情 報 保 護 學 會 誌
第20卷 第6號, 2010. 12

인터넷상 주민번호 이용을 대체하기 위한 아이핀 2.0 서비스 프레임워크

최 광 희*, 안 종 찬**, 이 강 신***, 안 승 호****

요 약

정부는 계속되는 대량 개인정보 침해사고로 인한 피해를 방지하고 인터넷상 무분별한 주민등록번호 사용을 최소화하기 위하여 2005년부터 아이핀을 개발하여 보급중이나 대부분의 웹사이트가 주민등록번호 기반으로 개발되어 아이핀 도입 및 활용이 미흡한 상황이다. 본 논문에서는 지금까지 아이핀 서비스가 활성화되지 못한 기술적 원인을 분석하고, 최근 편이성 대폭 개선된 아이핀 2.0의 주요 서비스와 향후 개선 방향을 소개함으로써 초창기 아이핀 서비스에 대한 오해를 개선하고자 한다.

Ⅰ. 서 론

주민등록번호는 한번 부여 받으면 변경할 수 없다는 고정 불변성, 1인당 1개씩만 부여되는 유일성, 생년월일, 성별 등의 유용한 개인정보를 숫자로 담고 있는 이용 편리성으로 국내 웹사이트에서 광범위하게 활용되고 있으며, 국내 인터넷 사이트의 60% 이상이 회원 가입 시 본인확인 등을 위해 주민등록번호를 수집·저장하고 있다[1]. 하지만 최근 해킹, 내부관리 소홀, 마케팅 경쟁 심화 등 다양한 원인으로 인해 주민등록번호가 대량으로 유출 개인정보침해사고가 계속 발생하고 있으며, 유출된 주민등록번호를 이용하여 명의도용 등의 2차적 피해도 계속되고 있어 웹사이트에서 무분별한 주민등록번호번호 수집·저장이 인터넷상의 신뢰구조 전체를 위협하는 심각한 위험으로 확대되고 있다.

이에 정부는 2005년부터 국내 웹사이트에서 주민등록번호를 이용하지 않고도 본인확인, 성인인증 등의 서비스가 가능한 아이핀(i-PIN) 서비스를 개발하여 보급 중에 있다. 아이핀(i-PIN)은 사업자 측면에서 이미 국내에 많은 웹사이트가 다양한 목적으로 주민등록번호를 이용하고 있는 점을 고려하여 사업자의 DB 변경을 최소화하면서 기존 주민등록번호가 이용되던 서비스를 대체할 수 있도록 개발 되었으며, 이용자 측면에서는 본인확인에 필요한 주민등록번호 등 주요 개인정보를 제3의 신뢰기관에 보관하고 웹사이트에는 서비스제공에 필요한 최소한의 정보만 제공함으로써 주민등록번호 유출 위험의 최소화하는 전략적 서비스 프레임워크를 기본으로 구성되었다.

하지만 지금까지 아이핀(i-PIN)은 주민등록번호 유출 위험을 최소화 하려는 목적에만 중점을 두어 실제 도입하려는 웹사이트의 내부 업무처리의 용이성이나 개인 이용자의 사용 편리성에 대한 고려가 부족하여 보급과 이용 활성화가 미진한 것이 사실이었다. 이러한 기존의 이용 불편을 대폭 개선하여 아이핀(i-PIN) 보급 및 이용을 활성화하기 위하여 웹사이트간 동일인 식별, 아이핀(i-PIN) 발급기관 자동 식별, 해외거주 국민의 아이핀(i-PIN) 발급 등이 가능한 아이핀(i-PIN) 2.0 서비스를 개발하여 2009년 7월부터 적극 보급중에 있다.

본 논문에서는 아이핀(i-PIN) 서비스 구성 및 이용방법, 아이핀(i-PIN) 2.0에서 개선된 서비스 내용을 중심으로 소개하여 초창기 아이핀(i-PIN) 서비스에 대한 오해로 인한 아이핀(i-PIN) 도입 및 이용을 꺼리는 문제를 개선시키고자 한다.

* 한국인터넷진흥원 책임연구원(khchoi@kisa.or.kr)
** 한국인터넷진흥원 팀장(jcahn@kisa.or.kr)
*** 한국인터넷진흥원 단장(kslee@kisa.or.kr)
**** 전남대학교 교수(shahn@chonnam.ac.kr)

Ⅱ. 국내 개인정보 침해사고 현황 및 사례

한국인터넷진흥원에 접수된 개인정보 침해 신고 및 상담 건수를 분석해보면 2004년부터 2008년까지 4년간 2배 이상 증가하였으며, 대량 개인정보 유출 사고가 많이 발생한 2008년도에는 전년 대비 36%나 증가하였다[1].

