情 報 保 護 學 會 誌
第21卷 第6號, 2011. 10

국내외 전자인증수단 및 전자인증 연구 동향

조 효 제*, 이 동 희**, 김 홍 근***, 염 흥 열****

요 약

전자인증 서비스의 보안에 대한 중요성이 높아지고 있는 반면 금융권에서 사용할 수 있는 가이드는 있으나 다양한 분야에 범용적으로 사용할 수 있는 가이드라인이 존재하지 않는다. 본 논문에서는 국내 환경에 적합한 새로운 전자인증 가이드라인 개발에 필요한 요구조건을 분석해 본다. 현재 사용되고 있는 전자인증 수단과 기존의 전자인증 가이드라인 연구동향을 살펴보고 기존 가이드라인의 문제점을 분석한다.

Ⅰ. 서 론

오프라인에서 제공되는 서비스들이 온라인 환경으로 옮겨가면서 전자인증 수단의 중요성이 중요하게 부각되게 되었다. 이러한 환경의 변화로 인해 기존의 단순한 인증방식보다 더욱 높은 보안성을 요구하게 되었다. 또한 최근 금융권 및 대형 포털 해킹 사건 등이 빈번히 일어나면서 개인정보 및 프라이버시 보호를 위한 전자인증수단들이 제안되고 있고 이러한 전자인증수단의 도입을 위한 가이드라인 등이 연구되고 있다.

본 고 에서는 2장에서 국내외에서 사용되고 있는 전자인증 수단에 대해 알아본 후 3장에서 국내에서 공개된 전자인증 연구동향을 살펴보고 4장에서 국외의 전자인증 연구동향을 살펴본다. 5장에서는 국내 환경에 적합한 새로운 전자인증 가이드라인 개발을 위해 기존의 가이드라인들을 분석하고 마지막으로 6장에서 결론을 맺는다.

Ⅱ. 국내외 전자인증 수단

전자인증[1]이란 비대면 환경에서 상대방 및 자신을 신원을 확인하는 방법을 의미하며 이러한 전자인증 과정에서 자신을 식별할 수 있는 수단을 전자인증 수단이라 한다. 전자인증수단은 크게 지식기반, 소유기반, 특징기반의 세 분류로 나누어지며 국내외에서 사용되고 있는 대표적인 전자인증 수단들을 [표 1]과 같다.

지식기반은 사용자가 알고있는 정보를 이용해 인증하는 방식으로 대표적인 예로 아이디/패스워드 방식이 있다. 이 방식은 간단하고 편리하다는 장점을 가지지만 보안성이 높지 않다는 단점이 있다.

보다 높은 보안성을 가진 소유기반은 사용자가 소지한 인증 수단인 토큰을 이용해 자신을 인증하는 방법이다. 소유기반 인증수단에서 사용되는 토큰은 인증서와 같이 소프트웨어의 형태나 혹은 OTP와 같은 하드웨어의 형태로 존재하며 이러한 특성은 높은 보안성을 자랑하지만 토큰에 대한 관리가 중요도가 높아져 편의성이 부족하다.

가장 높은 보안성을 지닌 특징기반은 사용자가 가진 특징을 이용해 인증을 하는 방식으로 크게 신체적인 특징과 행동적인 특징으로 나눌 수 있다. 신체적인 특징은 지문이나 홍채와 같이 사용자 가진 고유한 신체특징을 인증수단으로 사용하며 행동적인 특징은 사용자 고유의 습관 등을 이용하여 방식이다. 세 가지 방식 중 가장 높은 보안성을 가지지만 구축에 어려움이 있고 유출시 교체가 불가능 하다는 단점을 가진다. 또한 일치여부가 100%일 수 없기 때문에 본인거부율과 타인인식률에 의

본 연구는 행정안전부의 출연금으로 수행한 전자서명 인증관리 사업의 결과입니다.
* 순천향대학교 정보보호학과 (sfkino@gmail.com)
** 순천향대학교 정보보호학과 (leemeca@msn.com)
*** 한국인터넷진흥원 공공정보보호단 단장 (hgkim@kisa.or.kr)
**** 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)

