중계모듈을 이용한 주민번호대체수단의 연동방안

김승현*, 이춘식**, 진승헌*
*한국전자통신연구원 SW 콘텐츠연구부문
**㈜드림시큐리티
e-mail : ayo@etri.re.kr

A Relay Technique to interoperate between i-PIN(internet Personal Identification Number) services

Seung-Hyun Kim*, Chun-Sik Lee**, Seung-Hun Jin*
*S/W Contents Research Division, Electronics and Telecommunication Research Institute
**Dream Security

요 약

대부분의 온라인 전자거래업체는 사용자의 신원을 확인하기 위해 주민등록번호를 요구하고 있다. 그러나 최근 발생하고 있는 대규모 개인정보 유출사고 등으로 주민등록번호가 노출되는 사례가 빈번하며, 주민등록정보를 타인이 도용하여도 효과적으로 확인 및 제어하는 수단이 없다는 문제가 있다. 이러한 문제를 해결하기 위해 주민번호대체수단이 제안되었으나, 최근 공공 i-PIN 과 민간 i-PIN 으로 구분되는 기술들의 연동 문제로 인해 적극적인 도입이 우려되는 상황이다. 따라서 본 논문은 최소한의 수정으로 이들 주민번호대체수단이 연동할 수 있는 방안을 제시한다. 기존의 민간 i-PIN 연동 프로토콜을 공공 i-PIN 에 적용하며 프로토콜 간의 연동 모듈을 두어 각 프로토콜을 처리한다. 제안된 기술은 공공 i-PIN 에 적용되어 현재 전국적으로 구축 중이다.

1. 서론

온라인에서 주민등록번호는 매우 중요한 가치를 가진다. 이름과 주민등록번호를 이용하며 모든 사이트에서 사용자의 신원을 확인할 수 있다. 현재 인터넷 사이트 가입 시에 사이트 중복 가입 방지, 14 세 이상 여부, 성인 여부를 확인하기 위하여 대부분의 전자거래업체에서 주민등록번호를 요구한다. 이러한 상황에서 발생하는 가장 큰 문제는 신원확인을 위하여 수집되는 주민등록번호에 너무 많은 개인정보들이 포함되어 있다는 것과, 다른 사람이 타인의 주민등록 번호를 도용하는 경우 이를 실효성 있게 확인 및 제어하기 위한 수단이 없다는 점, 그리고 온라인인 경우 사용자가 실제 그 주민등록번호에 해당하는 사용자인지를 확인하는 신원 인증 기능이 부족하다는 점이다.[1]

이러한 주민등록번호의 문제를 해결하기 위해서 주민번호대체수단이 제안되었다. 주민번호대체수단은 개인정보를 포함하지 않으며, 가입자가 언제든지 갱신, 폐지를 할 수 있기 때문에 자기정보 통제권을 수립할 수 있게 된다. 최근에 발생한 대규모의 개인정보 유출사고 등으로 주민번호대체수단의 의무도입이 고려되고 있는 시점이지만, 보안성, 편의성, 연동 문제 등이 우선적으로 해결되어야만 한다. 따라서 본 논문은 기존의 민간 i-PIN 연동 프로토콜을 공공 i-PIN 에 적용하며 프로토콜 간의 연동 모듈을 통해 주민번호대체수단의 연동 문제를 해결하는 방안을 제시한다.

본 논문의 구성은 다음과 같다. 2 장에서 주민번호대체수단을 소개하고, 기존에 제시된 단점의 하나인 연동 문제를 소개한다. 3 장에서는 민간 i-PIN 과 공공 i-PIN 을 연동하기 위한 방안을 제시하고, 마지막으로 4 장에서는 결론 및 적용 상황을 보인다.

