情 報 保 護 學 會 誌
第20卷 第1號, 2010. 2

프라이버시 보호기능을 제공하는 온-오프라인 환경의 새로운 국민식별번호체계 제안

이 형 효*, 박 희 만**, 조 상 래***, 진 승 헌***

요 약

우리나라에서 국민식별번호로 사용되고 있는 주민등록번호는 국민을 유일하게 식별할 수 있는 유일식별성과 그로 인한 국민정보 관리편리성으로 인해 오랜 기간 공공 및 민간부문에서 사용되어 왔다. 특히 정보시스템의 일반화되면서 행정기관이나 민간기업들이 서비스 제공에 필요한 국민 또는 고객의 정보를 관리하면서 식별정보로써 그리고 정보들을 연결하는 연결자로써 널리 사용해 왔다. 비록 지금까지 오랜 기간 주민등록번호가 공공 및 민간분야에서 개인식별번호로 널리 사용되어 왔지만, 최근 발생횟수가 증가되고 사회적, 경제적 피해가 심각해지고 있는 주민등록번호 도용과 그에 따른 프라이버시 침해 문제의 심각성을 고려할 때 새로운 체계의 국민식별번호 및 관련 인프라에 대해 연구가 필요한 시점이다. 따라서 본 고에서는 현재 우리나라의 온라인, 오프라인 환경에서 개인식별번호로서 널리 사용 중인 주민등록번호의 보안 및 프라이버시 관점에서의 문제점을 살펴보고 이를 보완할 수 있는 새로운 국민식별번호체계를 제안한다.

Ⅰ. 서 론

근대적 국가체계에서의 주민등록제도는 신분등록제도와 주거등록제도로 구성되어 있다. 신분등록제도는 민법관계를 분명하게 하기 위한 가족관계 및 출생, 사망의 증명을 위한 제도로서 출생, 혼인, 이혼, 사망을 등록하는데 그 목적이 있다. 주거등록제도에서는 신분등록제도에서 다루는 업무 외에 행정적 통제와 급부 내지 통계의 목적으로 업무를 정의하고 있다. 우리나라는 1962년 주민등록법이 최초로 제정되면서 국민에 대한 거주관계를 파악하고 상시로 인구의 동태를 명확히 하기 위하여, 국민에게 이름, 성별, 생년월일, 주소, 본적을 시·읍·면에 등록하도록 하였다. 그리고 1975년 현재와 같은 13자리 숫자로 구성된 주민등록번호가 개인식별번호로서 도입되어 현재까지 사용되고 있다.

비록 지금까지 오랜 기간 주민등록번호가 공공 및 민간분야에서 개인식별번호로 널리 사용되어 왔지만, 최근 발생횟수가 증가되고 사회적, 경제적 피해가 심각해지고 있는 주민등록번호 도용과 그에 따른 프라이버시 침해 문제의 심각성을 고려할 때 새로운 체계의 국민식별번호 및 관련 인프라에 대해 연구가 필요한 시점이다. 주민등록번호 자체에 개인과 관련된 정보가 필요이상으로 저장되어 있어 개인정보 노출에 매우 취약하고, 출생 때 발급된 주민등록번호는 변경과 재발급이 사실상 불가능하여 한번 유출될 경우 그로 인한 제2, 제3의 피해를 막기 어려운 점이 있다. 개인식별번호로서 갖추어야 할 유일식별성은 주민등록번호가 제공하는 필수적인 특성이지만 재발급이나 변경이 불가능한 제약점으로 인해 프라이버시 침해에 대응하는데 한계가 있을 수밖에 없다.

본 고에서는 현재 우리나라의 공공 및 민간부문의 온라인, 오프라인 환경에서 개인식별번호로서 널리 사용 중인 주민등록번호가 가지고 있는 문제점들을 보안 및 프라이버시 관점에서의 살펴보고 이를 보완할 수 있는 온-오프라인 환경의 새로운 국민식별번호체계를 제안한다.

본 연구는 지식경제부 및 한국산업기술진흥원의 국제공동기술개발사업의 일환으로 수행하였음.
[2007-S-601-03, 자기통제 강화형 전자 ID 지갑 시스템 개발]

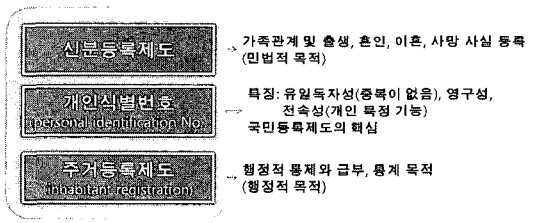
* 원광대학교 정보·전자상거래학부, 정보과학연구소 (hlee@wonkwang.ac.kr)
** 전남대학교 시스템보안연구소 (hareup@lsrc.jnu.ac.kr)
*** 한국전자통신연구원 인증기술연구팀 ({sangrae, jinsh}@etri.re.kr)

Ⅱ. 국내외 국민식별번호체계 현황

2.1 국민식별체계 일반

근대국가의 체계적인 국민등록제도는 신분등록제도와 주거등록제도로 구성되어 있다. 민법관계를 분명하게 하기 위한 가족관계 및 출생, 사망의 증명을 위한 신분등록제도는 기본적인 것으로 출생, 혼인, 이혼, 사망을 등록하는데 그 목적이 있다.

신분등록제도 외에 행정적 통제와 급부 내지 통계의 목적으로 요구하는 주거등록제도(inhabitant registration)가 있다. 이 두 제도는 우리나라나 일본처럼 분리되어 있는 경우도 있고, 서유럽처럼 혼합되어 있는 경우가 있다. 민법적 목적과 행정적 목적이 혼합되어 있거나 보다 상위에 있는 제도를 본 고에서는 국민등록제라는 용어를 이용하여 지칭하며, 국민등록제를 이루고 있는 구성요소는 [그림 1]과 같다.



〔그림 1〕 국민등록제 구성요소

개인식별번호(personal identification number, personal reference number, universal identification number) 제도는 부여대상자 중에 중복되는 것이 없으며(유일독자성), 일생동안 변하지 않고(영구성), 개인을 특정하는데 사용하는(전속성) 것으로 출생등록과 동시에 또는 거주등록을 하거나 국가신분증을 발행하면서 부여하는 것을 말한다. 개인식별번호가 도입되어 있는 나라에서는 국민등록제도의 핵심이라고 할 만큼 중요한 제도이며, 특히 등록정보가 전산처리되는 현실에서 더욱 그러하다.

2.2 국외 국민식별체계 사례

국내외 국민식별체계에 대한 주요 내용과 특징은 참고문헌[1]의 내용을 인용하여 정리하였다.

2.2.1 우리나라 주민등록제도

현행 우리나라 주민등록제도는 1962년 1월 15일 국가재건최고회의에서 만들어졌으면 1가구별 1용지의 기류부에 본적지 이외의 일정한 장소에 30일 이상 주소 또는 거소를 정한 자에게 신고의무를 부과하는 기류법을 제정하였다가, 1962년 5월 10일 기류법을 폐지하고 주민등록법을 제정하였다. 제정 주민등록법은 주민의 거구관계를 파악하고 상시로 인구의 동태를 명확히 하기 위하여, 기류법과 달리 본적지를 떠났는지 여부에 관계없이 모든 대한민국 국민에게 이름, 성별, 생년월일, 주소, 본적을 시·읍·면에 등록하도록 하고, 세대의 전부 또는 일부가 이동할 때에도 퇴거와 전입신고를 하도록 의무화하였다.

주민등록제도의 또 다른 축은 주민등록증 제도와 전국민 개인식별코드인 주민등록번호제도이다. 주민등록증 제도는 제정 주민등록법에서는 도입되지 않았으나, 1968년 5월 29일 주민등록법 제1차 개정 때 도입되었다. 이 개정법에서는 18세 이상의 주민에 대하여 주민등록증을 발급할 수 있다고 하여 발급을 강제하지 않았으나, 1970년 1월 1일 주민등록법 제2차 개정에 의하여, 치안 상 필요한 특별한 경우에 주민등록증을 제시하도록 규정하였다.

초기의 주민등록번호는 2부분으로 구분된 6자리 숫자(모두 12자리)로 이루어졌으나, 1975년 8월 26일 주민등록법 시행령과 동시행령 시행규칙의 개정으로 생년월일, 성별, 지역을 표시하는 13자리의 숫자 체제로 바뀌어 현재에 이르고 있다.

