온라인상에서 디지털 사용자 신원 확인 가이드에 대한 연구

김종배
세종사이버대학교 컴퓨터소프트웨어학과
e-mail: jb.kim@sjcu.ac.kr

A Study on Digital Identity Guidelines of NIST

Jong-Bae Kim
*Dept of Computer and Software, Sejong Cyber University

요 약

본 연구는 미국 상무부 소속 국립표준기술연구소(NIST)에 의해 제시된 온라인상에서 디지털 신원 지침(digital identity guidelines)에 대한 내용을 살펴보고, 디지털 신원 서비스를 구현하기 위한 기술적인 요구사항들에 대해 검토 후 국내 본인확인서비스에 적용이 가능한 방안을 제시한다. 온라인상에서 사용자의 신원을 확인하기 위해 다양한 방안이 제시되고 있으며 현행 국내 본인확인서비스의 경우 과도한 개인정보 제공으로 사생활 침해 이슈가 제시되고 있다. 따라서 NIST의 디지털 신원지침에서 제시하는 차등화된 서비스 제공 방안에 대해 검토하고 국내 본인확인서비스에 적용 가능한 방안을 모색한다. 제시한 방안에서 획일화된 본인확인서비스에서 본인확인수단, 인증, 정보제공에 대한 차별적인 방안을 제시함으로써 보다 안전하고 건전한 본인확인서비스의 실현이 가능함을 알 수 있다.

1. 서론

온라인상에서 비대면 거래 확대로 인해 거래 대상 상대방의 디지털 신원을 확인하고 사용자의 개인정보를 보호하기 위한 효율적인 방안들이 제시되고 있다[1-6]. 국내에서는 주민등록번호 수집 금지에 따른 주민등록번호 대체수단 기반의 본인확인서비스가 온라인상에서 본인확인 수단으로 널리 활용되고 있으며, 유럽의 경우는 전자신분증(eID)의 확대로 인해 국경간 전자신분증을 사용한 디지털 상의 본인확인서비스의 적용이 활발히 진행되고 있다[4]. 또한 미국에서도 NIST의 디지털 신원 확인 지침[7]의 공표로 인해 안전하고 보다 이용자 측면의 이익이 보장되는 방향으로 온라인상의 본인확인서비스의 활성화를 꾀하고 있는 상황이다. 이처럼 온라인상에서 비대면 거래에 있어 상대방의 신원확인은 거래의 신뢰성 확보에 중요한 이슈로 부각되고 있다. 국내에서는 다양한 관련법에서 온라인 상대방의 신원을 명확히 확인하도록 요구하고 있으며 재화나 금전거래 시 소비자 보호를 위한 방안으로 신원확인 요구, 청소년 연령 확인을 통해 건전한 온라인 서비스 시장의 활성화를 꾀하고 있다. 그러나 국내 온라인 서비스 시장에서는 온라인 사업자들이 본인확인을 위해 서비스 적용이 고려해야할 사항들에 대한 안내나 기준 제기가 없는 상황이다. 물론 「정보통신망법」과 「개인정보보호법」등에서 사용자의 개인정보수집 시 최소 수집을 원칙으로 하고 있으며 수집 이후 목적 달성 시 지체 없이 파기하도록 규정하고 있다. 하지만, 최소 수집 원칙에 대한 기준과 목적 달성에 대한 기준이 존재하지 않아 온라인 사업자들 입장에서는 온라인 거래에서 수집한 본인확인 관련 정보들에 대해 법적 대항력 확보 등을 이유로 본인확인서비스 관련 개인정보들을 보관하고 있는 상황이다[4]. 개인정보 보관 사유로는 소비자 불만 대처, 피해 보상 시 사용자 식별, 민원 대응 등의 목적으로 기인하고 있다. 결국, 국내 온라인 사업자들은 민원대응이라는 명분하에 본인확인서비스의 과도한 적용이 실질적인 문제점 발생이 원인이라 할 수 있다. 즉, 온라인 서비스 회원가입, 서비스 이용, 질문, 정보 변경 등에서 주민번호 대체수단 기반의 본인확인서비스를 적용함에 있다. 게다가 온라인 서비스 이용자 역시 본인확인서비스를 통해 제공하는 개인정보에 대한 선택권 없이 획일적인 본인확인 정보 제공 동의에도 과도한 개인정보 제공에 문제점으로 귀결될 수 있다. 국내와 달리 국외사례에서는 온라인 서비스 이용자의 보호에 집중하여 과도한 개인정보의 사업자 제공을 원천적으로 차단하고 있는 상황이다. 따라서 본 연구에서는 국외 온라인 본인확인관련 동향을 확인하고 특히 미국의 NIST의 디지털 신원 지침[7]에 대한 살펴보고 국내 적용 가능한 방안을 제시하고자 한다. 이를 통해 국내에서 과도한 본인확인서비스 적용, 개인정보 제공의 선택권 보장, 온라인 사업자의 적용 가이드라 제시 등으로 현행 본인확인서비스의 안전성 확보가 가능함을 알 수 있다.

