인터넷상의 주민등록번호 대체수단의 문제점들과 해결방법*

안 정 희**

Problems of alternative means of Inhabitants Registration Identification Number on Internet and their Countermeasures

Ahn, Jeong Hee

〈Abstract〉

As internet is wide spread, the number of internet service provider is increased. Internet service providers gather the personnel information with inhabitants registration identification number for the user management and the adult authentication. The personnel information is spreaded thorough the Internet by the system hacking, mismanagement and malicious resale. And the personnel information is used for spam email, phishing scams, etc. by malicious others. So the Ministry of Information and Communication Republic of Korea developments I-PIN system of the personnel identification. But, I-PIN has some problem the guideline for it and the method of 5 I-PIN services. In this paper, we analyze the problem about the guideline for I-PIN and the method of 5 I-PIN services. And we propose the countermeasure about the problem.

Key Words : I-PIN(Internet Personal Identification Number), PKI, Certificate, Hash Value

Ⅰ. 서론

개방형 유선통신인 인터넷이 국내에서도 급속히 보급되면서 인터넷을 통한 각종 온라인 서비스를 제공하는 여러 유·무료 웹사이트들도 빠르게 증가하고 있다. 대부분의 웹사이트들은 가입자에 대한 관리 즉, 접근통제를 위하여 편리한 아이디와 패스워드 방식을 주로 사용하게 되었으며 해당 웹사이트에 사용자가 가입 시에 아이디 혹은 패스워드로 주민등록번호를 요구하거나 가입자 인적 사항에 주민등록번호를 기입하도록 하는 웹사이트가 늘어나게 되었다. 그리고 웹 사이트에 수집, 저장된 다량의 가입자 주민등록번호가 오용이나 남용되고 해킹되거나 악의적인 관리자에 의해 전매되는 일이 빈번히 발생하게 되었다.

이에 따라 특정 웹사이트 가입이나 제한적인 자료를 제공하기 위한 성인 인증 시에 이용자가 해당 웹사이트에 자신의 주민등록번호를 직접 제공하지 않으면서도 본인임을 확인할 수 있는 방법의 도입이 필요하게 되었다. 정보통신부는 2005년 7월에 '인터넷상의 주민등록번호 대체수단 가이드라인'을 제정하고 이를 여러 번의 공청

* 본 논문은 2007년 두원공과대학 학술 연구비에 의해 연구되었음.
** 두원공과대학 컴퓨터정보과 부교수

회를 거쳐 2007년 초에 주민등록번호 대체수단인 I-PIN(Internet Personal Identification Number)으로 지정하기에 이르렀다.

그러나 이러한 주민등록번호 대체수단의 도입이 공청회를 거쳤음에도 불구하고 철저하고 객관적인 분석이 충분히 이루어지지 못한 것으로 사료된다. 따라서 본 논문에서는 인터넷상의 주민등록번호 대체수단의 도입과정 및 I-PIN을 객관적이고 종합적으로 분석하여 문제점을 지적하고 이에 대한 해결방법을 제시하고자 한다. 논문의 나머지 부분은 다음과 같이 구성되어진다. 2장에서는 인터넷상의 주민등록번호 대체수단의 도입과정에서의 문제점을 지적한다. 3장에서는 I-PIN 서비스들의 문제점들을 분석한다. 그리고 4장에서 이들 문제점들을 해결하기 위한 방법들을 제안하고 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 인터넷 상의 주민등록번호 대체수단의 도입과 문제점

한국정보보호진흥원에서 '인터넷상의 주민등록번호 대체수단'을 도입하면서 제정한 규칙 사항(이하 가이드라인)에는 인터넷 사업자에게 유리한 사항이 다수 존재하며 이를 분석해 보면 다음과 같은 문제점들을 가지고 있다.

2.1 인터넷 사업자의 주민등록번호 수집

가이드라인의 제2장 제4조 ④항을 보면 '인터넷사업자가 제1항의 규정에 의한 본인확인을 행하는 경우에는 주민등록번호를 이용하거나 제2조제1항 제2호의 본인확인정보를 이용하여 본인확인을 할 수 있다.'라고 되어 있다. 또한 제5조제2항을 보면 '인터넷사업자가 제1항의 규정에 의하여 주민등록번호를 수집하는 경우에는 주민등록번호의 도용을 방지하기 위한 수단을 강구하여야 한다.'라고 명시되어 있다 [1-5].

그러나 주민등록번호는 인터넷 상에 이미 많이 노출되어 있으며 주민등록번호 생성 소프트웨어가 존재하고 있어 이를 이용한 본인확인 방법은 문제점들을 가질 수 밖에 없다. 또한 일단 수집된 주민등록번호는 대기업의 인터넷 사업자들조차 사고나 실수로 대량 유출시키고 있다. 그러므로 재정이 약한 중소 인터네사업자들이 주민등록번호의 도용을 막을 수 있는 강력한 수단을 구축할 수 있을 런지는 의문이 아닐 수 없다. 따라서 인터넷 사업자가 사용자의 주민등록번호를 수집할 수 없도록 하여야 한다.