2.2.2 독일

독일은 신분등록에 관하여 신분법, 주거등록에 관하여는 각 주법, 국가신분증에 관하여는 신분증명법에 의해 규율되며, 각각의 제도는 서로 연계되어 있지 않다.

· 신분등록제도

독일의 신분등록제도는 서유럽 국가들과 유사하게 각 교구에서 소속 신자의 이름과 세례날자 등을 기록한 교회부(세례부, 혼인부, 매장부)에서 유래한다. 독일 신분등록제도는 출생을 공증하기 위한 출생부, 혼인을 공증하기 혼인부, 사망을 공증하기 위한 사망부, 친족관계를 증명하기 위한 가족부로 구성되어 있다.

· 국가신분증제도

독일 기본법 제116조 제1항에 의한 독일인은 16세가 되면 신분증을 소지하고 조사할 권한이 있는 행정청의 요구가 있을 경우 제시할 의무가 있다. 신분증에는 성과 이름, 학위, 예명, 출생일과 출생지, 신장, 눈의 색깔, 주소, 국적 등을 기재하고 일련번호를 부여하며, 성과 이름, 학위, 출생일, 일련번호, 유효기간에 관한 사항은 OCR로 자동판독이 가능하다. 위와 같은 내용만 보면 독일의 국가신분증제도는 상당한 침해적이라는 인식을 가질 수 있지만, 신분증명법은 위와 같은 제도가 갖는 침해적 요소를 배제하도록 하는 여러 장치를 마련해 두고 있고, 우리나라의 신분증제도와 근본적으로 다르다.

우선 신분증을 발급할 때 부여하는 일련번호는 새로운 신분증을 발급할 때 새로 부여되며, 일련번호에 인적사항이나 기타 사항을 암시하는 내용을 담을 수 없도록 명시하고 있고, 공적 부분은 물론이고 민간 부분에서도 일련번호를 자료에서 인적사항을 추출하는 것 또는 자료의 결부를 가능하게 하는데 이용할 수 없도록 규정하고 있다.

독일은 연방 차원의 신분등록제도, 국가신분증제도와 지방정부 차원의 주거등록제도를 두고 있으나, 각 제도는 서로 분리되어 관련이 없으며 특히 국가신분증은 엄격하게 독립되어 있다. 위와 같이 각 제도가 분리되어 있기에 당연히 국민에 대한 고유식별번호를 두지 않고 있다.

2.2.3 프랑스

프랑스는 모든 국민에게 개인식별번호를 부여하고 고유식별번호와 함께 중앙정부 소속인 통계와 경제에 관한 국가조사청이 선거인명부의 기능을 겸하는 국민의 신분기록을 보유하고 있으나, 강제적인 주거등록제도를 두고 있지는 않다. 국가조사청을 중심으로 한 프랑스정부는 1973년 개인고유번호를 기초로 각 행정부처가 보유하고 있는 개인정보를 서로 연결하려고 계획하였으나 취소되었고, 1979년에는 컴퓨터로 읽을 수 있는 형태의 개인신분확인카드의 발급을 계획하였으나, 이 계획 역시 시민과 언론의 비판에 부딪혀 중단되었다. 결과적으로 프랑스의 국민등록제도는 신분등록제도만으로 구성되어 있다고 할 수 있다.

프랑스의 신분등록제도는 민법 중 민적증명편에 의해 규율되며, 독일의 경우처럼 교회부에 그 유래를 두고 있으면서 출생, 혼인, 사망이라는 사건을 중심으로 편제하는 사건별 편제방식을 취하고 있다. 출생부의 경우 국적에 관계없이 프랑스 국내에서 출생한 모든 사람에게 신고의무를 부과하고 신고내용으로 출생지, 이름, 출생일, 부모의 이름, 직업, 주소 등을 요구하는 경우도 독일과 유사하며, 혼인부와 사망부도 마찬가지이다. 가족대장에 의해서 혈연관계가 증명된다는 점도 독일과 같으나, 프랑스의 가족대장은 부부의 혼인증서, 자녀의 출생증서 등의 역할을 겸하므로 있다.

2.2.4 일본

· 주거등록제도

일본 호적법은 호적등재인에 대한 주소에 관하여 어떠한 것도 요구하고 있지 않다. 주민기본대장법은 특별구를 포함하는 시정촌(市町村) 주민의 거주관계를 공증하고 선거인명부의 등록과 주민에 관한 기록의 적정한 관리를 도모하며 주민에 관한 기록을 정확하고 통일적으로 정함으로써 주민의 편리함을 증진하고 국가와 지방공공단체의 행정의 합리화에 기여하는 것을 목적으로 하는 것으로 되어 있으나, 오히려 대부분의 행정서비스와 복지서비스가 지방자치단체에 의해서 이루어지는 특성상 주소의 이동에 의해서 변경되는 주민의 지위를 분명히 하기 위한 것이 기본적인 목적인 것으로 보인다. 주민기본대장의 작성책임은 시정촌의 장에게 있다

주민표는 개인을 단위로 하여 세대마다 편성해야 하고, 이름, 출생일, 성별, 세대주, 호적의 표시, 주소, 종전주소, 선거인명부 등재기록, 국민보건보험과 국민연금에 관한 사항 등을 기재한다. 주민은 시정촌내에 주소를 정하거나 동일한 시정촌 구역 내에서 주소를 옮길 경우 14일 이내에 이름, 주소, 전입일 또는 전거일, 종전주소를 시정촌의 장에게 신고해야 하며, 시정촌의 구역 외로 주소를 옮길 때는 전출할 곳과 전출예정일을 신고하여야 한다.

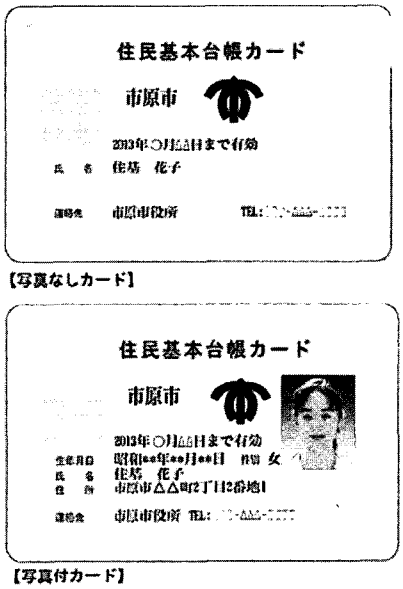
· 주민기본대장 네트워크

일본에서는 주민기본대장 네트워크 시스템(이하 주기네트)이 1994년부터 검토가 시작되었으며, 주민기본대장은 주민의 주거관계를 증명하고, 주거에 관한 사무처리의 기초자료가 된다. 이후 1999년의 개정에 거쳐 2002년 8월부터 시정촌의 구역을 넘어서 전국적 네트

워크화 되었다. 주기네트는 지금까지 각각 지방자치단체단위로 관리되어 온 국민의 주민등록정보를 온라인으로 중앙정부가 일원화 하는 것이다. 주기네트에는 주민의 성명, 주소, 생년월일, 성별 등 정보 외에 사회복지나 세금에 관련된 정보가 부가된다. 그리고 국민 개개인에 11자리의 주민표 코드가 부여된다. 이 코드는 누구와도 중복되지 않는 것으로, 컴퓨터로 무작위로 선택된다.

주기네트 의해 국민이 할 수 있는 것은 주민표 사본의 광역교부, 전입, 전출시 신청의 편리화 등을 들 수 있다. 또, 이 시스템의 도입에 따라 IC칩이 내장된 주민표기본대장카드가 발급된다. 이 카드는 주민표코드를 가진 주민본인의 희망에 따라 교부되며, 보통 IC칩에는 32,000문자를 저장할 수 있는 의 데이터 용량을 가진다.

일본의 주민기본대장카드는 2003년 8월 25일부터 희망자에 한하여 거주지의 시구정촌(市區町村)에서 교부하고 있는데, 2007년도 말(2008년 3월 31일) 현재 전국적으로 234만 장(인구비례 1.8%)이 교부되었다[2]. 주민기본대장카드는 본인의 희망에 따라 사진을 넣을 수도 있고 넣지 않을 수도 있는데, 사진이 포함된 경우에는 성명, 주소, 생년월일, 성별, 교부지방자치단체명, 유효기한(발행일로부터 10년간), 기타 사항 등을 기재하고 있다.