〔표 1〕 국내외 인증수단

인증	세부분류	인증수단	해설
지식	패스워드	비밀번호 (Password)	미리정의된 아이디와 패스워드를 이용해 인증
		I-PIN	주민등록번호 대신 사용할 수 있는 개인 식별번호
소유	H/W Token	OTP	OTP모듈로 일회용 패스워드를 생성해 인증하는 방식
		mOTP	모바일폰에 일회용 패스워드를 생성해주는 모듈을 삽입하여 생성
		보안카드	35개의 자리에 네자리 숫자를 표기한 카드, 표기된 숫자로 인증
	S/W Token	HSM(Hardware security module)	인증서의 보관 및 암호연산등을 담당
		PIN-Centry	단말기에 독립된 리더기와 카드를 이용해 인증과정을 진행
		인증서	x.509를 기반의 인증서를 이용해 사용자를 인증하는 방식
특징	생체기반	지문	신체 일부의 저장해 이를 비교하여 인증
		홍채	
		정맥	
	행동기반	음성	사용자의 습관 및 행동 등을 이용해 인증
		타자시 습관	
		서명	

한 문제점이 발생할 수 있다.

Ⅲ. 국내 전자인증 연구 동향

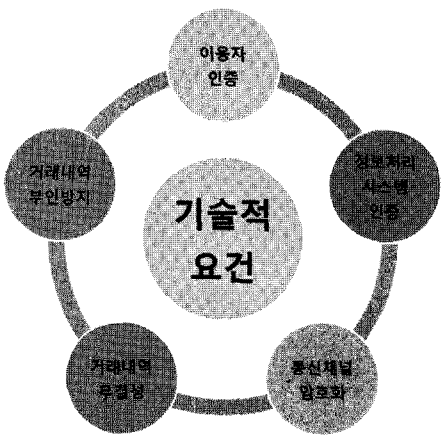
국내에서는 금융감독원이 인증수단 도입시 참조할 수 있는 가이드 라인을 공개하였고 한국 인터넷 진행원 등에서 전자인증수단 도입을 위한 가이드라인 등이 연구 중에 있다.

3.1 금융감독원의 인증수단 안전성 기술평가기준

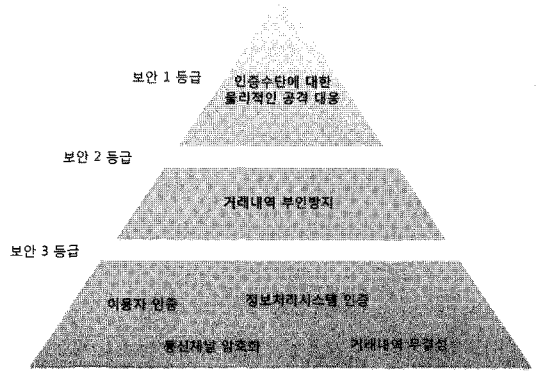
금융감독원은[2] 2011년 1월 31일 개최된 인증방법평가위원회에서 '인증수단 안전성 기술평가기준'을 제정하였다. 이는 전자금융거래에서 인증수단 도입을 위한 평가기준으로 금융기관 또는 전자금융업자가 전자인증수단을 도입할 때 안전한 인증방법을 선택할 수 있도록 기술평가 기준을 제시하는 것을 목적으로 하고 있다.

평가기준은 크게 인증방법의 기술적 요건과 보안등급, 보안 요구사항으로 나누어진다. 기술적 요건은 인증수단 및 전자금융 거래를 보호하기 위한 기술적인 요건들을 명시한 것으로 주요사항은 [그림 1]과 같다.

보안등급은 전자금융 거래 위협에 대해 가장 낮은 보안 등급인 보안 3등급에서 가장 높은 보안 등급인 보안 1 등급 까지 총 세 등급으로 나누어져 있다. [그림 2]는 각 등급에서의 간단한 요구사항을 기술한다.



