본인확인서비스의 안전성 강화를 위한 본인인증 수단 및 절차 개선 방안 연구

최중석, 김종배
서울디지털대학교 컴퓨터정보통신학과
e-mail:kjblove@hotmail.com

A Study of improving user authentication procedures for enhanced safety of personal authorization methods

Jung-Suk Chio, Jong-Bae Kim
Dept of Computer and Info. Communication, Seoul Digital University

요 약

본인확인이란 적법하고 합당한 절차에 따라 합의된 사용자임을 증명하고 인증하는 과정을 의미한다. 본 연구에서는 본인확인서비스에서 본인임을 인증하는 다양한 수단들의 특징에서 살펴보고 대표적인 본인확인수단인 아이핀과 휴대폰 서비스의 인증절차 개선 방안을 제안한다. 제안한 방안을 통해 안전성이 강화된 본인확인서비스 제공과 이용이 가능할 것이다.

1. 서론

2015년 3월에 해커에 의해 공공아이핀 시스템이 해킹되어 공공아이핀 약 75만 건의 부정발급이 발생하였으며 부정 발급된 공공아이핀을 게임 사이트 등에서 사용되어 긴급 차단 및 삭제 조치에 이르고 있다. 이후 사용자의 편의성 보다는 보안 강화 차원에서 2차 패스워드 등의 추가 인증서단 도입, 부정 IP 차단, 모든 공공아이핀 사용자의 본인확인 후 재사용, 공공아이핀의 유효기간을 1년으로 제한, 3개월에 최소 1회 이상 비밀번호 변경 등의 조치를 취하고 있다. 안전한 아이핀 환경 조성을 위해 범정부 차원에 대응을 피력하고 있으나 이를 바라보는 아이핀 서비스에 대한 대국민 신뢰는 현저하게 낮아졌다.

2014년 12월 에 실시한 한국인터넷진흥원에 “개인정보보호수준 실태조사-개인부분”[1]에 따르면 가장 안전하다고 생각하는 본인인증 수단이 공인인증서 48.5%, 휴대폰 25.5%, 그리고 아이핀이 22.8%로 조사되었다. 그나마 아이핀 서비스가 안전한 인증수단으로 생각하는 집단이 연령이 낮은 집단이 대부분이었다. 낮은 연령대의 경우는 휴대폰 소지 비율이 낮고 발급이 복잡한 공인인증서 대비 발급이 비교적 쉬우면 유지비용이 저렴한 아이핀 서비스 기반의 본인확인을 이용하는데 기인한다. 아이핀 서비스는 그림 1과 같이 이용자가 주민등록번호를 제공하는 대신에 서비스를 제공하는 웹사이트에 회원가입 및 서비스를 이용하기 위해 아이핀 정보를 제공하고 본인확인기관이 실명확인 및 아이핀 정보 확인 후 본인확인정보를 웹 사이트에 제공함으로써 이용자를 식별한다. 2015년 2월 한국인터넷진흥원이 발표한 아이핀 발급 건수는 공공아이핀 약 400만 건이며 민간아이핀은 약 1,500만 건에 이르는 것으로 조사되었다[2]. 하지만, 2015년 2월말 공공아이핀 해킹으로 아이핀 탈퇴 건수가 증가하였으며, 강화된 아이핀 사용자 인증절차인 2차 패스워드 사용, 본인인증 절차 추가 등의 아이핀 가입자 수는 크게 감소하였다.