개인정보 유출, 노출 등 침해사고는 매년 지속적으로 발생하고 있으나 국내의 경우 2008년도 특히 대량 개인정보 침해사고 많이 발생하였으며, 유출 원인 또한 다양하였다[3].

1) 외부자 해킹 : 옥션 고객정보 유출[4]

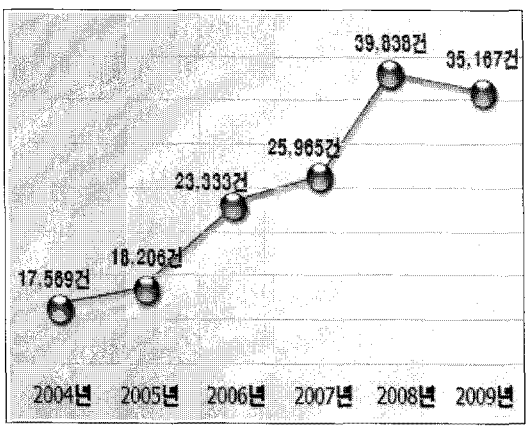
2008년 2월 중국 해커들이 옥션 고객 1,863만명의 이름, 주민등록번호, 주소, 이메일 전화번호-- 휴대폰번호, 카드번호 등의 개인정보 유출

2) 내부자 고의 유출 : GS 칼텍스 고객정보 유출[5]

2008년 8월 GS 칼텍스 자회사 직원이 1,150만명의 이름, 주민등록번호, 주소, 이메일 등의 고객정보를 DVD에 담아 유출

3) 내부자 정보 도용 : LG 텔레콤 고객정보 유출[6]

2008년 3월 LG텔레콤의 고객정보 위탁업체의 ID와 패스워드 등을 도용하여 170명의 주민등록번호와 휴대전화 가입일, 휴대전화 모델 등이 유출



〔그림 1〕 개인정보 침해 민원 및 신고 건수

4) 내부자 실수 : 한메일 정보 유출[7][8]

2008년 7월 서비스 개선을 위한 작업중 담당자 실수로 로그인한 55만명 회원의 이메일 목록과 내용이 무작위로 노출 되는 사고 발생

5) 담당자 무단 열람 : 국민건강보험공단[9]

2008년 3월 2,600여회에 걸쳐 개인별 진료일수와 투약일수, 진료비 지출내역 등을 열람해 자신의 석사 논문 작성 자료로 활용

6) 불법 마케팅 활용 : 하나로 텔레콤[10]

2008년 4월 600만명의 개인정보 8500여건을 전국 1000여개 텔레마케팅 업체에 불법으로 제공하여 활용

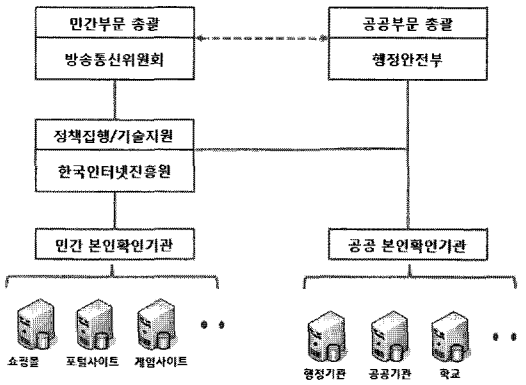
위 사례와 같이 고객의 개인정보가 다양한 원인으로 유출되고 있으며, 특히 주민등록번호의 경우는 생년월일, 성별, 출생지역 등의 개인정보를 함축하여 담고 있고 유출시 심각한 프라이버시 침해가 발생한다. 그럼에도 국내 웹사이트의 경우 아직도 대부분의 웹사이트가 회원가입시 주민등록번호를 수집·저장하고 있어와 주민등록번호 유출이나 노출로 인한 명의도용 등의 피해까지 위험이 높은 상황이다.

