아이핀을 이용한 오프라인 주민번호대체 및 접근제어 방법

김승현*, 김석현*, 진승헌*
*한국전자통신연구원 SW 콘텐츠연구부문 인증기술연구팀
e-mail : ayo@etri.re.kr

A Study on an Alternation of RNN and Access Control for Offline Environments by using I-PIN

Seung-Hyun Kim*, Seok-Hyun Kim*, Seung-Hun Jin*
*Authentication Research Team, ETRI

요 약

주민등록번호는 온오프라인에서 가장 많이 사용되는 본인확인 수단이나, 해킹이나 내부자 유출 문제로 인해 온라인 환경에서는 아이핀과 같은 대체방안이 제시되었다. 하지만 오프라인 환경에서는 다양한 문제가 우려되나 대체방안이 없는 상황이다. 따라서 본 논문에서는 아이핀을 오프라인 환경에서 사용하기 위한 방안을 제시한다. 아이핀 메시지의 특정 필드에 본인확인을 위한 정보와 접근 제어 정보를 암호화 한 뒤, 사용자의 휴대폰으로 아이핀 인증 요청/응답 메시지를 관리하고 기업의 출입시스템에서 본인확인과 접근제어에 활용하였다. 또한 제안한 시스템은 안드로이드가 탑재된 휴대폰에서 구현되었고 실제 서비스를 제공 중인 본인확인기관과 연계하여 본인확인 절차를 수행했다.

1. 서론

주민등록번호(Korean Resident Registration Number, ,RNN)는 1968 년부터 간첩 식별 편의 등의 목적으로 주민등록증이 발급되면서 부여되기 시작했다. 주민등록번호는 한국인을 유일하게 식별할 수 있는 가장 쉬운 수단이기 때문에, 정부가 아닌 사기업이나 웹사이트 등에서도 주민등록번호를 요구하고 수집한다. 또한 주민등록번호는 실명제[1]와 같은 법안과 연계되어 실명과 함께 본인확인수단으로 사용된다.

이에 따라 해킹이나 내부자 개인정보 유출로 인해 대규모의 주민등록번호와 실명이 노출되면서 주민등록번호를 본인확인 수단으로 사용하기 어려워졌다. 정부 측에서는 온라인 환경에서 주민등록번호를 대체하기 위한 수단으로 아이핀(i-PIN)을 제안하였다. 하지만 아이핀은 주로 웹사이트 가입에 사용되므로 발급번호의 개수 및 사용 빈도가 극히 낮은 실정이다.

오프라인 환경의 경우, 주민등록번호의 활용도는 높으나 신뢰성에 문제가 있다. 주민등록증의 위조 및 변조를 막기 위해 홀로그램 등 최신의 기술이 적용되었지만, 실제로 일반인들이 차이를 식별하기에는 무리가 있다. 주민등록증의 유효성을 검증하기 위해서는 제 3 자에게 이를 위탁해야 하지만, 이 과정에서 개인정보가 누출될 수 있다.

이에 따라 본 논문에서는 오프라인 환경에서 주민등록번호를 사용하는 일부 사례에 집중하여, 기업 방문시 본인확인 및 접근 제어를 아이핀으로 해결하였다. 본 논문의 구성은 다음과 같다. 2 장에서 온라인 환경에서의 주민번호대체기술인 아이핀에 대해 살펴본다. 3 장에서 아이핀을 오프라인 환경에서 사용하는 방안을 소개하고, 제안하는 시스템의 구조 및 흐름을 설명한다. 4 장에서 실제로 구현된 시스템의 환경 및 구동 화면을 보인다. 5 장은 제안하는 방식의 특징을 언급하고, 마지막으로 6 장에서 결론을 맺는다.

2. 아이핀

아이핀(Internet Personal Identification Number, i-PIN)[2][3]은 일종의 가상 주민등록번호 개념으로, 온라인 환경에서의 주민등록번호에 대한 대규모 유출, 도용, 각종 범죄 악용의 부작용을 해소하기 위해 한국정보보호진흥원이 개발하였다. 2005 년 가이드라인이 만들어지고, 2006 년부터 시행되었으며, 2009 년부터는 이용 편의성을 개선한 아이핀 2.0 이 제공된다.

아이핀 기술에 따르면, 6 개의 본인확인기관이 TTP(Trusted Third Party)의 역할을 수행한다. 본인확인기관은 사용자의 주민등록번호, 신용카드번호, 휴대폰 가입자 정보와 같은 본인확인정보를 보관하며, 개별 웹사이트에는 주민등록번호와 동일한 13 자리 크기의 가상 번호를 제공한다. 이 번호를 통해 웹사이트는 주민등록번호와 동일한 용도로 사용자를 유일하게 식별할 수 있다.

