情 報 保 護 學 會 誌
第18卷 第6號, 2008. 12

주민번호 대체수단(*i*-PIN) 개발을 위한 기술표준과 서비스 프레임워크

정 찬 주 *, 김 윤 정**, 김 진 원***, 박 광 진****

요 약

국내 인터넷 사이트의 60% 이상은 회원가입시 본인확인 등을 위해 주민번호를 수집·저장하고 있다. 인터넷 사이트의 주민번호 수집 목적은 개인식별(중복가입여부 확인)과 본인확인, 연령확인, 마케팅 활용을 들 수 있다. 그러나 인터넷 사업자들의 주민번호 수집이 증가하면서 개인정보 유·노출로 인한 피해도 늘고 있다. 인터넷 사이트에서 주민번호 수집을 제한하면서 주민번호 기능을 제공·유지하기 위해 마련된 것이 주민번호 대체수단(*i*-PIN)이다. 본인확인기관이라는 다수의 제3의 신뢰기관이 인터넷 이용자의 개인정보를 받아 저장하고 인터넷 사이트 가입 등 필요할 때, 인증을 해주는 방식이다. *i*-PIN 서비스의 구성요소와 기능, 제공 서비스 등 *i*-PIN 서비스 프레임워크를 설명하고, 복수의 본인확인기관이 이용자의 인증을 위해 주고받아야 하는 메시지의 종류와 형식, 방법에 대한 국내 기술표준을 소개한다. 또한 중복가입 확인이 필요한 인터넷 사이트를 위해 유일 식별값으로 사용되는 중복가입확인정보 생성방법과 메시지 교류 방법 등을 소개함으로써 인터넷 사이트가 주민번호 대체수단으로서 타 수단과 차별화된 전략을 소개한다.

Ⅰ. 서 론

주민번호는 국가정보화를 진행해오는 동안, DB의 주요 킷(key)값으로 사용하여 업무효율성을 증진시키는 주요한 식별수단으로 사용되어 왔다.

그러나 우리나라 전체 인터넷 사이트의 62.2%, 상위 200여개 인터넷 사이트의 90% 정도가 일반 인터넷사용자에게 회원가입시 주민번호를 요구하는 등 무분별한 주민번호의 이용은 개인정보 유출 위험을 증가시키는 요인이 되고 있다.

개인정보 유출사고 중 주민번호 유출이 가장 우려할 만한 이유는 주민번호를 한번 부여받으면 평생 바꿀 수 없다는 평생불변성과 주민번호는 1인당 1개씩만 가진다는 유일성이라는 우리나라 식별번호가 가진 특성 때문이다.

정책적으로, 사회적으로 혹은 정치적으로 인터넷 사용자의 식별이 필요한 우리나라 인터넷 환경에서는 주민번호와 같은 편리한 식별수단의 사용이 필요한 실정이다.

주민번호 대체수단이 개발된 데에는 이러한 한국 인터넷 환경의 특수성이 반영되어 있다. 인터넷 사이트에서는 회원가입, 게시판에 글쓰기, 성인확인 등을 위해 이용자 본인확인 또는 연령확인이 필요하고, 개인정보 유출 위험을 예방하기 위한 사회적 장치도 요구되는 현실이 그것이다.

이미 많은 인터넷 사이트에 도입되어 있는 주민번호를 고려하여 사업자의 DB 변경을 최소화하고 주민번호를 통해 얻을 수 있는 개인정보를 제공함으로써 업무차질을 최소화할 수 있는 대체수단으로 *i*-PIN이 개발되었다.

i-PIN을 통해 사용자들은 주민번호를 사용하지 않고 인터넷 사이트에 가입할 수 있고, 인터넷 사업자들은 주민번호를 수집·저장하지 않고도 주민번호 수집목적을 달성할 수 있게 되었다.

본 논문에서는 *i*-PIN이 주민번호 유출방지를 위해 채택한 제3의 신뢰기관 모델이라는 서비스 프레임워크와 인터넷 사이트의 주민번호 수집 목적을 달성하기 위해

* 한국정보보호진흥원 개인정보보호지원센터 기술지원팀 (cjchung@kisa.or.kr)
** 한국정보보호진흥원 개인정보보호지원센터 기술지원팀 (kyoonj@kisa.or.kr)
*** 한국정보보호진흥원 개인정보보호지원센터 기술지원팀 (kjwon@kisa.or.kr)
**** 한국정보보호진흥원 개인정보보호지원센터 기술지원팀 (kjpark@kisa.or.kr)