정부도 주민등록번호의 중요성을 인지하여, 2005년부터 인터넷상에 불필요한 주민등록번호 사용을 최소화하고자 인터넷에서 회원가입시 주민등록번호를 대체할 수 있는 본인인증수단으로 아이핀(i-PIN)을 만들어 국내 주요 웹사이트에 보급하는 정책을 추진 중이다

Ⅲ. 아이핀 1.0 서비스 개요

아이핀(i-PIN)은 온라인상에서 간단한 개인정보 입력과 본인확인과정을 통해 발급받을 수 있는 ID와 패스워드 형태의 인증수단으로 이용이 편리한 장점을 가지고 있다.

또한 다수의 웹사이트가 직접 주민등록번호를 수집·이용하면서 발생하는 문제점을 보완하기 위해 제3의 신뢰기관을 활용하는 방식으로 이용자는 아이핀(i-PIN) 발급기관(본인확인기관)에만 주민등록번호를



〔그림 2〕 아이핀 서비스 구성 체계도

제공하고 웹사이트 회원가입시에는 본인확인기관이 웹사이트에 성명, 생년월일 등의 인증정보를 제공한다. 따라서 웹사이트에는 이용자의 주민등록번호가 제공되지 않으므로 주민등록번호 노출을 근본적으로 방지할 수 있는 서비스 구조이다.[10].

3.1. 아이핀(i-PIN) 서비스 구성 체계

아이핀(i-PIN)은 인터넷상에서 신뢰할 수 있는 인증서비스 제공을 위하여 아이핀(i-PIN) 발급기관인 본인확인기관, 본인확인기관의 관리·감독 업무를 수행하는 감독기관(한국인터넷진흥원), 아이핀(i-PIN) 서비스를 도입하여 운영하는 웹사이트, 아이핀(i-PIN) ID/패스워드를 발급받아 이용하는 이용자로 구성되어 운영된다.

현재 아이핀(i-PIN) ID와 패스워드를 발급해주고, 웹사이트에 아이핀(i-PIN) 서비스를 보급하는 본인확인기관은 민간부문 5개 사업자와 공공부문 1개 기관(공공아이핀 센터)이 운영중이다. 공공 아이핀 센터는 행정안전부에서 직접 운영중이며 행정기관, 교육기관, 산하기관 등 국내 공공기관만을 대상으로 아이핀(i-PIN) 서비스를 무료로 보급중이다. 그밖에 5개 사업자는 방통통신위원회의 엄격한 심사를 통해 지정되어 운영중이며 민간과 공공기관 모두를 대상으로 아이핀(i-PIN) 서비스를 제공하고 있다[11].

공공아이핀 센터는 전문 기관에 위탁 운영중이며 행정안전부에서 관리·감독을 수행하고 있다. 민간 본인확인기관은 한국인터넷진흥원이 매년 서비스 운영상태, 시스템 취약점, 관련 법·규정의 준수 상태 등에 대하여 정기점검과 이행점검을 통해 서비스 안전성을 엄격히 관리하고 있다.

〔표 1〕 본인확인기관 운영 현황(2010.10월 현재)

구분	기관명	홈페이지
공공	공공아이핀 센터	www.g-pin.go.kr
민간	서울신용평가정보	www.siren24.com
	한국신용정보	www.idcheck.co.kr
	한국신용평가정보	www.vno.co.kr
	한국정보인증	www.sgipin.com
	코리아크레딧뷰로	www.ok-name.co.kr

3.2. 아이핀 서비스 이용

아이핀(i-PIN) 이용자는 본인확인기관중 1개 기관을 선택하여 아이핀(i-PIN) ID와 패스워드를 발급 받을 수 있으며, 발급기관에 상관없이 아이핀(i-PIN)이 도입된 공공과 민간 모든 웹사이트에서 동일하게 사용할 수 있다. 이용자가 웹사이트 회원가입시 실명인증 대신 아이핀(i-PIN) 인증을 선택하게 되면 웹사이트에 아이핀(i-PIN) 서비스를 제공하고 있는 본인확인기관으로부터 아이핀(i-PIN) 인증 요청이 이용자에게 송신된다[1].

이때 이용자는 아이핀(i-PIN) ID와 패스워드를 발급받아 본인확인기관에 송신하고 본인확인기관에서는 ID/패스워드를 검증하여 이용자의 인증정보를 웹사이트에 제공하게 된다. 웹사이트는 본인확인기관으로부터 이용자의 인증정보를 수신하여 기존에 회원으로 가입하였는지 등을 확인한 후, 회원가입에 필요한 추가 정보를 입력하게하고 회원가입을 허용하게 된다.

본인확인기관에서 웹사이트에 제공하는 이용자의 인증 정보는 주민등록번호를 이용한 서비스를 대체할 수 있도록 성명, 생년월일, 성별 등이 포함되어 구성되어 있다.

