개인정보보호를 위한 국제표준 기반 전자인증 등급과 관련 기준 분석

조효제, 고재남, 염흥열
정보보호학과, 순천향대학교
e-mail: sfkino@gmail.com, freeinlove1127@gmail.com, hyyoum@sch.ac.kr

Analysis of e-authentication assurance levels and their criteria based on an International Standard for protection of personal information

Hyo-Je Jo, Jae-Nam Go, Heung-Youl Youm
Department of Information Security Engineering, Soonchunhyang University

요 약

개인정보의 유출을 막기 위해서는 안전한 인증 수준을 이용해야 한다. 그러나, 인증 수단의 인증 등급은 응용 서비스의 중요성과 민감도에 비례해 선택되어야 한다. 본 논문에서는 국내 다양한 분야의 전자인증 환경을 분석하고, 국제 표준 (ITU-T X.1254 | ISO/IEC 29115) 에 근거한 4 가지 전자인증 등급과 기준을 분석한다. 또한, 국제표준방식의 인증 등급과 국내 분야의 인증 등급을 상호 비교한다.

1) 인증 보증 등급, 인증 기준

1. 서론

인터넷의 급격한 확장과 모바일 사용자 디바이스의 증가는 다양한 오프라인 서비스들을 온라인 환경으로 옮겨 놓고 있다. 이러한 환경 변화와 더불어, 이러한 편리성에 비례해 온라인 환경에서 대규모 개인정보가 유출되고 있고, 금전과 관계된 다양한 보안 사고가 빈번히 발생하면서 개인정보관리체계 (PIMS, personal information management system)의 중요성이 부각되고 있다. 이로 인해 사용자의 개인정보를 보호하기 위해 요구되는 전자인증의 중요성 또한 부각되었다.

전자인증은 온라인 환경에서 정당한 사용자임을 확인하기 위해 사용되는 인증 수단들로서, 온라인 환경에서 처리되는 다양한 서비스가 늘어나면서 다양한 형태로 발전하였다. 그러나, 국내에서는 전자인증 수단을 선택하고 도입하기 위한 국가적 차원의 명확한 등급이 존재하지 않아서 금융, 전자상거래, 전자민원 등의 분야에서 적합한 전자인증 수단의 선택에 어려움을 겪게 되었다. 이러한 문제점을 해결하기 위해 국내외에서는 전자인증 수단의 도입의 기준이 될 수 있는 다양한 가이드라인을 제시하고 있지만 국내 환경에 적합하면서 다양한 분야를 아우룰 수 있는 전자인증 등급과 기준은 아직 존재하지 않는다.

본 고에서는 현재 국내의 전자인증 환경에 맞는 가이드라인을 개발하기 요구되는 국내 다양한 인증 환경에 대한 인증방식을 분석하고, ITU-T X.1254/ISO/IEC 29115 (개체 인증을 위한 보안 프레임워크 ISO의 x.1254)에서 제시한 인증 보증 수준과 관련 기준을 분석한다.

1) 본 연구는 방송통신위원회의 지원을 받는 방송통신표준기술력향상사업의 연구결과로 수행되었음

* 주 저자. sfkino@gmail.com
* 교신저자. hyyoum@sch.ac.kr

2. 국내 전자인증 환경 분석[1]

국내 온라인 환경에서 전자인증이 적용된 분야는 크게 일반포털, 전자상거래, 전자민원, 금융거래로 구분된다. 각 분야들 <표 1>과 같이 취급하는 정보의 중요성, 피해 가능성 등에 따라 다양한 인증수단들을 도입하여 사용하고 있다.

2.1 일반포털

단순 검색 서비스만을 제공하던 초기의 포털들이 발전하여 개인메일, 홈페이지, 블로그, 카페 등의 개인사용자 맞춤 서비스를 도입하면서 사용자의 인증의 중요성이 부각되었다. 현재 포털들은 회원가입 시 주민등록번호와 I-PIN(internet-personal idnetification number)을 사용해 사용자를 본인확인하고 있으며, 서비스를 이용하기 위해서

는 ID/PASSWD를 사용하고 있다. 또한 일정 강도 이상의 패스워드를 사용하고 패스워드 사용 기간이 일정기간 이상 지났을 경우 패스워드를 교체하도록 권유하고 있다. 패스워드를 분실했을 경우 e-mail, 휴대전화 인증, 질문/응답 등의 방식으로 정당한 사용자임을 식별하는 과정을 거친다.