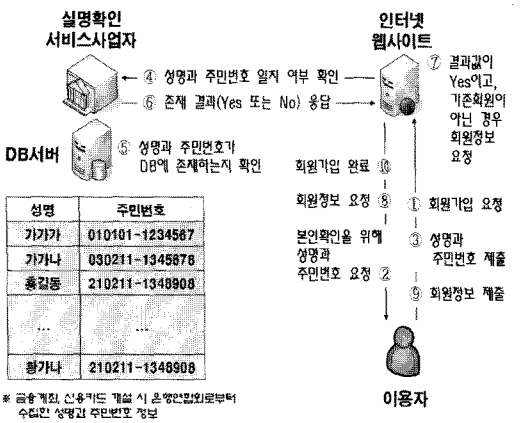
제공하는 서비스, 그리고 다수의 본인확인기관이 동일한 사용자의 인증을 위해 개발된 유일값인 중복가입확인정보와 메시지 전달 방법 및 형식등을 소개하고자 한다.

지난 6월 정통망법 개정으로 주민번호 이외의 회원가입방법 제공이 의무화됨에 따라, 대체수단의 활용이 증가할 것으로 보인다. 이에 인터넷 사업자와 이용자가 보다 편리하고 안전하게 *i*-PIN을 사용할 수 있도록 *i*-PIN 서비스 개선이 요구되고 있다. 본 고에서는 현재 *i*-PIN 서비스 내용을 담고 있으며, *i*-PIN 서비스 개선 사항은 다음 과제로 남겨두고자 한다.

Ⅱ. 주민번호 대체수단(*i*-PIN) 서비스 개요

1. 주민번호 실명인증 서비스

인터넷 사이트가 회원가입시 주민번호를 받는 목적은 대체로 두 가지로 정리된다. 첫째는 이용자의 성명과 주민번호 매칭 여부를 확인함으로써 본인인지 확인하고자 하는 목적이다. 이는 신용정보집중기관(은행이나 신용카드 회사)이 가진 주민번호와 성명 DB를 이용하여 확인값을 받는 것으로 엄밀한 의미로는 본인확인이 아니라 주민번호 실명확인이라 할 수 있다. 성명과 주민번호를 소유한 이용자가 실제 이용자인지 확인하지 않고 주민번호와 성명이 매칭되는지 여부만 확인하기 때문에 이미 노출된 주민번호와 성명으로 다른 인터넷 사이트에 가입할 수 있다는 위험이 존재한다.



〔그림 1〕 실명확인 방식을 이용한 회원가입 절차

둘째는 인터넷 사이트에서 개인정보 관리를 위해 주민번호를 수집·저장하는 것이다. 저장된 주민번호는 유료결제나 연령확인, 제휴서비스 등 기타 인터넷 사이트가 제공하는 서비스에 활용된다.

2. *i*-PIN 서비스 개요

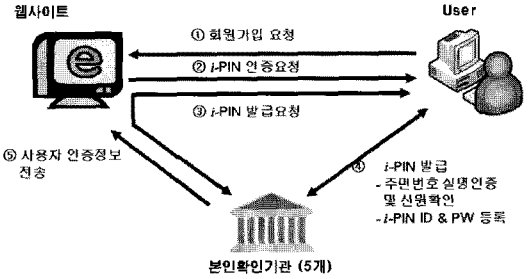
i-PIN은 인터넷 사이트의 주민번호 수집·활용 목적을 충족시키고 문제점을 보완할 수 있도록 제3의 신뢰기관을 이용하고 있다. 즉, 이용자가 인터넷 사이트에 직접 주민번호를 제공하는 대신 본인확인기관(*i*-PIN 발급기관)이라는 제3의 신뢰기관에 신원확인을 하고 인터넷 사이트에 주민번호 대신 *i*-PIN을 제공하여 회원가입 또는 성인인증을 할 수 있도록 한 것이다.

본인확인기관에 주민번호를 제공하고 본인임을 확인할 수 있는 신원확인 과정을 거치면 자신의 정보에 대한 통제권을 강화할 수 있는 장점을 가지게 된다.

또한 주민번호와는 달리 자신의 *i*-PIN이 노출되었다고 판단될 때는 언제든지 폐기하고 다른 *i*-PIN으로 재발급 받을 수 있어 개인정보 침해로 인한 피해를 최소화할 수 있는 장점이 있다.

i-PIN 서비스에서 신원확인과정은 이통사를 방문하여 개통한 휴대폰 SMS인증, 대면확인을 통해 발급한 신용카드의 번호, 유효기간, 비밀번호 확인을 통한 신용카드인증, 공인인증기관에서 대면확인을 통해 발급받은 공인인증서 인증 등이 있다.

