주민등록번호 수집금지에 따른 온라인 본인인증 기법 연구

손승완* · 김광석* · 이강수*

*한남대학교

A Study on Online Authenticate Themselves Techniques according to Resident Registration Number collect Prohibited

Seung-wan Son* · Kwang-seok Kim* · Gang-soo Lee*

*Hannam University

E-mail : son2898@hnu.ac.kr

요 약

2013년 2월 18일부터 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제 23조의 2항에 의하여 정보통신서비스 제공자는 주민등록번호를 수집할 수 없게 되었다. 이러한 법령 개정에 따라 주민등록번호를 대신하여 휴대폰 인증, I-PIN인증, 공인인증서 인증, OTP 인증과 같은 대체수단을 사용하게 되었다. 본 논문에서는 주민등록번호를 대체한 온라인 본인인증 기법을 소개하고 IMEI와 OTP를 이용한 온라인 본인인증 기법을 제안하고자 한다.

ABSTRACT

From February 18, 2013, an information and communications service provider, we will not be able to collect the resident registration number by paragraph 2 of Article 23 of the Act on the Promotion of the use and protection of information and information network. Rather than a revision in accordance with resident registration number, than these laws, it had been used in the alternative, such as OTP authentication phone authentication I-PIN authentication of certificates that are recognized as such authentication. In this paper, we propose a new online identity authentication technology was and Utilization of IMEI, the OTP to introduce online identity authentication technology replacing the resident registration number.

키워드

개인정보보호, 본인인증, IMEI, OTP

Ⅰ. 서 론

최근 개인정보 유출이 사회의 큰 문제로 대두되고 있다. 온라인 포털 사이트 해킹을 통한 개인정보 유출, 악성코드 배포를 통한 개인정보 유출 등 개인정보 유출은 현대 사회에 심각한 문제로 자리 잡았다.

이에 따라 정부에서는 2013년 2월 18일부로 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제 23조 2항을 제정 정보통신 서비스 제공자는 이용자의 개인 주민등록번호를 수집 및 이용을 금지 시켰다.

주민등록번호가 수집 금지됨에 따라 이를 대체하는 여러 가지 온라인 본인인증 기법이 사용되고 있다. I-PIN(Internet Personal Identification Number)인증, 휴대폰 인증, 공인인증서 인증, OTP(One Time Password)인증 등은 차세대 온라

인 본인인증 기법으로 각광받고 있는 기술이다.

표 1. 정보통신망 이용촉진 및 정보보호 등에 관한 법률[1]

정보통신망법	
제23조의2 (주민등록번호의 사용제한)	① 정보통신서비스 제공자는 다음 각호의 어느 하나에 해당하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용할 수 없다.
	1. 제23조의 3에 따라 본인확인기관으로 지정받은 경우 2. 법령에서 이용자의 주민등록번호 수집·이용을 허용하는 경우 3. 영업상 목적을 위하여 이용자의 주민등록번호 수집·이용이 불가피한 정보통신서비스 제공자로서 방송통신위원회가 고시하는경우
	② 제1항제2호 또는 제3호에 따라 주민등록번호를 수집·이용할 수 있는 경우에도 이용자의 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법(이하"대체수단"이라한다)을 제공하여야 한다.

본 논문에서는 주민등록번호 수집금지에 따른 대체 온라인 본인인증 기법을 소개하고, IMEI (international mobile equipment identity)와 OTP를 이용한 본인인증 기법을 제안한다.

II. 관 련 연 구

2.1 I-PIN(Internet Personal Identification Number)

I-PIN이란 인터넷 상에서 주민번호를 대신하여 아이디와 패스워드를 이용하여 본인확인을 하는 수단이다. I-PIN은 현재 서울신용평가정보, 나이스신영평가정보, 코리아크레딧뷰로, 공공아이핀센터 4곳에서 발급이 가능하다.

기존의 I-PIN은 각 발급기관마다 연동이 불가능하여 발급기관을 암기해야하는 불편함이 있었으나, 현재의 I-PIN(I-PIN2.0)에서는 각 발급기관마다 연계가 가능하도록 되어있다.[2]

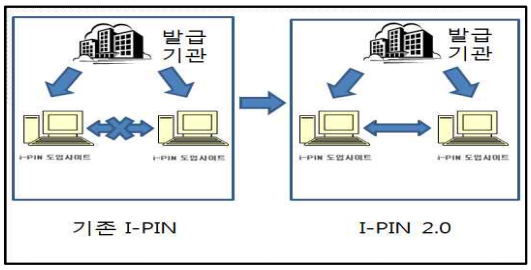

그림 1. 기존I-PIN 과 I-PIN 2.0

I-PIN을 이용 시 주민등록번호 유출을 예방할 수 있고 본인확인을 강화할 수 있다.