〔그림 1〕 인증방법의 기술적 요건



〔그림 2〕 보안등급

〔표 2〕 등급별 보안 요구사항

등급	보안 요구사항
3등급	비밀번호 추측 방지
	피싱 및 파밍 방지
	유출 및 노출 방지
	위조 및 변조 방지
	거래내역 무결성 확인정보에 대한 검증
	금융기관에 저장된 거래내역에 대한 안전한 보관대책 수립
	인증수단의 등록, 발급, 배포, 폐기 등에 대한 안전한 관리적 요건 수립
	안전성이 검증된 암호 알고리즘 및 암호키 길이 사용
	암호키 관리를 위한 물리적, 관리적 절차 마련
	인증관련 기록의 보존 및 변경에 대한 보호대책 제공
	인증 장애시 대응 방안 제공
2등급	3등급 보안 요구사항을 모두 만족
	인증정보 재사용 방지
	인증정보 생성값 유출 방지
	중간자 공격 대응
	세션 가로채기 방지
	거래사실 부인 방지
	부인방지 확인정보에 대한 합리적인 검증
	사용자의 부인방지 정보가 사용자에 속한 유일한 정보임에 대한 합리적인 검증
	부인방지정보는 거래여부에 대해 유일하게 증명
	부인방지 정보에 대한 위 변조 여부 확인
1등급	2등급 보안 요구사항을 모두 만족
	인증수단의 비밀정보의 물리적 유출 방지

보안 요구사항은 각 금융거래에서 사용되는 인증방법이 만족해야 하는 기술적 요건을 등급별로 명시하고 있다. 상위등급들은 하위등급의 요구사항을 모두 만족해야하며 등급별 자세한 보안요구사항은 [표 2]와 같다.

3.2 금융보안연구원의 전자금융 신 인증기술 연구보고서

금융보안연구원에서 2011년 3월에 공개된 전자금융 신 인증기술 연구보고서[3]는 금융회사들이 새로운 인증기술 도입 시 활용할 수 있는 검토항목 및 방법을 제시하는 것을 목표로 하고 있다. 이 보고서에서 대상이 되는 것은 다양한 인증수단들 중 전자금융에 적용 가능한 인증수단들로 국한되며 법·제도적 요건은 포함하지 않는다. 신 인증수단의 검토 시 적용성, 편의성, 보안성의 세 가지 항목을 검토하며 검토방법의 세부사항은 [표 3]과 같다.

〔표 3〕 전자금융 신 인증기술

고려사항	세부사항	검토순위
적용성	적용 가능성	높음
	적용비용	보통
	기술 중립성	보통
	기존 인프라 활용성	낮음
편의성	소지 편의성	높음
	사용 편의성	보통
	관리 편의성	낮음
	발급 편의성	보통
	교육 편의성	낮음
보안성	오프라인 공격대응	-
	온라인 공격대응	-
	거래조작 공격대응	-

적용성은 새로운 기술을 적용하기 위해 고려해야할 사항들을 의미하고 편의성은 휴대, 발급, 사용 등의 간편함을 의미한다. 인증수단들의 보안성의 경우 Dolev-Yao 위협모델을 기반으로 인증수단들의 보안성 여부를 판단한다. 각 고려사항들의 세부사항들의 중요성을 고려해 각 세부사항들에 대해 검토순위를 높음, 보통, 낮음으로 정하고 각 항목에 각각 3, 2, 1의 점수로 산정해 종합적으로 검토하며 그에 대한 평균 검토수치가 1~1.6은 미흡, 1.7~2.4는 보통, 2.5~3은 우수로 판별한다. 그러나 보안성의 경우 검토방법의 우선순위를 적용하기 힘들어 검토 우선순위를 설정하지 않았다.

Ⅳ. 국외 전자인증 연구 동향

4.1 FFIEC의 인터넷 뱅킹 환경에서 개선된 인증기준 (Supplement to Authentication in an Internet Banking Environmen)

연방금융기관점검위원회(Federal Financial Institutions Examination Council Agency)는 2005년 10월에 배포된 인터넷 뱅킹 환경에서 인증방식(Authentication in an Internet Banking Environment)를 개선한 문서인 인터넷 뱅킹 환경에서 개선된 인증기준(Supplement to Authentication an Internet Banking Environment)[4]를 공개하였다. 이 문서는 여러 가지 인증수단들과 금융기

관에 대한 위협을 대응하기 위해 지침에 기술된 계층형 보안 시스템의 구축을 권장하고 있다. 타 가이드라인들은 단계별로 보안 요구사항을 매기고 있는데 반해 이 가이드라인은 관리적 측면의 보안을 등급화 하지 않고 있으며 위험평가, 고위험 거래, 계층형 보안, 특정 인증기법의 효과의 네 가지 항목에 대해 권장사항을 다음과 같이 기술하고 있다.