현재 *i*-PIN 본인확인기관은 행안부 공공 *i*-PIN센터를 포함하여 5개로 인터넷 사이트에서 제공하는 *i*-PIN 본인확인기관과 이용자가 *i*-PIN을 발급받은 본인확인기관이 다르더라도 서비스가 가능한 상호호환성 서비스를 제공하고 있다.



〔그림 2〕 *i*-PIN 서비스 개요

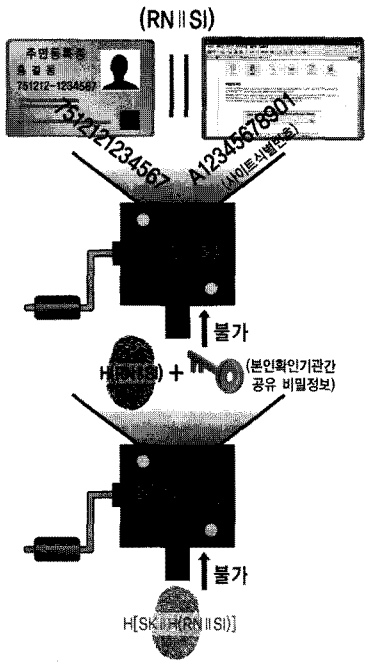
Ⅲ. *i*-PIN 제공 서비스

i-PIN 서비스는 인터넷 사이트가 도입한 본인확인기관이 이용자의 회원관리를 위해 필요한 정보를 인터넷 사이트에 전달한다. 본인확인기관이 인터넷 사이트에 전달하는 정보는 다음과 같다.

1. 중복가입확인정보 제공

인터넷 사이트는 회원관리를 위해 이용자를 유일하게 식별할 수 있는 정보를 필요로 한다. 현재 대부분의 인터넷 사이트에서는 주민번호를 이용하여 식별하고 있으나 *i*-PIN 서비스에서는 중복가입확인정보(DI)을 제공함으로써 유일 식별 기능을 제공한다.

중복가입확인정보는 이용자의 주민번호와 이용자가 가입하려는 인터넷 사이트의 식별정보를 이용하여 1차 해쉬한 값을 본인확인기관들이 가진 공유 비밀키로 2차 해쉬한 값이다.



〔그림 3〕 중복가입확인정보 생성 과정

2. *i*-PIN 번호(13자리) 제공

인터넷 사이트는 외부로부터 이용자의 정보제공을 요청받은 경우와 같이 이용자가 발급받은 본인확인기관이 어딘지 알아야 하는 경우가 있다.

본인확인기관은 이용자가 어떤 본인확인기관에서 *i*-PIN을 발급받았는지 알 수 있도록 *i*-PIN 번호(13자리) 중 3~4번째 자리에 본인확인기관 식별정보를 제공한다.

3. 생년월일정보 제공

「청소년보호법」 제17조에 따라, 청소년유해매체물 제공할 경우 인터넷 사이트는 이용자가 청소년인지 확인할 수 있도록 법적 연령을 확인해야 한다.

본인확인기관은 이용자의 실명확인과정을 통해 입력받은 주민번호를 이용하여 인터넷 사이트에 생년월일 정보를 제공한다.

4. 성별정보 제공

인터넷 사이트는 이용자의 성별에 따라 제공하는 서비스가 다를 수 있다. 본인확인기관은 성별에 특화된 서비스 제공이 필요한 사업자를 위해 인터넷 사이트에 성별정보를 제공한다. 그 외 제공 정보와 함께 정리하면 [표 1]과 같다.

〔표 1〕 *i*-PIN 제공정보

i-PIN 정보	내 용
성명	o 신원확인 수단을 이용한 본인확인을 수행하여 검증한 이용자의 실명
i-PIN (13자리 번호)	o 이용자의 본인확인을 수행한 이후에 본인확인기관이 이용자에게 부여하는 13자리 정보 (본인확인기관정보 2자리 이외는 난수 값)
중복가입확인 정보	o 회원가입 또는 글쓰기 권한을 얻고자 하는 인터넷 사이트 내에서만 유일하게 이용자를 식별할 수 있는 64byte 정보
생년월일	o 신원확인수단을 통한 본인확인을 수행하여 검증한 주민번호에서 추출한 8자리 정보(YYYYMMDD)
성별	o 신원확인수단을 통한 본인확인을 수행하여 검증한 주민번호에서 추출한 1자리 정보
연령대	o 신원확인수단을 통한 본인확인을 수행하여 검증한 주민번호에서 추출한 정보를 분류하여 제공하는 8단계의 법적연령대 1자리 정보
내·외국인	o 신원확인수단을 통한 본인확인을 수행하여 검증한 주민번호(또는 외국인등록번호)에서 추출한 1자리 정보