1) 성명정보

실명확인 및 본인확인을 통해 검증한 이용자의 실명

2) 생년월일정보

웹사이트의 경우 「청소년보호법」 제17조에 따라, 청소년유해매체물을 제공할 경우 인터넷 사이트는 이용자가 청소년인지 식별하기 위해 법적 연령을 확인해야 한

〔표 2〕 아이핀 1.0에서 제공되는 이용자 정보

제공정보	내용
성명	본인확인 수단을 이용하여 검증한 이용자의 실명
개인 식별번호	본인확인기관이 이용자에게 부여하는 13자리 정보(발급기관정보 2자리)이외는 난수값)
중복가입 확인정보	웹사이트내에서 이용자를 고유하게 식별할 수 있는 정보
생년월일	본인확인 수단을 통해 검증한 주민등록번호에서 추출한 정보
성별	본인확인 수단을 통해 검증한 주민등록번호에서 추출한 정보
연령대	본인확인 수단을 통해 검증한 주민등록번호에서 추출한 정보를 분류하여 8단계의 연령대 정보 제공
본인확인 수단	아이핀 발급시 이용한 본인확인 수단

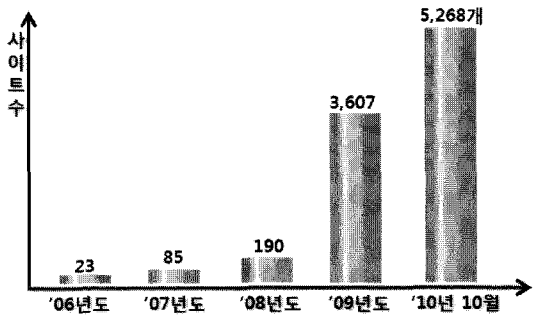
다. 따라서 본인확인기관은 본인확인을 통해 검증된 주민등록번호로부터 이용자의 생년월일정보를 추출하여 웹사이트에 제공한다.

3) 중복가입확인정보

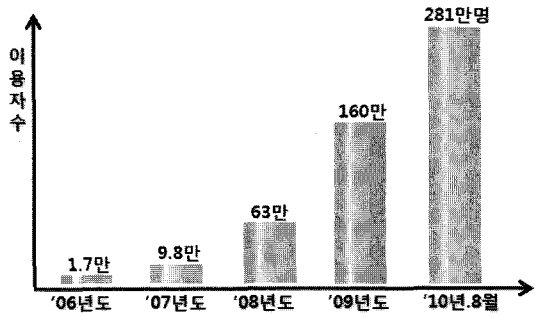
웹사이트는 효율적인IT 자원관리, 회원간의 신뢰 향상 등의 목적으로 회원의 중복가입을 제한하는 경우가 많으며 대부분 주민등록번호를 이용하여 중복가입을 방지하고 있다. 아이핀(i-PIN)은 본인확인기관에서 주민등록번호와 이용자가 가입하려는 웹사이트 정보를 이용하여 1차 해쉬한 값을 만들고, 본인확인기관간 공유한 비밀키를 이용하여 2차로 해쉬한 값을 생성하여 웹 사이트내에서 개개인을 고유하게 식별할 수 있는 정보를 만들어 웹사이트에 제공하고 있다.

Ⅳ. 아이핀 1.0 서비스 활성화 문제점

아이핀(i-PIN)은 현재 웹사이트 회원가입시 필요한 본인인증뿐만 아니라 회원관리 및 고객 맞춤형 서비스에 필요한 다양한 정보를 제공하고 있어 사업자 입장에서는 주민등록번호를 암호화 저장해야하는 부담을 줄이면서 기존 서비스를 유지할 수 있는 장점이 있다. 그럼에도 불고하고 아직도 많은 사업자가 아이핀(i-PIN) 도입을 꺼리고 있는 상황이다. 또한 이용자측면에서도 아이핀(i-PIN) 발급을 위해서 별도의 회원가입이 필요하고



〔그림 4〕 아이핀 도입 웹사이트 수



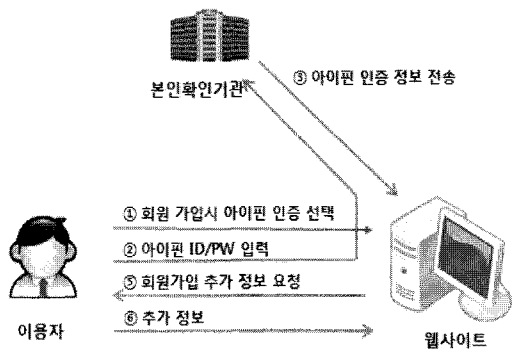
〔그림 5〕 아이핀 이용자수

주민등록번호가 사용하기 편리하다는 측면만을 고려하여 아이핀(i-PIN) 이용이 활성화 되지 못하는 실정이다.

