로 인증·전송되면 웹 시스템과의 연계하여 사용자 식별 정보와 i-PIN 본인확인기관 정보를 확인하고 일치하면 웹 시스템 접속 권한이 부여된다. i-PIN 본인인증 후 웹 시스템과의 자료 전송은 128비트 암호문인 AES 암호화 알고리즘을 이용하였다. AES 암호화 알고리즘은 다양한 블록크기인 128, 192, 256 비트 등 독립적으로 선택 될 수 있는 키를 가지고 각 단계의 암호화 과정이 반복되는 블록 암호 중 하나로 분류된다. 예를 들어 십진법으로 표시하면 128비트 키는 3.4×10^{38}개의 것이 가능하다. 또, AES 암호화 알고리즘은 그 안전성을 검증받아 차세대 암호 표준으로 사용되고 있다.

3. 시스템 구현

i-PIN을 이용한 본인 인증 과정을 대학 내 웹 정보시스템에 적용하여 구현하였다. 학내 웹 정보시스템의 구성은 메일, 게시판, 웹 하드, 업무관리 시스템으로 구성되며 사용자는 학생, 교원, 직원으로 분류되어 각각의 권한에 따라 웹 정보시스템에 접속이 부여된다. i-PIN을 이용한 학내 웹 정보 시스템의 서비스 구성 및 하드웨어 구성은 [그림 4]와 같이 구성되며, i-PIN 발급, 웹 사이트 본인 인증, i-PIN 유효성 검사와 i-PIN 서비스 센터의 장애 시를 대비한 i-PIN 프레임워크 구성으로 설명된다. i-PIN 서비스 프레임워크는 2개의 i-PIN 서비스를 연계하여 Active, Standby 형태로 무 중단 서비스가 지원되도록 구현하였다.

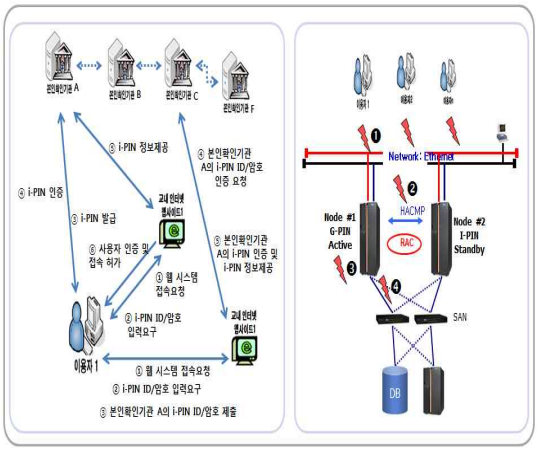

그림 4. 구현시스템-본인 인증 웹 서비스 및 하드웨어 구성도
Fig. 4. Implemented of the System-Personal Certification Web Service and Hardware Configuration

3.1 i-PIN 환경의 본인 확인 절차 웹 시스템 로그인

i-PIN을 이용하여 웹 시스템에 접속하기 위해서는 i-PIN 본인확인기관에서 i-PIN 아이디와 암호를 발급받는다. i-PIN은 공공 g-Pin과 일반 i-PIN 2개의 i-PIN을 발급받아 본인이 Main i-PIN과 Sub i-PIN으로 구분하여 사용한다. 인터넷 웹 사이트에 본인의 사용자 식별 정보(그룹, 학번/교번)를 입력한 후 로그인을 요청한다. 이는 웹 시스템과 접속할 때 내부인임을 확인 할 수 있는 정보로 사용된다. [그림 5]는 웹 시스템 로그인은 화면 구성이다.