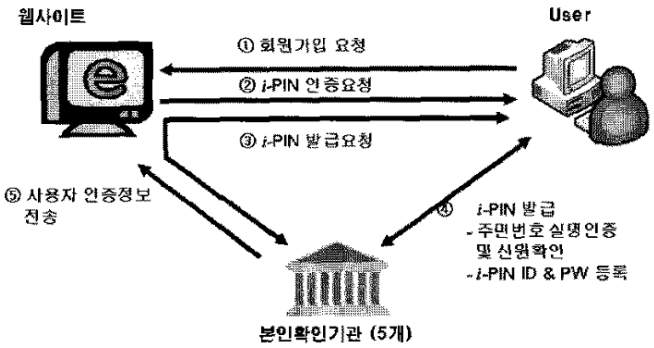

그림 1 아이핀 서비스 개요

그림 1 은 아이핀 서비스의 전반적인 구조 및 흐름을 보인다. 사용자가 웹사이트에 회원가입과 같이 본인확인이 필요한 특정 서비스를 요청할 경우(단계 1), 웹사이트는 아이핀 인증 요청 메시지를 사용자에게 반환한다(단계 2,3). 사용자가 본인확인 기관에 인증을 수행하면(단계 4), 아이핀 인증 응답 메시지가 웹사이트에 전달되어 본인확인 절차가 완료된다(단계 5)

표 1 과 표 2 는 아이핀 인증 요청 메시지와 응답 메시지의 주요 규격을 보인다.

표 1 아이핀 인증 요청 메시지 규격(WebsiteInfo)

필드명	설명
cpCode	웹사이트에게 부여된 식별코드
cpRequestNumber	웹사이트에서의 사용자 세션번호
returnURL	응답 메시지를 처리할 웹사이트 주소

표 2 아이핀 인증 응답 메시지 규격(PersonalInfo)

필드명	설명
virtualNo	아이핀 번호(13 자리)
realName	사용자의 실명
cpRequestNumber	인증 요청 메시지의 값과 동일
birthDate	생년월일(YYYYMMDD)

3. 제안하는 방법

본 논문에서 제안하는 방법은 오프라인 환경에서 아이핀을 이용한 주민번호대체 및 접근제어 절차이다. 오프라인에서 아이핀 본인확인 및 접근제어를 활용하기 위해서, 본 논문은 사용자가 인터넷이 되는 휴대폰을 소유하고 있다고 가정한다. 사용자의 신원은 사용자가 본인의 휴대폰을 소유하고 있고(have), 본인의 아이핀 계정 정보를 이용하여 인증(know)받았다는 사실로 확인한다.

앞 절에서 살펴본 바와 같이, 아이핀의 인증 응답 메시지에는 사용자의 실명 정보와 주민번호 앞자리가 제공된다. 이를 통해 주민등록번호에서 얻을 수 있는 정보를 확보할 수 있다. 접근제어의 경우, 우리는 아이핀 인증 메시지 규격의 세션번호 필드를 활용하였다. 이 필드는 원래 웹서버에서 사용자 브라우저의 세션번호를 기록하는 용도였으나, 실제로는 크기 제한 없이 다양한 문자열 정보를 포함할 수 있기 때문에 접근제어 정보를 포함시킬 수 있다.

기업의 무인단말기나 출입시스템을 통해 사용자의 휴대폰으로 아이핀 인증 요청 메시지를 수신하고, 본인확인기관과 통신하기 위해서는 RF 채널 기능 또는 온라인 통신 기능이 필요하다. 또한 기업 내의 출입단말에 아이핀 인증 응답 메시지를 전달하기 위해서는 RF 채널 통신이 필요하다. 본 논문에서는 사용자 휴대폰이 RF 채널 통신과 온라인 통신 기능을 수행할 수 있다고 가정한다.

3.1 아이핀 연동

본 절에서는 제한하는 방법에서 아이핀을 사용하는 방법을 상세하게 설명한다. 앞에서 언급했듯이, 제안하는 방법은 아이핀 인증 메시지 구조에서 세션번호를 저장하는 cpRequestNumber 필드를 본인확인 및 접근제어 용도로 활용한다. 접근제어 정보의 규격은 표 3 과 같다. 기업의 출입시스템은 표 1 의 아이핀 인증 요청 메시지를 작성하면서 해당 필드에 접근제어 정보를 암호화 하여 저장한다. 사용자가 본인확인기관으로부터 수신하는 표 2 의 아이핀 인증 응답 메시지는 아이핀 인증 요청 메시지의 cpRequestNumber 필드를 동일하게 저장하고 있으며, 전체 메시지는 본인확인기관과 기업의 출입시스템만이 공유하고 있는 보안키로 암호화된다.

