국내 전자금융 서비스 환경을 위한 ISO/IEC 29115와 ISO/IEC 29003의 갭분석☆

김 경 한* 유 동 현* 김 수 형** 윤 봉 중*** 염 흥 열*

◈ 목 차 ◈

1. 서 론

전 세계적으로 클라우드, 사물인터넷, 빅데이터 서비스가 활성화 되고, 최근 규제완화로 인하여 국내에서도 핀테크, 인터넷 전문은행 등의 서비스가 활성화 되고 있다. 이 신규 서비스의 이용에 있어 본인확인의 중요성이 대두되고 있다. 본인확인 이란 본인확인정보를 입력하고 인증 절차를 통하여 본인 여부와 본인이 등록한 정보의 정확성을 확인하는 것으로 크게 신원확인과 실체 인증으로 이루어진다. [5]

ISO/IEC 29115[1]에서는 4단계의 보증레벨(Level of assurance)을 제시하며, 인증 위협과 이에 대한 통제사항, 보증레벨 기준, 관련 용어, 관련 주체, 실체인증을 위한 프로세스 등을 제시한다.

ISO/IEC 29003[2]에서는 3단계의 신원 확인 레벨(Levels of identity proofing)과 요구사항을 제시하며, 신원확인 목표, 신원확인 정보, 관련 용어, 관련 주체, 신원확인 프로세스 등을 제시한다.

본 논문에서는 한국정보보호학회 학술지 논문[5]에 바탕을 두고, SC 27/WG 5에서 수행하고 있는 본인확인 국제 표준화 동향을 살펴보며 그 표준의 주요 내용을 제시한다. 본 논문의 2장에서는 ISO/IEC 29115의 적용과 활용 방안을 제시하고, 4단계의 보증레벨 기준 등을 분석한다. 또한, ISO/IEC 29003과의 비교를 통해 갭 분석(Gap analysis)을 진행한다. 3장에서는 개발중인 ISO/IEC 29003과의 상호 호환방안을 제시한다.

2. 본인확인 관련 국제표준

2.1 본인 확인 국제표준 개요

아이덴터티 및 프라이버시 작업반(WG5)의 실체 인증 보증 프레임워크는 [그림 1]과 같다. 본인 확인은 등록, 크리덴셜 관리, 인증 세 단계로 구성되며 전체 프로세스는 [그림 2]와 같다.

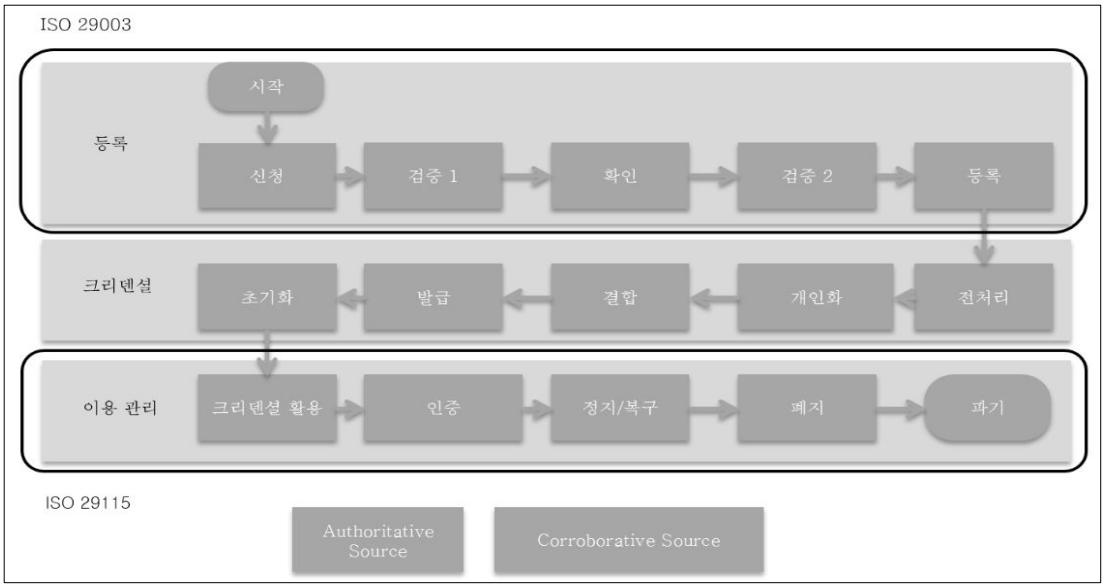
2.2 ISO/IEC 29115

ISO/IEC 29115는 실체 인증 보증 프레임워크에 관한 표준이며, 이 표준은 2013년 국제 표준으로 채택되었다. 이 표준에서는 4단계의 보증레벨을 제시하며, 인증 위협과 이에 대한 통제사항, 보증레벨 기준, 관련 용어, 관련 주체 등을 제시하고 있다. 실체 인증 보증 프레임워크의 주요 주체는 인간개체와 비인간 개체 및 크리덴셜 서비스 프로바이더, 등록 기관, 검증자로 구성된다.