3.2 사용자 등록

최초 사용자 등록과 i-PIN 본인 인증은 본인확인기관에서 발급받은 i-PIN 아이디와 암호를 이용해야 한다. 이는 i-PIN 서비스 모듈이 연계되면 로그인 시 본인 확인을 위해 i-PIN 아이디와 암호를 요청하기 때문이다. 웹 시스템 로그인 후 내부자 인증을 통해 내부인임이 확인되면 [그림 6]처럼 이미 부여되어 본인만 알고 있는 내부시스템 인증 암호 확인과 i-PIN 서비스 모듈 연계로 최초 사용자 등록을 처리한다. 이 때 내부 시스템과의 암호 확인 결과 거부되면 웹 시스템에 이용자로 등록을 할 수 없게 된다. 아울러 i-PIN 서비스 연계도 거부되어 웹 시스템에 접근이 불가능하게 된다. 기존 인터넷 웹 사이트에서의 회원가입 절차를 본 시스템에서는 i-PIN을 이용한 내부 이용자 등록으로 수행하게 하였다. 즉, 이 과정이 기존 인터넷 웹 사이트의 회원가입 과정과 동일하다고 볼 수 있다. 또한, i-PIN 서비스 모듈은 입력받은 이용자의 i-PIN을 본인 확인기관에 전송하고 이용자의 i-PIN 아이디가 사용되는 인터넷 웹 사이트 정보를 기록하여 관리한다.

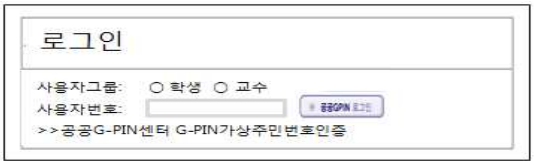

그림 5. 웹 시스템 로그인
Fig. 5. Web System Login

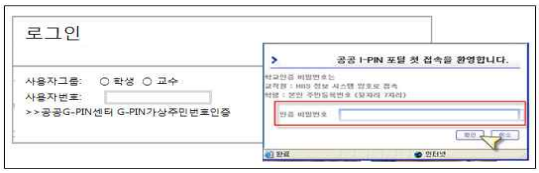

그림 6. 웹 시스템 최초 사용자 등록
Fig. 6. The First User Registration Web System

3.3 i-PIN 본인 인증

[그림 3]의 ①② 사용자 등록은 웹 시스템 접속 최초 1회만 수행되며 웹 시스템 접속 시에는 [그림 2]의 ① 로그인 버튼을 클릭하면 i-PIN 모듈이 연결된다. [그림 3]의 ③④의 과정을 [그림 7]과 같이 구현되며 i-PIN 인증 모듈이 구동되면 i-PIN 아이디와 암호를 입력 후 본인확인기관으로부터 유효성 검사를 진행 한 후 인증 값이 전달되면 본인 인증이 완료된다. 만약, i-PIN 센터의 장애가 발생되어 i-PIN 본인 인증 모듈이 구동되지 않으며 Standby i-PIN 센터의 서비스 모듈이 자동 구동되어 이 과정을 수행하게 된다.

3.4 웹 시스템 접속 완료 후 시스템 권한 부여

[그림 3] ③④에서 i-PIN 본인확인 인증 값이 정상적으로 전송되면 ①의 웹 시스템 로그인 시 입력받은 사용자 식별 정보를 AES 암호화 알고리즘에 적용하여 웹 시스템과 연동시켜 사용자의 권한에 부합하는 웹 시스템을 사용자에게 제공한다. [그림 8]은 i-PIN 본인확인 완료 후 접속되는 과정을 구현한 웹 정보시스템 메인 화면이다.

그림 7 i-PIN 본인 인증 확인 과정
Fig 7. Authentication Process of Personal Certification i-PIN