〔그림 2〕 일본 주기카드 샘플

2.2.5 미국

미국은 아주 느슨한 형태의 신분등록제도를 갖고 있으면서도 주거등록제도는 물론이고 개인식별번호도, 국가신분증제도도 없다. 미국에서는 출생기록이 곧 국적기록이 된다. 출생, 사망, 혼인의 사건별로 기록부가 작성되며 개인별로 기록하고 가족관계는 기록하지 않으므로, 철저하게 사건별, 개인별 기록제도로 유지된다. 각 기록 간에 연결요소도 없으므로 개인신분사항을 한 번에 알아볼 수 없어 누군가 사망하여 상속이 시작되어, 그 자녀가 몇 명이고 상속인인지 여부를 확인하려면 각각에 대한 출생증명서를 일일이 확인하는 수밖에 없다.

이처럼 허술한 등록제도를 유지하고 있는 미국이지만, 가장 엄격한 국민등록제도를 유지하고 있는 스웨덴 등 북구제국과 가장 유사한 제도를 갖고 있다는 지적이 가능한 이유는 사회보장번호때문이다. 미국의 사회보장제도와 사회보장번호는 미국에서 생활하는 데 필수적이므로 결과적으로 강제적인 주민등록과 개인식별번호를 부여하는 것과 동일한 효과를 주고 있다. 사회보장번호는 상당한 수의 18세미만의 거주자와 거의 모든 성인에게 부여되어 있다는 점에서 더욱 그러하다.

사회보장번호(SSN: Social Security Number)는 1935년의 사회보장법에 의해 도입되었으며, 미국의 사회보장은 고용주, 피고용자와 정부사이의 사회보험으로 피고용자가 은퇴, 불구의 사고를 당하거나 유가족이 있을 경우 및 의료혜택을 받기 위한 일종의 국민연금 및 보험의 복합형태의 것이다. 미국시민권자와 영주권자는 물론 합법적인 외국인 거주자도 발급받을 수 있는 사회보장번호는 9자리의 숫자 3부분으로 구성되어 있고, 첫 번째 세 자리 수는 신청지역, 중간 두 자리 수는 발급그룹 마지막 4자리 수는 발급순서를 나타내며, 범죄에 이용되는 등 특별한 사정이 없는 한 평생동안 사용하도록 되어 있다. 사회보장번호는 처음에는 사회보장제도에만 사용되었으나, 1961년 국세청이 사회보장번호를 납세자번호로 사용한 이래, 운전면허증의 취득, 은행거래, 외국인등록, 학생등록 등과 같이 공공부분은 물론이고 민간부분에서도 광범위하게 사용되고 있다.

2.3 인터넷 개인식별번호

우리나라의 경우 인터넷상에서 회원 가입 시 주민등

록번호 입력이 일반화되어 있으며, 입력된 주민등록번호는 실명확인, 성인인증 등 다수 용도로 광범위하게 사용되고 있다. 주민등록번호는 전 국민에게 발급되고 개인 식별성이 뛰어나, 사업자들이 고객DB 관리 · 제휴마케팅 등 주민등록번호를 폭넓게 활용되고 있는 것이 현실이나 주민등록번호 유출로 인해 금융사기, 계정도용 등 이용자에게 심각한 피해가 발생되고 있는 문제점이 있다. 주민등록번호는 변경 · 갱신이 어렵고 인터넷을 통해 무한 복제될 수 있어 침해가 지속적이고 광범위하게 발생할 가능성이 높으며 주민등록번호에는 다양한 개인정보가 포함되어 있어 개인 프라이버시 침해 우려도 크다는 지적이 오래 전부터 제기되어 왔다. 참고로 주민등록번호에는 생년월일 외에도 성별, 출생지 지역코드 및 해당지역 접수번호, 검증코드가 포함되어 있다.

또한, 이미 주민등록번호를 포함한 개인정보 침해사고가 다수 발생하여, 앞으로 주민등록번호가 안전한 본인인증수단의 역할을 하기 어려움도 존재한다. 주민등록번호를 포함한 주요 개인정보 유출사고로는 2006년 2월 주민등록번호 도용으로 인한 1,200만 여개의 게임 계정 대량 생성, 2008년 2월 옥션 사이트 해킹으로 고객정보 1,081만 건 대량 유출, 2008년 8월 중국인 해커에 의해 주민등록번호가 포함된 900만 건의 개인정보 유출, 2008년 9월 GS칼텍스 내부직원에 의한 1,110만 명의 고객정보 유출 사건 등이 있다.

이와 같은 주민등록번호 유출로 인한 명의도용 등 지속적으로 발생하는 개인정보 침해 문제 해결을 위해 언제든지 변경 가능할 수 있는 개인식별체계의 도입이 필요하게 되었다. 미국, 일본 등 대부분 국가는 변경 가능한 개인식별번호를 발급하며, 중국을 제외하고는 인터넷상에서 개인식별번호의 사용을 금지하고 있다.

그러나 현재 i-PIN은 사업자의 서비스가 i-PIN 도입으로 일부 기능 제한되는 점, 온라인 상에서 i-PIN을 통해 가입한 회원은 오프라인 상에서 본인확인이 어려워 서비스를 제공받기 어려운 점, 본인확인기관이 수집한 개인정보에 대한 안전한 관리 및 i-PIN 서비스의 안정적인 제공에 대한 법제도적 관리 근거 미약한 점, 그리고 이용자의 경우 i-PIN 이용이 주민등록번호에 비해 불편하다는 점 등이 i-PIN 활성화에 걸림돌로 지적되고 있다.

이에 따라 방송통신위원회는 인터넷 상에서 주민등록번호를 완전히 대체하기 위해 i-PIN 활성화 종합대책을 마련하였다[5]. 이 종합대책에 따르면, 1단계('09~11년)에서는 기존 i-PIN의 문제점을 개선하고 보급을 촉진하여 i-PIN의 이용을 확산하기 위한 기반을 조성하고, 2단계('12~13년)는 조세·금융을 제외한 민간분야, 3단계('14~15년)는 모든 민간분야로 i-PIN 도입을 점진적으로 확대하는 것을 추진할 예정이다[3,4].

〔표 1〕 국외 개인식별번호 이용 현황

구 분		미국	독일	일본	중국
개인식별번호	존재 유무	사회보장번호 (SSN)	없음 (출생, 사망 등 기록을 위한 신분등록제는 존재)	주민표 번호	신분증 번호
	변경 가능	가능		가능	가능
인터넷이용시 신원 확인		하지 않음	하지 않음	하지 않음	일부의 경우 신분증번호 요구

Ⅲ. 국민식별번호체계 요구사항

3.1 주민등록번호의 보안 취약점

2장에서 살펴본 바와 같이 현재 우리나라에서 국민식별번호로 사용되고 있는 주민등록번호는 국민을 유일하게 식별할 수 있는 유일식별성과 그로 인한 편리성으로 인해 오랜 기간 공공 및 민간부문에서 사용되어 왔다. 특히 정보시스템이 일반화되면서 행정기관이나 민간기업들이 서비스 제공에 필요한 국민 또는 가입자의 정보를 관리하면서 식별정보로써 그리고 관련된 정보들을 연결하는 연결자로써 주민등록번호를 널리 사용해 왔다.

그러나 주민등록번호의 유일식별성, 이용 및 관리 편리성 장점 이면에 주민등록번호의 도용에 대한 취약성과 도용된 주민등록번호에 대한 통제불가능 문제가 최근 매우 심각해지고 있다. 온라인 환경의 경우 많은 가입자들을 확보하고 있는 게임 사이트, 포털 사이트, 전자상거래 사이트 등에서 타인의 주민등록번호를 불법적으로 이용하여 회원으로 가입하거나 게임 아이템 및 물품을 거래하는 빈번히 발생하고 있다. 이는 주민등록번호가 가지고 있는 취약점들에 기인하고 있으며 각 취약점과 그에 대한 보완방안을 기술하면 [그림 3]과 같다.

〔그림 3〕 현 주민등록번호 보안 취약성 및 보완방안

3.1.1 필요이상의 정보 포함

주민등록번호에는 13자리 숫자 내에 생년월일, 성별, 출생지역 등에 대한 정보가 포함되어 있어 국민을 유일하게 식별하는 기능이 있지만 그 반면에 필요이상으로 많은 정보가 포함되어 있는 문제점이 있다. 따라서 국민 개인에 대한 구별을 위한 일련번호와 같이 최소한의 정보만 국민식별번호에 포함되는 것이 바람직하다. 우리나라의 i-PIN, 미국의 SSN이나 일본의 주기표번호 등이 최소정보가 포함된 국민식별번호의 사례로 들 수 있다.