2. 주민번호대체수단(i-PIN)

주민번호대체수단은 주민번호를 대체하기 위한 본인확인정보로서 출생연월일, 성별 등의 개인정보를 전혀 포함하지 않고 있으며, 가입자가 언제든지 갱신, 폐지를 할 수 있으며, 본인확인 정보는 가입자와 한정적인 시간 내에서만 유일성을 보장하고, 사용자가 신뢰하는 본인확인기관에 의하여 발급되는 난수이다.[1] 주민번호대체수단은 5 개의 일반 기업(한국신용평가정보, 한국신용정보, 서울신용평가정보, 한국정보인증, 한국전자인증)의 민간 i-PIN 과 행정자치부의 공공 i-PIN 에서 각기 다른 방식으로 제공되고 있다. 민간 i-PIN 의 경우 2008 년 2 월 기준으로 99 개 사이트에 도입되어 전체 114,112 건이 발급되었으며[2], 공공 i-PIN 은 2009 년까지 전 공공기관에 도입 예정이다[3].

주민번호대체수단을 통해 개인의 신원을 안전하게 확인하며, 개인정보에 대한 자기 통제권을 확보하게 된다. 그러나 주민번호대체수단이 더욱 활성화되기 위해서는 기존에 제시된 보안성, 편의성, 연동 문제를 해결해야 한다. 민간 i-PIN 으로 불리는 주민번호대체수단은 각기 다른 방식을 사용하였기 때문에 초기부터 각 i-PIN 서비스 간의 연동 문제가 우려되었다.

구분	공공 i-PIN	민간 i-PIN				
서비스 명	G-PIN	나이스 아이핀	가상 주민번호	사이렌 아이핀	OnePass	그린버튼 서비스
본인확인기관	행정자치부	한국신용정보	한국신용평가	서울신용평가	한국정보인증	이니텍, 한국전자인증
신원확인 방법	-주민등록확인 -공인인증서 -대면확인	-공인인증서 -대면확인 -신용카드정보 -휴대폰 SMS	-공인인증서 -대면확인 -신용카드정보 -휴대폰 SMS	-공인인증서 -대면확인 -신용카드정보 -휴대폰 SMS	-공인인증서	-공인인증서 -신용카드정보 -휴대폰 SMS
인증 방식	ID/PW	ID/PW	ID/PW	ID/PW	공인인증서 VID	전자메일주소 /PW
주요 서비스 대상	공공기관	민간기관				

(표 1) 주민번호대체수단 비교 [4]

표 1 은 각 업체가 제공하는 방식을 보여준다.

이를 해결하기 위해 KISA 는 i-PIN 연동 프로토콜을 개발하고, 이를 TTA 표준[5]으로 제정하였다. 이 표준은 민간 i-PIN 기관간에 호환 가능한 연동 메시지를 구성하는 요소와 공개키 기반구조를 이용하여 각 기관이 서명 및 암·복호화를 수행하는 방법을 정의한다.

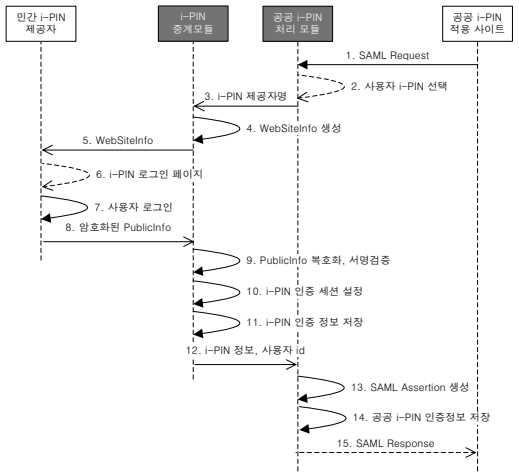
그러나 민간 i-PIN 의 연동방식은 공공 i-PIN 의 본인확인에 적용되지 못한 상태이다. 이로 인해 민간 i-PIN 을 발급받은 사용자는 공공 i-PIN 이 적용된 사이트를 사용할 수 없으며, 공공 i-PIN 을 발급받은 사용자도 마찬가지로 민간 i-PIN 사이트를 사용할 수 없다.