2.2 주민등록번호와 본인확인정보

가이드라인의 제2장 제4조 ④항을 보면 '인터넷사업자가 제1항의 규정에 의한 본인확인을 행하는 경우에는 주민등록번호를 이용하거나 제2조제1항 제2호의 본인확인정보를 이용하여 본인확인을 할 수 있다.'라고 되어 있다. 제2조제1항 제2항은 "본인확인정보"라 함은 본인확인을 위하여 본인확인기관이 가입자에게 부여하는 식별정보를 말한다.' 제12조제1항을 보면 '본인확인정보는 가입자의 개인정보를 보호하기 위해 생년월일, 출생지, 성별 등의 개인정보를 포함하지 않는 13자리 이상의 숫자나 영문자로 구성되어야 한다 [1-5]'.

2007년 8월 16일 네이버뉴스에 따르면 '우리나라 인터넷 이용자 5명 가운데 3명은 주민등록번호 폐지를 원하는 것으로 나타났다. 특히 주민등록번호 이외의 방법으로 개인 인증이 가능할 경우 72%의 네티즌이 주민등록번호 폐지에 찬성하는 것으로 조사됐다 [6].

KAIST 테크노경영대학원 문송천 교수팀은 2007년 6월 5일부터 3주간에 걸쳐 온라인 설문조사기관인 중앙리서치(research.joongang.com)와 월드서베이(wsurvey.net)를 통해 실시한 '정보화시대 주민등록번호 의식 설문조사' 결과 이 같이 나타났다고 밝혔다. 조사결과 주민등록번호 폐지에 찬성하는 네티즌은 전체 응답자 315명 중 58%에 이르는 183명인 반면, 반대하는 네티즌은 4%(13명)에 불과했다. 또 대다수의 네티즌들은 주민등록번호 생성기 등으로 자신의 개인정보가 도용될 수 있다는 사실을 알고 있다(91%)고 응답했다. 특히 온라인 또는 오

프라인 회원 가입시 개인의 주민등록번호를 등록하는 관행이 개선돼야 한다(83%)고 생각하는 것으로 나타나 주민등록번호 유출로 인한 피해 등 부작용을 걱정해 네티즌들이 폐지에 찬성하는 것으로 분석됐다. 이와 관련해 응답자 2명 중 1명꼴인 47%의 네티즌은 주민등록번호로 인한 개인정보가 불법 유출돼 피해를 입은 경험이 한번이라도 있다고 대답했으며, 개인 정보 도용 피해를 입었을 경우 주민등록번호 자체도 변경이 가능해야 한다고 생각하는 네티즌도 57%에 달해 현행 주민등록번호 제도의 개선 또는 폐지가 필요한 것으로 나타났다.

문송천 교수는 이번 조사 결과에 대해 "개인 정보 유출의 근본 원인이 주민등록번호 사용의 남용에 있는 만큼 주민등록번호 자체를 사용하지 않을 경우 개인 정보 사고의 대부분을 근절할 수 있을 것이라고 본다."고 지적했다. 문 교수는 "주민등록번호 제도를 계속 유지하더라도 선진국의 사회보장번호처럼 사고 발생 시에 민원에 의해 변경 가능한 형태로 개선한다면 정보화시대에 프라이버시 보호의 방패막이 될 것"이라고 덧붙였다.'

일단 본인확인정보에 개인정보를 포함하지 않도록 한 것은 개인정보가 더 이상 노출되지 않도록 한 정책으로 볼 수 있다. 그러나 본인확인정보는 또 다른 형태의 주민등록번호라는 데에 문제가 있다. 형태만 달라질 뿐, 본인확인정보는 주민등록번호처럼 사용자를 구별할 수 있으며 결국 주민등록번호의 대용으로 사용되어질 가능성이 높다. 위의 조사 결과와 같이 주민등록번호이건 본인확인정보이건 그 사용이 점차 줄어들고 있는 상황이다. 게다가 이러한 본인확인정보를 인터넷사업자와 본인확인기관이 취급하게 되므로 결국 본인확인정보가 노출될 가능성이 더욱 높아지게 된다.

2.3 본인확인 방법

가이드라인의 제13조제1항과 제2항을 보면 본인확인기관은 본인확인정보의 발급을 신청한 자의 신원을 확인하기위한 기준 및 방법을 명시하고 있다. 제13조제1항과 제2항의 각 호를 살펴보면 다음과 같은 방법들이 예시되어 있다 [1-5].