표 2. I-PIN과 주민등록번호 실명확인 비교 [2]

	I-PIN인증	주민등록번호 실명확인
검증방법	주민등록번호 실명확인 + 신원확인	주민등록번호 + 이름 일치여부 확인
주민등록번호 저장	웹사이트에 저장 안됨	개별 웹사이트에 저장
유출위험	주민등록번호 외부 노출 가능성 적음 .I_PIN 노출 시 폐지/신규발급 가능	주민등록번호 외부노출 가능성 많음
	주민번호 노출 시 변경 불가능	
사용방법	신원확인 후 본인확인기관에서 I-PIN발급	웹사이트에서 본인 확인 시 주민번호 사용
	웹사이트에서 본인확인 시 I-PIN 아이디/비밀번호 사용	

2.2 휴대폰 인증

휴대폰 본인인증 서비스는 인터넷상에서 주민번호를 대신하여 이용자의 최소 입력정보인 생년월일, 성명, 휴대폰번호를 이용해 실명확인 및 본인확인이 가능한 서비스이다. [3]

그림 2. 한국모바일인증(주) 휴대폰인증 제공창[3]

그림 2 에서와 같이 본인의 실명과 주민등록번호로 가입한 휴대폰을 이용하여, 기본적인 최소 입력정보의 입력만으로 휴대폰 본인인증이 가능하다. 인증 시에는 휴대폰 SMS 서비스를 통해 인증번호가 발송되고 인증번호를 입력 시에 본인인증이 되도록 되어있다.

2.3 공인인증서 인증

공인인증서란 우리가 일상생활에서 신원을 확인하거나 거래를 하려고 할 때, 주민등록증이나 인감 날인 또는 서명 등이 필요하듯이, 온라인 상에서 거래를 증명하거나 신원확인이 필요할 때 주민등록증을 대신하여 이를 확실히 보장해 주는 온라인 본인인증 수단이다.

공인인증서에는 소유자 이름(주민등록상 이름), 일련번호(주민등록번호), 소유자의 공개키(주민등록증 지문), 인증기관 전자서명(주민등록증 동사무소 날인) 등의 정보가 암호화되어있다. 이 인증서를 사용함으로 온라인 상에서도 주민등록증과 같은 기능을 수행한다.

이 공인인증서를 사용 시 암호화 되어있는 정보를 통해 개인정보 누출을 예방할 수 있다.[4]

표 3. 공인인증서 활용시의 장점

공인인증서 활용시의 장점
전자서명 인증을 통한 상대방의 신원확인
전자문서 교환에 따른 위/변조방지
전자문서 수신에 대한 부인방지
데이터 암호화를 통한 정보의 비밀성 유지

2.4 OTP(One Time Password)

OTP란 무작위로 생성되는 나수의 일회용 패스워드를 이용하는 사용자 인증 방식이다. 보안을 강화하기 위하여 도입한 시스템으로, 온라인 상에서 로그인 할때마다 일회성 패스워드를 생성하여 동일한 패스워드가 반복해서 사용됨으로 발생하는 보안상의 취약점을 극복하기 위해 도입되었다.[5]

OTP의 인증 방법은 다음 그림 3과 같다.

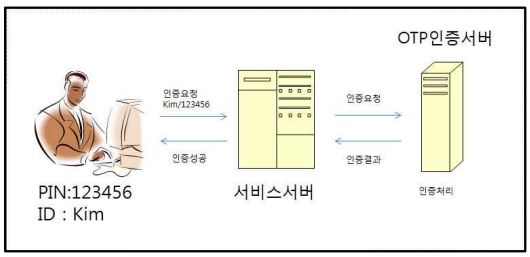

그림 3. OTP 인증 Flow[6]

사용자는 ID와 함께 발급받은 OTP Token에 표시된 OTP 값과 PIN을 입력한다. 사용자에게 서비스를 제공하는 서버는 사용자의 입력정보를 OTP인증서보로 전송하고, 인증서버에서는 사용자가 입력한 OTP값과 인증서버에서 계산한 사용자의 OTP값이 동일한지 확인한다. 사용자가 정상적으로 OTP값을 입력하면 인증서버에서 계산한 OTP값이 동일하며 인증에 성공하게 되고 사용자는 정상적으로 서비스를 이용할 수 있다.[6]

현재에는 유심기반 OTP기술이 개발되어 유심칩을 이용한 유심기반 OTP가 상용화 되어, 한층 더 강화된 안전한 OTP를 이용할 수 있다.