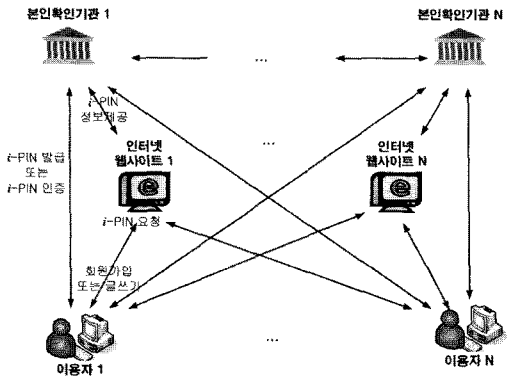
Ⅳ. *i*-PIN 서비스 프레임워크

1. 구성요소

i-PIN은 서비스를 이용하는 인터넷 이용자, 인터넷 사이트를 통해 정보를 제공하는 인터넷사업자 및 인터넷 이용자의 신원확인을 통해 인터넷 사이트에 이용자의 개인정보를 제공하는 본인확인기관으로 구성된다.

이용자는 여러개의 본인확인기관으로부터 *i*-PIN을 발급받을 수 있으며, 발급받은 *i*-PIN으로 회원가입이나 게시판 글쓰기를 위한 본인인증을 받을 수 있다.

인터넷 사이트는 이용자에게 *i*-PIN 서비스를 제공하기 위해 본인확인기관 중 하나로부터 *i*-PIN 서비스를 제공받아야 한다. 이용자가 발급받은 *i*-PIN 본인확인기관과 인터넷 사이트가 계약한 본인확인기관이 다른 경우, 이용자 발급 본인확인기관에서 인터넷 사이트 계약 본인확인기관으로 정보가 안전하게 전송되도록 인터넷 사이트는 하나의 본인확인기관과 계약을 하게 된다.



〔그림 4〕 *i*-PIN 서비스 프레임워크 구성

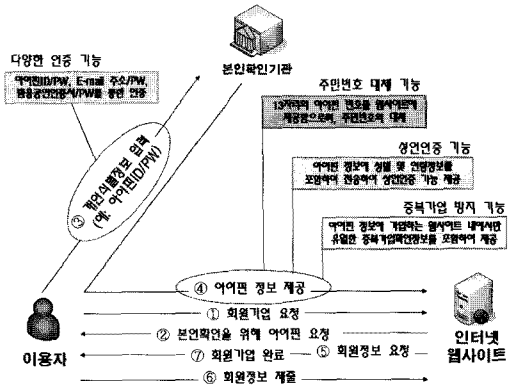
2. *i*-PIN 서비스 이용

이용자는 자신이 선호하는 본인확인기관에 자신의 개인정보를 제공하고 본인임을 확인함으로써 *i*-PIN을 발급받게 된다. 이용자가 방문한 인터넷 사이트에서 주민번호 실명인증 대신 *i*-PIN인증을 선택하고 자신이 발급받은 본인확인기관의 *i*-PIN을 요청한다. 인터넷 사이트가 적용한 본인확인기관과 이용자가 발급받은 *i*-PIN이 같은 경우는 해당 본인확인기관이 이용자가 입력한 *i*-PIN ID/비밀번호를 인증해주면 되지만, 이용자가 발급받은 *i*-PIN과 인터넷 사이트가 계약한 본인확인기관이 다른 경우는 본인확인기관간 인증값 전달이라는 내부 프로세스가 추가된다.

이용자가 이용하려는 인터넷 사이트에서 *i*-PIN 인증을 요구하면, 인터넷 사이트는 사이트와 계약한 본인확인기관의 *i*-PIN을 요청하게 된다. 이 때 이용자는 자신이 발급한 본인확인기관을 선택하여 최초 본인확인시 등록한 *i*-PIN ID와 비밀번호를 입력함으로써 인증받게 된다. 이용자 발급 본인확인기관은 이용자에 대한 인증이 완료되면 이용자가 가입하고자 하는 인터넷 사이트에서 신원확인된 이용자임을 증명할 수 있는 성명, *i*-PIN번호(13자리), 중복가입확인정보 등을 인터넷 사이트에 전달한다. 인터넷 사이트는 회원 DB에 본인확인기관으로부터 전달받은 중복가입확인정보가 존재하는지 확인한 후 없을 경우, 가입을 허용하게 된다.