아이핀(i-PIN) 활성화를 저해하는 요인은 다양하게 분석 될 수 있으나 본 논문에서는 기술적 요인에 한정하며 주요 요인은 다음과 같다.

1) 웹 사이트간 연계 서비스 불가

국내 웹사이트는 다른 웹사이트와 연계를 통해 마일리지, 사이버머니 등의 서비스를 제공하는 경우가 많이



〔그림 3〕 서비스 이용 절차도

있다. 이런 연계서비스를 위해서는 웹사이트간 동일인을 고유하게 식별할 수 있는 수단이 있어야 한다. 지금까지는 대부분의 웹사이트가 주민등록번호를 이용하여 동일인을 식별하였으나 아이핀(i-PIN)을 통해 회원가입을 할 경우 이용자의 주민등록번호가 없어 서비스가 불가능해지는 문제가 발생한다.

기존 아이핀 인증 정보 중에 개인 식별에 사용되는 정보로는 개인식별번호와 중복확인정보가 있으나, 개인식별번호는 본인확인기관별로 생성되는 번호로 동일한 이용자라도 아이핀을 발급 받은 기관별로 상이하여 이용자가 웹사이트별로 다른 아이핀을 이용하여 회원가입을 하였을 경우 동일인 식별이 불가능하다, 중복확인정보는 주민등록번호와 웹사이트 정보를 결합하여 해쉬한 값으로 동일한 이용자라도 웹사이트간 값이 상이하여 동일인 식별이 불가능하다[1].

2) 발급기관 암기

아이핀(i-PIN) ID는 각 본인확인기관별로 발급되고 관리되고 있어 이용자는 아이핀(i-PIN) 인증시 발급받은 기관을 먼저 선택하고 해당 기관에서 발급 받은 아이핀 ID와 패스워드를 입력하여야 한다. 하지만 대부분의 인터넷 이용자가 웹사이트 회원 가입을 자주 하지 않은 상황에서 발급기관을 암기하였다 이용시 선택하는 것은 이용자에게 큰 불편으로 작용한다[1].

3) 재외국민발급 이용 제한

2009년도 외교통상부 재외국민 현황을 보면 우리나라 국적을 유지하고 해외에 거주중인 국민이 286만명에 이른다. 하지만 재외국민의 경우 주민등록번호가 말소되었거나 본인명의로 국내에서 발급된 휴대폰, 신용카드, 공인인증서 없는 경우가 많아 아이핀(i-PIN) 발급이 어려운 상황이다.

현재 주민등록번호를 이용한 실명확인을 통해 웹사이트 회원가입시에도 불편을 겪었던 재외국민의 경우 아이핀(i-PIN) 서비스에서도 이용에 제한되어 국내 웹사이트 이용에 많은 불편을 초래하고 있다.

〔표 3〕 재외국민현황

재외국민			총계
영주권자	일반체류자	유학생	
1,219,561	1,306,462	343,898	2,869,921

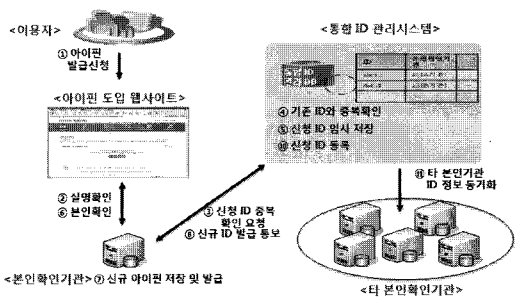
V. 아이핀 2.0

정부에서는 2009년 6월 정보통신망이용촉진및정보보호에관한법률에 따라 웹사이트에서 회원가입시 주민등록번호 이외의 대체수단을 제공해하는 1,039개 웹사이트를 공시하였으며, 공시된 웹사이트의 아이핀(i-PIN) 도입을 지원하고 아이핀 활성화를 위해 기존의 문제점을 대폭 개선한 아이핀(i-PIN) 2.0 서비스를 개발하여 2009년 7월부터 제공 중에 있다. 아이핀 2.0 서비스의 개선된 주요 사항은 아이핀 발급기관을 자동으로 식별하기 위한 통합 ID 관리시스템 구축, 마일리지 등의 서비스를 지원하기 위한 연계정보 생성, 여권 정보를 이용한 재외국민 발급 기능 등이 있다.

