아이리포 지식창고

나를 합격시킨 토픽 - 공인인증서, 인터넷전문은행, 블록체인

강현수
(bs.itpe@gmail.com)

공인인증서, 인터넷전문은행, 블록체인

Concept	공인인증서 적용기술 및 문제점, 인터넷전문은행 사설 인증 기술, 블록체인 인증
KeyWord	공인인증서 적용기술 및 문제점 : PKI, X.509, Active-X, IE 종속화, Lock-In현상 인터넷전문은행 사설 인증 방법 : 생체인증, 타계좌인증(1원이체), 영상통화 블록체인 : 탈중앙화, 분산처리, 합의알고리즘

나의 기술사 학습 태도 : 호기심으로 ICT 변화 패러다임을 경험하려는 태도

사람의 뇌에 신규 정보가 입력되면, 뇌는 정보를 장기기억이나 중요기억으로서 보존을 위해 판단하는 기준으로 **'감정', '경험'이 가장 중요한 요소**라는 글을 본적이 있다. 지금 이순간에도 새롭게 개발되고, 시도되는 신기술, 변화하는 IT 트랜드, 개정되는 정부 정책을 습득하여 기억하고, 답안으로 작성하기는 정말 쉬운 일은 아니다.

필자는 정보관리기술사를 준비하면서, **'이해기반'** 학습을 위해 노력했다. 특히, 기술에 **'호기심'**을 가지고 학습하면서 자연스럽게 재미를 느끼고, **색다른 경험**으로 뇌가 인식 할 수 있도록 다양한 노력을 시도했다. 신기술 관련 논문, 정부기관의 자료, 전자신문등의 기사들을 찾아 읽고, 무료 세미나를 참석하는 등의 다양한 채널로 기술을 경험하려고 했다. 이런 시도의 대표적인 예는, 인터넷 전문은행 서비스 가입 경험 이였다.

인터넷 전문은행의 서비스 상용화 소식을 접하고 신기술 학습을 위해 신규 가입했다. 인터넷 전문은행은 공인인증서 없이 개인 인증 및 식별 위해 '상담원과의 영상통화', '1 원이체', '신분증 스캔 후 전송', '카드배송자를 통한 신분증 검증' 실시했다. 인터넷 전문은행의 사설 인증방법을 경험하면서 자연스럽게 공인인증서의 의무화의 실효성에 의문을 갖게 되었고 학습시에 다양한 리포트, 정부자료를 살펴보게됐다. 114 회 정보관리 기술사에 유사한 문제가 출제되어 평소에 가지고 있던 생각을 적을 수 있었고, 해당 문제가 고득점을 받게 되었다.

기술 이해하고, 암기하고, 구조화된 답안을 쓰는 연습 만큼, **신기술 성숙도가 서비스 상용화 단계에 접어들었다면, 해당 신기술의 서비스나 사례를 이용해보는 것도 뇌의 장기기억으로 보존되고, 남과 차별화된 안목을 갖게 되는 좋은 학습방법이라고 생각한다.**

본고에서는 114 회 정보관리기술사 4 교시 2 번 문제를 기반으로 공인인증서 적용기술 및 문제점, 인터넷전문은행(카카오뱅크사례) 사설 인증 방법, 블록체인 방식의 인증 방법을 살펴보고자 한다.

I. 공인인증서 적용기술 및 문제점

가. 공인인증서 적용기술

보안성을 높이기 위해 PKI(Public Key Infrastructure) 기술에 기초하였으나, 전자서명 기능을 플러그인(Active-X)로 구현하면서 특정 웹브라우저(IE)에서만 작동하여 호환성 없는 비표준 기술이 되었다.