이때, 이용자가 *i*-PIN을 이용하여 인터넷 사이트에 가입하기 위해서는 이용자가 가입하고자하는 인터넷 사이트 식별정보를 이용자가 발급받은 본인확인기관에 전달해야 한다.

웹사이트 식별정보는 이용자 발급 본인확인기관이 이용자의 중복가입확인정보를 생성하는 데 이용되고, 또한 이용자가 자신이 발급받은 본인확인기관으로부터 전달받은 정보를 인터넷 사이트에 전송할 때 이용된다.



〔그림 5〕 *i*-PIN을 이용한 회원가입 절차 및 기능

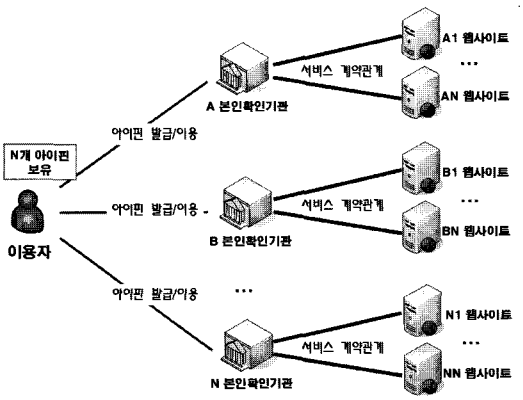
Ⅴ. *i*-PIN 서비스 전달메시지 형식

1. 본인확인기관간 상호연동

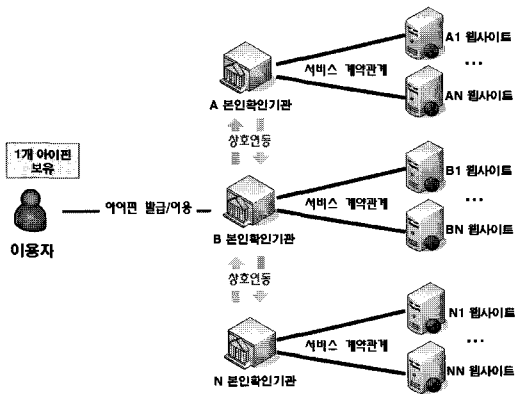
초기 *i*-PIN 서비스에는 본인확인기관과 인터넷 사이

트의 계약관계에 따라 서비스를 제공함에 따라 이용자는 해당 인터넷 사이트와 계약한 본인확인기관의 *i*-PIN을 발급받아야 인터넷 사이트를 이용할 수 있는 문제점이 있었다. 이를 해결하기 위해 현재 서비스를 제공하고 있는 5개 본인확인기관간 상호연동을 통해 하나의 *i*-PIN 발급으로 *i*-PIN이 적용된 모든 인터넷 사이트를 이용할 수 있도록 하였다. 상호연동을 위해서는 프레임워크에서 정의한 구성요소 간에 송·수신 메시지를 정의해야 했기 때문에 전달메시지 형식 표준이 필요했다.

(A) 상호연동 전 서비스 구조



(B) 상호연동 후 서비스 구조



〔그림 6〕 본인확인기관간 상호연동 전·후 서비스 구조

[그림 6]의 (B)에서 보는 것과 같이 이용자는 B 본인확인기관으로부터 하나의 *i*-PIN을 발급 받아 A 본인확인기관과 서비스 계약을 맺고 있는 A1부터 AN까지의 인터넷 사이트를 이용할 수 있다. 본인확인기관간 상호연동 방법은 인터넷 사이트가 모든 본인확인기관과 계약하지 않더라도 모든 이용자를 수용할 수 있는 구조로 상호연동된 상황이다.

2. 본인확인기관간 전달메시지 형식

인터넷 사이트는 이용자에게 *i*-PIN을 요청할 때, 이용자에게 자신이 발급받은 본인확인기관을 찾을 수 있도록 발급기관 찾기 기능을 제공한다. 이용자가 *i*-PIN 서비스를 제공하는 본인확인기관 중에서 이요자의 개인정보가 등록된 본인확인기관을 선택하게 된다. 인터넷 사이트는 일반적으로 자신이 계약한 본인확인기관의 팝업창을 제공한다.

이 때, 다음과 같은 인터넷사이트 정보를 이용자 발급 본인확인기관에 전달해야 한다.