아이핀 인증 응답 메시지를 복호화 한 뒤, cpRequestNumber 에서 복호화 된 접근제어 정보를 비교하여 사용자의 본인 확인 및 접근제어를 수행한다. 실명, 생년월일 정보로 본인 확인 여부를 확인하고, 접근제어 정책에 설정된 방문위치, 유효기간 등으로 기업의 출입 여부를 판단한다. 한 번 아이핀 인증 응답 메시지를 받으면, 유효기간 동안 자유롭게 사용가능하다. 또한 유효시간이 지나면 자동으로 폐기하거나 기업의 중앙 출입시스템의 요청으로 임의 폐기하는 절차도 가능하다.

3.2 시스템 구조

제안하는 시스템의 전체 구조는 그림 2 의 모습을 보인다. 시스템은 크게 사용자 휴대폰, 본인확인기관, 기업의 출입관리시스템의 3 부분으로 나뉜다.

사용자 휴대폰은 오프라인에서의 본인확인 및 접근제어를 위해 아이핀 인증 메시지를 저장하는 매체이다. 아이핀 인증 요청/응답 메시지와 본인확인기관의 인증 정보는 휴대폰 내에서도 USIM 의 보안 영역에 보관된다. USIM 에 설치된 자바 애플릿은 사용자가 PIN 번호를 올바르게 입력한 경우에 상기 정보를 로드하여 사용하도록 만든다. 사용자 휴대폰은 본인확인기관과 온라인 통신을 수행하며, RF 채널을 통해 기업의 출입시스템과 통신을 수행한다.

본인확인기관은 사용자의 휴대폰을 통해 아이핀 인증 요청 메시지와 인증 정보를 수신한 뒤, 아이핀 인증 응답 메시지를 반환한다.

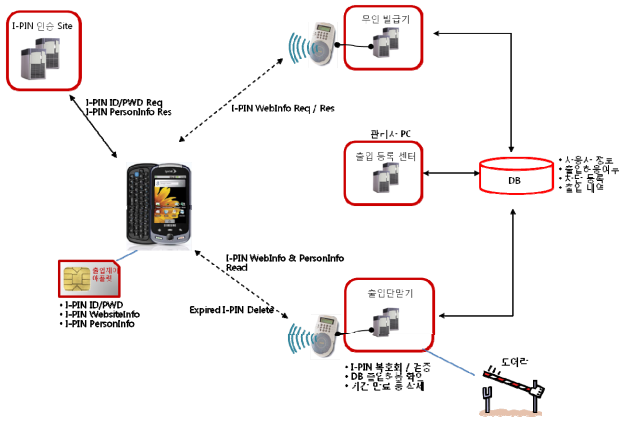

그림 2 제안하는 시스템의 구조도

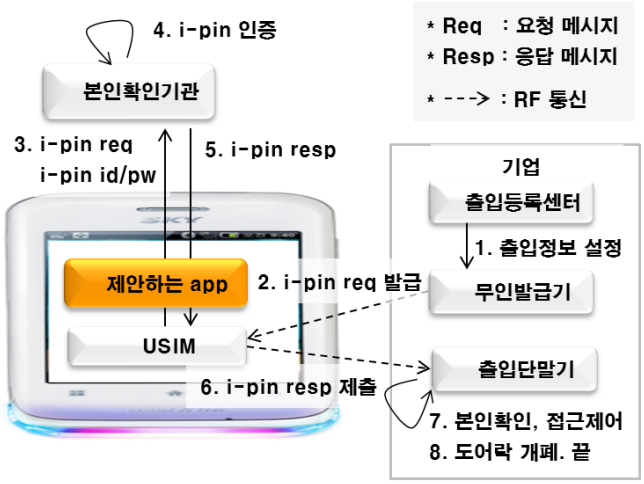

그림 3 제안하는 시스템의 흐름도

기업의 출입시스템은 출입등록센터, 무인발급기, 출입단말기로 구성된다. 출입등록센터는 관리자가 기업에 방문할 사용자의 본인확인정보와 접근제어 정보를 설정한다. 해당 정보는 아이핀 인증 요청 메시지의 cpRequestNumber 에 출입시스템만 알고 있는 보안키로 암호화된다. 다음은 접근제어 정보에 내역을 보인다.