5.1. 통합 ID 관리시스템을 통한 발급기관 자동안내

각 본인확인기관별로 발급·관리되던 아이핀(i-PIN) ID를 통합하여 발급기관과 아이핀(i-PIN) ID쌍을 별도 DB에 저장하고 각 본인확인기관이 관련 정보를 실시간으로 공유하게 하는 통합 ID 관리시스템을 구축하여 발급기관을 자동으로 안내하는 기능이 추가되었다.

먼저 통합 ID 관리시스템을 통한 아이핀(i-PIN) 신규 발급 절차를 살펴보면, 이용자는 아이핀(i-PIN)을 신규로 발급받기 위해 실명확인후, 사용하려는 ID가 이미 사용중인지를 통합 ID 관리시스템을 통해 확인하게 된다. 사용 중이지 않는 ID인 경우 임시로 통합 ID 관리시스템에 저장되고, 본인확인기관에서 이용자의 본인확인을 거쳐 최종 아이핀(i-PIN) ID가 발급되면 통합ID 관리시스템상에 최종 등록되고 저장되게 된다. 이렇게 신규로 등록된 아이핀 ID와 발급한 본인확인기관 정보



〔그림 6〕 아이핀 신규 ID 발급 절차

는 타 본인확인기관에 실시간으로 전송되어 각 본인확인기관이 전체 아이핀(i-PIN) ID와 발급기관 현황을 유지할수 있게 된다.

이렇게 각 본인확인기관마다 아이핀(i-PIN) ID와 발급기관 정보가 실시간으로 공유되어 이용자가 아이핀(i-PIN) 인증시 ID를 입력하면 본인확인기관에서 해당 ID의 발급기관을 식별하여 해당 관을 통해 아이핀 인증을 처리하게 된다. 따라서 이용자가 일일이 발급기관을 암기하고 아이핀(i-PIN) 이용시 발급기관을 선택하여하는 불편이 해결되게 되었다.

또한 통합 ID 관리시스템이 장애시에는 각 본인확인기관이 자체 보유중인 아이핀 ID 정보로 신규 발급을 수행하고 장애 복구후에 자체 발급된 ID 정보를 통합 ID 관리시스템으로 전송하여 본인확인기관간 동기화가 진행되도록하였다. 이러한 장애대응 절차를 통해 통합 ID 관리시스템에 장애로 인하여 아이핀(i-PIN)이 신규로 발급되지 못하는 우려가 해소 되었다.

5.2. 연계서비스를 위한 고유식별정보 생성

아이핀(i-PIN) 2.0에서는 마일리지 등 다양한 웹사이트간 연계 서비스를 지원하기 위하여 아이핀(i-PIN) 인증정보에 주민등록번호를 기반으로 개인을 고유하게 식별할 수 있는 연계정보(CI)를 추가 하였다.

연계정보는 주민등록번호을 일방향 해쉬하여 생성되는 값이다. 아이핀(i-PIN) 이용자의 주민등록번호에 패딩값을 추가하고 첫 번째 임시값을 생성하고 이 임시값과 신뢰기관에서 보유하고 있는 비밀값을 익스클루시브 오아 연산을 통해 두 번째 임시값을 생성한다. 생성된 임시값은 512bit의 비밀키로 동작하는 일방향함수의 연산을 통해 연계정보(C)로 만들어지게 된다. .

이렇게 만들어진 연계정보(CI)가 아이핀 이용자가 가입한 각 웹사이트에 전달됨으로 웹사이트간 동일인을 식별하여 마일리지 등을 생성하여야 할 경우 각 웹사이트에 저장된 연계정보를 상호 비교하면 동일인 식별이 가능해 진다.

또한 비밀값과 비밀키값은 신뢰기관에서 안전하게 관리 하여 유노출의 유험을 최소화 하였으며, 비밀값이나 비밀키값의 노출 또는 해쉬 알고리즘의 안전성 문제 발생에 대비하여 침해사고 발생시 연계정보(CI)를 갱신할 수 있는 메시지 양식과 절차가 함께 마련되어 운영중에 있다.