1. 신원확인증표를 통한 대면확인
2. [전자서명법]에 따른 공인인증서를 이용한 확인
3. 금융 계좌번호, 계좌 패스워드 등 금융계좌정보를 통한 확인
4. 신용카드 번호, 신용카드 유효기간, 신용카드 패스워드 등 신용카드정보를 통한 확인
5. 휴대전화의 인증번호를 통한 확인

<표 1> 본인확인 방법의 비교

본인확인방법	보안 강도	취약점	보완책
대면확인	가장 높음	사진의 최신성, 눈으로 비교	상이한 본인확인방법추가
공인 인증서	높음	재발급시의 확인, 1년의 사용기간	재발급시의 보안 강화
금융계좌정보	낮음	필기 가능성	-
신용카드정보	높음	분실과 신고 사이의 공백	
휴대전화 인증번호	높음	폰 분실시, 대포폰 사용자	

위의 <표 1>에서 1의 방법은 가장 강력하고도 안전한 실지명의에 대한 확인 방법이다. 공인인증서 발급도 초기에 직접 대면을 이용한 본인 확인 방법에 의해 이루어진다. 따라서 2의 방법도 역시 1의 방법을 포함하고 있는 안전한 방법이다. 그러나 3, 4 그리고 5의 방법은 통장이나 신용카드 그리고 휴대폰을 분실하는 경우에 분실 신고가 제대로 이루어지지 않는다면 악의적인 공격자가 불법적으로 본인확인을 받을 수 있게 된다. 신용카드나 휴대폰의 분실은 사용자가 이를 인지하기가 용이하지만 계좌번호와 패스워드는 그 노출의 인지가 어렵거나 늦을 수밖에 없다. 우리는 여러 개의 은행 통장, 인터넷에 대한 아이디와 패스워드를 일일이 기억하기 힘들어 수첩에

적어 놓곤 한다. 따라서 이를 적어 놓은 수첩을 분실하게 되면 역시공격자에 의해 불법적인 본인확인정보가 생성되게 된다. 특히 계좌번호와 패스워드는 분실되더라도 급박하게 인식하지 않게 된다. 왜냐하면 은행창구에서 이를 이용하여 돈을 출금시키려면 통장, 도장이 추가로 있어야 하고 인터넷을 이용하여 출금을 하려면 인증서, 인증서 패스워드 그리고 보안카드도 있어야 하기 때문에 금융 계좌번호 및 패스워드의 분실을 대수롭지 않게 생각하게 된다. 따라서 이러한 생각과 편리함을 위하여 통장 뒷면에 패스워드를 적어 놓는 사용자도 있다. 아울러 통장이나 신용카드 그리고 휴대폰을 분실하는 경우에 분실 신고에 따른 본인확인기관으로의 정보전달이 원활하게 이루어져야 하는데 지금의 체계는 이러한 절차가 전혀 이루어져 있지를 못하다. 또한 휴대폰은 현재 본인명의로 휴대폰을 개통하고 실제로는 다른 사람이 사용하는 경우도 상당수 존재한다. 실례로 연로하신 부모님께 휴대폰을 개통해 드릴 때에 부모님 명의로 구입하지 않고 자식 명의로 구입하기도 한다. 혹은 아직 미성년자인 어린 자식에게 부모들이 자신의 명의로 휴대폰을 구입하여 사용하도록 하는 것 등이 있을 수 있다. 그러나 이러한 경우보다 더욱 심한 경우는 바로 대포폰이다. 대포폰을 이용하는 사용자가 상당수 존재하며 범죄에도 이용되기도 한다. 2006년 10월, 정보통신부는 불법목적으로 개통된 타인명의 휴대폰(일명 대포폰)을 활용한 사기 및 불법 스팸 등 피해를 차단하기 위한 대책들을 경찰청 및 이동통신사와 함께 시행할 계획이라고 10월 9일 밝혔다. 정보통신부는 명의도용 예방을 위해 대리점 등에서 본인명의 휴대폰 가입 신청이 들어오는 경우, 해당 이용자에게 직접 SMS로 이와 같은 사실을 알려 사전에 명의도용을 예방할 수 있는 모바일 세이퍼(M-safer)서비스에 대한 홍보를 강화할 계획이다. 또한, 이동통신사가 유령 법인으로 의심되는 경우 가입 회선 수를 제한할 수 있도록 약관을 개정하고, 대포폰 이용자에 대한 데이터베이스를 사업자들이 축적하여 활용토록 할 예정이다 [7].

따라서 3, 4 그리고 5의 방법은 1과 2의 방법에 비해 강력하지 않으며 안전하지 않다. <표 1>은 이러한 본인확인 방법들을 비교한 것이다.

