情報保護學會論文誌
第 21 卷 第 5 號, 2011. 10

OTP에 기반한 비연결성을 보장하는 온라인 본인확인에 대한 연구

김 정 동,† 조 관 태, 이 동 훈‡
고려대학교 정보보호대학원

A Study of Online User Identification Based on One-Time Password with Guaranteeing Unlinkability

Jung-Dong Kim,† Kwan-Tae Cho, Dong-Hoon Lee‡
Financial Information Security, Graduate School for Information Security, Korea University

요 약

최근 개인정보보호법 제정으로 온라인 회원등록시 본인확인과정에 주민등록번호를 사용하지 않는 방안이 필요한 상황이다. 대부분의 웹사이트는 주민등록번호를 사용하지 않는 신원확인 방안으로 아이핀(i-PIN)을 사용하고 있다. 하지만, 아이핀의 경우 고정된 정보(아이디, 패스워드) 값만 탈취하면 개인정보유출의 위험이 있다. 본 논문에서는 OTP를 이용하여 비연결성을 보장하는 신원 확인할 수 있는 방안을 제안한다. 제안된 방식은 웹사이트 회원가입시 아이디, 패스워드 같이 일관된 정보를 사용하지 않고, 웹사이트마다 각기 다른 정보로 회원가입을 하기 때문에 개인정보보호에 활용 가치가 높을 것이다.

ABSTRACT

Recently by the privacy & data security law, when a user registers the online membership, we need to take action to check a progress of identification without resident registration number. On the most of websites, I-PIN is used by identification instead of the resident registration number. However, I-PIN causes dangerous situations if someone steals the ID and a password, the personal data can be easy to exposure. In this paper, we propose the OTP, which can solve all these problems by guaranteeing the identification of unlinkability. This type of method would help the process of membership registration without fixed data like ID and a password in online so it would be very useful to security of private data.

Keywords: OTP, I-PIN, identification, registration number, privacy & data security law

I. 서 론

국내 인터넷 서비스의 성공 요인 중 하나는 주민등록번호를 사용한 비대면의 신원확인 수단이 존재하였기 때문이다. 대한민국에서 해외에 거주하지 않는 모든 국민은 주민등록법에 부여된 주민등록증에 적혀있는 유일성을 지닌 식별번호인 주민등록번호를 부여받는다. 이로 인해 지금까지 대부분의 웹사이트를 가입하려는 이용자는 주민등록번호를 이용하여 신원확인을 해왔고, 주민등록번호 유출시 개인정보유출의 통로가 될 수 있었다. 또한, 주민등록번호를 악용한 명의도용을 통해 전자거래 상의 문제를 일으킬 수 있었고, 가명사용이나 위조 주민등록번호 사용으로 가입한 회원들의 익명성에 의한 허위사실의 유포를 할 수 있는

접수일(2011년 4월 12일), 수정일(2011년 6월 6일), 게재확정일(2011년 7월 12일)
† 주저자, space1984@korea.ac.kr
‡ 교신저자, donghoonlee@hankook.re.kr

문제를 지녔다. 뿐만 아니라 주민등록번호는 13자리 숫자로 생년월일, 성별, 출생지역, 출생 신고순서 정보가 포함되어 있어 하나의 개인정보가 되므로 주민등록번호는 국내 인터넷 상에서는 매우 중요한 정보가 될 수 있다.

2011년 3월 29일에 제정된 개인정보보호법에서는 웹사이트의 주민등록번호 남용으로 인한 문제들로 인해 '제24조(고유 식별정보의 처리 제한) ② 대통령령으로 정하는 기준에 해당하는 개인정보처리자는 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입할 경우 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.'를 통해 개인정보 유출 원인으로 지목되는 무분별한 인터넷상 주민등록번호 수집 관행을 최소화할 것을 기술한다[1]. 국내 웹사이트에서 제공되는 주민등록번호를 사용하지 않는 온라인 본인확인 방법은 아이핀(i-PIN) 서비스가 유일하다. 아이핀을 사용한 본인인증을 할 경우에 다른 수단을 통한 본인인증을 하는 경우에 비해 주민등록번호의 남용을 줄여 개인정보 유출과 명의도용의 위협을 줄일 수 있다. 국내와는 다르게 금융 웹사이트를 제외한 국외의 웹사이트의 경우에는 주로 이메일을 통한 인증을 한다. 이메일만 있으면 본인확인이 되기 때문에 인터넷만 되면 어느 곳에서도 인증을 받을 수 있다. 국내에 진출해 있는 애플, 구글, 페이스북 등과 같은 국외 웹사이트들도 이메일 인증을 사용하고 있다. 하지만, 아이핀 서비스나 이메일을 통한 본인확인도 아이디, 패스워드에 의존한 본인확인을 하기 때문에 탈취될 경우 위험하다.

비연결성이란 두개의 메시지가 주어졌을 때, 그 두 개의 메시지가 동일한 객체로부터 생성된 것인지 각각 다른 객체로부터 생성된 것인지 판별이 불가능한 것을 의미한다. 비연결성 온라인 본인확인은 본인 인증을 요청할 때마다 새로운 값을 이용하여 신원을 확인함으로써, 기존에 본인인증에 사용되었던 값을 재사용하지 않는 것을 의미한다[2]. 예를 들어 웹사이트 회원가입, 회원정보변경 등을 할 때마다 새로운 값을 이용하여 본인확인을 하는 것이다. 대부분의 웹사이트들이 제공하는 본인확인 방법은 주민등록번호, 아이디, 패스워드, 인증서, 카드정보와 같은 고정된 정보에 의존하므로 고정된 정보의 경우 탈취됐을 경우에 악용 가능하다. 주민등록번호를 제외하고 다른 수단은 이용자가 탈취되었음을 인식하였을 경우 변경이 가능하지만, 이미 명의도용이나 허위사실 유포, 개인정보유출로 악용된 이후에 탈취를 인식될 수 있다. 본 논문에서는 개인정보 유출 원인으로 지목되는 무분별한 인터넷상 주민등록번호 수집 관행을 최소화하고 유출되었을 때 피해를 최소화하기 위해 OTP를 이용하여 비연결성을 보장하는 온라인 본인확인 방안을 제안한다.