- 접객인 정보
- 방문자 이름
- 방문자 생년월일
- 메시지의 유효 시간(시작, 끝)
- 접근 가능한 기업 내 시설물

무인발급기는 관리자가 출입등록센터에서 미리 설정한 접근제어 정보를 이용하여 아이핀 인증 요청 메시지를 생성하고 사용자 휴대폰으로 발송하는 역할을 수행한다. 그림 2 에서는 RF 채널을 사용하도록 표시되어 있으나 MMS(멀티미디어 메시지) 또는 온라인 통신을 통해 전송할 수도 있다.

출입단말기는 기업 내의 각 시설물의 출입구에 위치한다. 사용자 휴대폰과 RF 채널 등으로 통신하여 아이핀 인증 응답 메시지를 전달받는다. 수신된 메시지를 본인확인기관과 공유한 보안키로 복호화하고, cpRequestNumber 에 설정된 접근제어 정보를 출입시스템만이 알고 있는 보안키로 복호화한다. 접근제어 정보와 아이핀 응답 메시지의 본인확인 정보를 비교한 뒤, 접근제어 정보를 확인하여 해당 시설물의 출입문을 개폐한다.

3.3 흐름

그림 3 은 본 논문에서 제안하는 시스템의 흐름도를 보인다. 먼저 관리자가 출입제어시스템을 통해 사용자의 본인확인 정보와 접근제어 정보를 설정한다(단계 1) 출입제어시스템은 암호화 된 상기 정보를 아이핀 응답 요청 메시지에 포함시켜 사용자의 휴대폰에 전송한다(단계 2). 표 3 은 접근제어 정보의 예제를 보이고, 표 4 는 아이핀 요청 메시지의 예제를 보인다. 실제 아이핀 기관에서는 cpRequestNumber 라는 필드명 대신 SESSION_NO 를 사용한다.

표 3 접근제어 정보 예제

4270|김승현|791220|20101021144200|20101021180000|1-101,2-202,3-303,4-404,5-505

표 4 아이핀 인증 요청 메시지 예제

CPCODE=AETRI0000039&RETURNURL=http%3A%2F%2F129.254.186.19%2Fipin%2Freceive.jsp&SERVICE=1&SESSION_NO=85%233…%23&JUMIN_NO=

휴대폰에 전송된 아이핀 인증 요청 메시지는 USIM 내의 자바 애플릿에 의해 관리되고 보안 영역에 저장된다. 상기 애플릿은 사용자의 아이핀 인증정보도 함께 저장하여 관리할 수 있다. 사용자 휴대폰은 이들 정보를 본인확인기관에 전달하여(단계 3,4) 아이핀 인증 응답 메시지를 수신하고 상기 애플릿은 보안 영역에 저장한다(단계 5). 표 5 는 아이핀 응답 메시지의 예제를 보인다.

표 5 아이핀 인증 응답 메시지 예제

CPCODE=32%23116%23102%2397%23125%235%236 %23113%2381%231%231%2310%23&CP_CODE=32%23116%23102%2397%23125%235%236%23113%2381%231%231%2310%23&SESSION_NO=89%234…%2317%23&NAME=%B1%E8%BD%C2%C7%F6&NAME_UTF=%25EA%25B9%2580%25EC%258A%25B9%25ED%2598%2584&VIRTUAL_NO=84%236%233%235%230%233%236%23112%2385%237%2310%230%232%23&DUP_INFO=44%23114…%23124%23&AGE=86%23&SEX=80%23&BIRTHDATE=80%238%235%2310%235%237%234%23113%23&AUTHINFO=80%23&NATIONALINFO=81%23&CI1=9%23112…%23124%23

사용자가 기업의 출입단말기에 자신의 휴대폰을 접근시키면 RF 채널을 통해 USIM 의 자바 애플릿이 자동으로 구동하여 아이핀 인증 응답 메시지가 전달된다(단계 6). 출입단말기는 본인확인기관과 공유한 보

안키를 이용하여 표 5 와 같은 메시지를 복호화하고, SESSION_NO 필드는 출입시스템만 알고 있는 보안키를 이용하여 다시 복호화한다. 마지막으로 출입단말기는 표 3 과 같이 복호화된 메시지를 검증하여(단계 7) 본인확인 및 접근제어를 수행한다(단계 8).