2.4 주민등록번호와 본인확인정보의 파기

가이드라인의 제3장제7조를 보면 '인터넷사업자는 이용자의 요구가 있는 때에는 지체 없이 본인확인을 위해 수집·이용 중인 주민등록번호를 파기하여야 한다.'고 되어 있다. 그러나 그 구체적인 방법이나 확인 절차에 대해서는 언급되어 있지 않다. 또한 본인확인기관이 발급한 본인확인정보의 파기에 대한 언급도 없다 [1-5].

인터넷사업자가 수집·이용 중인 주민등록번호나 본인확인정보는 이용자의 요구나 더 이상 사용이 되지 않을 경우에는 완전한 파기가 이루어져서 악용이나 사고에 의한 유출이 이루어지지 않도록 하여야 한다. 또한 관리기관을 두어 사용되지 않는 주민등록번호들에 대한 완전한 파기가 이루어 졌는지를 주기적으로 감독 및 관리하여야 한다.

2.5 본인확인기관의 사후관리

가이드라인의 제6장제26조에서 제6장제32조까지를 보면 본인확인기관에 대한 적합성 평가와 정기점검에 대한 사항이 명시되어 있다. 본인확인기관에 대한 적합성 평가를 통하여 개인정보에 대한 영향평가를 수행, 인증마크를 부여하는 관리 방법은 적절하다. 그러나 본인확인기관의 사후 관리에 대한 부분 중에 본인확인기관의 폐지 시에 대한 적절한 관리역시 무척 중요하다 [1-5].

본인확인기관은 수많은 사용자의 본인확인을 수행하므로 대량의 개인정보를 축적하게 되며 데이터베이스 등의 전산시스템을 구축하게 된다. 따라서 이를 폐기할 시에는 적절하고도 완벽한 조치가 이루어져야 한다. 특히 최근 상용 포렌식 툴에 의한 하드디스크의 복구가 문제점으로 지적되고 있다. 2007년 2월 최윤성 등은 "삭제된 공인인증서의 복구 및 개인키 암호화 패스워드의 검출"이라는 논문에서 삭제된 인증서와 개인키 저장 파일을

상용 포렌식 툴을 이용하여 복구해낼 수 있는 가능성을 제기하였다 [8]. 따라서 개인이 사용하던 하드디스크도 폐기 시에 철저한 조치가 이루어져야 하지만 대량의 개인정보를 관리하기위해 사용되었던 하드 디스크의 폐기는 보다 완벽한 처리가 이루어져야 하겠다.

2.6 인증서와의 기능 중복

2006년 10월, 국회 과학기술정보통신위원회 소속 한나라당 서상기 의원은 정보통신부가 인터넷 개인정보 유출 방지를 위해 추진 중인 주민등록번호 대체수단인 아이핀(I-PIN)으로 인해 행정 업무 및 인력이 중복되고 있다며 "기존 우리나라 국민 1000만 명 이상이 사용하고 있는 공인인증서를 제대로 활용하는 것이 주민등록번호 대체수단인 아이핀의 추진으로 인해 발생되는 불필요한 행정업무 손실을 막을 수 있다."고 주장했다 [9].

또, 서 의원은 "이미 1000만 명 이상에게 은행업무 등 용도제한용으로 발급된 공인인증서를 사용하는 편이 오히려 타당하며, 이는 기존 공인인증서의 역할만 축소하는 것"이라고 지적했다. 이에 대해, 이홍섭 한국정보보호진흥원장은 "용도제한용으로 발급된 공인인증서는 특정 분야 사용에 한정돼 있고 법적 제한이 있어 범용 공인인증서로 활용하기에는 무리가 있어 유보했다"며 "카드나 휴대폰 결제의 수단으로 활용되는 150만여 명이 이용 중인 범용 공인인증서의 본인확인 수단으로 활용할 계획"이라고 응답했다.

현재 우리나라는 공인인증서가 NPKI(National Public Key Infrastructure) 형태로 잘 구축되어 있으며 수년간의 운영으로 이제는 안정적으로 유지되고 있다. 따라서 공인인증서가 이제 시작 단계의 I-PIN에 비하여 사용자에게 보다 안정적이고도 편리한 서비스를 제공해줄 수 있다. 또한 인증서에는 사용자의 주민등록번호가 포함되지 않으며 사용자의 이름만이 포함된다. 그리고 사용자 본인인 지를 등록기관(은행 본·지점이나 증권 본·지점 창구)을 통한 대면 확인을 통하여 본인 여부를 확인한 뒤, 인증기관이 이를 서명을 통하여 입증해주고 있다.

5가지의 I-PIN 서비스들이 모두 범용 공인인증서를 추가적인 본인 확인수단으로 채택하고 있다. 물론 그 외의 다른 본인 확인수단도 제공하고 있지만 인증서를 본인 확인수단으로 사용한다면 인증서를 사용하는 것과 동일하며 사용자측면에서는 오히려 번거로움을 갖게 될 수 있다.