그림 8 i-PIN 본인 인증 웹 시스템
Fig 9. Personal Certification of i-PIN Web System

3.5 본인인증기관 장애 시 웹 사이트 i-PIN 서비스 연동

본 논문에서 적용한 i-PIN 웹 정보시스템은 i-PIN 본인확인기관의 장애 발생 시 이용자의 불편을 최소화하고자 i-PIN 웹 정보시스템을 Active, Standby 형태로 구성하였다. 만약, Active i-PIN 서비스 제공기관에 장애가 발생되면 대기하고 있던 Standby 민간 i-PIN 서비스로 자동 전환되어 웹 정보 시스템 접속이 가능토록 구성 하였다. Active, Standby 형태의 i-PIN 웹 시스템의 장애 발생 시 자동 연동 과정은 [그림 9]로 도식화 하였다. 이 때 사용자는 서비스 웹 시스템이 변경되었는지를 알 수는 없다. [그림 9]의 i-PIN 본인인증기관 장애 시 설계된 i-PIN 서비스 프레임워크의 서비스 연계 과정은 다음과 같다. ① Active, Standby i-PIN 웹 정보시스템은 항상 RS232 Asynchronous Adaptor Heartbeat 구성으로 i-PIN 웹 정보 시스템과 i-PIN 본인확인기관의 서비스 지원 여부를 상시 확인한다. ② 웹 시스템 연계 i-PIN 본인확인기관에 장애가 발생 하면 사전에 미리 구성되어 있는 HACMP(High Availability Cluster Multi Processing)에 의해 ③④ Standby i-PIN 웹 정보시스템으로 IP 전환이 이루어진다. ⑤ 민간 i-PIN Standby 웹 정보시스템은 Active 공공 i-PIN 웹 정보시스템으로 전환 되며 웹 서비스를 시작한다. ⑥⑦⑧ i-PIN 메인 시스템의 장애 조치가 완료되면 현재의 Active 시스템은 Standby 상태로 자동 전환된다.

4. 구현시스템 분석

성능테스트는 구현된 i-PIN 적용 웹 사이트를 대상으로 최대 부하를 발생시켜 성능목표(응답시간, TPS, 시스템자원 사용률 등)의 만족 여부를 확인하였다. 시스템 성능 결과를 토대로 대량의 트랜잭션 발생 시 본 구현 시스템의 부하량을 미리 예측하여 인터넷 웹 서비스 시스템의 부하 분산을 유도하고 시스템의 실용성과 안정성 등에 대하여 검토하였다.

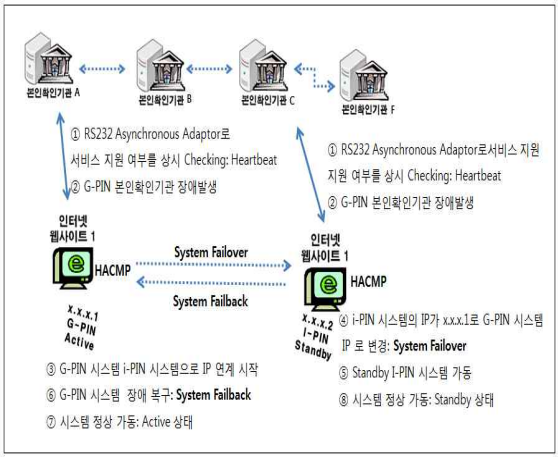

그림 9 i-PIN 본인인증기관 장애 시 서비스 연계도
Fig. 9. Linked the Personal Certification Service Failure

4.1 구현시스템 성능테스트 시나리오

제안시스템 테스트를 위한 시나리오는 인터넷 웹 사이트 로그인 접속 → g-PIN센터 → 본인인증 → 웹 사이트 로그인 → 게시판 접속 → 인터넷 웹 사이트 메인 → 게시판 접속 → 인터넷 웹 사이트 메인 → 로그아웃'의 과정을 가상으로 유도한다. 또, 가상의 유저는 V-User500으로 가정하였다. 통상 동시사용자 수는 시스템을 일반적인 상황에서 동시에 사용하고 있는 사용자수를 의미하나 본 성능테스트에서 사용하는 V-User는 쉬는시간(think time)을 제외한 실제 액션 시간만을 고려한 사용자수(동시액션사용자)로 하였다. V-User 산정은 가장 트래픽이 많아지는 Peak time 때의 환경을 고려하여 산정했으며, V-User 산정 방법은 다음과 같다.