4. 구현

제안하는 시스템은 아래와 같은 환경에서 구현되었다. 사용자의 휴대폰은 '스카이 이자르(IM-A630K)'로 안드로이드 2.2 버전[4]을 운영체제로 탑재하고 RF 통신이 가능하다. USIM 의 자바 애플릿은 JAVACARD 2.1.1 버전[5]에서 개발되었으며, 애플릿을 설치하기 위해 KT 의 개발용 인증서를 발급받았다. 자바 애플릿에서 정보를 로드하고 본인확인기관과 통신하는 부분은 안드로이드 어플리케이션으로 개발하였으며, 자바 애플릿 통신 부분은 KT 의 KAF(KT Application Framework) 라이브러리를 활용하였다. 본인확인기관은 한국정보인증[6]을 대상으로 했으며, 한국정보인증으로부터 아이핀 CP 계정(CPCODE, 보안키)을 발급받았다. 출입제어시스템은 비주얼베이직으로 개발하였으며, 아이핀 복호화 및 검증 모듈은 자바로 개발하였다.

무인발급기와 출입단말기는 RF 동글이 부착되어있다. 따라서 아이핀 인증 요청/응답 메시지는 RF 채널을 통해 교환된다. 본인확인기관과의 통신은 WIFI 를 사용하였다. 정식 USIM 이 아닌 테스트 USIM 을 사용해야만 자바 애플릿을 탑재할 수 있기 때문에, 3G 망으로 통신이 어렵다. 또한 아이핀 프로토콜은 HTTPS 채널이 기본이고 키보드 보안과 백신 프로그램을 설치해야 하지만, 프로토콜을 분석하여 HTTP 통신으로 처리하도록 흐름을 변경하였다.

5. 분석

제안하는 시스템은 기존의 오프라인 환경에서 주민등록번호의 노출 없이 본인확인을 수행할 수 있다. 온라인 환경에서 본인확인대체수단으로 활용되는 아이핀을 오프라인에 적용했기 때문에 별도의 시스템 구축은 최소화할 수 있다. 아이핀의 프로토콜 메시지 또한 준용하였기 때문에 본인확인기관의 수정 또한 없다.

제안하는 방식은 아이핀을 그대로 활용했기 때문에 그 장점 또한 동일하게 유지된다. 신분증과 달리 개인정보의 노출 및 도용이 어렵고, 사용자 휴대폰 분실 시 악용이 어려우며 재발급이 용이하다. 사용자 휴대폰에 저장된 아이핀 메시지는 휴대폰 PIN, 안드로이드 어플리케이션 로그인 정보, 자바 애플릿 PIN, 본인확인기관의 인증정보 순으로 보호받고 있다. 휴대폰의 특성을 감안하여 사용자 편의를 위해 낮은 레벨 순서대로 자동 입력할 수 있다.

접근제어 정보는 기업의 출입시스템에 의해 암복호화되기 때문에 조작이 어렵다. 아이핀 인증 응답 메시지 또한 USIM 의 보안영역에 의해 보호되기 때문에 다른 방법으로 조작되기 어렵다. 만일 사용자 본인이 해당 내용을 변경할 경우, 기업의 보안키와 본인확인기관의 보안키를 모두 알지 못한다면 복호화시 에러가 발생한다.

그림 4 사용자 휴대폰 구동 화면

6. 결론

본 논문은 오프라인 환경에서 아이핀을 이용한 주민번호대체 및 접근제어 절차를 제안하였다. 아이핀 메시지의 특정 필드에 본인확인을 위한 정보와 접근제어 정보를 암호화 한 뒤, 사용자의 휴대폰으로 아이핀 인증 요청/응답 메시지를 관리하고 기업의 출입시스템에서 본인확인과 접근제어에 활용하였다. 제안한 시스템은 안드로이드가 탑재된 휴대폰에서 구현되었고 실제 서비스를 제공 중인 본인확인기관과 연계하여 본인확인 절차를 수행했다.

제안하는 방식은 아이핀의 규격을 준용하면서 오프라인에 적용하였기 때문에 별도의 시스템 구축을 최소화할 수 있다. 또한 신분증과 달리 개인정보의 노출이나 분실시 대처가 용이하다. 접근제어 정보는 여러 단계의 보안으로 보호받기 때문에 편의성을 고려하여 다양한 보안 레벨로 활용 가능하다.

참고문헌

[1] 황성기, "인터넷 실명제에 관한 헌법학적 연구", 2008,http://www.hanyang.ac.kr/home_news/H5EAFA/00002/101/2008/1-1.pdf.

[2] TTA, "i-PIN 서비스 프레임워크", 정보통신단체표준, TTASKO-12.0054, 2007

[3] TTA, "i-PIN 서비스 전달메시지 형식", 정보통신단체표준, TTASKO-12.0055, 2007

[4] Android 2.2 Platform, http://developer.android.com/sdk/android-2.2.html

[5] Java Card Technology, http://www.oracle.com/technetwork/java/javacard/overview/index.html

[6] 한국정보인증, http://www.signgate.com