〔표 4〕 연계정보 생성방법

〈CI 생성 방법〉

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

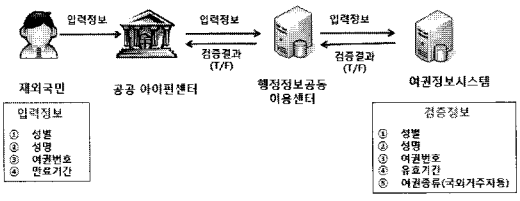
- ▷ CI : 서비스 연계를 위한 웹사이트 간 공동 식별자로 64바이트의 암호화된 코드
- ▷ $H()$: 512비트 이상의 출력을 갖는 암호학적으로 안전한 해쉬 함수
- ▷ RN : 주민등록번호 (13byte=104bit)
- ▷ $Padding$: 입력 값을 512bit로 만들기 위해 주민번호 104bit를 제외한 408bit를 채워 넣음
- ▷ S_A : 신뢰기관 보유 비밀정보(64byte=512bit)
- ▷ sk : 신뢰기관 보유 비밀키(64byte=512bit)
- ▷ $\|$: concatenation, 기호의 앞뒤를 연접

5.3. 여권정보와 연동을 통한 재외국민 아이핀 발급

주민등록번호가 말소되었거나, 본인명의로 발급받은 국내 신용카드, 휴대폰, 공인인증서 등의 본인확인 수단이 없는 국외 거주자의 아이핀(i-PIN) 발급을 위하여 외교부 여권정보를 이용한 재외국민 아이핀(i-PIN) 발급 기능이 구축되었다

아이핀(i-PIN) 발급시 여권정보를 이용한 본인확인을 하는 방법은 성명, 성별, 여권번호, 여권만료 일자를 입력하면 본인확인기관(공공 아이핀 센터)*에서는 외교부 여권정보시스템에 입력한 정보의 진위 및 여권의 유효성 검증을 요청하고 결과가 유효할 경우 아이핀(i-PIN) 발급이 이루어지게 된다.

여권정보를 이용한 아이핀(i-PIN) 발급의 문제점은 여권이 갱신될 경우 여권번호가 변경되어 여권번호를 기반으로 생성된 인증정보인 중복확인정보(DI) 및 연계정보(CI)가 변경되어 여권갱신 전에 가입한 웹사이트와



〔그림 7〕 재외국민 여권정보 검증절차

* 여권정보를 이용한 재외국민 아이핀 발급은 현재 공공 아이핀센터에서만 가능

여권 갱신 후에 가입한 웹사이트에서 동일인을 식별할 수 없는 상황이 발생한다.

이런 문제를 해결하기 위하여 재외국민의 경우 아이핀(i-PIN) 최초 발급시 여권번호와 갱신된 여권번호를 모두 저장하고 중복확인정보와 연계정보는 최초 가입시 여권번호를 기반으로 생성하여 운영함으로써 이러한 문제를 해결하였다.

Ⅵ. 결론

아이핀(i-PIN)은 인터넷상에서 불필요한 주민등록번호 사용을 최소화하기 위한 기술적 대책으로 정부가 개발하여 보급중에 있으며 주민등록번호가 사용되던 다양한 인터넷 서비스에 적용되면서 지속적으로 서비스 형태를 개선해나고 있다.

현재 주민등록번호기반의 공공부문 서비스나 금융서비스에도 아이핀(i-PIN)을 도입하기 위한 방안이 연구중에 있어 곧 새로운 서비스 형태가 추가될 것으로 예상되며, 공공과 금융분야까지 아이핀(i-PIN) 서비스가 도입된다면 인터넷상에서 불필요한 주민등록번호 사용이 획기적으로 줄어들 것으로 예상 된다.

지속적으로 발생하는 대량 개인정보 유출 사고를 고려할 때 웹사이트에서 회원가입이나 본인확인시 주민등록번호와 이름을 통한 실명확인은 더 이상 안전한 본인확인 방법이 될 수 없다. 웹사이트에서는 불필요한 주민등록번호 사용을 최소화하는 노력이 우선되어야 하며, 서비스를 위하여 주민등록번호가 꼭 필요한 경우는 아이핀(i-PIN)과 같은 주민등록번호 대체수단을 활용하는 방법을 도입해야 한다.