- 개인 PC 내, 개인키 보관 장소 접근이 가능하여, 개인키 훼손, 유출등의 해킹 위험이 노출됨

구분	적용기술	적용기술 설명	역할
표준	PKI	암호화된 내용을 비인가된 사용자가 열람할 수 없도록 공개키와 개인키로 나누어 해독하는 암복호화 알고리즘	전자서명
	X.509	공개키 기반(PKI)의 ITU-T 표준 인증 알고리즘	인증알고리즘
비표준	Active-X	인터넷 익스플로러 브라우저에서 PC의 프로그램을 구동하기 위한 플러그인(Plug-In)	전자서명 구동
	보안 3종 프로그램	공인인증서의 암호입력 등을 보호하기 위한 키보드 보안, 방화벽, 백신 프로그램	암호보안

- 악성코드들이 보안 3 종 프로그램으로 위장/설치된 사례가 있듯이, 사용자가 무의식적으로 설치

나. 공인인증서 문제점

- 전자서명법 상 '전자서명생성정보를 가입자가 지배 관리해야 한다' 라는 요건을 충족하기 위해 사용자가 직접 공인인증서를 발급하고 관리하게 되었다. 공인인증서의 전자서명 기능을 구현할 때 필요한 인증서 관리와 보안문제를 해결하고자 채택한 플러그인 방식(Active-X)은 1996 년에등장한 기술로 제작사인 마이크로 소프트社 조차 보안 취약성을 이유로 사용하지 않을 것을 2006 년에 권고했다.

구분	(제도) 공인인증서	(기술) Active-X 플러그인
범위	국내 금융거래, 전자상거래, 전자 정부 서비스 등	MS Windows OS를 채택한 모든 기기
유래	1999년 전자서명법	1996년 Internet Explorer 3에서 지원
문제점	이용 불편, 이용자 보안 위험 관리 책임 부담	보안위험, 비표준 기술로 주요기업 미지원, 국내 인터넷 환경 갈라파고스 현상 유발
현황	공인인증서 '의무' 사용 폐지	MS사, '06년 비스타 이후 Active-X 미사용 권고 MS사, 윈도우10 엣지브라우저 Active-X 미지원

- 전자서명법 개정으로 공인인증서의 문제점을 개선 및 대체 인증 기술로 인증 마련 필요

구분	문제점	문제점 설명	개선방안
기술 관점	Active-X 사용	Active-X의 보안취약점으로 인해 악성프로그램 설치 통로 타 브라우저에서 사용 불가하며 별도 설치 필요	HTML5도입 표준기술 사용
	저장방식	C:₩...₩NPKI 폴더에 개인키 저장 폴더 복사로 쉽게 개인키 탈취 가능	HSM 도입 블록체인 이용
사용 관점	책임전가	사용자에 대한 Zero Liability 미적용 금융사고 발생시 사용자가 금융사 책임 입증 필요	서버인증 시행
	사용자 불편	소액결제 시에도 강제로 플러그인 설치 다단계 인증절차를 거쳐 사용자 편의성 저하	생체인증 간편결제 도입
관리 관점	갈라파고스 규제	국내에만 존재하는 규제로 해외 사용자의 국내 인터넷 전자거래 불가	네거티브 규제
	사용기간 제한	1년에 한번씩 공인인증서 갱신 필요	기한 설정
	개별 등록	갱신된 공인인증서는 각 금융사 마다 별도 등록 필요	블록체인 인증

II. 인터넷전문은행 사설인증 (카카오뱅크 사례)

가. 인터넷전문은행(카카오뱅크) 비대면 실명확인 요건

- 공인인증은 아니지만, 정부가 요구하는 비대면 실명확인 요건을 충족(카카오뱅크 채택사항 굵게 표시)

필수여부	분류	설명
필수사항 (택2)	**실명확인증표 사본 제출**	**사진촬영·스캔 후 신분증진위확인 서비스를 이용하여 확인**
	영상통화	고객과 영상통화를 실시하여 신분증표 사진과 대조
	접근매체 전달시 확인	현금카드, 보안카드, OTP 등 접근매체 전달 시 실명확인 수행
	기존계좌 활용	**기존 금융거래에서 사용하던 계좌를 이용, 소액을 이체하도록 해서 실명확인 수행**
	기타 이에 준하는 방법	지문인식, 정맥인증 등 생체인증처럼 필수 인증기술에 준하는 신뢰도 확보가 가능한 인증기술 적용
권고사항	다수의 개인정보 검증	고객이 제공하는 개인정보와 신용정보사가 보유한 정보를 대조하여 실명확인 수행
	타기관 확인결과 활용	**공인인증서, 핸드폰, 아이핀 등 타 인증기관에서 신분 확인 후 발급된 결과 활용**