위험평가는 전자금융에서 일어나라 수 있는 위험을 평가하기 위한 고려사항으로 기관들의 최소 12개월마다 위험평가를 권장하고 기존의 위험평가에서 위협 환경의 변화, 전자금융의 고객기반 변동, 기능의 변화, 실제 보안사건을 고려해야 하고 이에 국한되지 않은 요인들 또한 고려할 것을 권장하고 있다.

고위험 거래를 위한 고객인증은 전자거래 규모에 따라 적절한 인증수단을 권고할 것을 권장하고 있다.

계층형 보안 프로그램은 보안성을 향상을 위해 하나의 거래 프로세스에 대해 여러 지점에 통제수단을 사용하여 것을 권장한다.

특정 인증기법의 효과에서는 단순한 인증보다는 좀 더 복잡한 인증방법을 이용하는 것을 권장하며 사용자로부터 일어날 수 있는 보안사고를 막기 위해 고객 인식교육을 권장한다.

4.2 NIST의 전자인증 가이드라인(Electronic Authentication Guideline)

미국 국립 표준 기술원(NIST)에서는 SP 800 시리즈 중 전자인증 가이드라인에 대한 문서인 SP 800-63 전자인증 가이드라인(Electronic Authentication Guideline)[5]을 공개하였다. 이 문서는 미국 관리 예산국(OMB : Office of Management and Budget)에서 기관들의 전자인증을 위한 가이드라인으로 배포한 연방지관을 위한 전자인증 가이드라인(E-Authentication Guidance for Federal Agencies), OMB M-04-04)[6]를 보완하여 만들어진 문서로 2006년 4월부터 업데이트 되어 현재 세 번째 드래프트 문서가 공개되어 있다. 이 문서는 등록 및 발행, 토큰, 토큰과 크레덴셜 관리 등 인증 프레임워크별 위협과 보증레벨들을 정의하고 있으며 [표 4]에서 기술된 것과 같이 가장 낮은 보안성을 요구하는 1등급에서부터 가장 높은 보안성을 요구하는 4등급까지 총 네 단계의 기술요구사항을 제공하고 있다.

이 문서는 관리적인 측면의 보안 보다는 기술적인 측면의 보안을 강조하고 있으며 특히 전자인증수단의 보안성을 강조하고 있다.

〔표 4〕 레벨별 기술 요구 사항

단계	기술요구사항 또는 특성
레벨 1	엄격한 신분증명이 요구되지 않으며 동일한 사용자가 보호된 정보나 작업에 접근을 보장
	패스워드에 암호학적 기법 적용을 요구하지 않음
	오랫동안 사용된 인증 비밀값이 노출 가능성 존재
레벨 2	한가지 인증수단을 이용해 증명 가능
	도청, 재사용, 온라인 추측 공격 방어 가능
	오랫동안 사용한 인증 비밀값이 외부 유출 불가
	NIST에서 승인된 암호기술 사용
레벨 3	CSP를 통한 신분증명을 요구에 대해 사용자 신분증명 정보를 제공
	인증토큰 유출을 막을 수 있는 암호 매커니즘 요구
	인증시 암호프로토콜을 통해 비밀키나 일회용 패스워드의 소유여부 증명을 기반
	멀티팩터 인증수단을 이용한 사용자 인증을 요구
	모든 동작에서 NIST에서 승인한 암호기술 사용
레벨 4	하드웨어 기반 암호토큰만을 사용해야하며 중요데이터 전송시에도 인증필요
	모든 참여자와 중요 데이터 전송에 대한 강력한 암호학적 인증을 요구
	악성코드로부터 비밀정보 보호 필요
	도청, 재사용, 온라인 추측, 검증자 위조, 중간자 공격 및 세션 가로채기 등의 공격에 대해 안전해야 함.
	NIST에의해 승인된 강력한 암호기술을 모든 동작에 사용