WebsiteInfo ;;= SEQUENCE {

verificationURL PrintableString
- 이용자 선호본인확인기관의 팝업창 URL 주소로 [RFC 1738]을 준수

idpCode PrintableString,
- 계약한 본인확인기관이 인터넷 사이트에 부여하는 코드

cpCode PrintableString
- 최초 계약한 본인확인기관이 인터넷 사이트에 부여하는 코드로 중복가입확인정보 생성에 필요한 인터넷 사이트 식별정보(12자리)

cpRequestNumber PrintableString,
- 이용자의 개인정보를 본인확인기관으로부터 인터넷 사이트가 전달받기 위해 인터넷 사이트가 부여하는 번호

returnURL PrintableString,
- 이용자 발급 본인확인기관으로부터 이용자의 개인정보를 전달받은 인터넷 사이트 계약 본인확인기관이 인터넷 사이트로부터 IDENTUFYDATA를 전달할 URL 주소로 [RFC1738]을 준수]

i-PIN 서비스는 하이퍼텍스트 전송규약(Hyper Text Transport Protocol)을 기본 통신프로토콜로 사용하고

있어 본인확인기관간 이용자의 개인정보 전달은 모두 이용자를 거쳐 전달하게 된다. 통신 프로토콜의 특성 때문에 앞에서 정의한 WebsiteInfo 구조체의 정보를 전달해야 한다.

3. 인터넷 사이트에 전달되는 개인정보 형식

이용자 발급 본인확인기관은 이용자가 제출한 *i*-PIN ID/비밀번호로 이용자를 확인하게 되는데 해당 인터넷 사이트와의 계약관계 유무에 따라 인터넷 사이트에 개인정보를 전달할 것인지 또는 이용자가 가입하려고 하는 인터넷 사이트의 계약 본인확인기관에 이용자의 개인정보를 전달할 것인지 결정하게 된다.

3.1. 본인확인기관이 인터넷 사이트에 전달하는 개인정보 형식

이용자 발급 본인확인기관과 인터넷 사이트 계약 본인확인기관이 같은 경우 해당 본인확인기관은 Ⅲ장에서 소개했던 *i*-PIN 제공서비스에 해당하는 개인정보(*i*-PIN번호, 중복가입확인정보, 생년월일 등)를 암호화하여 인터넷 사이트에 전달하게 된다. 이때 암호화된 정보 안에는 아래와 같은 정보를 포함하여 전달해야 한다.

```
PersonalInfo ::= SEQUENCE {
  dupInfo          PrintableString
      - 이용자의 중복가입확인정보(PEM)
  virtualNo        PrintableString,
      - i-PIN 번호(13자리)
  cpCode           PrintableString,
      - 최초 계약한 본인확인기관이 인터넷 사이트에 부여하는 코드로 중복가입확인정보 생성에 필요한 인터넷 사이트 식별정보(12자리)
  realName         UTF8String,
      - 이용자의 실명
  cpRequestNumber          PrintableString,
      - 이용자의 정보를 전달할 인터넷 사이트 세션정보
  age    [0] AgeGroup      OPTIONAL,
      - 이용자의 연령대 정보
  sex    [1] BOOLEAN       OPTIONAL,
      - 0 : 여성, 1: 남성
  nationalityInfo  [2] BOOLEAN OPTIONAL,
      - 0 : 내국인, 1 : 외국인
  birthDate  [3] PrintableString  OPTIONAL,
      - YYYYMMDD 8자리 숫자의 이용자 생년월일 정보
  authInfo  [4]  AuthenticationInformation
                 OPTIONAL,
      - PIN 발급 시 신원확인수단 정보
  extensions  [5]Extensions OPTIONAL }
```

3.2. 본인확인기관간 전달하는 개인정보 형식

이용자 발급 본인확인기관과 인터넷 사이트 계약 본인확인기관이 같지 않은 경우 이용자 발급 본인확인기관은 이용자의 개인정보에 대하여 전자서명을 수행하고 본인인기관들이 공유하고 있는 비밀키 또는 임의로 선택한 비밀키로 암호화하여 전달한다. 이때 임의로 선택한 비밀키는 인터넷 사이트 계약 본인확인기관의 공개키 인증서의 공개키로 암호화하여 전달하거나 또는 인터넷 사이트 계약 본인확인기관의 공개키 인증서가 인산대수 또는 타원곡선상 이산대수 문제에 기반한다면 Diffie-Hellman 방식의 키 합의를 통해 생성한다.

이용자 발급 본인확인기관은 이용자의 주민번호를 이용하여 PublicInfo 구조체를 만들어 해쉬함수를 입력하여 해쉬값을 획득하고, 해쉬값에 대해 자신의 전자서명용 인증서의 개인키를 이용하여 전자서명을 수행한다.

$$\text{Signature} = D_{PRI_I}(H(\text{PublicInfo}))$$

이용자 발급 본인확인기관이 PublicInfo를 암호화하기 위해 필요한 비밀키(ISP_{SK})를 생성하는 방법은 2가지로 나눌 수 있다. 첫 번째는 본인확인기관간 키분배 프로토콜을 수행하여 암호화용 비밀키를 설정하는 방법과 계약한 본인확인기관의 암호화용 공개키 인증서를 활용하여 암호화용 비밀키를 인증서의 공개키로 암호화하여 전달하는 방법이 있다.