3.1.2 취약한 위조검증 체계

우리나라의 주민등록번호는 맨 마지막 숫자 하나가 주민등록번호의 오류점검을 위한 검증코드로 사용되므로, 주어진 주민등록번호가 올바른 것인지 그렇지 않은 것인지 주민등록번호 숫자만을 이용하여 확인이 가능하다. 따라서 주민등록번호 검증규칙을 이용하여 악의적 목적으로 주민등록번호를 생성하면, 해당 검증코드 점검규칙에 따라 검증할 경우 올바른 주민등록번호로 검증되게 된다. 이는 주민등록번호가 자체적으로 검증이 되도록 이용하는 오류검증코드 규칙이 공개된 이유이며 이로 인해 발생되는 문제를 예방하기 위해서는 오류검증코드 생성규칙을 비밀로 하거나 제3의 신뢰기관에서 식별번호에 대한 검증기능을 수행하는 방법 등이 있을 수 있다.

오류검증코드 점검규칙을 비밀로 하는 접근방식은 해당 점검규칙이 노출될 경우 우리나라 주민등록번호 경우와 같이 자체검증이 가능하다는 문제점을 가지게 되므로, 국민식별번호에 대한 검증기능을 신뢰할 수 있는 제3의 기관이 수행하는 방식이 적절하다. 이런 방식을 채택할 경우 신뢰된 제3기관은 국민식별번호 관리정보 등을 활용하여 해당 국민식별번호가 정당한 번호인지를 검증하는 기능을 수행하게 된다.

3.1.3 영구성(불변성)

우리나라 주민등록번호는 출생신고 시 한 번 부여받으면 수정되거나 재부여 받기 매우 어려운 특징을 가지고 있다. 비록 주민등록법 및 동법 시행령에 법 제14조에 따라 주민등록사항을 정정한 결과 주민등록번호를 정정하여야 하는 경우, 주민으로부터 주민등록번호 오류의 정정신청을 받은 경우, 주민등록번호에 오류가 있음을 발견한 경우에 한정하여 지정된 서식에 의해 주민등록번호 정정 요구를 할 수 있도록 규정되어 있으나, 매우 제한적으로 이루어지고 있는 실정이다. 옥션과 하나로텔레콤에서 발생한 대규모 개인정보 유출사태 피해자들이 해커에 의해 불법적으로 유출된 주민등록번호의 제2, 제3의 추가 피해를 우려하면서 주민등록번호 조합방식을 바꾸어 원하는 사람들에게 변경, 발급될 수 있도록 하는 제도 도입을 촉구한 사례도 있다[8].

만일 국민식별번호 변경이나 재발급을 허용하는 경우 고려되어야 할 사항은 동일한 국민에 대해 기 발급된 국민식별번호와 새로 발급받은 국민식별번호 간 연관성을 관리할 필요성이다. 국민식별번호가 변경되었다 하더라도 해당 사용자의 이력정보 관리나 통계처리, 디지털 포렌식 과정 등에서 서로 다른 국민식별번호이지만 한 사용자에 배정한 번호임을 확인할 필요가 있기 때문이다.

또한 서비스 특성에 따라 일회용 국민식별번호를 사용할 경우도 고려되어야 한다. 한 사용자에 대해 변하지 않는 식별번호를 사용하는 대신 서비스에 따라 일회용 국민식별번호를 이용하고 즉시 또는 나중에 해당 국민식별번호를 검증할 수 있는 기능도 필요하다.

3.1.4 유일식별성

유일식별성이란 주어진 식별번호에 의해 오직 단 한 명의 사용자가 식별되는 성질을 의미한다. 우리나라 주민등록번호는 국가기관에 의해 출생신고 시 중복없이 부여되고 관리되므로 유일식별성을 만족하고 있다. 유일식별성은 사용자나 국민에 대한 정보관리 측면에서는 매우 편리하면서 효과적인 특성이지만 해당 식별번호와 연결된 사용자나 국민에 대한 정보를 손쉽게 파악하고

추적할 수 있어 프라이버시 침해 위협이 존재한다.

따라서 국민식별번호를 이용하는 기관이나 서비스 사이트가 사용자나 국민을 유일하게 식별하지만 해당 사용자가 정확히 누구를 가리키는 지 은닉할 수 있는 익명성이 요구될 수 있다. 익명성은 은닉서명(blind signature) 기법 등을 이용하여 구현될 수 있다. 그러나 이러한 익명성은 법률 등에서 엄격히 규정된 경우에 한하여 제거될 수 있어야 하며 익명성 제거는 소유자 추적(owner tracing) 기술을 이용하여 이루어질 수 있다.

3.1.5 본인확인기능 미비

주민등록번호는 번호자체에 대한 유효성 검사가 쉽게 이루어질 수 있기 때문에 초기 정보시스템이나 온라인 사이트에서 주민등록번호의 검증만 거친 후 회원가입이나 서비스 제공 등이 이루어졌다. 그러나 불법적인 주민등록번호 생성기 등에 의한 위조 주민등록번호로 인한 문제가 증가하면서 실명인증 서비스가 이용되기 시작하였다. 비록 인터넷 상에서 개인의 주민등록번호와 성명의 실제 존재 및 일치 여부를 확인해 주는 실명인증 서비스가 있지만 이는 단순히 주민등록번호와 이름 간 일치여부만을 확인해 줄뿐 해당 주민등록번호의 실제 소유자인지를 검증하는 본인확인기능은 제공하지 못한다. 따라서 주민등록번호의 이러한 단점을 보완하기 위해 현재 공인인증서, 휴대폰인증 등을 이용한 본인확인 절차가 이용되고 있다.

한편 i-PIN의 경우 13자리 숫자 중에서 i-PIN 발급기관에 대한 식별정보가 i-PIN 번호의 몇 번째에 위치하는지에 대해서만 결정되어 있을 뿐 주어진 i-PIN 정보가 정확한 것인지를 i-PIN 번호만을 이용하여 검증하는 것은 불가능하다. i-PIN의 경우 자신이 발급받은 i-PIN 서비스 제공기관에 접속하여 발급과정에서 사용자가 설정한 ID와 비밀번호 등을 입력함으로써 본인확인절차를 거치게 된다.

3.1.6 모든 서비스 영역대상 이용

우리나라의 경우 국가 및 공공기관뿐만 아니라 기업, 민간기구 등에서 개인 또는 사용자의 식별자로서 대부분 주민등록번호를 이용하고 있다. 이는 국민들이 자신의 주민등록번호를 암기하고 있어 언제든 이용이 가능하며 주민등록번호가 한 명의 국민을 유일하게 식별할 수 있고 그 정보가 출생부터 사망 때까지 변하지 않으므로 거의 모든 기관에서 주민등록번호를 관행적으로 식별자로 활용했기 때문이다. 그러나 이로 인해 한 번 유출된 주민등록번호는 공공 및 민간기관에서 도용될 수 있는 위험성에 노출되어 있으며, 재발급이나 변경이 매우 제한적인 특성으로 인해 침해를 받은 프라이버시를 복구할 수 없는 어려움이 따르게 된다.

따라서 실생활에서 서비스 제공기관의 공공성 여부나 서비스 중요도, 주민등록번호가 해당 서비스 제공을 위해 필수적인지 사전에 분석하여 그에 따라 주민등록번호를 수집하거나 저장, 활용할 수 있도록 하는 제도적, 관리적 방안을 연구해야 한다. 주민등록번호가 필수적으로 필요하지 않은 부문이나 서비스에서는 주민등록번호의 수집과 활용을 법률 또는 기관별 규정을 통해 엄격히 제한해야 하고 주민등록번호를 대신하여 다른 정보를 식별정보로 이용하도록 하는 방안도 연구되어야 한다.