2. NIST 디지털 신원 지침(Digital Identity Guidelines) 개요

디지털 신원 지침은 미국 상무부 소속 국립표준기술연구소(NIST)에 의해 작성되었으며, 디지털 신원 서비스를 구현하는 정부기관에게 기술적인 요구사항을 정의하고 있다[ ]. 디지털 신원확인을 위한 프로세스, 인증 프로세스, 인증 환경 및 속성 정보를 신뢰 당사자(Relying Party)에게 전달하는 데 사용되는 연합 환경에서의 이용자가 본인이라고 주장(assertion)은 수단의 강도 보장 프로세스 세 부분으로 나누어 각 프로세스를 상세히 설명하고 있다. 디지털 신원확인 지침에서 인증 절차를 나타내는 인증 프로토콜은 본인확인을 요청하는 청구자가 자신의 신원을 확인하기 위해 하나 이상의 유효한 인증자를 소유 및 제어권을 갖고 있음을 입증하고, 선택적으로 청구자가 의도한 검증자(verifier)와 통신하고 있음을 입증하는 청구자와 검증자 사이의 정의된 메시지 순서를 정의하고 있다. NIST에서 제시하는 디지털 신원 확인을 위한 모델은 그림 1과 같다. 디지털 신원확인을 위한 절차는 다음과 같이 수행한다.

① 신청자는 등록 절차를 통해 CSP(credential service provider, 본인확인기관)에 가입신청 한다.
② CSP는 신청자의 신원 증명을 수행한다.
③ 인증자(예: ID, 여권번호, 신용카드번호, 휴대폰 번호)와 인증자에 대응하는 증명서(예 : ID/PSW, 여권, 신용카드)가 CSP와 가입자 간에 설정된다.
④ CSP는 증명서의 상태와 증명서의 수명주기 동안 수집한 등록 데이터를 유지·관리 한다.

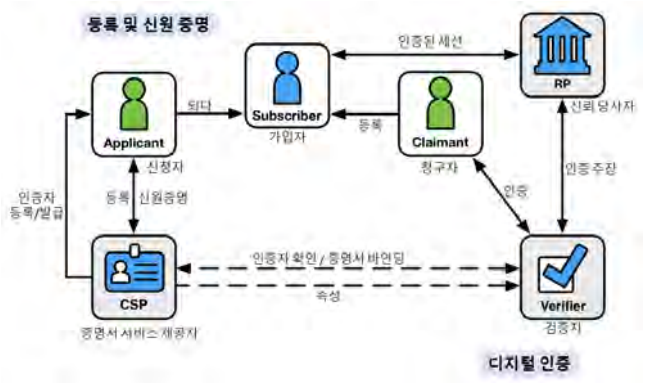

그림 1 NIST의 디지털 신원 모델[7]