4.3 ITU-T의 개체 인증 보증 프레임워크(Entity authentication assurance framework)

ITU-T의 개체 인증 보증 프레임워크(Entity authentication assurance framework)[7]는 엔티티 인증보증 관리 프레임워크 제공에 대한 표준이며 현재 국제 표준화가 진행 중이다. 총 네 단계의 보안요구사항을 가진 이 표준은 인증위협 완화를 위한 보증레벨, 엔티티 인증보증의 단계 지침, 다른 인증 스킴과의 매핑에 대한 지침 등을 포함하고 있으며 이 외에도 엔티티 인증 프레임워크의 구성요소, 관리 및 운영시 고려사항, 위협 및 제어, 운영 서비스 보증 레벨 등을 포함하고 있다. x.eaa은 특히 크레덴셜 생성부터 폐기까지의 과정에 대한 보안 요구사항을 제시하며 관리적인 측면을 강조하고 있다.

Ⅴ. 기존 가이드라인 분석

5.1 국내외 가이드라인 비교분석

금융감독원의 가이드라인과 금융보안연구원의 보고서 모두 대상이 금융권이라는 측면은 같지만 금융감독원의 가이드라인의 경우 명확한 등급이 나누어져 각 항목의 보안 요구사항이 명확하게 명시되어 있고 금융보안연구원의 자료의 경우 등급을 매길 수 있는 기준을 제시하긴 하지만 기준에 맞는 보안 요구사항을 제시하지 않았다. 또한 금융감독원의 보안요구사항은 현재 금융권에서 사용되고 있는 전자인증수단을 대상으로 하고 있지만 금융보안연구원의 보고서에서 제시한 검토항목은 새로운 전자인증수단의 적용여부를 위한 것으로 금융감독원의 가이드라인과 금융보안연구원의 보고서에서 제시한 검토항목은 서로 다른 관점으로 전자인증 수단을 평가하고 있었다.

국내 가이드라인의 경우 대상이 금융권의 전자인증 수단에 한정되어 있는데 반해 국외 가이드라인은 전자인증 수단에 대한 보안 요구사항 또는 전자인증의 관리적인 보안 요구사항과 같이 전자인증의 다양한 분야에 대해 연구가 진행되고 있었다. FFICE의 가이드라인은 금융권의 관리적인 보안을 강조하고 있고 NIST의 전자인증 가이드라인은 전반적인 전자인증수단들에 대한 기술적 보안을 강조하고 있으며 ITU-T의 경우 전자인증의 전반적인 과정에서의 관리적, 기술적 보안을 강조하고 있다.

5.2 기존 가이드라인의 문제점 분석

본 논문에서 언급된 가이드라인들을 분석해본 결과 각각의 적용분야가 상이하고 국외 환경에 맞춰 개발되어 국내 환경에 적용하기 힘들 것으로 판단되었다.

국내 가이드라인들과 FFIEC의 가이드라인의 경우 금융권의 전자인증 서비스를 기반으로 개발되어 비 금융권의 전자인증 서비스에 적용하기에는 무리가 있었고 국외 전자인증 환경과 국내 전자인증 환경이 상이하여 국내에 전자인증 환경에는 일부 맞지 않는 부분이 존재한다는 문제점을 가지고 있었다.

금융보안연구원의 보고서에서 사용한 평가기준과 FFIEC의 가이드라인의 경우 세부적인 기준이 명확히 명시되어 있지 않고 보안 요구사항에 대한 등급이 나누어져 있지 않아 전자인증 환경의 명확한 기준을 내릴 수 없다는 문제점이 존재하였다. NIST의 전자인증 가이드라인과 금융감독원의 인증수단 안전성 기술 평가기준은 기술적 요구사항에 대해 자세하고 명확하게 기술되어 있다는 장점을 가지지만 전자인증 서비스의 전반적인 과정에 대한 보안 요구사항은 명시되어 있지 않았다. ITU-T의 개체 인증 보증 프레임워크는 전반적인 전자인증 과정에서의 보안 요구사항에 대해 자세하게 기술되어 있지만 기술적인 측면에서의 보안위협에 대한 등급화 된 보안 요구사항이 명시되어 있지 않았다.