2.2 전자상거래

전자상거래 서비스는 사용자가 필요로 하는 재화들을 온라인 환경에서 구매 할 수 있는 서비스로 오프라인 환경보다 자본금이 적게 드는 등의 다양한 이점으로 온라인 전자상거래가 활성화되기 시작했다. 전자상거래는 일반 포털과 달리 금전적인 거래가 이루어지기 때문에 좀 더 높은 보안성을 요구하며 사용자 인증 방식 또한 강화되어야 한다. 전자상거래 서비스 사이트에 접근하기 위한 사용자 인증과 식별과정은 포털 사이트와 거의 동일하지만 전자상거래 서비스에서는 추가적으로 재화의 거래 시 거래액수와 결제수단 등에 따라 인증과정이 추가된다. 대표적인 인증 방법으로는 공인인증서, 안심클릭, 휴대폰 결제 등이 있다.

2.3 전자민원

전자민원 서비스는 대면환경에서만 처리할 수 있었던 행정 민원서비스들을 온라인 환경에서 처리할 수 있도록 하는 서비스이다. 이러한 전자민원 서비스가 활성화 되면서 사용자가 시간과 장소의 제약에서 벗어나 자유롭게 민원 서비스를 받을 수 있게 되었으며 높은 편의성을 제공하게 되었다. 그러나 전자민원 서비스는 사용자의 민감한 개인정보들을 담고 있어 정보의 접근 및 취급에 대해 높은 보안성을 제공해야 한다. 전자민원을 위한 홈페이지인 민원24에서는 취급하는 정보에 따라 ID/PASSWD, 공인인증서, I-PIN,G-PIN, 주민등록번호 등의 방법으로 사용자를 본인확인 한다.

2.4 전자금융

전자금융은 온라인 환경에서 은행거래, 주식거래 등의 다양한 금융 서비스를 가능하게 하는 온라인 금융거래 서비스이다. 이체, 대출, HTS (Home Trading System)등의 금융서비스는 다른 서비스들과 달리 사용자의 자산에 직접적인 영향을 미치므로 높은 보안성을 필요로 한다. 현재 온라인 뱅킹 에서는 잔액조회 와 같은 단순 조회서비스에 접근하기 위해 ID/PASSWD를 이용하며 계좌이체 등의 직접적인 자산의 변동을 주는 서비스는 올바른 사용자를 확인하기 보안카드, 계좌 비밀번호, 공인인증서 등의 사용자 인증, 식별 수단들을 사용한다. HTS와 같은 주식거래 시스템은 ID/PASSWD와 공인인증서를 통해 사용자를 인증한다.

3. 전자인증을 위한 국제표준 분석

전자인증을 위한 국제표준인 ITU-T의 개체인증을 위

<표 1> 서비스별 전자인증 수단 이용 사례

서비스	항목	인증 & 식별 수단
공통	회원가입	▪ 주민등록번호, I-PIN
	비밀번호 분실 (전자금융제외)	▪ 주민등록번호 + 공인인증서, ▪ 주민등록번호 + 등록된 휴대폰 ▪ 주민등록번호 + E-mail ▪ 주민등록번호 + 질문/응답
포털 서비스	로그인	▪ ID/PASSWD
전자상거래 서비스	로그인	▪ ID/PASSWD
	거래	▪ 실시간 계좌이체, 은행송금(현금결제, 전자금융을 이용) ▪ 안심클릭, Internet Secure Payment (카드결제, 거래 전 카드사에 미리 제출한 비밀번호 입력) ▪ 공인인증서 (30 만원 이상 거래시)
전자민원 서비스	로그인	▪ ID/PASSWD ▪ 공인인증서
	민원신청	▪ 주민등록번호, I-PIN (중요도가 낮은 정보) ▪ ID/PASSWD + 공인인증서 (중요도가 높은 정보)
전자금융 서비스	로그인	▪ ID/PASSWD ▪ 공인인증서 ▪ ID/PASSWD + 공인인증서 (Home Trading System)
	금융거래	▪ 공인인증서, 보안카드, 계좌 비밀번호, OTP, 지문인식 (다양한 인증수단을 복합적으로 사용)
	비밀번호 분실	▪ 통장 계좌정보 ▪ 공인인증서