3.1.7 개인정보 간 연결자로써 과도한 이용

대부분의 공공기관 및 민간기관 등에서 사용자 정보를 관리할 때 현재까지 주민등록번호가 사용자의 식별정보로 이용되고 있는 현실이다. 서비스를 제공하는 기관마다 수집, 저장, 활용하고 있는 개인정보 종류가 서로 다르지만, 이러한 정보를 서로 연결시킬 수 있는 연결정보로서 가장 널리 이용되는 것이 주민등록번호이다. 따라서 주민등록번호를 키로 하여 여러 종류의 정보를 연계하면 한 사용자에 대한 거의 모든 정보를 통합할 수 있는 장점과 함께 심각한 프라이버시 침해요소로서 악용될 위협이 된다.

그러므로 각 기관이 관리하고 있는 개인정보를 주민등록번호를 통해 통합하는 행위를 법률 등을 통해 엄격히 제한해야 하며 필요한 경우 개인정보 소유자로부터 사전 동의를 얻도록 하는 절차도 마련되어야 한다. 또한 개인정보를 저장, 관리, 활용하고 있는 기관 간 개인정보 연결이 필요할 때 가명(pseudonym)을 이용하여 주민등록번호가 연결자로써 과도하게 사용되지 않도록 제한하여야 한다.

3.2 새로운 국민식별번호체계 인프라

본 고에서 제안하는 국민식별번호체계 지원 인프라는 다음과 같이 기본적인 운영 및 관리환경을 가정하고 있으며, 각 가정사항은 다음과 같다.

3.2.1 국민식별번호 형태

본 고에서 가정하고 있는 국민식별번호는 현재 사용중인 주민등록번호와 같이 사용자들이 인식하고 암기할 수 있는 제한된 길이의 숫자 형태와는 동일하지 않다. 현재 사용 중인 공인인증서에 포함된 공개키 정보가 사용자에 대한 유일한 식별번호로서의 기능을 가지고 있지만 사용자가 해당 정보의 구조와 내용을 암기하지 않더라도 사용하는 것처럼 본 고에서 제안하는 새로운 국민식별체계 내 국민식별번호 역시 주민등록번호와의 구조적 유사성을 가정하고 있지 않다.

3.2.2 본인확인기관과 국민식별번호발급기관 분리

본인확인기관은 국민식별번호를 발급받으려는 사용자가 본인이 맞는지 확인하는 기능을 수행한다. 본인확인 수단으로는 대면확인을 포함하여 공인인증서, i-PIN, 휴대폰인증 등의 방법이 활용될 수 있다. 일반적으로 본인확인기관은 국가기관을 포함하여 국가기관이 설정한 기술적, 관리적 기준을 충족하여 인증받은 신뢰된 기관이 될 수 있다. 따라서 본인확인기관은 사용자 본인확인과 관련된 기본정보를 보유하거나 이용할 수 있어야 하며 본인확인에 필요한 기술적, 운영적, 관리적 요건을 만족해야 한다.

국민식별번호발급기관은 신뢰된 본인확인기관으로 본인확인과정을 마친 사용자에 한해 국민식별번호를 발급하고, 관리하는 역할을 담당한다. 국민식별번호발급기관은 본인확인을 완료한 사용자에 대해 국민식별번호를 발급하고 해당 발급정보를 관리하게 된다. 발급된 국민식별번호는 발급기관의 전자서명 등을 통해 출처인증과 무결성을 검증함으로써 주민등록번호 자체검증 기능보다 보안이 강화된 검증이 가능하도록 한다.

이와 같이 본인확인기관과 국민식별번호발급기관을 분리하여 운영하는 이유는 한 기관에서 두 개의 기능을 동시에 수행할 경우 내부자 또는 외부 공격자에 의한 공격에 의해 사용자의 익명성이 손상될 수 있을 뿐만 아니라 국민식별번호 발급과 검증 기능이 집중되어 있어 시스템 장애로 인해 전체 서비스가 중지될 수 있는 위험성이 존재하기 때문이다. 따라서 본 고에서는 본인확인과 국민식별번호 관리기능 간 임무분리원칙을 적용하고 국민식별번호 발급 및 관리정보의 안전한 관리를 위해 두 기관을 분리, 운영하는 구조를 채택하였다.

3.2.3 서비스 영역별 본인확인기관과 국민식별번호발급기관 분리

현재 주민등록번호는 공공 및 민간영역에서 전 국민을 유일하게 식별할 수 있는 식별번호로서 활용되고 있으며, 영역 간 개인정보를 결합할 때 연결자로서의 기능도 제공하고 있다. 이러한 주민등록번호의 특징은 정보운영 및 관리 관점에서는 유용한 기능이지만 정당한 관리자에 악의적 목적이나 외부 침입자에 의해 개인정보의 무차별 결합으로 인한 프라이버시 침해와 도용된 주민등록번호를 이용한 제2, 제3의 프라이버시 침해 문제가 발생될 수 있는 원인이 된다.

따라서 본 고에서는 크게 공공영역과 민간영역에서 사용되는 국민식별번호를 별도로 발급, 활용하게 하고 필요하다면 각 영역의 서비스별, 중요도별로 국민식별번호를 이용할 수 있는 구조를 고려하고 있다. 물론 한 사용자에게 여러 개의 국민식별번호를 부여하고 관리하는 업무가 복잡할 수 있는 문제는 있으나, 본 고에서 제안하는 지원인프라가 영역별, 서비스별로 국민식별번호를 발급, 관리하고 검증하는 체계를 지원함으로써 향후 제안하는 인프라가 실제 적용될 경우 기능확장성이나 융통성이나 확보하기 위함이다.

3.2.4 국민식별번호발급기관과 서비스 제공사이트 간 사전 신뢰관계 설정

본인확인을 거쳐 국민식별번호발급기관에 의해 사용자에게 발급된 국민식별번호는 사용자가 온라인, 오프라인 환경에서 회원가입이나 서비스 신청 등 다양한 분야에서 개인식별정보로 이용될 수 있다. 이 과정에서 사용자로부터 국민식별정보를 제공받아 서비스를 제공하는 사이트들은 국민식별번호가 관련 기관들에 의해 정당하게 발급된 것인지, 국민식별번호를 제공한 사용자

가 해당 식별번호의 실제 소유주인지 확인하는 작업을 수행하게 된다.

이 과정에서 공개키 기반구조(PKI: Public Key Infrastructure)의 인증기관을 신뢰하고 사용하는 것처럼 국민식별번호발급기관을 모든 서비스 제공사이트가 신뢰한다는 가정이 필요하다. PKI 환경에서 전자서명 검증을 통해 다양한 보안서비스가 제공된 것과 같이 국민식별번호발급기관과 서비스 제공사이트가 사전에 설정된 신뢰관계를 바탕으로 전자서명 검증과 같은 절차를 거쳐 국민식별번호에 대한 검증과 본인확인 서비스를 제공할 수 있게 된다.

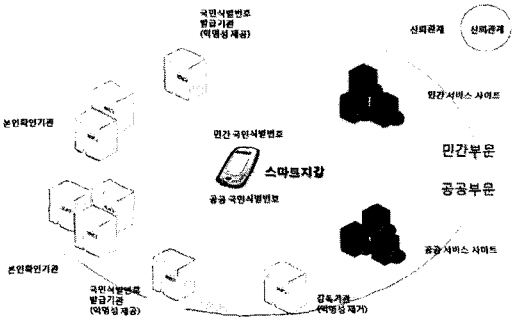
주어진 국민식별번호가 정당한 절차를 거쳐 신뢰된 국민식별번호발급기관에 의해 발급되었는지 확인하는 과정은 국민식별번호에 포함된 국민식별번호발급기관의 전자서명을 검증함으로써 이루어지며, 국민식별번호를 제출한 사용자가 해당 국민식별번호의 정당한 소유자인지를 점검하는 과정은 사용자로부터 본인확인에 필요한 추가정보를 전달받아 국민식별번호발급기관에 의해 수행된다. 단, 이 과정에서 국민식별번호발급기관은 비록 본인확인기능을 수행하지만 검증되는 국민식별번호의 실제 소유자가 누구인지 신원을 확인하지 못하는 익명성이 보장되어야 한다. 서비스 제공사이트의 경우 제공하는 서비스의 특성에 따라 사용자 이름이 필요하지 않는 서비스의 경우 사용자로부터 입력받은 본인확인에 필요한 추가정보를 국민식별번호발급기관이 처리할 수 있다. 이 때 사용되는 추가정보는 사용자에 의해 입력된 정보가 해쉬함수와 같이 원래의 형태로 복원될 수 없도록 처리되어 서비스 제공사이트와 국민식별번호발급기관에 전달되므로 사용자의 신원이 서비스 제공사이트나 국민식별번호발급기관에 의해 노출되지 않도록 하여 익명성을 보장한다. 그러나 법률 등에 의해 규정된 바에 따라 사용자의 익명성을 제거할 수 있는 기술적, 제도적 지원체계도 고려되어야 한다.