Ⅵ. 결론

지금까지 국내외 전자인증 관련 연구동향을 살펴보았다. 국내의 경우 전자인증수단 도입을 위해 참조할 수 있는 가이드라인으로 금융감독원의 인증수단 안전성 기술평가기준 외에는 존재하지 않았으며 금융감독원의 가이드라인 또한 금융권에만 국한되어 비 금융권에서 전자인증 수단을 도입하기 위해 참조하기에는 적합하지 않았다. 국외의 전자인증 관련 연구의 경우 기술적인 측면과 관리적인 측면 등 세분화되어 진행되고 있으며 비 금융권의 전자인증 서비스에도 적용할 수 있도록 연구되고 있었다. 그러나 국외 가이드라인의 경우 국내환경과 일부 맞지 않는 부분이 존재하였으며 이로 인해 국내 전자인증 환경에 바로 적용시키기에는 한계가 있었다. 하지만 ITU-T의 개체 인증 보증 프레임워크에 기술된 관리적인 보안요구사항이 국내환경에 적합하게 수정하고 NIST의 전자인증 가이드라인이나 금융감독원의 인증수단 안전성 기술평가기준 등에 기술된 전자인증 수단들에 대한 보안 요구사항 등이 보강된다면 국내 전자인증 환경에 적합하고 전자인증 서비스 도입 시 참조할 수 있는 새로운 국내 가이드라인이 개발될 수 있을 것이다.

참고문헌

[1] Ant Allan, "A Taxonomy of Authentication Methods, Update," Gartner, May 2011,

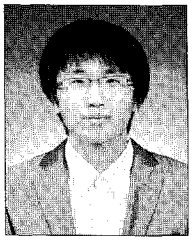
[2] "전자금융거래 인증방법의 안전성 세부 기술평가기준", 금융감독원, 2011년 2월.

[3] "전자금융 新인증기술 연구보고서," 금융보안연구원, 2011년 4월.

[4] "Supplement to Authentication in an Internet Banking Environment," FFIEC, 2011.
[5] William E. Burr, Donna F. Dodson Elaine M. Newton, Ray A. Perlner, W. Timothy Polk, Sarbari Gupta, Emad A. Nabbusm "Electronic Authentication Guideline," SP-800-63-1, NIST, June 2011
[6] "E-authentication Guidance for Federal Agencies," M-04-04, OMB, December 2003,
[7] "Entity authentication assurance framework," X. eaa, ITU-T, 2011

〈著者紹介〉

조 효 제 (Hyo-Je Jo)
학생회원
2011년 2월 : 순천향대학교 정보보호학과 졸업
2011년 3월~현재 : 순천향대학교 정보보호학과 석사과정
<관심분야> 정보보호



이 동 희 (Dong-Hee Lee)
학생회원
2010년 2월 : 순천향대학교 정보보호학과 졸업
2010년 3월~현재 : 순천향대학교 정보보호학과 석사과정
<관심분야> 정보보호, 역추적

김 홍 근 (Hong-Geun Kim)
종신회원
1985년 : 서울대학교 컴퓨터공학과 (공학사)
1987년 : 서울대학교 대학원 컴퓨터 공학과 졸업(석사)
1994년 : 서울대학교 대학원 컴퓨터공학과 졸업(박사)
1994년~1996년 : 한국전산원
1996년~2009년 : 한국정보보호진흥원
2009년~현재 : 한국인터넷진흥원
<관심분야> 병렬처리, 컴퓨터 보안, 소프트웨어 보안 등

염 흥 열 (Heung-Youl Youm)
종신회원
1981년 2월 : 한양대학교 전자공학과 졸업
1983년 2월 : 한양대학교 대학원 전자공학과 졸업(석사)
1990년 2월 : 한양대학교 대학원 전자공학과 졸업(박사)
1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 정교수
1997년 3월~2000년 3월 : 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월 : 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재 : 한국정보보호학회 총무이사, 학술이사, 교육이사, 논문지편집위원(역), 수석부회장(현)
2005년~2008년 : ITU-T SG17 Q.9 Rapporteur(역)
2006년 11월~2009년 2월 : 정보통신연구진흥원 정보보호전문위원
2009년 5월~현재 : 국정원 암호검증위원회 위원
2009년~현재 : ITU-T SG17 부의장/SG17 WP2 의장
<관심분야> 인터넷보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