① V-User 산정 = 동시사용자수/think time 적용 계수
② 동시사용자수 = 총사용자 * 피크 타임 시 사용자 사용률
③ think time 적용 = [(평균트랜잭션응답시간+평균트랜잭션 thinktime)/평균 트랜잭션 응답시간] 계수

성능평가 기준은 각 Tire 간의 성능을 측정하고 이를 바탕으로 중요 Process의 성능을 측정하여 임계치를 정하고 충족하도록 하였다. 제안시스템은 대량의 트랜잭션이 발생할 경우 제안한 i-PIN 웹 시스템도 서비스 지연 현상이 초래 할 수 있다는 전제하에 성능 테스트를 진행하였다. 성능평가 시 이용된 관련 S/W와 H/W는 [표 4]에 성능평가 기준과 목표 및 방법은 [표 5]에 설명하였다.

표 4. 제안시스템 성능평가 H/W 및 S/W
Table 4. Proposed System Performance Evaluation Hardware and Software

구분	명칭				비고
S/W	App Perfect 9.5				1pc: 100 Users
	PHAROS				웹 모니터링 툴
H/W	TEST수행 PC				PC 5대
V-User 500	No	Instance	V-User	Polling	Thread
	1	2	500	200/200	
	2	2	500	200/200	
	3	2	500	200/200	

표 5. 제안시스템 성능평가 기준표
Table 5. Proposed System Performance Evaluation Standard

목적	성능목표	방법
i-PIN 웹 서비스의 신뢰성 확인	최고 부하 시에 i-PIN 웹 서비스에 오류가 발생하지 않아야 한다.	부하상황에서 i-PIN 웹 서비스의 에러 확인 ① Web, WAS, DB, 서버의 부하 측정 ② i-PIN 웹 서비스의 정상적인 수행 모니터링
i-PIN 웹 서비스의 서버의 성능측정 (정량화)	동시요청 사용자수 500 V-USER 시 성능목표	부하상황에서 응답시간, TPS 측정 ① Web, WAS, DB, 서버의 부하 측정 ② i-PIN의 정상적인 모니터링 수행

4.2 제안시스템 성능테스트 결과

측정결과 i-PIN 서비스 모듈 연계 웹 정보시스템은 대량의 트랜잭션이 발생하여도 시스템 부하량은 일반 웹 정보시스템과 다르지 않았다. 성능테스트를 제시한 V-User500은 웹 서비스 시스템에 접속하여 싱크 타임이 없다는 전제하에 대략 2,000 여명 정도의 동시접속자가 접속하여 웹 서비스를 수행하였다. 웹 서비스 모니터링 툴로 확인한 결과는 V-User500의 사용자가 동시에 i-PIN 웹 서비스 시스템에 접속 했을 때 초당 1664명의 동시접속자의 접속이 가능했고 시스템 응답시간은 초당 0.5초 DB 응답시간은 0.2초 정도로 i-PIN 웹 서비스에 접속 할 수 있음이 확인되었다. 이상의 결과를 분석하면 ① Oracle DB SGA 영역 사용률이 CPU 사용률에 비해 낮았고 ② DataBase Disk I/O가 많이 발생하지 않고 안정적으로 운영되어 ③ SQL문 Parsing 및 Cash hitting율이 양호하게 나왔다. 또한 i-PIN서비스 모듈 연계 시 사용된 SQL문으로 최적화 되지 못하면 SQL Parsing 및 Cach hitting율이 떨어져 CPU 사용률이 증가하게 되는데 측정 모니터링 결과는 그러하지 않았다. 이는 측정결과 i-PIN 서비스 모듈이 연계되어도 성능은 저하되지 않는다는 결과이다. [그림 10]의 결과 값으로 WAS의 CPU 사용률은 모두 90~100(%)으로 비슷한 비율을 보였으나, 3차에는 크게 향상되었음을 알 수 있었다. 이 결과로 볼 때 i-PIN 서비스를 웹 시스템에 연계하여 대량의 트랜잭션이 발생한다 해도 성능에는 큰 영향이 없음이 확인되었다.