(그림 1) 아이핀 서비스 개요

<표 1> 아이핀 발급 건수 [2]

부분	공공	민간		
시행시기	2008년 8월	2005년 7월		
발급기관	공공 I-PIN	SIREN24	NICE i PIN	KCB 아이핀
	공공아이핀센터 (gpin.go.kr)	서울신용평가정보 (siren24.com)	나이스신용평가정보 (idcheck.co.kr)	코리아크레딧뷰로 (ok-name.co.kr)
관리감독	행정자치부	방송통신위원회		
발급현황	426만건	1550만건		

하지만, 주민번호 대체수단은 대국민 보편타당한 수단이 되어야 함으로써 유지비용 부담이 없으며 국내 거소 재외국인, 대면확인 등을 통한 서비스 가입이 가능한 특징을 가진 아이핀 서비스는 지속적으로 사용될 것으로 본다. 이를 위해서는 아이핀 서비스 이용자의 사용 불편함 감소, 안전성 강화를 위한 방안이 도입된다면 다시금 많은 이용자를 확보하고 높은 서비스 이용률을 가질 것이다. 본 연

구에서는 주민번호 대체수단인 아이핀 기반의 본인확인서비스 등 다양한 본인확인 수단의 특징을 분석하고 현재 사용 중인 아이핀 서비스의 본인인증 절차를 개선하기 위한 방안을 제안한다.

2. 본인인증 수단의 특징

일반적으로 대면확인은 은행에서의 창구거래나 혹은 주민 센터 등에서의 서면 작성 등에 의한 자필 증가가 있기 때문에 대면확인은 이용자를 상대적으로 확인하기 쉽다. 하지만, 온라인상에서 전자금융서비스, 온라인 거래 등과 같은 직접 대면하지 않은 환경에서는 사용자의 신분을 확인할 수 없음으로 안전한 온라인 거래를 위해서는 비대면 사용자의 식별과 인증 방안이 필요하다. 비대면 상황하에서 본인인증 수단들에는 다음과 같이 나열할 수 있다.

(1) 공인인증서(전자서명)를 이용한 서비스

전자서명은 전자적 거래의 신원확인, 거래내용의 위변조 금지, 거래내용의 기밀성 유지, 거래 사실의 부인방지 등을 통하여 안전하고 신뢰할 수 있는 보안환경을 제공한다. 따라서 공인인증기관으로부터 발급 받은 인증서를 사용하여 전자적 서명을 이행했을 경우 이는 본인확인수단으로서 이용될 수 있다. 공인인증서 이용자는 공인인증기관 또는 등록대행기관을 방문하여 신원확인을 하고, 생성한 공개키와 개인키 쌍을 이용하여 공개키에 대응하는 개인키로 전자서명을 수행하여 공인인증서를 발급 받아야 인증이 가능하다. 공인인증서 발급은 사용자의 주민등록번호와 비밀번호를 이중 해쉬하여 공인증서에 삽입함으로써 만약 사용자의 성명과 주민등록번호가 노출되었을 경우에도 공인인증서가 있어야하므로 실명확인 서비스에 비해 안전하다. 그러나 공인인증서 역시 저장매체에 종류와 방법에 따라 고도화된 해킹이나 사용자 또는 발급자의 부주의로 인해 공인인증서와 패스워드가 탈취될 수도 있기 때문에 완벽히 안전하다고 할 수는 없다. 본인확인을 위해 사용되는 공인인증서는 용도제한이 아닌 범용공인인증서만 가능하고 현재 범용 공인인증서는 사용자가 1년마다 갱신을 해야 함으로써 비용 부담의 문제를 갖고 있다.

(2) 휴대폰의 문자 서비스를 이용한 서비스

휴대폰을 이용한 본인인증은 휴대폰 가입 시 이동통신사에 제공한 성명, 주민등록번호 등의 정보를 이용하여 사용자가 소지한 휴대폰으로 6자리 난수를 문자로 전송하여 본인임을 확인받은 방법이다. 휴대폰 기반의 본인확인서비스는 기존의 사용자를 식별하기 위한 연계정보(CI)와 중복방지 값(DI)을 생성하거나 저장하지 않고 해당 본인확인 요청 기관에게 전달하는 역할만 수행한다. 휴대폰을 이용한 본인인증은 성명과 주민등록번호뿐만 아니라 휴대폰을 소지하고 있어야 함으로 실명확인 서비스에 비해 안전하다고 할 수 있다. 그리고 이동통신 서비스 가입자는 5,000만 명을 넘어 평균적으로 '1인 1폰'을 넘어서기 때문에 매체에 저장하여 별도로 소지해야 하는 공인인증서에 비해 활용도가 높은 것이 사실이다. 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. 무엇보다도 휴대폰 개통 시 본인확인을 철저히 이행하는 것이 필요하다. 최근 인터넷을 통한 휴대폰 개통 시 타인의 신분증을 사용하여 대포폰을 개통하는 문제가 발생하고 있다. 결국 대포폰의 개통으로 인해 부정인정의 사례가 다수 발견되고 있으며 이를 막기 위한 근본적인 대책이 요구된다. 이러한 일련의 부정인증 사건들로 인해 휴대폰 문자기반의 본인확인서비의 신뢰도가 떨어지고 있으며, 인터넷 서비스 제공업체 입장에서는 휴대폰 인증 및 문자 발송 비용에 대한 부담도 날로 커지고 있는 상황이다.