그림 1과 같이 본인확인서비스 이용자가 본인확인기관에게 본인의 신원을 확인받고 이후 신원이 증명되면 이용자에게 본인확인기관이 가입자로 처리하고 관련 신분증명수단을 제공하게 된다. 이러한 처리과정은 국내 본인확인서비스와 유사하다고 할 수 있다. 다만, 국내 본인확인서비스와의 차이점은 다음과 같다. 디지털 신원확인 시스템은 단일 보증수준(Level of Assurance, LOA)이 아닌 디지털 인증의 각 개별 구성요소에 대한 위험과 영향을 평가하여 가증 효과적인 신원확인 서비스를 제공하도록 구성하고 있다. 결국, 디지털 신원 지침에서는 온라인상에서 본인확인을 수행하기 위한 절차를 마련하고 이후 발생할 수 있는 위험들, 즉 신원증명오류(가짜 신청자), 인증오류(가짜 청구자), 사업자간 오류(정보손상) 등에 대해 개별적으로 평가하여 각 서비스 적용 시 필요한 보증 수단을 결정하도록 정의하고 있다.

3. 보증 수준의 종류

디지털 신원지침에서는 디지털신원확인 과정에서 발생하는 다양한 오류들에 대해 사전에 위험을 분석하고 그 위험을 근거로 위험을 회피하거나 처리하기 위한 적절한 보증 수준을 정의하고 있다. 그 보증 수준들은 표 1과 같이 나열한다.

표 1. NIST 디지털 신원 지침의 보증 수준[7]

보증수준	내용
IAL	서비스 이용자의 신원 확인 수준
AAL	서비스 이용자가 제시하는 인증 수단 및 증거 수준
FAL	사업자에게 제공하는 서비스 이용자의 개인정보 전달 수준

표 1과 같은 디지털 신원확인에서 보증수준들은 다시금 3단계로 구분한다. 신원보증수준((Identity Assurance Levels, IAL)은 증명 없이 이용자가 제시한 것으로 인증(IAL1), 디지털 신원 지침에 따른 원격 신원 증명 또는 대면 신원 증명(IAL2), 그리고 본인확인기관으로부터의 신원 증명(IAL3)로 구분한다. 인증자에 대한 보증수준(Authenticator Assurance Levels, AAL)은 단일 인증(AAL1), 이중 인증(AAL2), 높은 수준의 암호화 인증(AAL3). 연합 보증 수준(Federation Assurance Levels, FAL)애에서는 본인확인기관에 제공한 정보의 암호화(FAL1), 온라인 사업자만이 복호화할 수 있는 정보의 암호화(FAL2), 개인정보 소유자가 승인하여 복호화할 수 있는 정보의 암호화(FAL3)로 구분한다. 이처럼 각각의 보증수준을 결정하기 위해 본인확인서비스 제공에 있어 발생가능한 잠재적인 위험을 평가하고 그 위험을 최소화하기 위한 보증수준을 적용하도록 정의하고 있다. 위험을 평가하기 위한 범주에는

① 불편함, 고통, 명성 또는 평판에 대한 손상
② 금전적 손실 또는 정부기관 책임
③ 정부기관의 소관업무나 공공 이익에 끼치는 해
④ 민감한 정보의 무단 공개
⑤ 개인의 안전

이와 같이 본인확인서비스 적용 시 보증수준을 채택하

기 위해 위험평가를 통해 각 위험에 대한 높고 낮음을 평가하고 그 결과를 바탕으로 본인확인서비스 시 거래 당사자의 신원을 확인할 것인지 아닌지를 결정하도록 제시하고 있다. 그림 2는 IAL 결정을 위한 선택 트리를 나타낸 그림이다.