* 순천향대학교 정보보호학과
** ETRI 인증기술 연구실
*** 금융결제원 표준화팀

기술적		관리 및 운영
등록단계	시작 및 신청 등록 신원 확인 레코드 보관 및 기록 신원 검증 ISO 29003	서비스 설립 법적, 계약적 컴플라이언스 금융 규정 정보보호관리 및 감사 외부 서비스 구성요소 운영 인프라 운영능력 측정
크리덴셜 관리	크리덴셜 전처리 크리덴셜 대체 크리덴셜 초기화 크리덴셜 갱신 크리덴셜 결합 레코드 보관 크리덴셜 생성 및 저장 크리덴셜 발급 및 활성화 크리덴셜 정지/폐지 및 파괴	
실체 인증	인증 레코드 보관 ISO 29115	

(그림 1) 실체 인증 보증 프레임워크



(그림 2) 본인 확인 프로세스

관련된 소스로는 권위기관(Authoritative source)과 협력기관(Corroborative source)이 있다. 권위기관은 국내에서는 정부기관에 해당하며, 협력기관은 실체 인증을 수행하는 관련 서비스 프로바이더가 해당된다.

실체 인증 보증 프레임워크에서는 각각의 단계에서 LoA에 따른 위협을 식별하고 이에 대한 통제 사항들을 제시한다. 통제사항들은 인간개체와 비인간개체에 대하여 개별적으로 제시된다. 등록단계에서는 정책고수, 대면, 정보출처에 대한 위협을 식별하고 통제사항을 제시하며 크리덴셜 관리 단계에서는 위변조, 유출, 복제, 가용성 등에 대한 위협을 식별하고 통제사항들을 제시한다. 인증단계에서는 온/오프라인 게싱, 피싱, 도청, 중간자 공격 등에 대한 위협을 식별하고 통제사항들을 제시한다. 실체 인증 보증 프레임워크에서 보증레벨을 적용하는 기준은 [표 1]과 같다.

(표 1) 보증 레벨

LoA	설명	목표	검증 방법	처리 방법
1 - 낮음	주장 혹은 증언된 신원에 대한 낮은 수준의 신뢰도	컨택스트 내에서의 유일성	자가 주장 또는 자가 증언	Local/ remote
2 - 중간	주장 혹은 증언된 신원에 대한 중간 수준의 신뢰도	컨택스트 내에서의 유일성 + 존재성	협력기관의 신원정보를 활용한 신원 확인	Loal/ remote
3 - 높음	주장 혹은 증언된 신원에 대한 높은 수준의 신뢰도	컨택스트 내에서의 유일성 + 존재성 + 약한 수준의 연계성	협력기관의 신원정보를 활용한 신원 확인 + 신원 정보 검증	Local/ remote
4 - 매우 높음	주장 혹은 증언된 신원에 대한 매우 높은 수준의 신뢰도	컨택스트 내에서의 유일성 + 존재성 + 강한 수준의 연계성	협력기관의 신원정보를 활용한 신원 확인 + 신원 정보 검증 + 실체에 대한 대면 목격	Local

2.2 ISO/IEC 29003

ISO/IEC 29003은 신원확인에 관한 표준이며, 이 표준은 작성시점에 2차 CD상태에 있다.

이 표준에서는 3단계의 신원 확인 레벨(Levels of identity proofing)과 요구사항을 제시하며, 신원확인 목표, 신원확인 정보, 관련 용어, 관련 주체, 신원확인 프로세스 등을 제시한다. 신원확인의 주요 주체는 개체, 아이덴터티 소스, 검증 기관이 있으며, 개체는 신청의 주체이다. 아이덴터티 소스는 협력기관과 권위기관으로 나뉘며 권위기관은 속성에 대한 최상위 신뢰계층으로써 국내에서는 정부기관이 이에 해당하고 협력기관은 관련 서비스 프로바이더 이다. 검증기관은 각 개체가 서비스나 크리덴셜을 받기 위해 주장하는 신원에 대한 정확성을 검증하며, 검증기관이 아이덴터티 소스를 운영한다. 이 표준에서 제시하는 신원 정보들은 [표 2]와 같고, 신원확인 레벨과 목표는 [표 3]과 같다.

(표 2) 식별정보와 속성

목적	설명	속성의 예시
식별 속성	컨택스트 내에서 하나이상의 속성들이 결합되었을 때 유일한 신원을 형성하는 것	가명 이름 출생일 출생지 생체특성 주소 전화번호 이메일 출생시간
지원 속성	신원 확인에 도움이 되는 속성	다른 이름, 관계 증거의 참조번호 제시된 증거와 관련된 정보

(표 3) 신원 확인 레벨

LoIP	설명	목표
1	주장 혹은 증언된 신원에 대한 낮은 수준의 신뢰도	컨택스트 내에서의 유일성
2	주장 혹은 증언된 신원에 대한 중간 수준의 신뢰도	컨택스트 내에서의 유일성+약한 수준의 존재성 + 연계성
3	주장 혹은 증언된 신원에 대한 높은 수준의 신뢰도	컨택스트 내에서의 유일성+강한 수준의 존재성 + 연계성