(3) 아이핀(i-PIN)을 사용한 인증 방법

아이핀은 인터넷 상에서 주민등록번호를 사용하는 대신에 사용자가 직접 생성한 아이디와 패스워드를 이용해 본인을 확인하는 수단이다. 본인확인은 제 3자의 기관에게 대신확인 받게 함으로써 신뢰성 있는 수단으로 자리 잡고 있으며, 사용자 입장에서는 본인의 주민등록번호를 서비스 업체에게 제공하지 않아도 됨으로 개인정보유출의 위험을 크게 줄일 수 있다. 사용자가 자신의 신원정보를 신뢰할 수 있는 기관(본인확인기관)에 제공하여 본인임을 확인받은 뒤, 한국인터넷진흥원이 인정한 기술이나 방식을 이용하여 본인확인 정보를 발급받아 인터넷 사이트 회원가입이나 성인인증 등을 위해 주민등록번호 대신에 사용하는 것이라고 정의되며 I-pin이라고 통칭되고 있다[3]. 아이핀 서비스는 서로 다른 웹사이트 간에도 동일 이용자를 구분할 수 있도록 연계정보를 웹사이트에 제공함으로써 이용자의 주민등록번호를 통해 가입한 경우에도 i-PIN과 연계할 수 있도록 주민등록번호를 연계정보로 변환할 수 있는 모듈 개발・제공하고 있다. 따라서 주민등록번호 사용 대신에 연계정보를 제공함으로써 비록 아이핀이 노출이 되더라도 폐기 및 재발급이 가능하여 개인정보 유출로 인한 피해를 최소화할 수 있지만 최근 공공아이핀의 부정발급 등 사용자의 편리성과 보안성 문제로 인해 서비스 이용률이 낮은 상황이다. 아이핀 서비스가 가진 근본적인 문제점은 아이디/패스워드 방식으로써 해당 방식은 파밍 공격에 취약하고, 아이핀 발급을 위해 인증수단으로 휴대폰을 이용할 경우 대포폰 명의자의 아이핀 발급이 가능한 문제점이 있다. 더구나 최근 공공아이핀 해킹사고와 같이 아이핀 서비스 업체의 관리자의 관리 실수나 아이핀 서비스 업체 데이터베이스 해킹이 이루어진다면 개인정보유출위험이 존재한다[4]. 다행히 공공아이핀의 부정발급 사례 이후 OTP, QR코드, 2차 패스워드의 다양한 추가 2차 인증방법을 도입하였다. 또한 아이핀 발급기관별로 1년 이상 이용

실적이 없는 휴면 아이핀을 별도로 관리하고 이용자가 재이용을 원할 경우 본인확인 절차를 거치도록 조치하였으며 비밀 번호도 1년마다 주기적으로 변경하도록 하는 기존 정책에서 강화하였다.