3. 제안하는 방법

공공 i-PIN 과 민간 i-PIN 을 연동하기 위해서는 두 가지 요구사항을 먼저 고려해야만 한다. 첫 번째는 각 i-PIN 제공자와 적용 사이트를 최소한으로 수정하는 것이다. 이미 온라인으로 서비스를 제공중인 사이트를 변경하는 절차 없이 최대한 기존 프로토콜 표준을 준용하는 방식을 사용해야 한다. 두 번째는 공공 i-PIN 사이트가 요구하는 필드를 고려하여 i-PIN 연동 프로토콜을 연계시키는 것이다. 공공 i-PIN 는 SAML[6]을 기반으로 한 SSO(Single Sign-On) 서비스로 주민번호대체수단을 제공하는데, i-PIN 연동 프로토콜이 지원하는 정보와의 매핑이 요구된다. i-PIN 연동 프로토콜을 공공 i-PIN 적용 사이트에 직접 사용할 수 없으며, 공공 i-PIN 이 요구하는 필드를 추가로 고려해야 한다.

본 논문에서 제안하는 방법은 공공 i-PIN 과 민간 i-PIN 을 연동하기 위해 i-PIN 연동 프로토콜을 적용한다. 기존에 구축된 환경을 최소한으로 수정하기 위해서 도입 초기인 공공 i-PIN 제공자만 전환하는 방안을 채택하였으며, 기존의 민간 i-PIN 제공자간에 사용중인 연동 프로토콜을 적용한다. 공공 i-PIN 제공자와 적용 사이트의 통신을 수행하는 SAML 프로토콜 또한 변경이 어려우므로 별도로 중계 모듈을 두어 각 프로토콜의 내부 정보를 매핑하는 로직을 둔다. 이에 따라 중계 모듈은 다음과 같은 기능을 수행한다.

- 공공 i-PIN 서비스 모듈과 연동
- i-PIN 연동 요청 프로토콜 생성/파싱

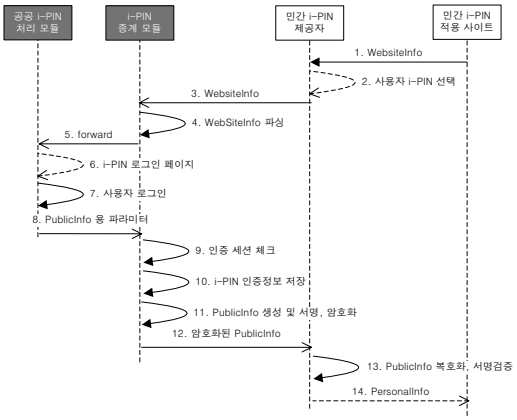


(그림 1) 민간 i-PIN 가입자가 공공 i-PIN 사이트를 이용하는 경우

- i-PIN 연동 응답 프로토콜 생성/파싱
- 서명/검증 및 암복호화
- 인증 세션 설정

중계 모듈은 공공 i-PIN 에 적용되었으며, 공공 i-PIN 제공자에 본인확인을 요청하는 사용자가 민간 i-PIN 제공자를 선택한 경우 또는 민간 i-PIN 제공자에 본인확인을 요청하는 사용자가 공공 i-PIN 제공자를 선택한 경우에 동작한다. 적용 환경에는 주민번호대체수단 제공자인 공공 i-PIN 과 민간 i-PIN 제공자, 각 주민번호대체수단을 적용한 사이트들이 존재한다. 이들 사이트는 공공 i-PIN 또는 민간 i-PIN 중 하나만 지원하는 경우가 일반적이다.