3. 갭 분석 및 국내 본인확인 제안

ISO/IEC 29115에서 제시하는 4단계의 보증레벨은 최근 FIDO[3]와 같이 대두되고 있는 생체특성을 활용한 인증방식 혹은 이와 동일한 강도를 가지는 인증방식에 대하여 고려하지 않는 반면 ISO/IEC 29003에서는 [표 2]에서 제시하는 것과 같이 생체특성들을 고려한 보증 레벨을 제시하고 있다. 또한, 본인확인이 신원확인과 실체 인증으로 이루어지는 점을 감안하면, ISO/IEC 29003에서는 3단계의 신원 확인 레벨을 ISO/IEC 29115에서는 4단계의 보증 레벨을 제시하므로 ISO/IEC 29003개발에 있어 이 격차를 보완할 필요가 있다.

현재 국내 본인확인의 경우 주민번호 사용이 전면 금지됨에 따라 아이핀이나 마이핀 등을 사용하지만, 이 또한 발급 시 주민등록번호가 필요하고, 해킹사례가 존재한다. 이 외에도 핸드폰 인증, 공인인증서 인증, 활성 계정 인증 등 여러 가지 형태의 본인 인증이

존재한다. 하지만 아직까지 본인확인에 대한 보증등급 및 강도가 정의되어 있지 않다. 새로운 전자금융 서비스환경을 포용하기 위해서는 ISO/IEC 29003의 등급을 고려하여 현재 실시되고 있는 본인확인 방식들을 에 대한 등급을 재정의 하는 등 기존 방식의 개선이 필요하다.

현재는 서비스 이용 전에 신원 확인 레벨 및 보증 레벨을 사전규제(Opt-in)방식이지만, 재난과 같이 사전규제가 어려운 경우를 고려하여 상황에 맞게 신원확인 레벨 및 보증 레벨의 상승이 이뤄지는 사후규제(Opt-out)방식의 적용이 필요하다. 또한, ISO/IEC 29115에서는 기존에 존재하던 온라인 신원확인만을 다루므로 FIDO와 같이 최근 대두되고 있는 새로운 유형의 온/오프라인 신원확인을 포함하지 못한다. 추가적으로, ISO/IEC 29115에서 제시하는 4단계의 보증 레벨은 민간, 정부 영역 혹은 금융거래, 일반 웹 서비스 등과 같이 영역별 중요도를 고려하지 않는다. 국내에서는 협력기관 혹은 검증 기관이 권위기관으로써의 역할을 대신하는 경우가 있으므로 국내 상황에 적용 시 이에 대한 고려가 필요하다.

4. 결 론

본 논문에서는 ISO/IEC JTC 1/SC 27/WG 5의 본인확인 관련 국제 표준화 동향을 살펴보았고, ISO/IEC 29003과 ISO/IEC29115의 갭 분석을 수행하였다.

본 논문에서 분석된 본인 확인 관련 국제표준의 갭 분석 결과와 2015년 10월 ISO/IEC JTC 1/SC 27/WG 5 인도 회의결과 결정된 ISO/IEC 29115에 대한 새로운 SP와 ISO/IEC 29003의 범위 변화 및 개정중인 NIST 800-63-2[4]의 결과를 고려하면 최근 대두되고 있는 인터넷 전문 은행 및 핀테크 서비스 등에 유용하게 활용될 수 있다.

참 고 문 헌

[1] ISO/IEC 29115:2013, Information security - Security techniques - Entity authentication assurance framework

[2] ISO/IEC 2nd CD 29003, Information security - Security techniques - Identity proofing

[3] FIDO Alliance, https://fidoalliance.org/

[4] NIST Special Publication 800-63-2 Electronic Authentication Guideline

[5] 김경한, 유동현, 김수형, 윤봉중, 염흥열. “비대면 본인 확인 가이드라인과 국제표준과의 갭 분석 및 적용방안”, 한국정보보호학회 동계학술지

◐ 저 자 소 개 ◑

김 경 한

2015년 순천향대학교 정보보호학과 학사
2015년~ 현재 순천향대학교 정보보호학과 석사과정
관심분야 : International Standards, Social Engineering, Cryptography, Financial Security, etc...

유 동 현

2015년 8월 순천향대학교 정보보호학과 졸업
2005년 8월 ~ 현재 순천향대학교 대학원 정보보호학과 석사과정
관심분야 : 정보보호, 악성코드, 웹, 서비스보안

염 흥 열

1990년 한양대학교 대학원 전자공학과 박사
1982년 ~ 1990년 8월 한국전자통신연구원 선임연구원
1990년 9월 ~ 1990년 현재 순천향대학교 공과대학 정보보호학과
2011년 1월 ~ 12월 한국정보보호학회 회장 (현) 명예회장
2007년 7월 ~ 현재 ISMS/PIMS 인증위원회 위원장
2014년 12월 ~ 현재 정보보호 준비도 평가 심의위원회 위원장
관심분야 : IoT 보안, 클라우드 컴퓨팅 보안, 개인정보보호 관리체계, 모바일 보안 등