3. 본인인증 절차 개선 방안

아이핀 기반의 본인확인서비스는 지식기반의 본인인증 방법으로 가장 쉽고 편리하며 간단한 인증방법임에 틀림없다. 그러나 아이핀을 이용한 본인확인서비스 이용률은 휴대폰 인증 및 공인인증서 기반의 본인확인 방법보다 현저히 저조한 상황이다. 앞에서 언급한바와 같이 휴대폰은 간단하고 부가적인 정보의 제공이 없다는 장점이 있으며 공인인증서는 다소 사용은 어렵지만 금융기관의 비대면 거래를 위해서는 법적으로 공인인증서 사용을 의무화하고 있어 그 사용빈도가 높아 사용자의 이용에도 큰 불편이 없는 상황이다. 이에 반해 아이핀 서비스는 법적・제도적 근거도 미미하여 요구처가 다양한지 못해 사용자의 사용빈도가 낮아 잦은 망각으로 인해 활성화 되지 못하고 있다. 이를 해결하기 위해서는 법적・제도적 방안 마련이 필요하지만 현실적으로 대체수단으로 아이핀 서비스를 요구하기에는 무리가 있는 상황이다. 그럼 결국 사용자의 사용에 편리성을 두거나 민간 인터넷 사업자들에게 아이핀 기반의 본인확인서비스의 확대를 요구하는 것이 필요하다. 본 보고서에서는 법적・제도적 방안 마련보다는 아이핀 서비스 이용자 입장과 민간 인터넷 사업자 입장에서 인증절차 개선 방안에 대해 논의하고 자한다. 우선, 사용자 입장에서의 아이핀 인증절차 개선 방안은 다음과 같이 나열할 수 있다.

① 사용자 편의성 증대를 위한 다양한 인증방안 마련 필요

현재는 아이핀 신규 발급 시 사용자 인증을 위해 영문자 등으로 구성된 text 기반의 패스워드 입력을 요구하고 있다. 사용자들은 자신을 인증하기 위해 선호하는 방법이 있음에도 민간 아이핀 서비스 기관에서는 획일화된 text 기반으로 사용자를 인증하는 것은 민간 아이핀 기관들의 편의성 때문에 기인한다고 할 수 있다. 예를 들어 본인을 인증하기 위해서는 text가 아닌 그림 문자, 서명, 생체정보, 매체 정보, 기기 정보 등 다양하게 방안을 마련해 둠으로써 사용자의 편의성을 증대할 필요가 있다. 현재의 패스워드 기반의 사용자 인증 방식의 경우 자주 사용하지 않게 되면 기억할 수 없게 되어 패스워드 초기화 및 변경이 빈번히 발생하고 그로 인해 재사용 시 패스워드의 기억을 더욱더 어렵게 할 수 있다. 사용자의 식별하기 위한 아이디의 경우 본인확인기관 간의 연계와 통합 ID 구성 등을 위해 필요한 사항임을 인지할 수 있으나 사용자 인증을 위한 패스워드 체계를 사용자의 특성에 맞게 편리성을 부각시킬 필요가 있다. 그 대표적인 사용자 인증 방안으로는 사전 아이핀 서비스 이용 기기 등록 및 인증제도, 그림 문자 패턴 기반의 인증제도, 지문 인식 기반의 인증제도, 서명 패턴 기반의 인증제도, 전화 발신 기반의 인증제도 등이 있을 것이다. 기기 사전 등록 제도는 금융기관에 안전한 금융서비스 이용을 위한 부가적인 보안장치로 마련하고 있는 환경으로 아이핀 서비스 이용 시에 등록된 기기에서 아이핀 로그 인 시 2차 인증을 생략하고 1차 인증만을 이용하는 방법도 한 예를 될 수 있을 것이다. 그림 문자 패턴 기반의 사용자 인증은 기억하기 어려운 패스워드의 특성을 그림으로 표현된 이미지를 순서적으로 나열함으로써 보다 친밀감과 편의성을 높일 수 있는 방안이다. 생체 정보인 지문 정보를 이용한 방식 역시 사용자의 편의성 및 보안성을 높일 수 있으며, 스마트폰을 통한 서명 기반의 인증제도 방안, 그리고 전화 수신이 아니 발신 기반의 사용자 인증도 존재할 것 이다. 과거 사용자 인증 비용에 대한 부담 가중을 민간 업체들은 아이핀 서비스 활성화에 걸림돌이라고 지적한 바 있다[5]. 따라서 최근 이동통신사 들에서 무제한 통화 요금제 등의 출시로 휴대폰 통화 및 문자 발신에 대한 거부감이 낮아진 편이다. 따라서 본인확인기관에 요구하는 사용자의 고유전화번호로 전화하여 ARS의 요구되고 번호를 입력하거나 혹은 요구하는 정보를 문자를 발송함으로써 사용자 인증이 가능할 것이다. 결국은 본인확인비용은 수익자 부담원칙에 입각하여 시각을 다르게 볼 수 있으며 만약 비용 발생 시 정부기관이 이를 보전해 주거나 감면 해 주는 제도가 필요하다. 국가긴급전화 번호인 112 등의 경우 휴대폰 개통 절차 없이도 무료로 통화 및 정보전달이 가능하기 때문이다.