먼저, 2장에서는 인터넷 상의 사용되고 있는 실명확인 서비스, 휴대폰, 인증서, 신용카드 정보를 사용한 본인확인 방법과 주민등록번호를 사용하지 않고 웹사이트에 회원가입을 하는 인증수단인 아이핀, 이메일을 통한 신원확인에 대해 분석을 하고, OTP의 기본개념에 대해 알아본다. 3장에서는 제안하는 OTP를 이용한 온라인 본인확인 방안을 논의한다. 4장에서는 기존의 방식과 비교하여 평가해 보고, 5장에서는 결론을 설명한다.

II. 온라인 본인확인 방법

본 장에서는 인터넷 상에 주민등록번호를 입력하는 본인확인 방법인 실명확인 서비스, 휴대폰, 인증서, 신용카드정보를 사용한 본인확인과 주민등록번호를 입력하지 않는 본인확인 방법인 이메일을 사용한 인증, 아이핀(i-PIN) 서비스를 사용한 본인확인에 대해 논의해보고, OTP의 기본개념에 대해 연구해보기로 한다.

2.1. 주민등록번호를 사용하는 온라인 본인확인 방법

2.1.1. 실명확인 서비스

실명확인 서비스를 통한 본인인증은 인터넷 웹사이트의 주민등록번호 오류검증 번호 검증방법의 문제점을 해결하기 위하여 이용자의 성명과 주민등록번호의 일치여부를 확인해주는 방법이다. 실명확인 서비스 업체인 신용평가 회사는 신용카드 발급, 금융계좌 개설, 휴대폰 개통 등에 사용된 성명과 주민등록번호 정보를 수집하여 구축한 데이터베이스와 한국정보통신산업협회의 실명 데이터베이스를 이용하여 성명과 주민등록번호를 비교하여 인증한다.

회원가입시 본인확인 절차는 이용자가 웹사이트 가입을 신청하면 이용자에게 본인 확인을 위해 이름과 주민등록번호를 요청한다. 이름과 주민등록번호를 전송하면 웹사이트에서 신용평가회사에게 이름과 주민등록번호를 보내어 실명확인을 요청한다. 신용평가회사는 실명확인 서버를 통해 입력한 이름과 주민등록번호가 데이터베이스에 존재하는지를 확인하여 결과 값

을 웹사이트에게 전송하여 본인확인을 완료한다[3].

실명확인 서비스를 통한 본인인증은 주민등록번호가 노출되었을 경우 위험하다. 옥션, GS칼텍스 등 여러 개인정보유출 사건을 통해 성명과 주민등록번호가 노출되었으므로 이를 악용할 경우 명의도용의 문제점이 있다.

2.1.2. 공인인증서 전자서명 인증 방법

공인인증서를 이용한 본인인증은 성명과 주민등록번호만 갖고 본인을 확인하는 실명확인 서비스의 문제점을 해결하기 위하여 공인인증서의 전자서명을 이용한다. 이용자는 공인인증기관 또는 등록대행기관을 방문하여 신원확인을 하고, 생성한 공개키와 개인키 쌍을 이용하여 공개키에 대응하는 개인키로 전자서명을 수행하여 공인인증서를 발급 받아야 인증이 가능하다. 공인인증서는 이용자가 신원확인 시에 제출한 주민등록번호를 이용자만이 알고 있는 비밀정보와 함께 이중 해쉬하여 공인인증서 안에 삽입하여 발급된다[4].

회원가입시 공인인증서를 이용한 인증 절차는 이용자가 웹사이트 가입을 신청하면 이용자에게 본인 확인을 위해 이름, 주민등록번호, 공인인증서, 이중 해쉬 검증정보 및 전자서명을 요청한다. 이용자가 이름, 주민등록번호, 공인인증서, 이중 해쉬검증정보 및 전자서명을 전송하면 웹사이트에서 전자서명을 검증하고, 공인인증기관에게 CRL을 전송받아 CRL에서 이용자 공인인증서 일련번호 존재유무 확인, 이용자의 성명 추출 및 주민번호 이중 해쉬 검증정보를 검증하여 본인확인을 완료한다[3].

공인인증서를 이용한 본인인증은 성명과 주민등록번호가 노출되었을 경우에도 공인인증서가 있어야하므로 실명확인 서비스에 비해 안전하다. 하지만, 고도화된 해킹이나 이용자 또는 발급자의 부주의로 인해 공인인증서와 패스워드가 탈취될 수도 있기 때문에 완벽히 안전하다고 할 수는 없다[5].

2.1.3. 휴대폰을 사용한 인증 방법

휴대폰을 이용한 인증은 성명과 주민등록번호과 휴대폰의 SMS를 인증 수단으로 사용한다. 회원가입시 인증 절차는 먼저 휴대폰을 소지한 이용자가 웹사이트 가입을 신청하면 이용자에게 본인 확인을 위해 이름, 주민등록번호, 통신사, 휴대폰 번호를 요청한다. 이용자가 이름, 주민등록번호, 통신사, 휴대폰 번호를 전송하면 웹사이트에서 PG(Payment Gateway, 지불 결제 사업자)에게 이름, 주민등록번호, 통신사, 휴대폰 번호를 보내어 본인확인을 요청한다. PG는 해당 이동통신사에게 이름, 주민등록번호, 휴대폰 번호를 전송한다. 이동통신사는 휴대폰번호 및 주민등록번호 데이터베이스를 확인하여 전송정보가 일치하면 전송된 휴대폰 번호로 SMS 발송번호를 전송한다. 이용자가 발송번호를 입력하면 PG를 거쳐 이동통신사에 전송되어 이전에 보냈던 SMS 발송번호와 비교하여 검증을 한다[6].

휴대폰을 이용한 본인인증은 성명과 주민등록번호 뿐만 아니라 휴대폰이 있어야 하므로 실명확인 서비스에 비해 안전하다. 또한, 무선이동통신 서비스 가입자는 5000만 명을 넘어 평균적으로 '1인 1폰'을 넘어서기 때문에 공인인증서에 비해 활용도가 높다[7]. 하지만 휴대폰을 이용한 본인확인도 악성코드와 같은 해킹을 통한 SMS 발송번호 탈취 또는 휴대폰 분실로 인한 개인정보유출의 위협을 갖고 있다. 고도화된 스마트폰의 보급에 따라 해킹을 통한 보안위협이 증대되고 있으며, 국내에서도 악성코드에 감염된 피해사례가 나타나고 있다[8].