- 비대면 실명확인 서비스를 이용해본 결과 기존계좌 활용 시 '1 원 이체'를 통해 실명인증 수행
- 인터넷전문은행(카카오뱅크) 실명인증 이후 스마트폰 앱을 통해, 이체시 획기적인 단계 축소로 사용자의 편의성을 증가 시킴

나. 인터넷전문은행(카카오뱅크) 이체 거래시 적용방식

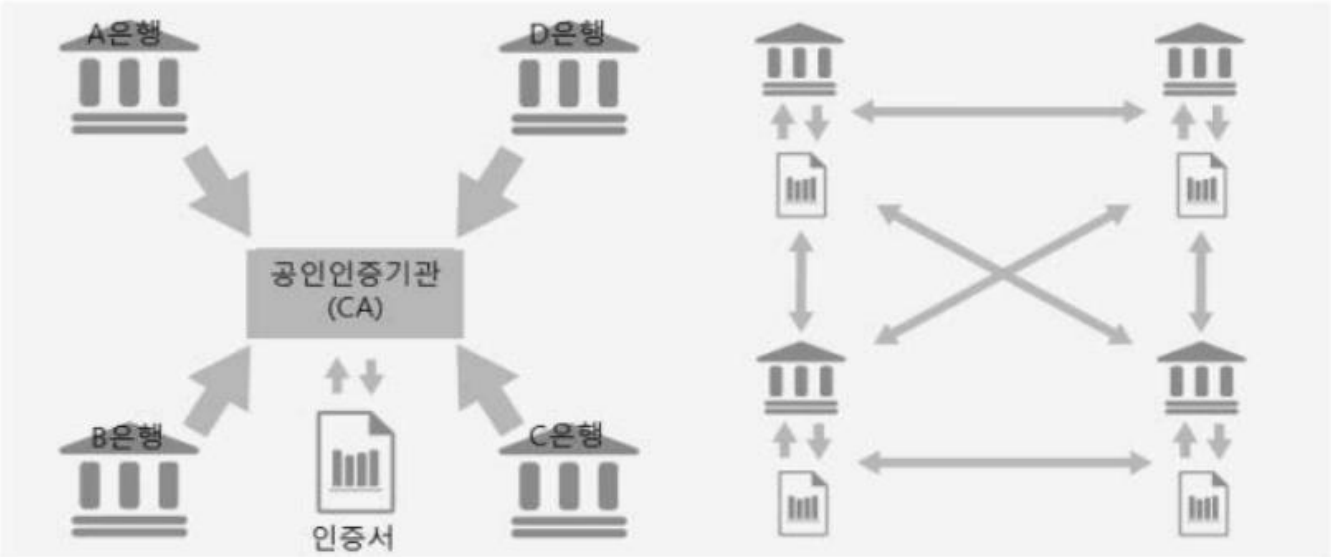
특성	카카오뱅크 사설인증 적용방식	일반은행 공인인증 적용방식
편의성	2단계 ❶ 로그인 인증(지문, 패턴) ❷ 인증비밀번호 (단, 이상거래로 의심되는 경우 ARS를 통한 추가인증, 고액거래의 경우 OTP 입력이 요구됨)	5단계 ❶ 로그인 인증(인증서 비밀번호) ❷ 계좌비밀번호 입력 ❸ 연락처본인확인 또는 ARS ❹ OTP나 보안카드 입력 ❺ 2차 인증(인증서 비밀번호)
안전성	❶ 사설 인증키 등 중요정보를 모바일 보호 영역*에 저장하여 키 보안 강화 ❷ 1인 1기기 정책+모바일 네이티브 앱+루팅 방지기술+양방향TLS로 취약한 환경에의 노출을 방지 ❸ 카카오뱅크에서만 활용가능	❶ 기존 공인인증서는 잘 알려진 일반폴더에 저장했으나, 최근 개선노력 중 ❷ 일반 PC환경 ❸ 등록시 범용적으로 활용가능