최근 생체 정보 기반의 사용자 인증이 다양한 곳에서 활용되고 있다. 특히 금융 기관에서는 온라인상에 비대면 거래를 통한 금융서비스 이용에 생체 정보를 이용하고 있다. 결국 생체정보 인식이 핀테크를 활성화 하는데 중요한 요소로 자리 잡고 있는 것이 사실이다. 아이핀의 사용자 인증을 위해서도 편리하고 보안이 보장되며 추가적인 정보 제공이 없는 서비스의 구현이 필요하다. 따라서 생체 정보 인식 기능을 가진 기기 보유 사용자라면 아이핀 사용자 인증 시 본인이 원하는 인증 조건을 선택할 수 있도록 하는 방안이 필요하다. 특히 생체정보 중 얼굴과 지문인증은 현재의 스마트폰 에서도 가능한 상황이다. 이러한 생체정보 인증은 많은 사람들 중에서 한 사람을 찾는 문제가 아니라 등록된 사용자의 정보가 얼마나 일치하는 지를 판단하는 문제로써 훨씬 간단하게 해결할 수 있다. 하지만, 사용자 입장에서는 본인확인기관에게 자신의 생체정보 제공에 대한 거부감이 있기 때문에 생체정보 제공이 아닌 본인확인기관들만의 가이드라인과 연동규격으로 정한 생체인식정보의 인증으로 서비스해야 할 것이다. 생체정보의 제공은 도난 유출 시 변경할 수 없는 문제점이 있는 반면에서 생체인식정보는 생체정보의 인식알고리즘 및 방법의 변경으로 그 정보는 얼마든지 변경할 수 있다. 따라서 방송통신위원회와 한국인터넷진흥원에서는 생체정보 사용을 위해 가이드라인 제정과 암호화 및 연동 규격을 정의할 필요가 있다.

② 2차 인증 수단의 간편화 방안 마련 필요

2015년 2월에 발생한 공공아이핀 부정발급 사건으로 인해 방송통신위원회는 민간 아이핀 사용자들에게 2차 패스워드 및 스마트 OTP등을 사용하도록 의무화하였다. 하지만, 아이핀 서비스 사용에 가장 큰 어려운 점이 편의성이었다. 더구나 패스워드 경우 아이핀 서비스 사용 빈도가 낮아 기억하지 어려워 사용 시마다 패스워드 초기화 후 재사용하는 패턴을 보이고 있는 것이 사실이다. 그러함에도 아이핀 서비스의 안전성 강화를 위해 2차 인증을 강제화 하여 사용자의 아이핀 사용 편리성이 크게 낮아진 상황이다. 따라서 사용자의 아이핀 사용의 편리성을 높이고 보안을 강화하는 차원에서 새로운 2차 인증 수단의 도입이 필요하다. 신규 인증 수단을 도입하기 위해서는 몇 가지 조건을 만족해야 한다.

1) 해당 인증수단으로 사용자는 어디에서는 인증을 받을 수 있어야 한다. : 결국 특정 저장 매체나 운영체제 등과 같이 한 특성에 종속적이지 않고 사용할 수 있는 수단을 제공해야 하는 것을 의미한다. 사용자는 인증을 등을 수행하기 위해서 Any time, Any where, Any places 에서도 인증이 가능할 있도록 보장함을 의미한다.