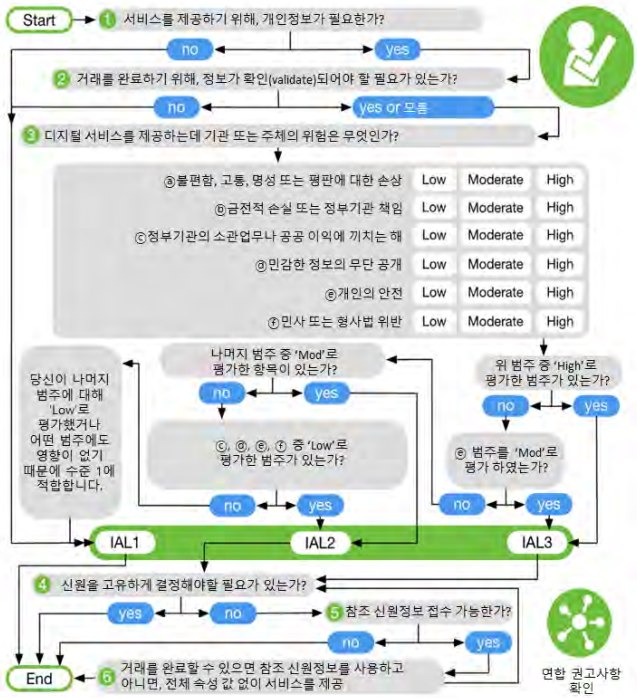

그림 2 IAL 결정 트리[7]

그림 3은 AAL 보증 수준 결정하기 위한 위험 평가 결과를 바탕으로 온라인 본인확인서비스 제공 시 가장 적합한 인증에 대한 요구사항을 선택할 수 있도록 제시한 선택 트리를 나타낸 그림이다.

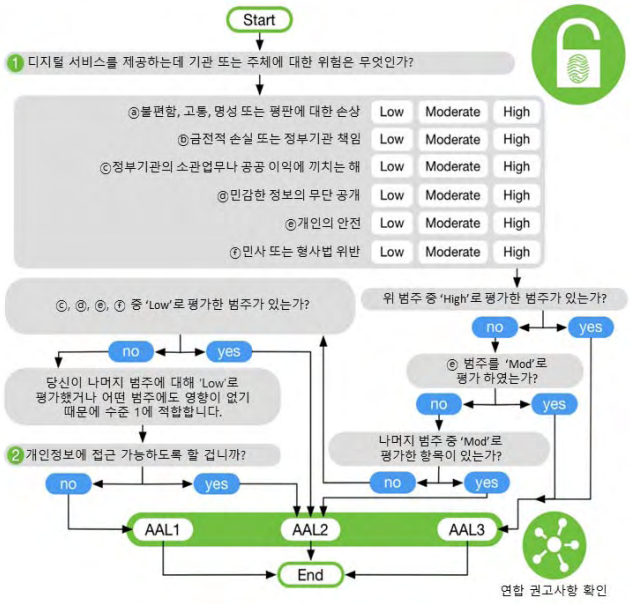

그림 3 AAL 결정 트리[7]

그림 4는 FAL 보증 수준 결정하기 위한 위험 평가 결과를 바탕으로 온라인 본인확인서비스 제공 시 가장 적합한 인증에 대한 요구사항을 선택할 수 있도록 제시한 선택 트리를 나타낸 그림이다.

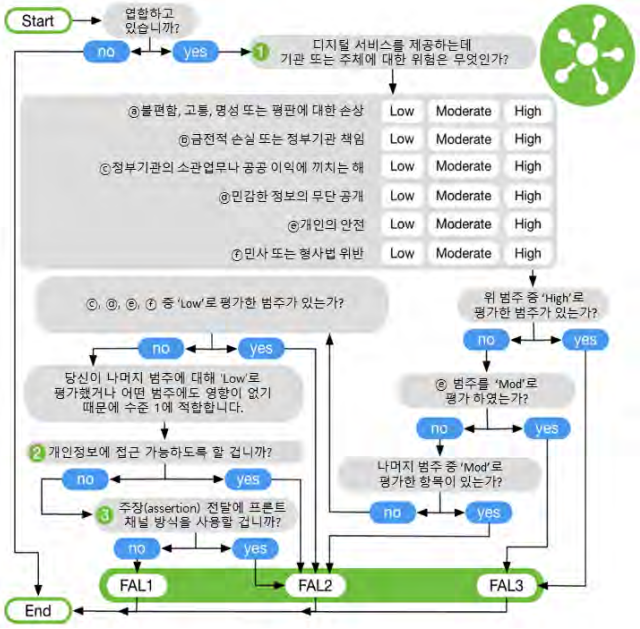

그림 4 FAL 결정 트리[7]