2.1.4. 신용카드 정보를 사용한 인증 방법

신용카드 정보를 인증에 사용하는 방법은 신용카드 사명, 신용카드번호, 유효기간, 비밀번호 앞 2자리, 주민등록번호를 신용카드사에 보내어 신용카드사 데이터베이스를 조회하여 검증하는 방법이다. 신용카드를 이용한 웹사이트 가입시 본인인증 절차는 웹사이트에서 신용카드사명, 신용카드번호, 유효기간, 비밀번호 앞 2자리, 이름, 주민등록번호를 요청하여 전송 받는다. 이름과 주민등록번호는 실명확인으로 사용되고, 신용카드사명, 신용카드번호, 유효기간, 비밀번호 앞 2자리, 주민등록번호와 같은 신용카드 정보를 VAN을 통해 신용카드사에게 보내어 진다. 신용카드 정보는 신용카드사의 데이터베이스에서 비교하여 일치하는 정보가 있는지 조회를 하여 인증 결과 값을 VAN을 통해 웹사이트에게 전달하여 본인확인을 완료한다[3].

신용카드 발급건수는 8514만장으로 국내 경제활동인구의 대부분이 소지하고 있다[9]. 하지만, 신용카드를 통한 본인확인 서비스는 경제활동인구를 제외하는 경우 소지에 제한이 있고, 신용카드사명, 신용카드번호, 유효기간, 비밀번호 앞 2자리와 같은 신용카드 정보는 고정되어 있으므로 노출될 경우에 악용할 소지가

있다. 신용카드 정보는 해킹을 통한 위협뿐만 아니라 신용카드에 표기되어 있기 때문에 분실이나 오프라인 결제시에도 노출될 수 있다. 또한, 실명확인 서비스, 휴대폰 인증, 공인인증서를 사용한 본인확인 서비스와 마찬가지로 본인확인을 할 때 주민등록번호를 사용하기 때문에 '개인정보보호법 제24조(고유 식별정보의 처리 제한)'에서 기술한 웹사이트에서 회원 가입시 주민등록번호를 사용하지 않는 방법으로 사용할 수 없다.

2.2. 주민등록번호를 사용하지 않는 본인확인 방법

2.2.1. 이메일을 사용한 인증 방법

이메일을 이용한 인증은 사전에 가입된 이메일을 인증 수단으로 사용한다. 회원가입시 인증 절차는 먼저 이메일을 갖고 있는 이용자가 웹사이트 가입을 신청하면 이용자에게 본인 확인을 위해 이메일 주소를 요청한다. 이메일 주소를 전송하면 웹사이트는 본인확인 이메일을 이용자에게 전송한다. 이용자는 가입 신청시 입력한 이메일에 있는 웹사이트의 검증용 이메일을 받고 웹사이트에게 검증용 이메일 수신확인 정보를 전송하면 인증이 완료된다.

이메일을 이용한 인증은 주로 국외 웹사이트에서 사용하는 방법으로 국내 웹사이트에서는 사용되지 않는 방법이다. 이메일만 있으면 본인확인이 되기 때문에 인터넷이 되는 어디에서든지 인증을 받을 수 있는 장점을 갖고 있지만, 이메일의 아이디, 패스워드만 얻어내면 악용할 수 있을 뿐만 아니라 안전한 인증을 거치지 않고 가입이 가능한 이메일을 사용할 경우 명의도용과 회원들의 익명성에 의한 허위사실의 유포가 가능하다.

2.2.2. 아이핀(i-PIN)을 사용한 인증 방법

아이핀(i-PIN)은 방송통신위원회와 한국정보보호진흥원이 인터넷상의 과도한 주민등록번호 사용을 해소하기 위해 만든 가상주민번호로 아이디와 패스워드로 구성된다. 아이핀 서비스를 사용하기 위해서는 아이핀의 발급이 필요하다. 발급은 한국정보보호진흥원이 지정한 아이핀 서비스 업체에서 받을 수 있다. 발급과정은 먼저 아이핀 서비스 업체에 회원가입 요청을 하면, 성명과 주민등록번호를 포함한 회원정보를 입력하여 실명확인을 하고, 방문인증, 모바일을 통한 인증, 신용카드를 이용한 인증, 공인인증서를 사용한 인증과 같은 본인확인 수단을 선택하여 인증을 한다. 이용자는 본인확인 수단 중 하나를 선택하여 본인확인을 마치면 아이핀을 발급 받을 수 있다. 웹사이트 가입시 아이핀을 이용한 본인 확인 절차는 먼저 이용자가 웹사이트에 가입요청을 하면 웹사이트는 아이핀 ID와 패스워드를 입력을 요청한다. 이용자는 아이핀 ID와 패스워드를 입력하면 웹사이트는 이를 전송하여 아이핀 서비스 업체에 본인확인을 요청한다. 아이핀 서비스 업체는 데이터베이스를 조회하여 본인확인 결과를 웹사이트에게 보내어 본인확인을 완료한다[10].

2006년 10월 법률 개정을 통하여 서비스가 개시된 아이핀은 아이디, 패스워드를 통한 인증으로 본인확인 절차가 매우 간편하고 무료로 제공되고 있다. 국내의 웹사이트들은 아이디, 패스워드만으로 본인확인을 할 수 있기 때문에 주민등록번호를 사용하지 않는 본인확인 방안으로 제공하고 있다. 아이핀은 노출이 되더라도 폐기 및 재발급이 가능하므로 개인정보 유출로 인한 피해를 최소화할 수 있다. 하지만, 아이핀은 '10년 10월 기준 발급건수가 250만건으로 아직 이용자가 미비하고[11], 고정된 값인 아이핀 ID와 패스워드로 이루어지므로 노출될 경우에 명의도용과 개인정보유출로 악용될 수 있다. 이용자의 이메일의 아이디와 패스워드를 알고 있는 경우나 신용카드 정보를 알 경우, 스마트폰을 통한 해킹이 이루어 질 경우, 공인인증서를 탈취했을 경우에는 아이핀 재발급 과정을 통해 아이핀 ID와 패스워드 정보는 유출될 수 있다. 또한, 아이핀 서비스 업체의 관리자의 관리 실수나 아이핀 서비스 업체 데이터베이스 해킹이 이루어진다면 개인정보유출이 심각해 질 수 있다.