인증서는 인터넷뱅킹, 주식거래는 물론이려니와 이제 인터넷 쇼핑에서 결재 시에 본인확인에 사용되기도 하고 있다. 따라서 인터넷에서의 주민등록번호 대체수단으로서 인증서를 확대 사용하는 것이 보다 설득력을 얻고 있다.

Ⅲ. I-PIN의 정책적인 문제점

앞에서 살펴본 바와 같이 도입 과정에서 여러 문제점을 가지고 있는 인터넷상의 주민등록번호 대체수단은 구체적으로 개발된 I-PIN에서도 문제점을 가지고 있다. 2007년 4월에 이미 최윤성 등은 "주민등록번호 대체수단에 대한 구현 취약점 분석"이라는 논문에서 현재 시행되고 있는 5가지의 I-PIN을 분석하여 보안상의 문제점을 지적하였다 [10]. 그러나 그 외에도 I-PIN은 다음과 같은 정책적인 문제점들을 가지고 있다.

(1) 1차 본인확인 방법의 실효성 여부

식별과 인증 기술들은 각기 장단점을 가지고 있어 한 가지 기술로 완벽한 효과를 거둘 수는 없다. 따라서 특정 기술과 이를 보안해주는 다른 기술을 같이 적용하여 보다 완벽한 효과를 내도록 하고 있다.

이러한 점을 고려하여, 도입된 I-PIN에서도 본인확인 절차 시에 1차적인 본인확인을 수행하고 추가적인, 다른 방법으로 보다 완벽한 신원확인을 하고 있다. 이를 정리하면 <표 2>와 같다. 표에서 알 수 있듯이 한국정보인증의 OnePass만이 1차 본인확인 과정에서 범용인증서를 사용하고 나머지의 I-PIN에서는 모두 성명과 주민등록번호를 이용하고 있다. 사용자의 성명 및 주민등록번호는

이제 더 이상 본인확인 혹은 성인 확인의 수단으로써의 의미를 상실하였다. 따라서 이러한 수단으로 1차적인 본인확인을 수행하는 것은 I-PIN의 본인확인 기능을 약화시키는 것이다.

<표 2> I-PIN 서비스들의 비교

종류	개발사	1차 본인확인	추가 본인확인 방법				
			인증서	신용카드정보	휴대폰 인증정보	대면 확인	보호자 인증
나이스 아이핀	한국신용정보	성명, 주민등록번호	○	○	○	○	×
가상주민등록번호	한국신용평가정보	가상주민등록번호, 성명	○	○	○	○	×
Siren24 아이핀	서울신용평가정보	성명, 주민등록번호	○	○	○	○	○
OnePass	한국정보인증	범용인증서	○	×	×	×	×
그린버튼	한국전자인증	성명, 주민등록번호	○	○	×	×	×

(2) 본인확인기관이 민간업체로 구성

현재 I-PIN 서비스에서 본인확인기관은 한국신용정보, 한국신용평가정보, 서울신용평가정보, 한국정보인증, 한국전자인증으로 구성되어 있다. PKI에서는 이와 상응하는 인증기관이 공공기관으로 되어 있는 것과 달리 I-PIN에서는 민간업체로 구성되어 있다. 본인확인기관은 사용자들의 성명, 주민등록번호, 식별번호, 인증서, 이메일 주소 등 상당수의 중요 개인정보가 집중되어 관리된다. 따라서 한번의 사고나 공격으로 큰 피해를 볼 수 있다. 따라서 이들 본인확인기관이 기술적으로도 보안에 대비해야 하지만 아울러 보다 공공성을 갖는 공인기관이 되어야 한다.

(3) 제2의 주민등록번호인 가상주민등록번호의 보안성

대부분의 본인확인기관은 사용자의 주민등록번호를 대신하는 가상주민등록번호를 이용하여 사용자들을 관리하고 있다. 이 가상주민등록번호는 형태만 다를 뿐, 앞에서 살펴보았던 주민등록번호와 동일한 역할을 하고 있다. 따라서 이 가상주민등록번호가 바뀌지 않는 한, 특정 사용자를 나타내는 일련번호가 되는 것이다. 따라서 가상주민등록번호를 이용한 웹사이트들 간의 링크 및 인터넷 감시를 통한 개인정보 유출의 가능성도 생기게 된다. 이를 막기 위해서는 주기적으로 변하는 가변 가상주민등록번호를 생각할 수 있다. 이를 위해서는 추가적 기능이 요구되어진다. 아울러 이 가상주민등록번호를 가급적 사용자와 인터넷서비스사업자에게 제공하지 않도록 하여 노출될 가능성을 줄어야 할 것이다.