그림 1 은 민간 i-PIN 가입자가 공공 i-PIN 이 적용된 사이트를 이용하는 흐름을 보여준다. 가입자가 사이트에 접근하여 본인확인을 수행할 때, 가입자는 공공 i-PIN 제공자로 포워딩되며 주민번호대체수단으로 특정 민간 i-PIN 제공자를 선택한다.(step1,2). 이때 전달되는 메시지는 SAML Request 형식을 따른다. 공공 i-PIN 제공자는 중계모듈을 통해 i-PIN 제공자가 처리할 수 있는 연동 요청 메시지(WebsiteInfo)를 생성하여 전달한다.(step 3,4,5) 민간 i-PIN 제공자는 수신받은 연동 요청 메시지를 파싱하고, 응답을 주기에 앞서 사용자의 신원을 파악한다.(step 6,7) 민간 i-PIN 제공자는 해당 사용자의 정보가 포함된 연동 응답 메시지(PublicInfo)를 생성하여 공공 i-PIN 제공자에게 전달한다.(step 8) 응답 메시지는 해당 공공 i-PIN 제공자만 해석할 수 있도록 암호화되어 있다. 공공 i-PIN 제공자의 중계모듈은 연동응답 메시지를 복호화하고, 해석한 i-PIN 연동 메시지 정보를 저장한다. (step 9,10,11) 그리고 공공 i-PIN 서비스는 사용자의 정보를 바탕으로 SAML Response 메시지를 작성하여 사이트



(그림 3) 공공 i-PIN 가입자가 민간 i-PIN 사이트를 이용하는 경우

에 전달한다.(step 12,13,14,15) 공공 i-PIN 적용 사이트는 해당 메시지를 해석하여 본인확인을 완료한다.

그림 2 는 step 15 에서 공공 i-PIN 제공자가 민간 i-PIN 가입자의 본인확인을 받은 뒤, 공공 i-PIN 적용 사이트에 전달하는 SAML Assertion 메시지의 예제를 보여준다. Assertion 을 발급한 공공 i-PIN 제공자는 Issuer 엘리먼트의 'g-pin.go.kr'로 표시되고, NameID 엘리먼트는 해당 사용자에게 할당된 식별자를 보인다. AuthnContextClassRef 엘리먼트는 사용자가 패스워드 방식으로 인증받았음을 나타내고, Attribute 엘리먼트에는 i-PIN 연동 메시지에 포함되는 정보들이 표시된다.

그림 3 은 공공 i-PIN 가입자가 민간 i-PIN 이 적용된 사이트를 이용하는 흐름을 보여준다. 가입자가 사이트에 접근하여 본인확인을 수행할 때, 가입자는 민간 i-PIN 제공자로 포워딩되며 주민번호대체수단으로 공공 i-PIN 제공자를 선택한다.(step1,2). 이때 전달되는 메시지는 연동 요청 메시지(WebsiteInfo)로, 해당 공공 i-PIN 제공자에게 포워딩 된다.(step 3) 공공 i-PIN 제공자의 중계모듈은 수신받은 연동 요청 메시지를 복호화하고, 응답을 주기에 앞서 사용자의 신원을 파악한다.(step 4,5,6,7) 공공 i-PIN 제공자가 해당 사용자의 정보를 전달하면(step 8), 중계모듈은 해당 정보를 이용하여 연동 응답 메시지(PublicInfo)를 생성하고 민간 i-PIN 제공자에게 전달한다.(step 9,10,11,12) 응답 메시지는 해당 민간 i-PIN 제공자만 해석할 수 있도록 암호화되어 있다. 민간 i-PIN 제공자는 연동응답 메시지를 복호화하고 i-PIN 응답 메시지(PersonalInfo)를 생성하여 사이트에게 전달한다.(step 13,14) 민간 i-PIN 제공자는 해당 메시지를 해석하여 본인확인을 완료한다.

그림 4 는 step 11-12 에서 공공 i-PIN 제공자가 공공 i-PIN 가입자를 본인확인한 뒤, 민간 i-PIN 제공자에게 전달하는 PublicInfo 메시지를 보여준다. 상단의 메시지는 i-PIN 중계모듈이 PublicInfo 를 생성하는 과정을 보인다. IPin.PublicInfo 의 114-125 에 해당하는 데이터가 PublicInfo 에 포함된다. 하단의 메시지는 생성된 PublicInfo 구조체를 개인키로 서명한 뒤, 제공자 간에 공유한 비밀키 또는 메시지를 수신할 i-PIN 제공자의 암호화용 공개키 인증서를 사용하여 암호화한 것이다.