2.3. OTP의 기본 개념

2.3.1. OTP의 정의 및 생성 메커니즘

OTP(One-Time Password)에 의한 인증은 매번 인증이 필요 할 때마다 1회용 패스워드를 사용하는 방법으로 현재 사용하는 패스워드로부터 다음에 사용할 패스워드를 유추하는 것이 수학적으로 불가능한 특성을 가진다. [그림 1]은 OTP 생성메커니즘을 도식화한 것이다. 입력값은 OTP 생성 알고리즘의 입력 데이터로 서버와 OTP 토큰 간에 공유된 OTP 비밀키와 부가 정보로 구성된다. 부가 정보는 OTP 생성 시 사용되는 부가 정보 종류에 따라 질의/응답 방식, 시간 동기화 방식, 이벤트 동기화 방식, 조합 방식으

〔그림 1〕 OTP 생성 단계

로 구분된다. OTP 생성 알고리즘은 입력 값으로부터 OTP값을 생성해내는 알고리즘으로, 일방향 해시 함수 또는 대칭 키 알고리즘에 기반한다. OTP 추출 함수는 OTP 생성 알고리즘을 통해 출력된 값으로부터 실제 OTP로 사용할 OTP값 6~8자리 숫자를 뽑아내는 함수를 의미한다[12].

OTP를 사용한 온라인 본인확인 방식은 비연결성을 보장하는 인증 방법으로 기존의 아이디, 패스워드 인증방식에서 문제가 되었던 패스워드 재사용 공격, 패스워드 탈취 공격 등의 여러 공격들로부터 안전하다[13]. 이 때문에 금융권 전자금융거래, 기업체 사내시스템 접근통제, 인터넷 포털 사이트의 이용자 인증 등 여러 분야에서 활발하게 사용되고 있고, 금융권 전자금융거래에 사용되고 있는 OTP는 발급건수가 400만 건이 넘었다[14].

2.3.2. OTP의 보안 요구 사항

OTP의 생성 알고리즘은 표준 알고리즘을 기본적으로 사용해야 한다. 키 생성 알고리즘은 표준에서 권고하거나 표준에서 요구하는 테스트를 통과한 의사 난수 생성 알고리즘을 사용(예측 불가능성 만족)하고, 128비트 이상의 엔트로피를 갖는 seed 값을 사용한다. OTP 생성 알고리즘에 사용하는 대칭 키 암호 알고리즘은 보안 강도 112비트 이상의 표준 암호 알고리즘을 사용하고, 일방향 해시 알고리즘을 사용할 때는 보안강도 112비트이상의 해시 알고리즘을 사용한다. 일방향 해시 함수를 사용하는 것에 비해 해시 기반 메시지 인증 코드 기법을 사용하는 것이 상대적인 안전성을 제공하며, 이때 입력하는 OTP 비밀 키는 160비트 이상을 사용한다. 생성되는 OTP의 길이는 최소한 10진수 6자리 이상이어야 한다. 또한, 본문에서 제안한 OTP 기기는 하드웨어 OTP이기 때문에 일련번호의 유일성을 보장해야 하고, OTP 비밀 키 및 부가 정보는 OTP 토큰 외부로 노출되지 않도록 보장해야 한다. OTP 비밀키는 토큰별로 유일해야 하며 OTP 비밀 키를 생성한 이후, 업체에서는 비밀 키를 주입하기 전에 유일성 테스트를 수행하여 중복이 없음을 확인해야 한다[12].

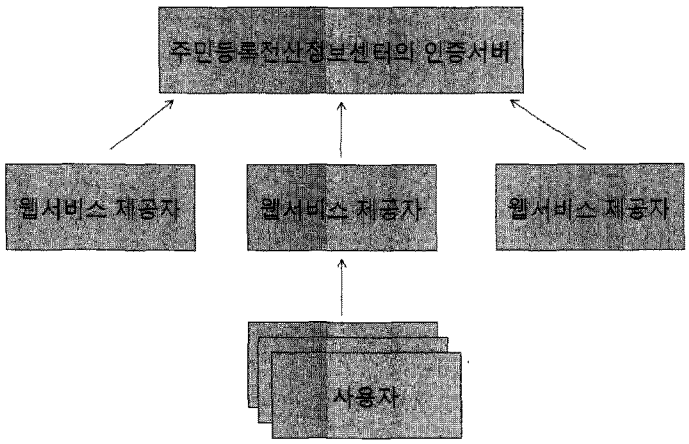
III. 제안하는 온라인 본인확인 모델

국내에 대부분의 웹사이트들은 아이핀 서비스와 실명확인 서비스와 모바일, 인증서, 카드정보를 이용한 인증을 연계한 온라인 본인확인 방법을 가입시 제공하고 있다. 하지만, 아이핀 서비스는 이용자의 발급이 미비한 상태이고, 아이핀 ID와 패스워드가 유출될 경우에 명의도용이 가능하다. 실명확인 서비스와 모바일, 인증서, 카드정보를 이용한 인증을 연계한 온라인 본인확인 방법의 경우에는 대포폰, 스마트폰의 해킹, 이용자 부주의로 인한 인증서 탈취, 카드정보 탈취 등으로 인한 위협이 존재한다. 또한, 현재 사용되고 있는 모든 온라인 본인확인 방법은 주민등록번호를 포함한 개인정보를 유지하고 있는 데이터베이스 유출의 가능성이 있다. 이를 보완하기 위해 본 장에서는 논문에서 제안하는 OTP를 이용하여 비연결성을 보장하는 온라인 본인확인 방안에 대해 논의해보기로 한다.

3.1 용어 정의

이 절에서는 제안하는 온라인 본인확인 방안에 사용하게 될 용어를 설명한다.