(4) I-PIN 서비스들의 다양한 보안 문제

I-PIN 서비스들이 가지고 있는 다양한 보안상의 문제점들은 I-PIN을 개발하기 전에 요구 사항에 대한 충분한 검토 및 연구가 이루어지지 않았기 때문인 것으로 사료된다. 또한 기 개발된 I-PIN 서비스들에 대한 충분한 기간 동안의 시험운영을 거치지 않고 바로 서비스를 실시한 것에서도 기인한다고 볼 수 있다. 일반적으로 개발된 서비스들은 충분한 사전 시험 운영을 거쳐야 한다. 특히 보안에 관련된 서비스들은 충분한 시험운영을 거치지 않는다면 실제 서비스 중에 보안상의 문제점을 노출시키게 되어 중요한 정보들을 인터넷에 노출시킬 수 있다.

Ⅳ. 해결 방법

인터넷상에서 안전하게 사용할 수 있는 주민등록번호의 대체수단은 살펴본 바와 같이 도입 과정에서부터 여러 가지 문제점을 노출시켰고 따라서 이를 기반으로 도입된 주민등록번호 대체수단들도 보안상의 문제점들을 가지고 있다. 이러한 문제점들에 대한 해결 방법은 다음과 같다.

(1) 인터넷사업자들은 사용자들의 식별정보를 절대로 저장 및 관리해서는 안된다.

식별정보는 또 다른 형태의 주민등록번호이다. 주민등

록번호를 사용하지 않고 식별정보를 사용하는 것은 형태만 바뀌었을 뿐, 사용자들을 구분하고 인식할 수 있는 방법을 제공해주기는 마찬가지이다. 이러한 식별정보를 인터넷사업자들이 수집하여 저장하고 관리하면서 사용자들의 사용 형태를 분류하거나 추적, 관리하게 된다면 이 역시 문제점이 아닐 수 없게 된다. 따라서 주민등록번호이건 이를 대체하는 식별번호이건 인터넷사업자들이 이를 수집하지 못하도록 하여야 한다.

(2) 불가피하다면 본인확인기관은 식별정보를 이용하여 사용자들을 관리하도록 할 수 있다.

본인확인기관은 사용자가 본인인지의 여부를 확인하기 위해서 사용자들의 주민등록번호와 실명을 수집할 수 있으며 이를 관리하기 위하여 식별정보를 이용하여 저장, 관리할 수 있다. 그러므로 이들 본인확인기관들에 대한 관리를 주기적으로 철저히 하여 사고나 해킹 등으로 유출되지 않도록 하여야 한다. 아울러 앞에서도 문제점으로 지적한 바와 같이 현재 민간업체로 되어 있는 이들 본인확인기관들을 보다 신뢰성이 있는 공공기관으로 격상시켜야 한다.

(3) 본인확인기관들은 서로 자료가 공유되어서 이중 가입자가 생기지 않도록 해야 한다.

현재 I-PIN의 5가지 서비스에서 발생하는 문제이기도 한 것으로서 본인확인기관들은 서로 사용자에 대한 자료가 공유되어서 이중 가입자들을 원천 봉쇄하여야 한다. 현재 이러한 기능은 권고 사항이어서 실시 여부가 불투명한 상태인데 한 사용자가 여러 곳의 I-PIN에 가입하다면 물론 본인은 다른 식별번호를 사용하므로 보안을 더욱 강화시킨다고 생각할 수 있다. 그러나 이중 가입자가 늘어난다면 본인확인기관들의 정보량을 늘여 효율을 저하시키는 부작용이 생기게 될 수 있다. 최윤성 등의 논문에서도 이러한 문제점을 지적한 바가 있다 [10].

(4) 현재로서는 인증서가 대안이다.

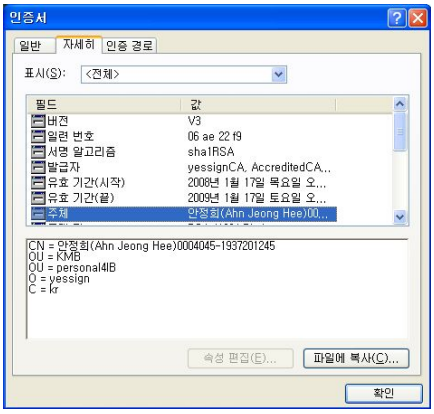
위와 같은 대응책을 만족하는 인터넷상의 주민등록번호 대체수단을 만들기가 힘들다면 현재로서는 PKI, 즉 인증서가 최선의 대안이 될 수 밖에 없다. PKI는 그동안 수년간 서비스를 수행해 왔기 때문에 시스템이 안정화되어있다. 그러나 인증서를 이용한 방법도 완벽한 방법은 아니다. 인증서는 계속적으로 해킹과 피싱을 이용한 공격 대상이 되고 있기 때문이다. 이는 2006년 6월 3일에 발생한 인터넷뱅킹 해킹사고가 공인인증서 재발급 체계의 허점을 이용했기 때문이다. 인터넷뱅킹 시스템을 해킹한 범인은 피해자의 공인 인증서 패스워드와 해킹한 인적사항 등을 이용하여 피해자의 인증서를 폐기했다. 그 뒤 자신의 컴퓨터에서 피해자의 인증서를 재발급 받아 이를 범행에 이용했다. 이를 위해 인증서를 재발급 받고자 할 경우 '재발급용 패스워드'를 입력하거나 '휴대폰 문자서비스(SMS) 인증제도'를 도입하는 방안이 도입이 검토되었었다. 과거에는 최초 발급시 부여받은 사용자 아이디(혹은 번호)와 패스워드, 주민등록번호만으로 인증서를 간편하게 재발급 받을 수 있었다. 그 외에도 주기적으로 인증서 발급 시스템 및 이를 이용하는 웹 사이트들을 검사하여 발생 가능한 해킹과 피싱을 이용한 공격에 대비하여야 한다.