4.3 기존 회원제 웹 시스템과 제안시스템 비교

다음은 대량의 트랜잭션이 발생하는 회원제 웹 시스템과 i-PIN 웹 시스템을 비교하였다. 비교 대상은 학내 웹 서비스 시스템 중 대량의 트랜잭션을 발생시키는 시스템을 기준으로 [표 3]과 동일 조건으로 시스템 부하를 비교하였다. [그림 11]는 기존 회원제 웹 시스템에 대량의 접속 트랜잭션을 발생시켜 CPU 및 DB 연결 건수 결과표이다. 기존 웹 서비스 시스템에 대량의 접속 트랜잭션이 발생 했을 때 CPU, DB, 웹서버 사용률이 70~80%를 선회하는 결과가 나왔다. 이는 i-PIN 웹 서비스 모듈 연동 후 부하량 보다 더 상위한 결과로 실제 서비스 관문에 i-PIN 웹 서비스를 연동해도 큰 영향을 받지 않는 결과라 판단할 수 있다.

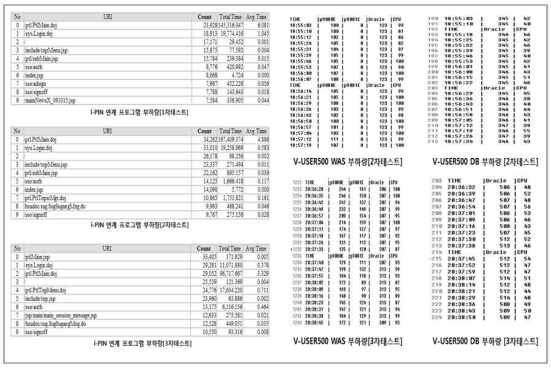

그림 10 i-PIN 서비스 프로그램 사용량 측정결과
Fig. 10. i-PIN Service Usage Measurement Program

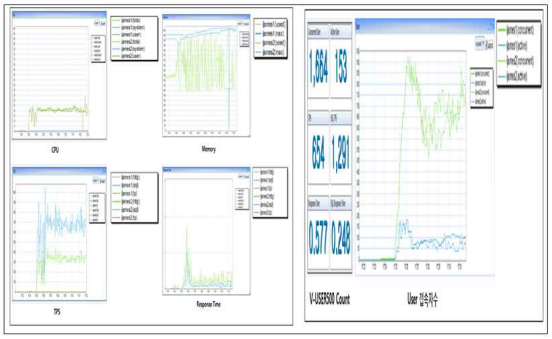

그림 11 최종 서버부하량, 최종 성능결과 및 접속자
Fig. 11. Last Server Load, Last Performance Result and the Visitor