2) 사용자의 편의성이 보장되어야 한다. : 아무리 보안이 뛰어난 인증 기술일지라도 사용자 인증 시 다소 어렵거나 거부감이 있다면 오히려 추가인증 수단 도입으로 혼란만을 가중하게 될 것이다. 만약 추가 인증수단을 도입한다면 사회에서 통용되거나 혹은 표준 등으로 검증된 인증수단을 사용함으로써 사용자 입장에서는 다른 서비스를 통해 체험을 해 본 경험을 가질 수 있어 사용에 거부감이 적을 수 있을 것이다.

3) 서비스 제공업체 혹은 사용자가 인증 서비스를 제공 및 이용하는데 경제적으로 합리적이야 한다. : 인증 서비스 적용에 있어 장기적인 안목을 가지고 오랜 기간동이 변경 없이 사용 할 수 있는 수단을 제공해야 하고 해당 인증 서비스 이용을 위해 사용자가 보편적이지 않은 방안으로 추가적인 비용이 발생한다면 해당 인증서비스의 이용이 어려울 것이다.

4) 사용자의 편리성과 더불어 안전한 보안 체계를 유지해야 한다. : 추가 인증 도입에 앞서 사용자의 편리성만 강조하다 보면 보안성에 대해 간과할 수 있는 문제에 빠지게 된다. 따라서 일정 수준 이상의 보안조건을 만족하는 인증기술이 도입돼야만 다양한 침해사고를 예방할 수 있다.

5) 인증 수단의 유지 등을 위해 간편하고 서비스 기관에서 감당할 수 있는 수준이어야 한다. : 사용자의 편의성과 보안성을 높이기 위해 강화된 인증 수단의 도입 시 실제 인증 서비스 제공이 기관에 비용적인 문제에서 부담이 발생할 수 있다. 경제적인 면의 보장함과 동시에 해당 서비스 제공에 있어 기존의 기술을 접속하여 유연하게 적용할 수 있는 수단의 제공이 필요하다.

6) 여러 기기에서도 적용이 가능해야 한다. : Any Device와 같이 특정 기기에 종속되지 않고 인증코자 하는 사용자의 다양한 환경적인 요인을 분석하여 적시 적소에 인증 할 수 있는 방안 마련이 필요하다.

4. 결론

본 연구에서는 본인확인서비스에서 본인임을 인증하는 다양한 수단들의 특징에서 설펴 보고 대표적인 본인확인수단인 아이핀과 휴대폰 서비스의 인증 절차 개선 방안을 제안하였다. 제안한 방안을 통해 보다 안전성이 강화된 본인확인서비스 제공과 이용이 가능할 것이다.

Acknowledgment

이 논문은 2015년 한국인터넷진흥원의 지원을 받아 수행된 연구임.

참고문헌

[1] 개인정보보호수준 실태조사-개인부분, 한국인터넷진흥원, KISA-WP-2014-0051

[2] 미니투데이 뉴스, http://www.mt.co.kr/view/mtview.php?type=1&no=2015031113304730789&outlink=1

[3] 최윤성, 이윤호 외, “주민등록번호 대체수단에 대한 구현 취약점 분석”, 정보보호학회논문지, 한국정보보호학회, 145~185, 2007.

[4] 한국정보인증, 인터넷상의 주민번호 보호수단으로 공인인증서 이용 기술 개발, KISA-WP-2010-0023, 한국인터넷진흥원 , 2010.

[5] 조태희, “아이핀 서비스 현황과 활성화 방안”, pp.210-240. 한국학술정보, 2011.

[6] 박병찬, “전자금융서비스 본인인증수단의 이해”, pp 123-150, 스마트 시대 정보보호 전략과 법 제도 2, 한국학술정보, 2012.

[7] Jonathan Penn, ″What to look for in consumer strong authentication solutions″, Forrester, 2005.3