3.2.5 온라인, 오프라인 환경 지원

현재 사용 중인 주민등록번호의 또 다른 문제점 중의 하나는 온라인과 오프라인 환경에서 동일한 정보인 국민식별번호인 주민등록번호가 이용되고 있고, 오프라인 환경에서 출력물 형태의 양식에 기입된 주민등록번호가 악의적인 사용자에 의해 당초 목적 외 다른 이용목적으로 주민등록번호 소유자의 동의를 얻거나 통보되지 않고 반복하여 사용될 수 있다는 점이다. 따라서 사용자 식별정보를 미리 허가되지 않는 상황에서 불법적으로 반복 사용되는 것을 탐지하고 차단할 수 있는 방법의 도입이 필수적이다.

새로운 국민식별번호체계 중 오프라인 환경에서 고려되어야 할 또 다른 사항은 사용 편리성이다. 온라인 환경에서는 전자인증서와 같은 형태로 국민식별번호를 설계하고 비록 사용자들이 새로운 국민식별번호의 구조에 대해 정확히 파악하지 못하더라도 이용할 수 있지만, 오프라인 환경에서는 출력물 형태의 양식에 기록하기 적합해야 하고 사용하기 적절한 길이 및 형태를 가져야 한다. 예를 들어 비록 온라인 환경의 국민식별번호가 전자인증서와 같은 디지털 정보 형태로 저장, 관리되는 반면, 오프라인 환경에서는 현재 사용 중인 주민등록번호와 같은 형태의 숫자 13자리 또는 16진수 형태의 10여 자리 내외의 오프라인 환경의 국민식별번호가 요구하며, 동일한 사용자의 온라인 국민식별번호와 오프라인 국민식별번호는 국민식별번호 발급기관에 의해 연계되어 있어야 한다.

[그림 4]는 이상에서 살펴 본 국민식별번호체계 특성 지원을 위한 인프라를 나타내고 있다. [그림 4] 구성요소 중 스마트지갑은 사용자의 식별번호(온라인, 오프라인용)를 포함하여 인증정보 등 개인정보를 저장, 관리, 처리할 수 있는 기능을 가지고 있는 무선통신기능을 제공하는 휴대가능한 단말기를 가정하고 있다.



[그림 4] 국민식별번호체계 지원 인프라 구성요소

Ⅳ. 온라인, 오프라인 환경의 지원 인프라

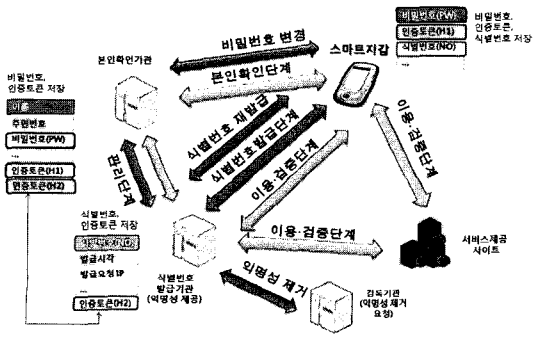
4.1 온라인 환경의 지원 인프라

온라인 환경의 국민식별번호체계 지원 인프라는 각 구성요소들이 유무선 통신을 통해 연결된 상태를 가정하고 있으며, 이 때 사용되는 온라인 국민식별번호는 현재 주민등록번호 구조와는 다른 전자인증서와 같은 디지털정보 형태를 가지고 있다. 이와 같은 형태의 온라인 국민식별번호의 특징은 식별번호의 가독성(readability) 보다는 최소정보 포함성, 익명성, 신뢰도 높은 위조검증 기능, 식별번호 재발급, 소유자 검증 기능 등을 제공하기 위함이다.

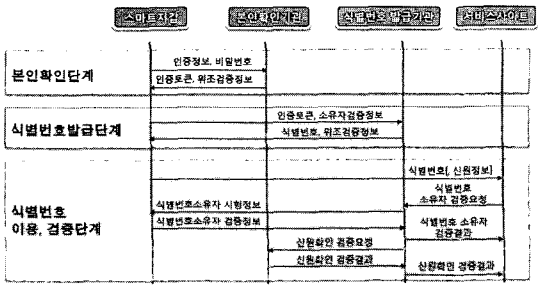
온라인 환경의 지원 인프라에서 구성요소 간 전달되는 정보는 안전한 채널을 통해 비밀성과 무결성이 보장된다고 가정한다.

4.1.1 동작단계

[그림 5]는 온라인 환경의 국민식별번호체계 동작단계를 개략적으로 나타내고 있다. 전체적인 동작단계는 스마트지갑 소유자가 본인확인기관에 먼저 접속하여 인증과정을 수행하는 본인확인단계, 본인환인단계에서 본인확인기관이 발급한 인증토큰을 제시하고 국민식별번호 발급기관으로부터 온라인 국민식별번호를 발급받는 식별번호 발급단계, 발급된 식별번호를 서비스 제공사이트에게 제시하고 제시된 온라인 식별번호가 정당하게 발급된 식별번호인지를 국민식별번호 발급기관에게 확인하는 이용 및 검증단계, 식별번호 재발급이나 스마트지갑 소유자의 비밀번호 변경, 익명성 제거 기능을 수행



〔그림 5〕 온라인 환경의 식별번호체계 동작 단계



〔그림 6〕 온라인 환경의 국민식별번호 관리체계 동작절차

하는 관리단계로 이루어져 있다.

[그림 6]은 온라인 환경에서 국민식별번호 발급과 이용을 위해 필요한 본인확인단계, 식별번호 발급단계 그리고 이용 및 검증단계별로 각 구성요소 간 연동절차 및 전달되는 정보의 종류를 개략적으로 나타내고 있다.

본인확인단계에서 사용자가 본인확인기관에게 자신의 신분을 증명하기 위해 인증정보, 비밀번호(PW)를 보내면, 본인확인기관은 2개의 인증토큰 H_1, H_2를 생성한다. H_1은 사용자와 본인확인기관만이 알고 있고 사용자의 신원을 확인할 수 있는 정보를 해쉬한 값으로 두 구성요소만이 계산해 낼 수 있는 인증토큰이다. 그리고 H_2는 H_1값에 비밀번호를 연결한 정보를 해쉬한 값으로 H_1 인증토큰을 재계산하지 않고 사용자 비밀번호 변경할 수 있도록 사용되는 인증토큰이다.

식별번호발급단계에서 식별번호발급기관은 사용자가 직접 계산하여 전달하는 인증토큰과 본인확인기관이 생성하여 사용자를 통해 전달하는 인증토큰을 비교함으로써 사용자가 정당한 본인확인과정을 통과하였음을 확인한 후 온라인 식별번호를 발급하게 된다. 본인확인기관은 사용자를 통해 전달하는 인증토큰은 식별번호발급기관만이 복호화할 수 있도록 처리되어 전달된다. 이 단계에서 발급된 식별번호는 사용자에게만 전달될 뿐 본인확인기관에는 전달되지 않으므로 본인확인기관은 주어진 식별번호만을 이용하여 어떤 사용자인지를 확인할 수 없게 되므로 사용자의 프라이버시가 보장되게 된다.

식별번호 이용 및 검증단계에서 사용자가 서비스 제공사이트로 접속한 후 식별번호를 제공하면 서비스 제공사이트는 식별번호발급기관에게 해당 식별번호를 제시한 사용자가 식별번호의 실제 소유자인지 검증을 요청하게 된다. 식별번호발급기관은 식별번호를 제시한 사용자에게 시험정보(challenge)를 보내고 사용자가 회신한 결과값(response)을 자신이 계산한 값과 비교함으

로써 사용자가 식별번호의 실제 소유자인지를 검증하게 된다. 이 과정에서 식별번호발급기관은 본인확인기관으로 전달받은 H_2 인증토큰을 이용하는데 H_2와 시험정보를 연결하여 해쉬한 값을 사용자가 정확히 계산하여 회신하는지를 비교하게 된다.