- 주민동록전산정보센터의 인증서버 : 서비스 제공자인 정부의 주민동록전산정보센터가 운영하는 OTP 인증서버로 OTP 인증 요청에 대한 검증 기능(패스워드, OTP 검증요청번호를 검증)을 수행
- OTP 토큰 : 일회용 패스워드를 생성하는 기기
- OTP 일련번호 : OTP 토큰 각각의 유일한 번호
- OTP 비밀정보 : 이용자와 인증서버 간에 공유된



[그림 2] 제안하는 OTP 서비스 모델

비밀키로 OTP 생성 알고리즘에 사용
- 패스워드 : 이용자가 OTP 발급시 정하는 기억할 수 있는 고정된 비밀번호, 이용자는 인증과정에서 OTP 검증요청번호와 같이 전송하여 검증에 사용
- 인증요청번호 : 인증서비스 대상을 구분하기 위한 번호(웹사이트 식별자 || 시퀀셜 넘버)
- OTP 검증요청번호 : 이용자 인증을 위해 OTP 기기에서 생성되는 일회용 패스워드

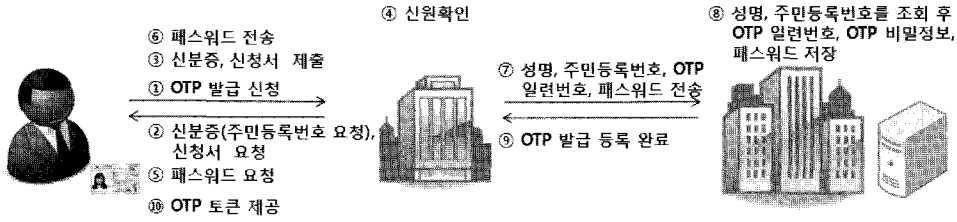
3.2 제안하는 OTP의 발급과정 및 본인확인 절차

제안하는 온라인 본인확인 방안에서는 OTP 인증서비스를 제공하고자 하는 기관은 정부가 되고 OTP 인증서버는 정부의 주민등록전산정보센터가 관리한다. 서비스 제공자인 정부는 온라인 확인 절차가 악용되지 못하도록 신뢰할 수 있는 웹사이트일 경우에만 제안하는 온라인 본인확인 서비스를 이용할 수 있도록 웹사이트를 사용할 수 있도록 해야 한다. [그림 2]는 제안하는 OTP 서비스 모델을 도식화 한 것이다.

주민등록전산정보센터는 OTP 기기를 토큰 공급자에게서 받으면 OTP 일련번호와 검증번호생성을 위한 비밀키를 안전하게 등록 및 보관해야 한다[15]. OTP 인증서비스를 제공하고자 하는 정부의 기관인 읍, 면, 동 사무소는 이용자에게 나누어 줄 OTP 기기를 주민등록전산정보센터에 일련번호와 검증번호생성을 위한 비밀키를 등록한 이후에 분배받는다. [그림 3]은 OTP를 발급받는 절차이다.

1) 이용자는 OTP 기기를 발급하기 위해 읍, 면, 동 사무소에 방문을 하여 발급요청을 한다.
2) 읍, 면, 동 사무소의 OTP 발급 담당자는 신분증, 신청서를 요청한다.
3) 이용자는 신청서류를 작성 후 신분증과 제출한다.
4) 담당자는 신원확인을 한다.
5) 담당자는 이용자가 사용할 패스워드를 요청한다.
6) 이용자는 자신이 사용할 패스워드를 입력장치를 통해 직접 입력하여 정한다.
7) 담당자가 입력한 성명, 주민등록번호와 OTP 일련번호와 사용자가 입력한 패스워드가 주민등록전산정보센터의 데이터베이스에 전송된다.
8) 주민등록전산정보센터는 데이터베이스에서 OTP 발급을 요청한 이용자를 찾아 OTP 일련번호, 일련번호에 대응하는 비밀키와 패스워드를 등록한다. 등록시 OTP 비밀키는 해쉬나 암호화를 통해 식별할 수 없게 저장한다.
9) 주민등록전산정보센터는 OTP 발급 등록이 완료되었음을 읍, 면, 동 사무소에 알린다.
10) 담당자는 등록된 OTP 기기를 이용자에게 지급하여 발급을 완성한다.

이용자는 OTP 기기를 분실 또는 도난을 당할 경우 악용될 수 있으므로 패스워드를 사용하여 패스워드를 알고 있는 이용자만이 OTP 기기를 사용할 수 있게 하였다. 이용자는 OTP 기기를 분실 또는 도난을 당하면 재발급을 받아야 하고, 재발급 절차는 다음과 같다. 이용자는 읍, 면, 동 사무소에 재방문하여 신원확인을 한 후 OTP에 사용할 패스워드를 정한다. 주민등록전산정보센터에 이용자 성명, 주민등록번호, OTP 일련번호와 패스워드를 전송한다. 주민등록전산정보센터는 데이터베이스에서 요청한 이용자를 찾아 기존의 OTP 일련번호와 비밀키의 정보를 삭제하고 새로운 OTP



주민등록전산정보센터의 데이터베이스

성명	주민번호	OTP 일련번호	OTP 비밀키	패스워드	...
홍길동	830123-1234567	123456	ABC90B QWEU9C	1234	...
김철수	900223-1987654	234567	V5C9NE G2TY1Y	2345	...
이영희	761212-2234567	345678	4BRRQ1 3ECTK2	1573	...
...	...	...	...	...	...

〔그림 3〕 제안하는 OTP 발급 절차

일련번호와 비밀키를 등록한다. 주민등록전산정보센터는 OTP 발급 등록이 완료되었음을 읍, 면, 동 사무소에 알리고 새로 등록된 OTP 기기를 이용자에게 지급하여 재발급을 완성한다.

〔그림 4〕는 제안하는 OTP를 이용하여 온라인 본인확인을 하는 과정이다.