Ⅵ. 중복가입확인정보 생성

인터넷 사이트는 이용자의 중복가입여부를 확인하기 위해 실명확인 과정에서 수집한 주민번호를 사용하고 있었다. 하지만 *i*-PIN을 적용한 인터넷 사이트는 이용자의 주민번호를 수집할 수 없기 때문에 이용자를 유일

하게 식별할 수 있는 정보가 필요하다. 또한 서로 다른 본인확인기관이 이용자에게 발급하는 *i*-PIN 13자리 번호는 본인확인기관정보 2자리를 포함하는 난수 정보이므로 이용자가 서로 다른 본인확인기관을 통해 인터넷 사이트에 회원가입을 하는 경우에 중복가입여부를 *i*-PIN 13자리 번호를 가지고 확인할 수 없다. 따라서 이러한 문제점을 해결하기 위해 이용자가 가입하는 인터넷 사이트 내에서 이용자를 유일하게 식별할 수 있는 중복가입확인정보를 인터넷 사이트에 제공해야 한다.

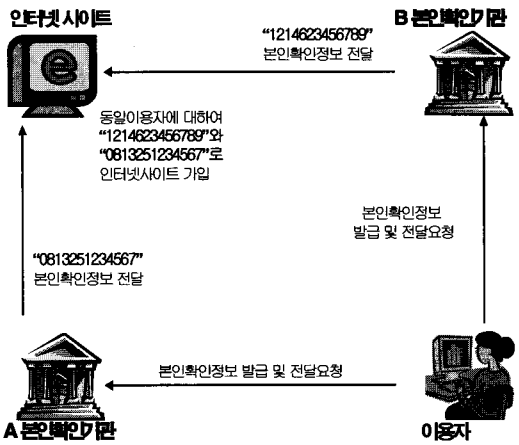
가능한 중복가입 상황은 [표 2]와 같다.

〔표 2〕 중복가입의 종류

분 류	설 명
상황 1	o 인터넷사업자가 2개 이상의 본인확인기관에서 발급하는 본인확인정보를 이용하여 회원가입을 받는 경우
상황 2	o 인터넷사업자가 주민등록번호 또는 본인확인정보를 이용하여 이용자의 회원가입을 받는 경우
상황 3	o 본인확인기관에 보관된 이용자의 개인정보가 삭제된 후 인터넷사업자의 사이트에 재가입 하는 경우

1. 2개 이상의 본인확인기관을 통한 중복가입

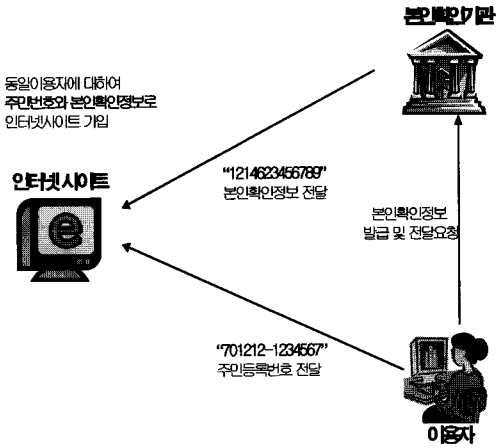
인터넷사업자가 2개 이상의 본인확인기관에서 발급하는 본인확인정보를 이용하여 회원가입을 받는 경우는 [그림 7]과 같다.



〔그림 7〕 2개 이상의 본인확인기관을 통한 중복가입

2. 주민번호와 *i*-PIN을 이용한 중복가입

인터넷사업자가 주민등록번호 또는 본인확인정보를 이용하여 이용자의 회원가입을 받는 경우는 [그림 8]과 같다.



〔그림 8〕 주민번호와 *i*-PIN을 이용한 중복가입

3. *i*-PIN 폐지후 재가입

이용자가 A 본인확인기관으로부터 본인확인정보를 발급받아 인터넷사업자가 운영하는 사이트에 회원가입을 한 후, 본인확인기관에 본인확인정보 폐지 요청을 수행하여 이용자의 개인정보가 본인확인기관에서 삭제된 경우이다.