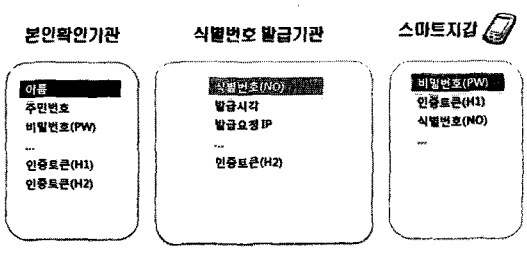
그리고 이 과정에서 본인확인이 필요한 경우 사용자가 입력한 신원정보를 본인확인기관만이 복호할 수 있도록 처리하여 전달하게 된다. 이렇게 함으로써 식별번호발급기관은 사용자 신원정보를 알 수 없게 되므로 사용자의 프라이버시를 보장할 수 있게 된다.

만일 식별번호 소유자의 신원정보를 확인하는 익명성 제거과정을 수행하려면 해당 상황이 법률 또는 이에 준하는 규정의 의해 정의되어 있어야 하며, 식별번호 소유자의 신원확인을 요청하는 지정된 감독기관의 요청이 선행되어야 한다. 감독기관은 식별번호발급기관에게 신원확인을 위한 식별번호를 전달하게 되며 식별번호발급기관은 자신이 저장, 관리하고 있는 정보 중 전달된 식별번호와 연관되어 있는 인증토큰 H_2를 본인확인기관으로 다시 전달한다. 본인확인기관은 전달된 인증토큰 H_2를 검색하여 해당 사용자의 신원정보를 감독기관으로 전송하게 된다.

4.1.2 관리정보 간 관계

[그림 7]은 온라인 환경에서 본인확인기관, 식별번호 발급기관, 스마트지갑이 저장, 관리하고 있는 정보 및 해당 정보 간 연관성을 나타내고 있다. 본인확인기관이 주민등록번호를 저장하고 있는 이유는 본인확인단계에서 인증수단으로 주민등록번호를 사용할 때를 가정한 것이며, 인증수단으로 다른 정보가 이용된다면 해당 정보를 본인확인기관이 저장하게 된다.

본인확인기관은 온라인 식별번호(NO)를 저장, 관리하고 있지 않고 식별번호 발급기관은 스마트지갑 소유자에 대한 신원정보를 관리하고 있지 않으므로 어느 하나의 기관에서 스마트지갑 소유자의 신원정보 확인과 온라인 식별번호를 이용한 이용내역 등을 동시에 조회하거나 통제할 수 없는 특징을 제공하고 있다.



[그림 7] 식별번호 관리기관별 주요 관리정보 구조

4.2 오프라인 환경의 지원 인프라

4.2.1 동작단계

오프라인 환경에서 국민식별번호 이용방법은 온라인 환경과 몇 가지 다른 점이 있다. 온라인 환경이란 서비스 제공사이트와 스마트지갑 간에 상시 연결된 안전한 무선통신기술을 이용하여 실시간으로 식별번호 검증 및 본인확인을 위한 추가정보가 전송되는 환경을 의미한다. 그리고 스마트지갑, 서비스 제공사이트 간 전달되는 온라인 식별번호는 현재 사용 중인 주민등록번호와는 구조적, 기능적 측면에서 서로 다르고, 전자인증서와 같이 사용자의 가독성보다는 식별정보의 안정성, 검증 가능성에 중점을 두고 있는 특징이 있다.

따라서 온라인 식별번호는 국민식별번호체계를 관리하는 데이터베이스의 키로 사용되거나 전자서명 검증 등을 수행하는데 적합한 형태를 취하고 있어야 하며, 출력물 양식에 필기도구를 이용하여 기입하는 데 적합하지 않는 구조를 가지고 있다.

한편, 오프라인 환경에서는 사용자가 오프라인 서비스 제공자가 제공하는 회원 가입 및 서비스 신청서 양식에 국민식별번호를 필기도구를 이용하여 기입하고 추후 해당 국민식별번호를 온라인으로 검증하는 과정을 거치게 된다. 그러나 이 때 스마트지갑에 저장된 국민식별번호를 사용자가 출력된 양식에 기록하는 것은 적절하지 않으므로 출력된 양식에 기록하기 적합한 형태를 가지는 오프라인 환경용 국민식별번호가 필요하게 된다. 이러한 오프라인 국민식별번호는 사용자가 이용하기 쉽도록 주민등록번호와 같이 비교적 짧은 길이를 가지는 숫자 또는 문자로 구성되어야 한다. 그리고 출력물에 기입된 오프라인 식별번호가 당초 제공된 기관 외에서 불법적으로 이용되거나 다른 목적으로 이중사용되는 등의 도용 방지를 위해 특정 시간동안만 유효하거나 사용횟수를 제한할 수 있는 특성을 지원해야 한다.

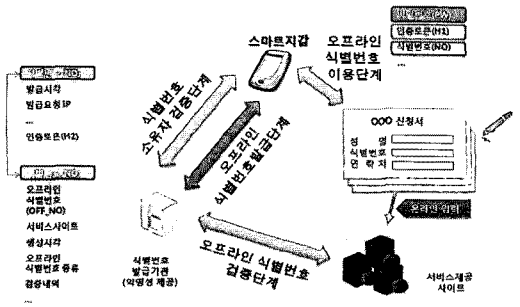
[그림 8]은 오프라인 환경에서 국민식별번호체계 동작절차를 보이고 있다. 오프라인 환경의 식별번호체계 동작단계는 사용자가 자신의 식별정보를 종이 형태의

양식에 기록하기 위해 오프라인 식별번호를 발급받는 단계부터 시작된다. 사용자는 오프라인 식별번호를 발급받기 위해 자신의 스마트지갑에 미리 설치된 오프라인 식별번호 발급 소프트웨어를 이용하여 식별번호발급기관에 접속하게 된다. 이 과정에서 사용자는 자신의 온라인 식별번호를 제시하게 되고 식별번호발급기관은 현재 접속한 사용자가 전달된 식별번호의 실제 소유자인지를 먼저 검증하게 된다. 이 과정은 4.1.1에서 설명한 인증토큰 H_2와 사용자 비밀번호(PW)를 이용한 challenge-response 방식의 검증단계를 거쳐 이루어지게 된다.

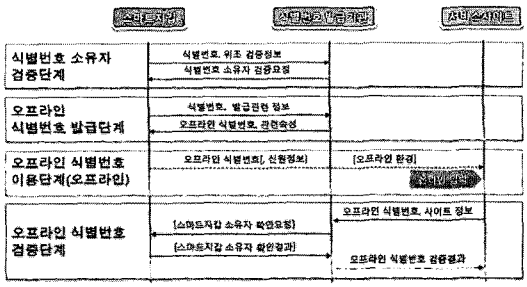
사용자 검증이 성공적으로 이루어지면 식별번호발급기관은 사용자에게 발급할 오프라인 식별번호를 생성하고 안전한 통신채널을 통해 사용자에게 전달한다. 이 때 생성되는 오프라인 식별번호는 사용자가 지정한 사용횟수(일회용, 반복사용용), 오프라인 식별번호 제공처, 반복사용용인 경우 해당 정보(최대 사용횟수, 사용기간) 등의 속성값과 함께 식별번호발급기관에 의해 저장, 관리되어야 한다.

사용자는 스마트지갑에 표시된 오프라인 식별번호를 종이 등 오프라인 양식에 기입하게 된다. 이와 함께 오프라인 식별번호는 스마트지갑에 설치된 오프라인 식별번호 관리 소프트웨어에 의해 저장, 관리되어야 한다.

오프라인 식별번호를 제공받은 서비스제공기관은 오프라인 양식에 기입된 사용자 식별번호를 처리하기 위해 디지털 정보 형태로 변환하는 입력과정을 수행하게 된다. 그리고 디지털 형태로 저장된 사용자의 오프라인 식별번호를 이용하여 서비스 제공을 위한 처리과정을 수행하기 전 오프라인 식별번호가 식별기관에 의해 생성된 정당한 식별번호인지, 해당 오프라인 식별번호가 정당한 사용자에 의해 생성요청이 된 것인지 확인과정을 거쳐야 한다. 이러한 과정들이 오프라인 식별번호 검증단계에서 수행하게 되며 검증방식은 식별번호발급기관과 사용자 간 challenge-response 방식을 통해 이루어진다.