III. IMEI와 OTP를 이용한 본인인증 기법

본 논문에서는 온라인 본인인증 기법의 한 방법으로 IMEI와 OTP인증을 결합한 본인인증 기법을 제안한다.

IMEI란 국제 모바일 기기 식별 코드로 스마트

폰마다 할당되는 유일한 식별자이며 표x와 같이 15자리의 숫자로 구성되어 있다.[7]

표 4. IMEI의 구성[7]

정보	TAC	SNR	Spare
크기	8bit	6bit	0 or 1 bit
TAC : Type Allocation Code			
SNR : Serial Number			

이 IMEI와 OTP를 조합하여 사용하면 해당 스마트폰에 대한 유일한 식별자에만 OTP 생성기를 설치하여 본인인증을 할 수 있다. 본 논문에서 제안된 IMEI와 OTP를 이용한 본인인증 기법의 구성도는 그림4 와 같다.

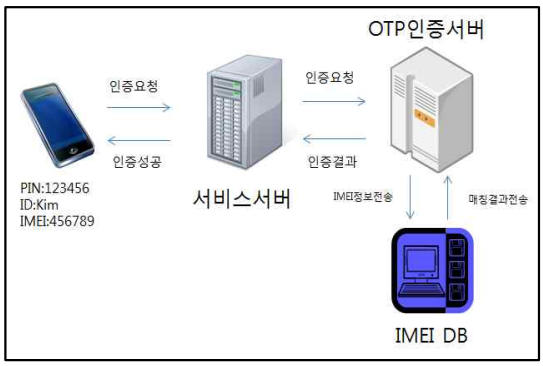

그림 4. IMEI를 이용한 OTP 인증 Flow

OTP생성기가 설치되어 있는 스마트 폰에서 기존의 OTP를 사용하는 것과 같이 인증을 요청하게 되면, 스마트폰 고유 식별 넘버인 IMEI 정보가 같이 전송이 된다. OTP서버에서는 IMEI DB 검색을 통해서 인증요청된 사용자가 고유의 기기를 사용하고 있는지 검색을 하게 되고 매칭이 될 겨우 정상적인 서비스를 이용가능하게 한다.

이 기법의 특징은 다음 표와 같다.

표 5. IMEI를 이용한 OTP 본인인증의 특징

IMEI를 이용한 OTP 본인인증의 특징
고유의 기기(스마트폰) 에만 OTP인증기를 설치하여 특정 기기에서만 인증이 가능.
휴대폰 인증, OTP인증 I-PIN인증의 장점을 모두 갖추고 있음.

Ⅳ. 결 론

본 논문에서는 주민등록번호 수집금지에 따른 새로운 온라인 본인인증 기법과 IMEI와 OTP를 이용한 본인인증 기법을 제안하였다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률의 제정으로 인해 주민등록번호의 수집이 제한되었고, 주민등록번호를 대체하기 위해 다양한 온라인 본인인증 기법이 개발 되었다.

해킹기술은 나날이 발전하고 있다. 기존의 기술 또한 해킹의 위험에서 안전할 수는 없다.

개인정보 유출이 사회에 큰 이슈가 되는 만큼 개인정보의 보호를 위해 기존의 기술보다 더 개선된 기술을 개발하여야 한다.

향후 과제로는 본 논문에서 제안한 IMEI와 OTP를 이용한 본인인증 기법을 구현하고, 유심기반의 OTP와 결합하여, 보안성이 강화된 기법을 제안하고자 한다.

참고문헌

[1] 정보통신망 이용촉진 및 정보보호 등에 관한 법률,“시행 2012.9.16. 법률 제 11048호”.
[2] KISA 아이핀, “http://www.i-pin.kisa.or.kr”
[3] 한국모바일인증, “http://kmcert.com”
[4] 한국전자인증, “http://www.crosscert.com”
[5] 두산백과, “http://www.doopedia.co.kr”
[6] 미래테크놀로지,“http://www.mirae-tech.co.kr”
[7] 김대중, “스마트폰에서 공인인증서의 안전성 향상을 위한 기법”, 2011년 1월