4. 결론

본 논문에서는 공공 i-PIN 과 민간 i-PIN 을 연동하기 위해 별도의 중계 모듈을 제안하였으며, i-PIN 연동 프로토콜을 적용하였다. 기존에 구축된 환경을 최소한으로 수정하기 위해서 도입 초기인 공공 i-PIN 제공자에 연동모듈을 추가하는 방안을 채택하였으며, 기존 민간 i-PIN 제공자간에 사용중인 연동 프로토콜을 적용했다. 이를 통해 기존에 서비스를 제공 중인 민간 i-PIN 제공자와 사이트를 수정할 필요가 없으며 공공 i-PIN 적용 사이트도 마찬가지로 수정 없이 운영된다. 공공 i-PIN 제공자만 중계 모듈을 적용하여 각 방식간의 메시지를 변환하는 작업을 수행하는 것으로 공공 i-PIN 과 민간 i-PIN 이 연동된다. 본 기술은 ETRI 에서 개발하여 기술이전 하였으며, 행정자치부 공공 i-PIN 사이트에 적용되었다. 그리고 2008 년 8 월부터 전국적인 구축을 시작한 상태이다.

5. Acknowledgement

본 연구는 지식경제부 및 정보통신연구진흥원의 IT 핵심기술개발사업의 일환으로 수행하였음. [2007-S-601-02, 자기통제 강화형 전자 ID 지갑 시스템 개발]

참고문헌

[1] 염흥열, 이석래, "인터넷 상에서 주민등록번호 대체수단 발전방향", 전자공학회지 제 32 권 제 11 호, pp.61-73, 2005.11

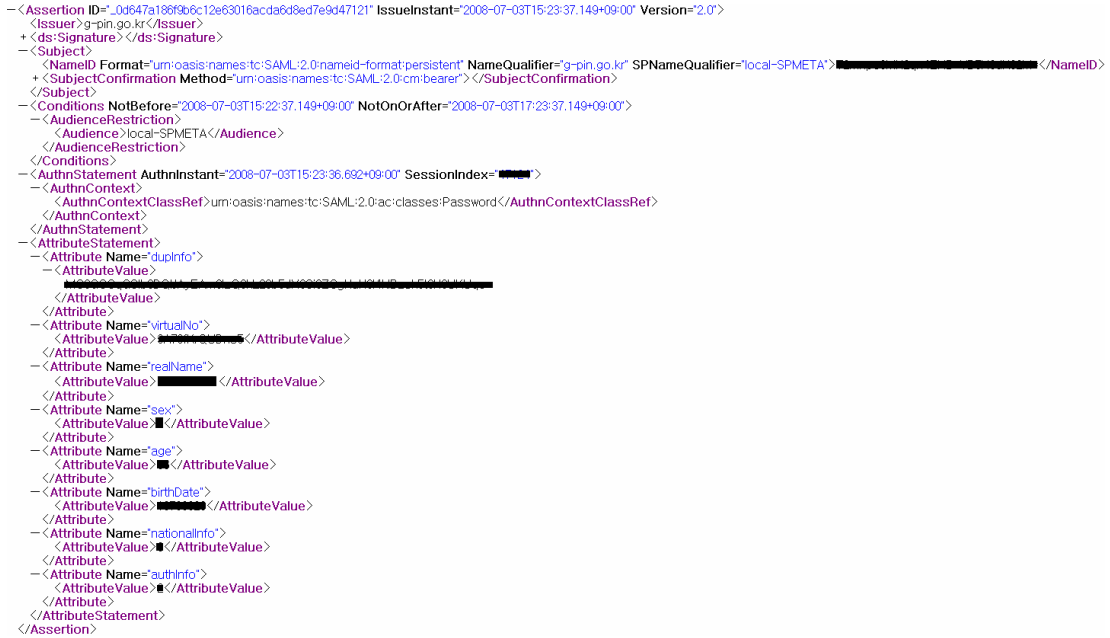
[2] 인터넷상 개인정보 침해방지 대책, 방송통신위원회, 2008/4/24