(5) 익명인증이 최선책이다.

인터넷상에서의 주민등록번호를 대체하기 위한 수단은 그 목적이 개인 정보 유출 및 명의도용에 의한 피해를 방지 하는 것이다. 따라서 일단 현재로서는 인증서가 대안이 될 수밖에는 없지만 그렇다고 인증서가 최선의 방법은 아니다.

<그림 1>은 현재 국내의 금융권에서 사용되고 있는 공인인증서를 컴퓨터에서 본 내용이다. 인증서는 특별한 사고가 발생하지 않는 한 통상 그 유효기간이 1년이다. 따라서 1년 동안 동일한 사용자에 대해 관리, 감시, 추적, 통계 등을 수행할 수 있다는 것이다. 게다가 사용자가 고정 IP를 사용한다면 이러한 공격은 더욱 용이하고 완벽하게 이루어질 수밖에 없다. 따라서 이러한 문제점을 사전에 그리고 완벽하게 막기 위해서는 인터넷서비스제공자가 거래 상대방이 주민등록이 되어 있는 성인이고 도

용되지 않았음을 확인 할 수 있고 더 이상의 개인정보를 수집할 수 없도록 하여야 한다.



<그림 1> 인증서의 내용

암호학에서는 수학적으로 풀기 어려운 문제에 기반한 '익명 인증'이라는 분야가 실명 인증에서 문제가 되었던 개인정보 유출에 대한 문제를 최소화하고 높은 안전성과 편의성을 줄 수 있다. 이러한 사실은 2005년 12월에 서방남, 윤효진이 "주민등록번호 대체수단 분석"이라는 논문에서도 주장된 바가 있다. 이에 따르면 익명인증 기법을 응용하면 익명 인증서의 획득 단계는 물론 발급 이후에도 사용자의 모든 행동에 익명성이 보장되어 개인정보 유출을 근본적으로 막을 수 있다 [11].

따라서 가장 최선의 대책은 이러한 익명인증 기법을 이용하여 인터넷상에서 사용자들의 개인정보를 보호하면서 본인 혹은 성인인지의 여부를 확인하도록 해주는 것이다. 물론 이러한 익명인증이 도입되더라도 사용자들이 취급하기 쉽고 시간이나 경제성이 양호하여야 할 것이다. 익명인증이 이러한 조건이 부합하기는 하지만 다소 복잡하고 연산 비용이 늘어날 수 있다.

(6) 일방향 해쉬함수를 이용한 방법이 효율적이다.

본인확인기관의 관여없이 인터넷서비스제공자들이 직접 본인확인을 수행할 수 있는 방법이 효율적이다. 2002년 Micali는 NOVOMODO라는 논문에서 일방향 해쉬함수를 이용하여 인증서의 유효 및 폐지를 나타내는 방법을 제안하였다. 그 이후, 2003년 Jianying Zhou 등에 의해 제안된 "A Efficient Public-key Framework"이 제안되었으며 역시 같은 해에 양종필 등이 Jianying Zhou의 프레임워크를 개선하였다. 2004년에는 Satoshi Koga와 Kouichi Sakurai가 "A Distributed Online Certificate Status Protocol with a Single Public Key, Public Key Cryptography"이라는 논문에서 D-OCSP 서버의 유효성을 입증하는 방법을 제안하였으며 2005년부터 최근까지 일방향 해쉬함수를 이용한 방법들과 해쉬체인을 이용하여 인증서의 유효성을 제공하려는 방법 등이 제안되었다 [12-14]. 이들 논문에서 공통된 이론은 다음과 같이 역계산이 불가능한 해쉬함수 h를 이용하여 해쉬체인을 생성한다.

$$X_1 \xrightarrow{h} X_2 \xrightarrow{h} X_i \xrightarrow{h} \cdots \xrightarrow{h} X_N$$

그런 다음 X_N을 인증서에 포함하여 거래 상대방에게 보내고 전자서명을 수행하여 보낼 때마다 중간값을 역순인 X_i, X_2, X_1의 순서로 보냄으로써 거래 시의 전자서명 및 인증서의 유효성을 입증할 수 있다. 물론 새로운 인증서에는 소유자의 이름과 주체대체이름이 포함되지 않도록 해서 개인을 구별할 수 없도록 하여야 한다. 이러한 방법을 이용한다면 저렴한 계산비용과 빠른 연산으로 거래 상대방 모두가 효율적이고 안전한 사이버 거래를 할 수 있다.