한 보안 프레임워크 (ITU-T X.1254 | ISO/IEC 29115)은 금년 9월 연구반 17회의에서 최종 승인되었고, 현재 ISO/IEC JTC 1에서는 FIDS 진행중이다. 본 표준은 개체 인증을 위한 보증 레벨 수립 기준을 제시하고 있다. 구체적으로, 총 4단계의 인증 보증 등급을 제시하고 있고 각 인증 보증 등급별 요구조건, 대처 가능한 위협 등을 기술하고 있다.

3.1 인증 보증등급[2]

보증 등급은 가장 낮은 등급인 1등급에서 가장 높은 등급인 4등급까지 총 네 등급으로 나누어진다.

1등급에서는 주장된 신원정보(identity)에 대해 최소한도나 거의 신뢰하지 않아도 되는 경우에 사용된다. 이 인증 등급은 인증 실패 시 최소한의 위험이 초래되는 경우에 사용된다. 또한 이 등급에서 사용되는 암호학적 인증 방식의 이용을 요구하지 않는다. 이 등급에 적용될 수 있는 인증수단은 사용자가 직접 등록한 ID/PASSWD을 들 수 있다.

2등급에서는 주장된 신원정보에 대해 약간의 신뢰성이 있는 경우에 이용되며, 인증이 실패하는 경우 적정한 위험이 초래되는 경우 사용한다. 또한 이 등급에서는 단일요소(single-factor) 인증을 허용한다. 주요 통제는 도청 및 온라인 추측 공격의 효과성을 감소하고, 저장된 인클리덴셜에 대한 공격을 막을 수 있는 통제를 작동해야 한다.

3등급에서는 주장된 신원정보에 대한 높은 신뢰성이 존재하며, 인증이 실패한 경우 높은 위험을 초래하는 경우 사용된다. 인증 정보는 이 등급에서는 다중 인증을 요구하며, 인증 과정동안 교환되는 어떤 비밀도 암호학적으로 보호되어야 한다. 클리덴셜은 일반 컴퓨터 또는 전용 하드웨어 상에서 생성되고 저장된다. 인증의 실패 시 실질적인 위험을 초래한다.

4등급에서는 주장된 신원정보에 대해 매우 높은 신뢰성을 가지며 인증 실패시 매우 높은 위험을 초래하는 경우 사용된다. 이 등급에서는 모든 정보들을 하드웨어 장치를 사용해 보호하도록 지침하고 있으며 내부자에 의한 사용자 신원확인 과정이 추가되었다. 또한 인증프로토콜에서 사용되는 개인식별정보 (Personally Identifiable Information)를 포함한 모든 데이터를 암호화 하도록 지침하고 있다.

<표 2> 보증등급별 위협 영향

인증 실패의 잠재 결과	인증 실패 잠재 영향 정도			
	1	2	3	4
불편, 고통, 또는 명예 훼손	min	mod	sub	high
금융 손실 또는 기관 책임	min	mod	sub	high
조직, 조직 프로그램 그리고 공익의 피해	-	min	mod	high
민감 정보의 비인가 공개	-	mod	sub	high
개인의 안전	-	-	min mod	sub high
인권 침해 또는 형사적 범죄		min	sub	high

3.2 보증 등급을 선택하기 위한 등급별 위협 영향 평가[3]

응용 서비스 제공자는 업무와 서비스의 중요도 그리고 인증 실패시 잠재적인 영향에 따라 인증 보증 등급을 선택해야 한다. 보증 등급에 대한 위협은 인증이 실패할 경우 발생할 수 있는 여섯 가지 항목에 대한 영향을 낮음(min), 보통(mod), 높음(sub), 매우 높음(high) 으로 구분 비교하여 각 항목에 대한 등급별 위협 영향 정도는 <표 2>와 같다.