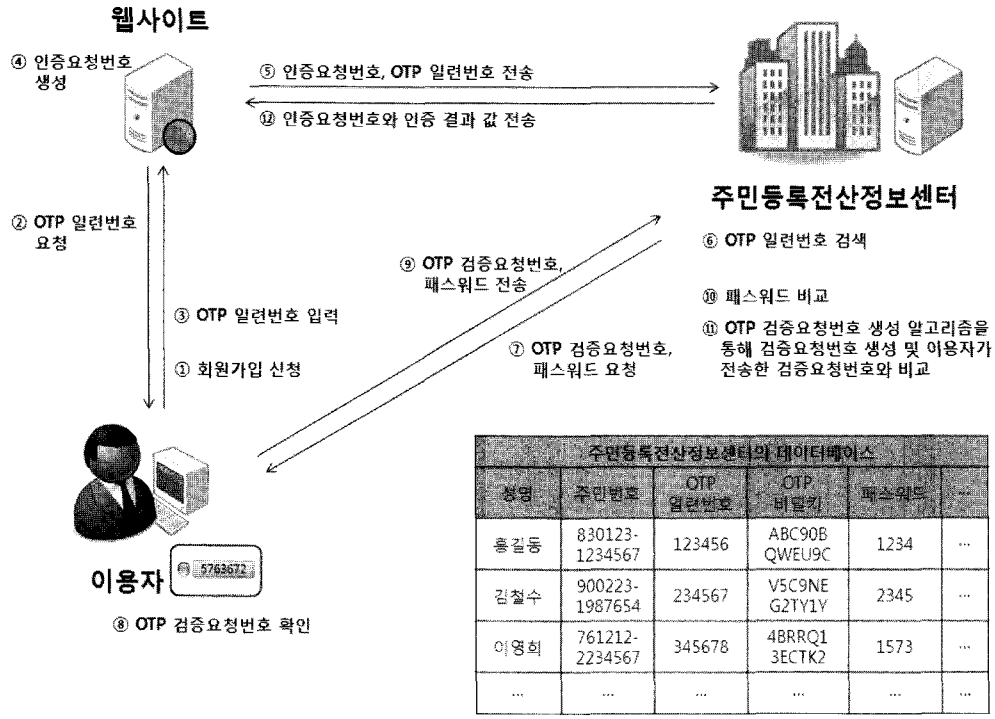
1) 이용자는 웹사이트에 가입을 요청한다.
2) 웹사이트는 OTP 일련번호를 요청한다.
3) 이용자는 OTP 일련번호를 입력한다.
4) 웹사이트는 인증요청번호를 생성한다.
5) 웹사이트는 인증요청번호와 OTP 일련번호를 주민등록전산정보센터에게 전송한다.
6) 주민등록전산정보센터는 OTP 일련번호를 검색한다.
7) 주민등록전산정보센터는 OTP 검증요청번호와 패스워드를 요청한다.
8) 이용자는 OTP 검증요청번호를 생성하여 확인한다.
9) 이용자는 OTP 검증요청번호, 패스워드를 전송한다.[1)]
10) 주민등록전산정보센터는 패스워드를 비교한다.
11) 주민등록전산정보센터는 OTP 검증요청번호 생성 알고리즘을 통해 검증요청번호 생성 및 이용자가 전송한 검증요청번호와 비교한다.
12) 주민등록전산정보센터는 인증요청번호와 인증결과 값을 웹사이트에게 전송하여 본인확인을 완료한다.

3.3 제안하는 OTP 활용방안

MOTP(Mobile One Time Password)는 OTP의 토큰은 전용 장치를 사용하지 않고, OTP 생성 알고리즘이 소프트웨어 모듈로 모바일 기기에 탑재된 형태를 의미한다〔12〕. 모바일 OTP의 연구는 현재에도 계속되고 있으며, 보안성과 안전성이 보장되는 모바일 OTP 방식이 개발될 경우 제안한 OTP 본인확인 서비스를 모바일에 탑재한다면 보안성과 안전성을 지키면서 기기를 소지해야 하는 불편과 비용을 줄일 수 있다.

다른 방안으로 카드형 OTP를 사용할 경우 OTP 생성과 디스플레이를 하기 위한 전력이 필요하다. 현재 사용하고 있는 카드형 OTP의 경우 수명은 3년 이내이므로 짧아서 재발급의 불편함을 갖고 있다. 이를 개선하기 위해 배터리의 충전을 위해 전자주민등록증에 전력을 제외한 데이터를 주고 받을 수 없는 충전단자를 사용한다〔16〕. 또는 근접통신(NFC) 기술을 사용하여 OTP를 생성하여 NFC 리더기로 받아오는

1) 패스워드 전송 및 검증으로 인해 주민등록전산정보센터 서버의 부하가 크다고 판단될 경우, 입력 자판을 탑재한 OTP 기기를 사용하여 OTP 기기 상에서 PIN을 검증하는 방안으로 대체할 수 있다. 하지만, 이러한 방안은 OTP 기기 단가 상승의 요인으로 작용할 수 있다.



주민등록전산정보센터의 데이터베이스

성명	주민번호	OTP 일련번호	OTP 비밀키	패스워드	...
홍길동	830123-1234567	123456	ABC90B QWEU9C	1234	...
김철수	900223-1987654	234567	V5C9NE G2TY1Y	2345	...
이영희	761212-2234567	345678	4BRRQ1 3ECTK2	1573	...
...	...	...	...	...	...

〔그림 4〕 제안하는 OTP를 이용한 본인확인 절차

방식을 활용할 수 있다. PC에 NFC 리더기가 설치된 경우나 스마트폰에 NFC 칩이 장착될 경우 OTP를 받아 올 수 있다[17].

카드형 OTP는 행정안전부가 추진 중인 전자주민등록증에 내장하여 활용할 수 있다. 행정안전부는 주민등록증의 경신이 가까워짐에 따라 2012년까지 새로운 전자주민등록증 설계 및 발급을 추진하고 있는 중이다. 전자주민등록증은 기존의 플라스틱 증에 위·변조 문제와 개인정보 노출 문제를 개선하기 위한 방안으로 주민등록증 속에 전자칩(IC칩)을 장착하여, 전자칩 안에는 주민등록증 기능에 맞게 신원확인항목 만을 수록할 계획이다. 〔표 1〕은 현행과 신설될 주민등록증의 수록항목이다[18].