인터넷 사이트에서는 회원가입하는 이용자의 중복가입확인정보를 본인확인기관으로부터 전달받아 보관하고, 이후에 가입하는 이용자의 중복가입확인정보와 비교하여 중복가입여부를 확인할 수 있다. 또한 1인당 3계정을 허용하는 인터넷 사이트의 경우에도 회원계정 데이터베이스에 동일한 중복가입확인정보의 개수를 더해서 3보다 작으면 계정 생성을 허용하고 3이상 인 경우에는 회원가입을 거절할 수 있다. 중복가입확인정보는 [그림 3]과 같이 생성된다. *i*-PIN은 주민번호로 인터넷 사이트에 가입한 기존 회원에 대한 중복가입확인정보도 본인확인기관에서 일괄 생성하여 제공할 수 있는 유연한 방법이다.

Ⅶ. 결 론

인터넷 사업자는 주민번호를 잘못 관리했을 경우, 회사를 위기로 몰고갈 수 있다는 사실을 최근의 몇 차례 발생한 개인정보 유출 사고를 통해 인식하고 있다.

그러나 아직도 인터넷 사업자나 이용자 모두 편의에 의해 혹은 관습에 의해 주민번호를 무의식적으로 수집·사용하고 있다.

주민번호 유출로 인한 피해를 줄일 수 있는 방법은 이용자와 사업자 모두가 주민번호를 가급적 사용하지 않는 사회 분위기를 만드는 데 있다.

또한 인터넷에서는 *i*-PIN과 같은 대체수단을 적극적으로 활용함으로써 주민번호 수집을 최소화시켜야 한다.

본 고에서는 인터넷 상 주민번호 대체수단 서비스와 관련한 프레임워크, 전달메시지 형식, 중복가입확인정보에 대해 알아보았다.

주민번호가 모든 인터넷 거래의 인프라로 사용되고 있는 현실에서 *i*-PIN이 해결할 수 없는 거래도 있다. 특히 전자결제나 조세신고 등 행정업무 효율화를 위해 사용되는 주민번호의 사용을 규제할 방법은 없다.

결제와 같이 주민번호가 인프라로 사용되는 거래에서도 대체수단을 활용하기 위한 기술적, 제도적 과제가 현재 남아있으나, 주민번호 유출을 줄이면서 기능을 최대한 살릴 수 있는 현재로선 유일한 방법이 대체수단이라 할 수 있다.

참고문헌

[1] TTA, "*i*-PIN 서비스 프레임워크", 정보통신단체표준, TTASKO-12.0054, 2007

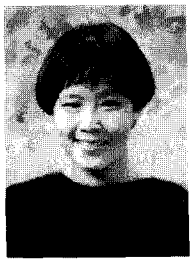
[2] TTA, "본인확인서비스 중복가입확인정보", 정보통신단체표준, , TTASKO-12.0038, 2006

[3] TTA, "*i*-PIN 서비스 전달메시지 형식", 정보통신단체표준, , TTASKO-12.0055, 2007

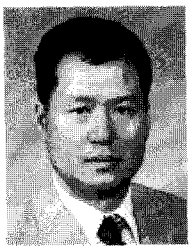
〈著者紹介〉

정 찬 주 (Chan-Joo Chung)
특별회원

1993년~1999년 : 강남대학교 전자계산학과 학사
1999년~2001년 : 성균관대학교 전기전자컴퓨터공학과 석사
2003년~2005년 : 성균관대학교 컴퓨터공학과 박사 수료
2000년 12월~현재 : 한국정보보호진흥원 선임연구원
2005년 3월~현재 : TTA 정보보호 기술위원회(TC5) 개인정보보호 및 ID관리 프로젝트 그룹(PG502) 위원
<관심분야> 암호이론, PKI, 개인정보보호



김 윤 정 (Kim Yoon Jeong)
1991년 : 연세대학교 불어불문과 학사
2002년 : 한국정보통신대학원대학교 경영학 석사
2003 ~ 현재 한국정보보호진흥원 선임연구원
관심분야 : 개인정보보호, 신원관리



김 진 원 (Kim Jin Won)
1988년 : 명지대학교 전자계산학 학사
2003년 : 명지대학교 전자계산학 석사 (전공 :정보보호)
1997년 ~현재 : 한국정보보호진흥원 기술지원팀 팀장
관심분야 : 정보보호

박 광 진(Kwangjin Park)
정회원

1982년 2월 : 동국대학교 전자계산학과 졸업
1988년 2월 : 한양대학교 전자계산전공 석사
1998년 : 광운대학교 컴퓨터과학과 박사과정 수료
1983~1988 : 한국전기통신공사
1988~1996 : 정보통신정책연구원 책임 연구원
1996~현재 : 한국정보보호진흥원 개인정보보호지원센터 센터장