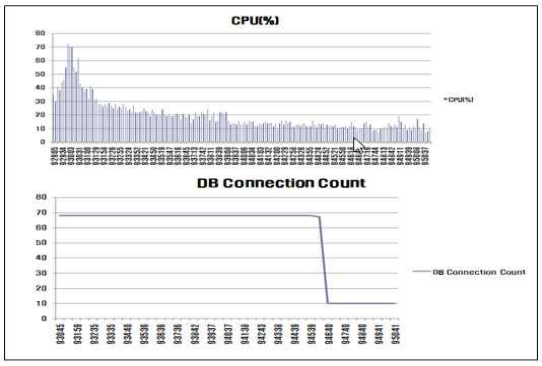

그림 12 회원제 웹 시스템의 부하 결과
Fig. 12 Load Result of Member System Web System

IV. 결 론

본 논문에서는 웹 시스템 접속 시 i-PIN을 이용한 본인인증 시스템을 구현하였다. i-PIN을 이용한 본인 인증은 그 간 인터넷에서 사용되어 온 주민등록번호 사용을 대체하고 인터넷에서 남용되는 웹 사이트별 회원의 ID와 암호를 i-PIN 하나로 연계하여 사용 할 수 있다. 또, 한번 부여받으면 평생 바꿀 수 없는 주민등록번호와 달리 i-PIN은 언제든지 폐기가 가능하다. i-PIN 폐기 후에는 언제든 새로운 i-PIN으로 발급이 용이하며, 이미 노출된 i-PIN은 해독이 불가능하여 개인정보 침해로 인한 피해를 최소화 할 수 있는 이점이 있다. 특히, PKI 공인인증서에서 제공되지 않는 개인의 생년월일, 성별 등의 정보를 i-PIN에서 제공되므로 성인 인증을 필요로 하는 웹 시스템에서 더 유용하다 할 수 있다. 본 논문에서 구현한 i-PIN은 국가에서 제공하는 공공 i-PIN 표준 모델로 TTA 표준서비스 규격에 준수되어 개발된 기술 표준으로 인터넷 전체 웹 사이트에서 적용이 가능하다. 아울러, i-PIN 본인 인증 후 웹 시스템과의 데이터 전송은 128bit AES 암호화 알고리즘을 적용하여 데이터 전송의 안정성을 확인하였다. 그러나, i-PIN 서비스는 i-PIN 서비스 제공기관에 장애가 발생되면 i-PIN과 웹 시스템과의 서비스 연동이 불가능하여 장애 복구 시까지 i-PIN 본인 인증 시스템에 접속 할 수 없는 단점이 있었다. 이를 해결하고 i-PIN 서비스를 주 서비스(Active)와 서브 서비스(Standby)로 구성하여 장애 시에도 지속적인 서비스 지원이 가능토록 하였다. 즉, 주 서비스(Active)의 공공 i-PIN 서비스 제공기관에 장애가 발생되면 i-PIN 서비스를 대기하고 있던 서브 서비스(Standby) 민간 i-PIN 서비스로 전환시켜 웹 정보시스템 접속이 가능토록 하였다.

향 후 연구 과제로 본 논문에서 제시한 i-PIN 본인 인증 활성화를 위해서는 현재의 i-PIN 표준 서비스 지원 방법을 사용자 입장에서 용이하게 구성해야 할 것이다. 더불어 본 서비스가 비영리 목적의 교육·공공기관의 웹 사이트에서 i-PIN이 개인인증서로 사용된다면 개발 예산 절감으로 인한 경제적 가치의 향상과 정보시스템의 안전성의 증대를 기대 할 수 있을 것이다. 현재 i-PIN을 인증서로 사용하는 연구가 꾸준히 전개되고 있다. 이를 뒷받침하기 위해서는 합리적인 서비스 정책과 정보기술도 반드시 수반되어야 할 것이다. 예를 들면 금융 기관의 경우 금융실명제법으로 인해 주민등록번호를 반드시 사용해야함을 들 수 있다. 합리적인 정책과 정보 기술은 i-PIN 활용과 경제성 및 개인정보 보호에 도움이 될 것 이다.

참고문헌

[1] J.Y. Hwang, “Variation of the ubiquitous environment protection of information and response strategies Facts”, Korea Internet Security Agency, 2008.

[2] “Social security number on the Internet as a means of protection available technology certificate”, Korea Information Certificate Authority Inc, pp. 13-14, 40-42, 2010. 09.

[3] Digital daily, http://www.ddaily.net/news/news_view.php?uid=79077

[4] Daejonilbo, http://www.daejonilbo.com/news/newsitem.asp?pk_no=960693

[5] Y.S. Cho, S.H. Jin, “Overview and Comparison of Internet Identity Management System”, Electronics and Telecommunications Trends 22(3), pp. 137, 2007. 6.

[6] K.S. Min, “Spread dissemination as an alternative to social security numbers required i-PIN”, Korea Press Foundation Newspapers and Broadcast, pp. 168, 2008. 05.