현재의 안에 따르면 발행번호를 주민등록번호 대신 사용하여 주민등록번호 유출 및 오·남용 방지를 줄여 나갈 계획이다. 발행번호는 일반 오프라인 업무에서 사용되고 온라인 업무시 아이핀(i-PIN)과 유사한 방식으로 주민등록번호의 대체용으로 사용된다. 하지만, 아이핀과 같이 고정된 값인 발행번호와 패스워드로 이루어지므로 노출될 경우에 명의도용과 개인정보유출로 악용될 수 있다. 본문에서 제안하는 OTP를 전자주민등록증에 도입한다면 인증시마다 새로운 값을 본인확인 수단으로 사용하기 때문에 고정된 정보가 노출이 될 경우에도 안전성이 보장된다. OTP를 현재 추

〔표 1〕 주민등록증 수록 항목

구분	현행 항목	전자주민등록증 항목	
		기 존	신 설
표면	① 성명 ② 사진 ③ 주민등록번호 ④ 주소 ⑤ 지문 ⑥ 발행일 ⑦ 주민등록기관 ※ 혈액형(주민신청시)	① 성명 ② 사진 ③ 주소 ④ 발행일 ⑤ 주민등록기관 ※ 혈액형(주민신청시)	⑥ 생년월일 ⑦ 성별 ⑧ 발행번호 ⑨ 유효기간 ⑩ 국외이주국민(해당자만 기재)
IC칩	-	주민등록번호, 지문, 성명, 사진, 주소	생년월일, 발행번호

진 중인 전자주민등록증에 포함하기 위해서는 전자주민등록증의 유일성을 보장하는 발행번호를 제안하는 OTP의 일련번호로 사용하고, IC 칩에 OTP 생성 모듈을 내장한다.

IV. 토의 및 평가

본 장에서는 2장에서 언급했던 현재 사용되고 있는 온라인 본인확인 방안과 논문에서 제안하는 온라인 본인확인 모델에 대하여 비교하여 토의 및 평가한다. [표 2]는 온라인 본인확인 방안과 제안하는 모델의 내용이다. 제안하는 방안은 주민등록번호를 사용하지 않는 본인확인 방법으로 처음 발급받을 때 물리적으로 신원을 확인한 후에 발급하기 때문에 OTP 기기를 발급할 때 명의도용하기 어렵고, OTP를 사용하여 비연결성을 보장하는 본인확인을 함으로써 고정된 정보인 일련번호와 패스워드가 해킹을 통해 유출될 경우에도 악용될 가능성이 매우 낮다[5]. 또한, 물리적으로 OTP 기기를 도난이나 분실하였을 경우에도 패스워드를 알아야 본인인증이 가능하기 때문에 악용하기 어렵다. 현재 사용되고 있는 온라인 본인확인 서비스 중 대부분의 경우 주민등록번호를 포함한 민감한 정보를 각 인증기관의 데이터베이스에 유지한다. 그러므로 인증기관 중 하나라도 개인정보유출사고가 터질 경우 모든 기관에서 유출되는 것과 같은 파급 효과를 가져 올 수 있다. 하지만 제안하는 방식은 민감한 주민등록번호를 주민등록전산정보센터에서만 유지하기 때문에 주민등록전산정보센터의 안전성만 보장된다면 민감한 개인정보의 유출 위협이 감소한다.

NIST 전자 인증 가이드라인 표준문서는 인증시 사용하는 토큰에 따라 보증레벨을 4단계로 분류하였다. 주민등록번호를 사용하지 않는 본인확인 방법 중, 이메일과 아이핀을 통한 본인확인은 아이디와 패스워드만을 사용하는 'Memorized Secret Token'이므로 레벨 2가 된다. 반면, 제안하는 방안은 패스워드와 OTP를 사용하여 'Memorized Secret Token'와 'Single Factor One Time Password Device'를 사용한 Multi-Token Authentication이므로 레벨 3가 된다. 주민등록번호를 사용하지 않는 본인확인인 아이핀이나 이메일에 비해 보증레벨이 높아 이용자에게 신뢰성을 제공할 수 있다[19].

제안하는 온라인 본인확인 모델은 다른 온라인 본인확인 방법들에 비하여 OTP 기기의 사용을 통해 높은 보안성을 보장하며, 민감한 정보인 주민등록번호의 사용을 감소시키고, OTP와 패스워드를 같이 사용하여 인증하므로 기기 분실시 발생할 수 있는 문제점을 줄인다. 또한, 주민등록번호 사용의 감소를 통해 민감한 DB 관리의 어려움을 줄일 수 있다. 이에 반해 제안 모델은 몇 가지의 문제점들을 갖고 있다. OTP를 사용하기 위해 주민등록전산정보센터 내에 OTP 검증 서버가 있어야 하므로, OTP 검증 서버를 새로 만들어 유지하기 위한 비용과, 이용자들에게 새로이 발급되는 OTP 기기들로 인한 비용 등 추가적인 비용이 소요된다는 문제를 갖고 있다. 하지만, 개인정보보호의 중요성이 갈수록 높아지는 현 시점에서 제안하는 방안을 통해, 이용자들에게 한층 강화된 개인정보 보

[표 2] 다양한 온라인 본인확인 방식과 제안한 방식의 비교

방안 / 구분	실명확인	공인인증서	휴대폰 SMS	신용카드 정보	아이핀	이메일	제안방안
주민번호 사용여부	주민등록번호를 사용하는 본인확인				주민등록번호를 사용하지 않는 본인확인		
본인확인 방법	성명과 주민등록번호	전자서명 및 이중 해쉬 검증 값	SMS 발송번호 및 주민등록번호	신용카드정보 및 주민등록번호	아이핀 ID와 패스워드	이메일 주소	OTP 일련번호, 검증요청번호 및 패스워드
명의도용 방법	성명과 주민등록번호	개인키 및 주민등록번호	휴대폰 및 주민등록번호	신용카드번호, 비밀번호 2자리 및 주민등록번호	아이핀 ID와 패스워드	아이디와 패스워드	OTP 기기와 패스워드
민감한 정보	주민등록번호	이중 해쉬 검증 값	주민등록번호	카드번호, 유효기간, 비밀번호 및 주민등록번호	아이핀 ID와 패스워드	아이디와 패스워드	OTP 일련번호, 패스워드
민감한 DB 관리	신용평가회사	공인인증서 발급기관	이동통신사	신용카드사	아이핀 사업자	이메일 서비스 업자	주민등록전산정보센터
보증레벨	레벨 1	레벨 4	레벨 3	레벨 3	레벨 2	레벨 2	레벨 3

호 방안을 제공할 수 있다면, 소요되는 추가적인 비용은 합리적이라 판단된다.