〔그림 8〕 오프라인 환경의 식별번호체계 동작 단계



〔그림 9〕 오프라인 환경의 식별번호 관리체계 동작절차

오프라인 식별번호를 생성하는 구성요소는 본 고에서 제안한 식별번호발급기관 외의 스마트지갑도 가능하다. 오프라인 식별번호를 식별번호발급기관에 의해 생성하는 경우 생성되는 오프라인 식별번호의 중복방지와 오프라인 식별번호의 중복사용방지 및 검증이력관리 측면에서 장점이 있는 반면 오프라인 식별번호 생성을 위해 사용자가 이용하는 스마트지갑과 식별번호발급기관이 통신이 매번 이루어져야한다는 단점이 있다.

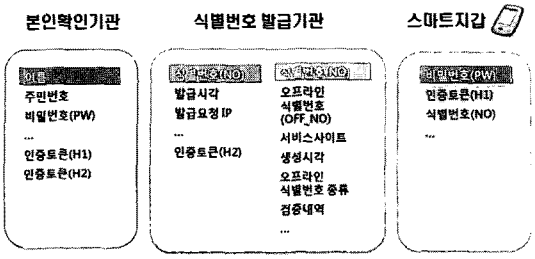
반면 오프라인 식별번호를 스마트지갑에서 생성하는 방식은 오프라인 식별번호 생성때마다 식별번호발급기관과 통신채널을 생성할 필요가 없는 장점이 있는 대신 스마트지갑에서 생성되는 오프라인 식별번호의 중복방지 점검기능을 수행해야 하고 오프라인 식별번호에 대한 검증 및 사용이력 관리를 직접 수행해야 하는 부담이 존재한다.

[그림 9]는 오프라인 환경의 국민식별번호체계에서 오프라인 식별번호 발급을 위해 필요한 소유자 검증단계, 오프라인 식별번호 발급단계 및 이용단계, 검증단계별 동작절차를 나타내고 있다.

4.2.2 관리정보 간 관계

[그림 10]은 오프라인 환경에서 오프라인 식별번호 발급과 검증과 관련되어 본인확인기관, 식별번호 발급기관, 스마트지갑이 관리하고 있는 주요 정보 구조와 연관관계를 나타내고 있다.

본인확인기관과 스마트지갑이 저장, 관리하고 있는 정보는 온라인 환경과 유사하지만 식별번호 발급기관은 프라인 식별번호 발급 및 검증 정보 저장을 위해 의해



〔그림 10〕 오프라인 환경의 식별번호 관리정보 구조

추가 관리정보를 유지하고 있다. 오프라인 식별번호(OFF_NO)는 온라인 식별번호(NO)와 연관되어 저장, 관리되고 있으며 각각의 오프라인 식별번호에는 발급시각, 발급대상 서비스제공 사이트 또는 기관, 종류 및 검증 내역 등이 추가로 유지, 관리되고 있다.

V. 결 어

본 고에서는 지금까지는 우리나라 국민의 개인식별번호로써 사용되고 주민등록번호의 특성을 보안 및 프라이버시 보호 측면에서 분석하고 이를 보완할 수 있는 새로운 국민식별번호체계를 제안하였다. 현재 사용 중인 주민등록번호는 개별 국민을 유일하게 식별하는데 필요한 정보 외에 필요이상의 정보가 포함되어 있는 점, 주민등록번호 구성방법이 공개되어 쉽게 위조할 수 있는 점, 한 번 발급된 주민등록번호는 평생 변경이 불가능한 점, 주민등록번호를 통해 우리나라 국민 중 유일한 한 사람을 식별할 수 있다는 점, 온라인이나 오프라인 환경에서 주민등록번호를 제시한 사용자가 제시된 주민등록번호의 실제 소유자 여부를 검증하기 쉽지 않다는 점 등이 보안 및 프라이버시 보호 관점에서 취약점으로 지적되고 있다.

본 고에서 제안된 새로운 국민식별번호체계에서는 현재 주민등록번호가 가지고 있는 취약점들을 보완할 수 있는 국민식별번호 구조와 함께 이를 지원하는 인프라를 함께 제시하고 있다. 기본적으로 새로운 국민식별번호는 국민을 식별하기 위한 정보만으로 구성되어 있어 개인에 대한 필요 이상의 정보를 포함하고 있지 않고, 온라인 국민식별번호의 경우 전자서명을 이용한 위조여부 검사를 수행함으로써 위조나 변조가 불가능하며, 국민식별번호 발급기관과 본인확인기관을 분리, 운영하도록 설계함으로써 국민식별번호만으로는 어떤 국민을 가리키는 지를 확인할 수 없도록 지원하는 익명성을 제공하고 있다. 그렇지만 법률이 정한 경우 또는 특별히 정해진 경우에 한해 익명성을 제거할 수 있는 절차도 설계되었다.

또한 오프라인 환경에서 현재 사용 중인 주민등록번호와 같이 사용자들이 읽고 기록하기 쉬운 형태를 가지는 오프라인 국민식별번호와 관련 지원체계도 함께 제안되었으며, 사용자가 제공한 서비스제공 사이트 외 타 사이트에서 이용되거나 제한된 횟수나 사용기간을 초과하여 사용되려 할 때 이를 검사하고 통제할 수 있는 기술적, 제도적 방법도 제시되었다.

그러나 제안된 새로운 국민식별번호체계는 기술적 장치만을 이용하여 현재 주민등록번호체계가 가지고 있는 보안 및 프라이버시 보호 측면의 문제점들을 모두 해결할 수 없으므로 기술적 조치를 보완, 지원할 수 있는 법률적, 제도적 지원이 요구된다.

참고문헌

[1] 김기중, "국가의 국민관리체계와 인권: 호적과 주민등록제도를 중심으로," 세계 인권선언 50주년 기념 학술행사 발표논문집, 1999.

[2] 정보화동향분석, "일본의 주민정보 네트워크 구상 계획 및 의의," 한국정보화진흥원, 2000.

[3] 방송통신위원회, 인터넷상 주민번호 대체수단(i-PIN) 활성화 종합대책안, 2009. 3.

[4] 행정안전부, 공공 i-PIN 확대 보급계획, 2009. 4.

[5] 오상진, "이제는 주민번호 대신 '아이핀'으로," 나라경제, 방송통신위원회, 2009. 5.

[6] 보안뉴스, "2015년 온라인서 주민번호 사용 사라진다," 2009. 4.

[7] 이윤경 외, "익명 인증 기술과 동향," 전자통신동향분석 제23권 제4호, 2008. 8.

[8] 진보네트워크센터 "옥션과 하나로텔레콤 피해자, 주민등록번호 변경 신청," http://acton.jinbo.net/webbs/view.php?board=policy&id=1399, 2008. 5.

〈著者紹介〉

이 형 효 (HyungHyo Lee)

종신회원

1987년 2월: 전남대학교 계산통계학과(학사)
1989년 2월: KAIST 전산학과 (석사)
2000년 2월: 전남대학교 대학원 전산학과(박사)
1990년~1992년: 삼보컴퓨터 기술연구소
1993년~1997년: 한국통신 연구개발원
2001년 3월~현재: 원광대학교 정보·전자상거래학부 부교수
<관심분야> 프라이버시보호, Identity 관리시스템, 보안 온톨로지, 응용보안

박 희 만 (HeeMan Park)

정회원

2006년 2월: 전남대학교 대학원 정보보호학과 석사
2009년 2월: 전남대학교 대학원 정보보호학과 박사
2009년 3월~현재: 전남대학교 시스템연구센터 연구교수
<관심분야> 접근통제, 유비쿼터스 보안, 이벤트 시스템

조 상 래 (Sangrae Cho)

정회원

1996년: College of Science, Technology and Medicine, 전산과 (학사)
1997년: Holloway, University of London, 정보보호 (석사)
1997년~1999년: LG 종합기술원 연구원
1999년~현재: 한국전자통신연구원 연구원
<관심분야> 정보보호(PKI, Identity Management 기술, 프라이버시보호기술), 컴퓨터/네트워크 보안

진 승 헌 (SeungHun Jin)

정회원

1995년 2월: 숭실대학교 (석사)
2004년 2월: 충남대학교 대학원 컴퓨터과학과 (박사)
1996년 4월: (주)대우통신 종합연구소 연구원
1999년 5월: (주)삼성전자 통신연구소 전임연구원
2003년 7월~현재: 한국전자통신연구원 인증기술연구팀장
<관심분야> 정보보호(PKI, 인증/인가기술, 프라이버시 보호기술), 컴퓨터/네트워크 보안