첫 번째 항목인 불편, 스트레스, 명예훼손은 실질적인 금전적인 피해는 입히지 않지만 정신적인 피해를 일으키거나 온라인 활동에 불편을 끼치는 것을 의미하며, 두 번째 항목인 금융적 손실 및 기관의 책임은 실제 금액적인 피해를 입거나 법적 책임을 물어야 하는 상황을 의미한다. 세 번째 항목인 공공의 피해, 프로그램의 손상 등은 위협으로 인해 프로그램이 손상될 수 있거나 다수 혹은 공공의 피해가 발생하는 경우를 의미한다. 네 번째 항목인 인가되지 않은 민감한 정보접근은 사용자 개인의 보호되어야 하는 개인정보들이 공개되거나 유출되는 경우를 의미한다. 다섯 번째 항목인 개인의 안전은 위협으로 인해 단순 온라인상의 피해가 아닌 오프라인 상의 사용자 피해가 발생할 수 있는 경우를 의미하며 마지막 항목인 민형사상의 위배는 민형사상의 조항에 위배되는 경우를 의미한다.

3.3 국내 인증 수준 매핑

국제표준에서 정의된 인증 등급을 국내환경에서 이용되고 있는 분야에 적용해 보면, 국내 일반 포털들은 인증이 실패할 경우 개인의 정보유출, 사생활 노출 등의 문제점이 발생할 수 있고 단일요소 인증을 사용되므로 국제표준에서 정의된 2등급과 매핑시킬 수 있으며, 금융거래는 인증의 실패가 개인의 자산에 직접적인 피해를 끼칠 수 있으므로 다중인증을 요구하며 인증과정의 모든 정보가 암호화 되며, 공인인증서, OTP 등의 인증수단들이 HSM과 같은 전용하드웨어 또는 사용자의 기억장치에 직접 저장되므로 국제표준에서 정의된 3등급과 매핑 된다고 볼 수 있다.

4. 결론

본 논문에서는 국내에 적용되어 있는 전자인증 환경을 알아보고 전자인증 국제표준을 분석했다. 국내의 전자인증 가이드라인으로는 금융감독원의 인증수단 안전성 기술평가기준이 있으나 이 가이드라인은 금융권 인증수단에만 해당되어 일반 분야의 다양한 전자인증 등급으로 적용하기에는 어려운 것이 사실이다. 국제표준(X.1254 | ISO/IEC 29115)에서는 네가지 종류의 인증 등급을 제시하고 있으며 각 등급별로 구체적인 요구사항과 기준을 제시하고 있다. 따라서 이 기준과 등급은 다양한 인증 환경에 적용 가능하다. 그러나 이 표준은 서비스에 비해 상대적으로 높은 수준의 보안성을 요구하고 있어서 국내 인증 환경과 적절하게 매칭되지 않은 측면이 있다.

따라서 국제표준을 근거로 한 국내 인증 등급과 기준을 개발할 경우 국내 인증 환경을 고려해 국내 환경의 다양한 인증 서비스에 적용 가능한 범용성이 높은 인증 등급과 기준에 대한 가이드라인이 개발되어야 할 것이다.

참고문헌

[1] 조효제, 이동희, 정영곤, 장기헌, 이상래, 염흥열 "전자인증 가이드라인 개발을 위한 보안위협 분석" 한국정보보호학회, 2011.11.

[2] 순천향대학교, "전자인증수단 이용기반 확대를 위한 안전성 기준 연구", 한국인터넷 진흥원, 2011.11.

[3] ITU-T X.1254 | ISO/IEC 29115, Entity Authentication Assurance Framework, 2012.