[3] 공공기관 홈페이지 개인정보 노출 방지 대책, 행정안전부, 2008/8/26

[4] 진승헌, 인터넷상의 주민번호 대체수단의 현황과 과제, 2008 년제 3 차 privacy round up, 한국 CPO 포럼, 2008/3/19

[5] i-PIN 서비스 전달 메시지 형식, TTAS.KO-12.0055, 2007/12/26

[6] Paul Madsen, Eve Maler, "SAML V2.0 Executive Overview", OASIS SAML TC, Committee Draft 01, 2005/4/12



(그림 2) 민간 i-PIN 가입자인 경우, 공공 i-PIN 사이트가 수신하는 SAML Assertion 메시지

9 월 25 05:03:28.264 오후 DEBUG - IPin.PublicInfo(114) | SERVICE_ORG = H
9 월 25 05:03:28.264 오후 DEBUG - IPin.PublicInfo(115) | VIRTUAL_NO = xxxxxxxxxx
9 월 25 05:03:28.265 오후 DEBUG - IPin.PublicInfo(116) | CP_CODE = K00000000000
9 월 25 05:03:28.265 오후 DEBUG - IPin.PublicInfo(117) | IDP_CODE = H
9 월 25 05:03:28.265 오후 DEBUG - IPin.PublicInfo(118) | DUP_INFO = yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy
9 월 25 05:03:28.265 오후 DEBUG - IPin.PublicInfo(119) | REAL_NAME = 홍길동
9 월 25 05:03:28.265 오후 DEBUG - IPin.PublicInfo(120) | CP_REQUEST_NUMBER = zzzzzzzzzzzzzzzzzz
9 월 25 05:03:28.266 오후 DEBUG - IPin.PublicInfo(121) | RETURN_URL = http://p-clean.kisa.or.kr/hp/sig/ipin_sig_return.jsp
9 월 25 05:03:28.266 오후 DEBUG - IPin.PublicInfo(122) | SEX = 1
9 월 25 05:03:28.266 오후 DEBUG - IPin.PublicInfo(123) | NATIONAL_INFO = 0
9 월 25 05:03:28.266 오후 DEBUG - IPin.PublicInfo(124) | BIRTH_DATE = 19720313
9 월 25 05:03:28.267 오후 DEBUG - IPin.PublicInfo(125) | AUTH_INFO = 0

9 월 25 05:03:28.283 오후 DEBUG - IPin.PublicInfo(141) | AltJuminUtil 처리결과(retStr) : MIIBugIBADAKBggqgxqMmkQBBAOB4QB8E3BNW/IIiEUdvgu0TwTnXYepemDAQglBgbHad7wgpQ5nSvoLLYo4yJdjEx5mN3lDTKo/uipePnCIFehaXGuYfgh/j0JlKhXPLwWJVNK9SwvU+dB1RTDfAdhjhtN2QrmvzYem+4rEoSNQXGc4xK7d79vIp/7olJZ4F2H3Wr+kedHNw++s+S/jKGdj8I6UanrnF6Y8eIL/pcdj7NY94HfqJZEnM3BamfCWCVcjevu/xjXGX/pNWnyY07pelkqpeAv2XhRY1F25LCJrtLJK7yKC0r3AcYuz+SWM7Iqk7Yq4QSxvdT1BY2NyZWRpdGVkQ0Esbz1LSUNBLGM9S1IwDQYJKoZIhmcNAQEFBQADwYEAapgaEPZuv5nKZLaKS1ZDw3bQIO6bH4KroKkrDiQ6iIcWvZdkY9R9CgCZyytim1/trI+0dk4e/4hTOqm4P/j252WG0sknu6v0EyqIFSd53cbGuv8qKpVzs/4x+aWS/2Iwa98lO7gXnI5IXYUkxPJZ2yiC7jLxMJcbW/yqx2t9WYY=

(그림 4) 공공 i-PIN 가입자인 경우, 공공 i-PIN 제공자가 민간 i-PIN 제공자에게 전달하는 PublicInfo 메시지