V. 결 론

2002년 인터넷 동창회 사이트에 가입한 회원의 개인 정보가 해킹된 데 이어 2008년 최대 규모의 옥션 회원의 개인정보가 유출된 사건, GS칼텍스, 하나로텔레콤을 비롯해 여러 통신사와 인터넷포털 등 개인정보 침해사고가 계속해서 이어져 왔고, 2011년 4월에 현대캐피탈에 대한 해킹으로 42만 명의 고객정보와 1만 3천여 명의 신용정보 유출사건이 발생하는 등 개인정보 유출위협은 점점 더 심각해지고 있지만, 대비책이 미흡한 상황이다[20]. 본 논문에서 제안하는 OTP를 사용한 비연결성을 보장하는 온라인 본인확인 서비스는 인증시 고정된 정보만을 사용하는 현재 사용되고 있는 온라인 본인확인 방안의 문제점을 극복할 수 있고, 민감한 정보가 사설 기관이 아닌 주민등록전산정보센터에서만 유지되게 하여 개인정보 유출 위협을 줄일 수 있다. 또한, 제안하는 방식은 최근 연구가 활성화되고 있는 MOTP나 행정안전부에서 도입을 추진중인 전자주민등록증과 연계하여 서비스를 할 경우 전국민을 대상으로 보급되어 활용될 수 있으므로, 개인정보보호 유출의 위협과 주민등록번호 오남용을 줄이는데 이바지 할 것이다.

참고문헌

[1] 개인정보보호법, 법률 제10465호, 제정 2011.3.29.

[2] A. Pfitzmann and M. Hansen. "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology," http://dud.inf.tu-dresden.de/Anon_Terminology.shtml, Feb. 2008.

[3] 정찬주, 김승주, 원동호, "금융보안 OTP를 이용한 온라인 본인확인 방안에 대한 연구," 한국정보보호학회지, 18(5), pp. 73-83, 2008년 10월.

[4] 한국정보보호진흥원, "식별번호를 이용한 본인확인 기술규격," 전자서명인증체계 기술규격, 2002년 10월

[5] MBC, " '만능인증서' 범용 공인인증서..범죄 악용 위험," MBC TV 사회 보도자료, http://www.imbc.com, 2011년 2월

[6] 강경석, 민상원, 심상범, "VM의 자동 변수 생성 방식 기반 모바일 지급결제 시스템," 한국정보과학회 논문지 12(6), pp. 367-378, 2006년 12월

[7] YTN, "스마트폰 가입자 1,000만 대... "모바일 비즈니스 인프라 구축"," YTN 경제 보도자료, http://www.ytn.co.kr, 2011년 3월.

[8] 이데일리, "스마트폰 앱 악성코드가 늘고 있다," 이데일리 IT 보도자료, http://www.edaily.co.kr, 2011년 3월

[9] 아주경제, "카드 이용실적, 2003년 카드사태 수준 급증," 아주경제 경제 보도자료, http://www.ajnews.co.kr, 2011년 3월.

[10] 장인용, 염흥열, "인터넷상의 본인확인수단인 아이핀의 활성화 방안 연구," 한국정보보호학회지, 19(5), pp. 81-94, 2009년 10월

[11] SBS, "주민번호 대신 '아이핀'으로 개인정보 유출 예방," SBS TV 경제 보도자료, http://www.sbs.co.kr, 2010년 11월

[12] TTA, "일회용 패스워드(OTP) 토큰 보안 요구사항," TTAK.KO-12.0130, 2010년 12월

[13] TTA, "일회용패스워드(OTP) 통합인증 서비스 프레임워크," TTAK.KO-12.0128, 2009년 12월

[14] DATANET, "OTP 관련 모든 궁금증, 인터넷으로 쉽게 푼다," DATANET 보도자료, http://www.datanet.co.kr, 2010년 9월

[15] TTA, "일회용 패스워드(OTP) 키 컨테이너, "TTAK.KO-12.0129, 2010년 12월

[16] Seok Koh and Heongsin Kim, "CARD BATTERY AND CARD BATTERY CONNECTOR," United States Patent Application Publication, US 2010/0209761 A1, Aug. 2010.

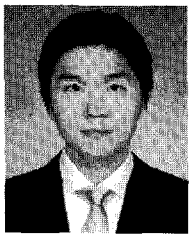
[17] 임선희, 전재우, 정임진, 이옥연, "NFC 보안 기술 분석 및 UICC 적용 효과 연구," 한국통신학회논문지, 36(1), pp. 29-36, 2011년 1월

[18] "전자주민등록증 도입 추진방안," 행정안전부, 2011년 3월

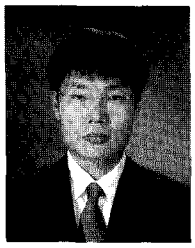
[19] NIST, "Electronic Authentication Guideline", NIST Special Publication 800-63-1, December 2008.

[20] 매일경제, "현대캐피탈 해킹…금감원 특별감사",매일경제 보도자료, http://www.mk.co.kr, 2011년 4월

〈著者紹介〉



김 정 동 (Jung-Dong Kim) 종신회원
2010년 2월: 경북대학교 컴퓨터공학과 졸업
2010년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 정보보호 정책, e-financial 보안, 스마트폰 보안, 네트워크 보안



조 관 태 (Cho, Kwan Tae)
2005년 2월: 고려대학교 컴퓨터학과(학사)
2005년 3월~2008년 2월: 고려대학교 정보보호대학원 (공학석사)
2008년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 USN 보안, VANET 보안, 키 교환

이 동 훈 (Lee, Dong Hoon)
1983년 8월: 고려대학교 경제학과(학사)
1987년 12월: Oklahoma University 전산학 대학원(공학석사)
1992년 5월: Oklahoma University 전산학 대학원(공학박사)
1992년 8월: 단국대학교 전자계산학과 전임강사
1993년 3월~1997년 2월: 고려대학교 전산학과 조교수
1997년 3월~2001년 2월: 고려대학교 전산학과 부교수
2001년 2월~현재: 고려대학교 정보경영공학전문대학원 교수
〈관심분야〉 암호프로토콜, 암호이론, USN 이론, 키 교환, 익명성 연구, PET 기술