온라인 서비스에 본인확인수단을 도입하기 위해 NIST에서는 디지털 신원지침을 통해 무분별한 본인확인서비스를 도입할 것이 아니라 사업자가 직접 본인확인서비스 도입에 따른 위험을 분석하여 각각의 보증수준에 적합한 본인확인 요구 수준을 적용하도록 정하고 있다. 각 보증수단에 따라 요구하는 요구 사항을 차등화 하여 제시하고 있다.

4. 결론

NIST의 디지털신원확인 지침과 같이 국내 본인확인서비스에서 제공과 적용에 있어서도 본인확인기관이 본인확인서비스 도입 시 고려해야할 사항을 정의하고 이를 바탕으로 온라인 사업자가 본인확인서비스를 도입 및 활용하는 것이 필요하다. 현행 본인확인서비스에서도 서비스 이용 시 사용자 입장에서는 동일한 보증 수준, 즉, 아이핀 ID/PW/2차 PW, 휴대폰 SMS, 신용카드 번호 및 비밀번호를 제공함으로써 온라인 사업자들에게 제공되는 정보는 동일한 수준의 개인정보가 제공되고 있다. 본인확인서비스의 수준과 용도에 따라 단순히 본인임을 증명하는 수준, 청소년 여부를 확인하는 수준, 다른 온라인 사업자들과의 서비스 연계 수준 등 목적에 따라 필요한 개인정보만을 제공하는 것이 필요하다. 이를 위해서는 본인확인기관이 온라인 사업자들이 왜 본인확인서비스 사용자의 개인정보가 필요한지는 입증 받아 그 입증에 타당한 개인정보만을 제공하는 과정의 제시가 요구된다. NIST의 디지털 신원

확인 지침과 같이 차등화된 본인확인서비스 수준을 제시하고 이를 활용하기 위한 방안을 개발하는 것이 필요하고 온라인 서업자들에게도 스스로 제공하는 서비스에 맞는 본인확인수준을 적용하도록 하는 정책적인 방안 제시가 필요할 것이다.

Acknowledgement

본 논문은 “교과부 일반연구자원사업”의 지원을 받아서 수행되었음(NRF -2016R1D1A1B03931986)

참고문헌

[1] J. B. Kim, “Safety Improvement Methods of Personal Identification Services using the I-Pin”, Journal of Information Technology Services, vol. 16, no. 2, pp. 97-110, 2017.

[2] J. S. Choi, S, J, Lee, J. B. Kim, “A Study on improvement of the reliability of personal identification service based on the replacement methods of resident registration number by differentiated assurance levels”, Proceedings of KICS, pp. 858-859, 2019.

[3] J. S. Choi, J. B. Kim, “A Study of improving user authentication procedures for enhanced safety of personal authorization methods”, Proceedings of KIPS, vol. 22, no.2, pp.668-671, 2015.

[4] 김종배, 최중석, 전동호, 이재호, 박기홍, "본인확인기관 지정기준 및 관리체계 개선방안 마련", 한국인터넷진흥원 연구보고서, KISA-WP-0138, 2018.

[5] 신영진, 신승호, 이자성, 한웅기,“한국에서의 본인확인수단 개선방안에 관한 연구”, 한국지역정보화학회지, 제18권, 4호, pp.69-88, 2015.

[6] 안정희, “인터넷상의 주민등록번호 대체수단의 문제점들과 해결방법”, 디지털산업정보학회, 제4권, 제3호, pp.45-53, 2008.

[7] NIST 디지털 신원 지침 가이드라인, https://pages.nist.gov/800-63-3/, 2019.