참고문헌

[1] 정찬주, 김윤정, 김진원, 박광진, " 주민번호 대체수단(i-PIN) 개발을 위한 기술표준과 서비스 프레임워크" *한국정보보호학회지* 18(6) pp.20-27, 2008

[2] 강달천, 허진수, 김동환, "*2009 개인정보분쟁조정사례집*", 한국인터넷진흥원 pp.14, 2010

[3] 장인용, 염흥열, "인터넷상의 본인수단인 아이핀의 활성화 방안 연구", *한국정보보호학회지* 19(5), pp.81-92, 2010

[4] EBN 산업뉴스, "옥션 해킹 피해자 1천863만 확정", http://www.ebn.co.kr/news/n_view.html?id=429093

[5] YTN, "GS 칼텍스 고객 1,100만명 개인정보 유출", http://www.ytn.co.kr/_ln/0103_200809081037189548

[6] Newsis, "LGT, 170명 주민등록번호 등 개인정보 유출", http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=101&oid=003&aid=0002061600

[7] 전자신문, " 다음, 개인정보 유출 소송 본격화 ", http://www.etnews.co.kr/news/detail.html?id=200808030022

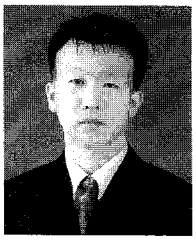
[8] views&news, "다음 비밀번호 등 개인정보 유출은 없어", http://www.viewsnnews.com/article/view.jsp?seq=38090

[9] 노컷뉴스, "개인정보 무단 열람한 국민건강보험공단 직원 검거", http://www.cbs.co.kr/Nocut/Show.asp?IDX=800853

[10] 한국경제, "툭하면 전화 온다했더니…하나로텔레콤, 600만명 개인정보 유출 `파문`", http://www.hankyung.com/news/app/newsview.php?aid=2008042473737

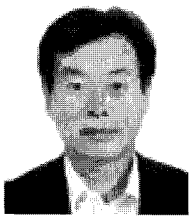
[11] *"i-PIN 2.0 도입 안내서"*, 한국인터넷진흥원, 2010

〈著者紹介〉



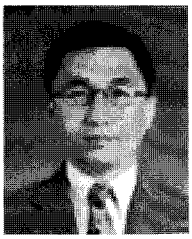
최 광 희 (Kwang-Hee Choi)
정회원

1997년 2월: 중앙대 산업정보과 학사
2002년 2월: 중앙대 정보시스템과 석사
2007년 2월: 전남대 정보보호협동과정 박사 수료
2002년 1월~2009년 7월: 한국정보보호진흥원
2009년 7월~현재: 한국인터넷진흥원
<관심분야> PIMS, IDM, 정보보호 거버넌스



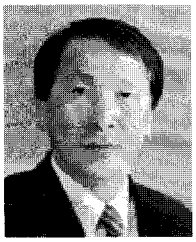
안 종 찬 (Jong-Chan Ahn)
정회원

1986년 2월: 인하대 물리학과 학사
2003년 9월: 한양대 경영정보학 석사
2008년 9월: 중앙대 최고경영자과정 수료
1999년 10월: 정보처리기술사
1986년 1월~1994년 9월: 현대건설 정보시스템 개발 과장
1984년 10월~2000년 5월: 현대정보기술 ERP 컨설팅팀 수석
2000년 5월~2002년 10월: 한국NCR 테라데이터 DW, CRM 컨설턴트
2003년 5월~2009년 12월: 정보통신국제협력진흥원 국제협력 총괄 단장
2010년 1월~현재: 한국인터넷진흥원 개인정보보호기술팀 팀장
<관심분야> DBMS, CRM, DW, 개인정보보호



이 강 신 (Gang-Shin Lee)
정회원

1987년 2월: 한양대 수학과 학사
1989년 8월: 한양대 수리통계 이학석사
2005년 8월: 고려대 정보보호대학원 공학박사
2000년 9월~2009년 7월: 한국정보보호진흥원 팀장
2009년 7월~현재: 한국인터넷진흥원 인터넷기반 • 개인정보보호단 단장
2006년 9월~현재: 건국대학교 겸임교수
2010년 Marquis who's who in the world 인명사전 등재
<관심분야> 개인정보보호, 네트워크 보안



안 승 호 (Seung-Ho Ahn)
정회원

1981년 8월: 전남대 수학과 이학석사
1985년 2월: 전남대 수학과 이학박사
1987년 12월~1989년 12월: 미국 미시건 대학 수학과 방문 교수
1983년 5월~현재: 전남대학교 수학과 교수
<관심분야> 암호학 분야