Ⅴ. 결론

인터넷상의 주민등록번호 대체수단은 기존의 주민등록번호를 대신할 수 있는 대체수단을 본인 확인기관이 신원 확인 후에 인터넷의 웹사이트 가입자에게 발급해주는 본인 확인 수단이다. 그러나 이러한 주민등록번호 대체수단의 도입이 공청회를 거쳤음에도 불구하고 충분한 분석이 이루어지지 못하였다. 그 근본적인 원인은 인터넷 상에서 유출되어 도용 혹은 남용되고 있는 주민등록

번호들의 사고 사례에 대한 면밀한 분석을 통하여 '주민번호 대체수단 가이드라인'이 제정되지 않았기 때문이다.

따라서 본 논문에서는 인터넷상의 주민등록번호 대체수단의 도입과정과 선정된 I-PIN을 객관적이고 종합적으로 분석하여 문제점을 지적하고 아울러 이에 대한 해결방법을 제시하였다. 이렇게 함으로써 있으며 이중적인 인증 방법의 무분별한 도입을 최소화하고 기존의 인증방법을 충분히 활용할 수 있어 사용자에게 불편함이나 혼란을 최소화할 수 있다.

참 고 문 헌

[1] 한국정보보호진흥원,"2006년 10월 개정 인터넷상의 주민번호 대체수단 가이드라인", http://www.kisa.or.kr/index.jsp, 2007.1.24.

[2] 한국정보보호진흥원,"2006년 11월 아이핀 설명회 발표자료", http://www.kisa.or.kr/index.jsp, 2007. 1. 24.

[3] 한국정보보호진흥원,"2006년 8월 인터넷상의 주민번호대체수단 가이드라인 개정 공청회 발표자료 및 개정안", http://www.kisa.or.kr/index.jsp, 2007. 1. 24.

[4] 한국정보보호진흥원,"주민번호대체수단 본인확인기관 적합성 평가항목", http://www.kisa.or.kr/index.jsp, 2007.1.24.

[5] 한국정보보호진흥원,"인터넷상의 주민등록번호 대체수단 공청회", http://www.mic.go.kr/index.jsp, 2005.10.31.

[6] naver 뉴스, http://www.naver.co.kr

[7] 동아일보, http://www.donga.com

[8] 최윤성, 이윤호, 박상준, 양형규, 김학범, 김승주, 원동호, "삭제된 공인인증서의 복구 및 개인키 암호화 패스워드의 검출", 한국정보보호학회 논문지, 제17권 1호, 2007.02, pp.41-56.

[9] YTN 뉴스, http://www.ytn.co.kr

[10] 최윤성, 이윤호, 김승주, 원동호, "주민번호 대체수단에 대한 구현 취약점 분석", 한국정보보호학회 논문지, 제17권 2호, 2007.4, pp.145-184.

[11] 서방남, 윤효진, "주민등록번호 대체수단 분석", 한국정보보호 학회 동계학술대회 논문집 Vol 15. No.2, 2005.12.3.

[12] Silvio Micali, "Efficient Certificate Revocation", Technical Report TM-542b, MIT laboratory for Computer Science, 1996.

[13] Silvio Micali, "NOVOMODO ; Scable Certificate Validation And Simplified PKI Management", 1st Annual PKI Research Workshop Preproceedings, 2002, pp.15-25.

[14] Satoshi Koga, Kouichi Sakurai, "A Distributed Online Certificate Status Protocol with a Single Public Key, Public Key Cryptography", 2004, LNCS 2947, 2004, pp.389-401.

■ 저자소개 ■

안 정 희
Ahn, Jeong Hee

1988년 2월 성균관대학교 정보공학과 졸업(공학사)
1993년 2월 성균관대학교 대학원 정보공학과 졸업(공학석사)
2000년 2월 성균관대학교 대학원 정보공학과 졸업(공학박사)
1996년 3월-현재 두원공과대학 컴퓨터정보과 부교수

관심분야 : 정보통신 보안, 전자 상거래 보안, 트래픽 제어
E-mail : jhpro@doowoon.ac.kr

논문접수일 : 2008년 7월 30일
수 정 일 : 2008년 8월 14일
게재확정일 : 2008년 8월 19일