[7] Ministry Public Administration And Security Public i-PIN Service, http://www.g-pin.go.kr/

[8] Y.D. Yun, “Social Security replaces public i-PIN

Service", Korea Regional Economic Research Institute, pp. 46 49, 2008, 11.

[9] In-Yong Jang, "Proposal for promoting i-PIN service by analyzing problems and offering alternatives", Soonchunhyang University, pp. 34-36 42-46, 2009.

[10] "i-PIN 2.0 Introduce Manual", Korea Communications Commission, Korea Internet Security Agency, 2009, 7.

[11] "i-PIN Policy Briefing And [Personal information, technical, and managerial safeguards standards] Reform hearings" Source Book, Korea Internet Security Agency, 2009.

[12] Kwang-Jin Park, "Number of residents(i-PIN) for the development of technical standards and service frameworks", Korea Institute of Information Security, pp. 20-26, 2008.

[13] "2009 Survey on state of Information Security ", Korea Internet Security Agency, pp. 122-125, 2010

[14] "Survey on the usage and satisfaction of i-PIN", Korea Internet Security Agency, A research paper , 2007.

[15] Younsung Choi, Yunho Lee, Seungjoo Kim, Dongho Won, "Security Analysis on the Implementation Vulnerabilities of I-PIN", Korea Institute of Information Security, pp. 148-149, 40, 2007. 4.

[16] "Framework for internet-Personal Identification Number Service", TTAS.KO-12.0054, TTA Standard, pp. 4-7, 2007.

[17] C.J. JUNG, Personal identification number from the Internet service and Standard, Korea Internet Security Agency, pp. 75-78, TTA Journal 2008.

[18] SangHwan Park, "Secure Korean-SSN Alternative Information Service", Korea University 2006.

[19] "Message Format for i-PIN Service", DidM-2008-001, DidM Standard, pp. 3-12, 2008.

[20] "Duplicated Joining Verification Information for i-PIN Service", TTAKKO-12.0038, TTAKKO-12.0038/R1, TTA Standard, pp. 7-9, 2008.

[21] Young-Hyun Lee, "A Study of Personal Identification Method for Preventing Personal Privacy Information Leakage", Seoul National University of Technology, pp. 19-20, 2009.

[22] Young-Ho Seo:Jong-Hyeon Kim:Young-Jin Jung:Dong-wook Kim, "ITC-CSCC 2000 PROCEEDINGS V.1 - VLSI Design & Applications 1", ITFIND , 2007. 07.

[23] Shuo Bai, "IWAP2001: First International Workshop for Asian PKI-PKI in China", ITFIND , 2001.10.

[24] Tae-Jin Yun, "Improved RFID Mutual Authentication Protocol using One-Time Pad and One-Time Random Number Based on AES Algorithm ", Korea Science Computer Institute, pp. 164, 2011. 11.

저 자 소 개

김 현 주

2010: 단국대학교 정보통신대학원 정보통신대학원 졸업(공학석사)

현 재: 단국대학교 대학원 전자전기공학부 박사과정

관심분야: 정보보안, i-PIN, 역추적, IT 융합, 스마트카드, 자바카드

Email : chopin@uhs.ac.kr

신 인 철

1973: 고려대학교 전자공학과 졸업(공학사)

1978: 고려대학교 대학원 전자공학과 졸업(공학석사)

1986: 고려대학교 대학원 전자공학과 졸업(공학박사)

현 재: 단국대학교 전자전기공학부 교수

관심분야: 병렬처리, 정보보안, 자바카드, 스마트카드

Email : char@dankook.ac.kr

이 수 종

1989: 국민대학교 전자공학과 졸업(공학사)

1992: 연세대학교 대학원 전자공학과 졸업(공학석사)

2000: 연세대학교 대학원 전기컴퓨터공학과 졸업(공학박사)

현 재: 협성대학교 컴퓨터공학과 부교수

관심분야: IT융합, 생체인식, 영상처리, 신호처리, 영상통신

Email : sjlee@uhs.ac.kr