- 인터넷 전문은행(카카오뱅크)의 이체시 2 단계로 기존 공인인증 적용방식의 5 단계를 축소시킴으로서, 사용자의 편의성을 극대화하여 인터넷전문은행의 상용화 가속화

Ⅲ. 블록체인 방식의 인증 기법

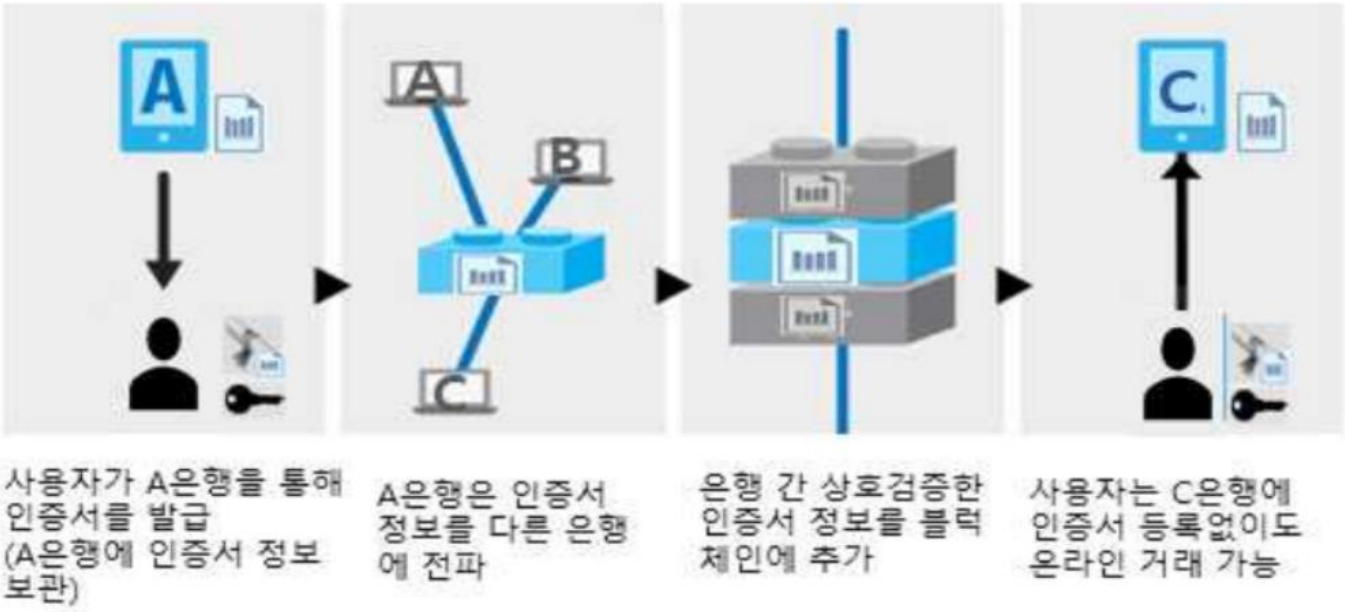
가. 블록체인 방식의 인증 기법

< 기존 방식 : 중앙집중 >　　< 블록체인 방식 : 분산 >



- 정보를 블록 단위로 쪼개 인터넷으로 연결된 다수의 컴퓨터에 분산저장한 후, 상호 검증하는 방식으로 온라인 거래의 위·변조를 방지하는 기술인 블록체인을 인증서에도 적용하는 방안이 개발됨
- 인증기관의 중앙서버에 인증서 정보를 보관하는 기존 방식과 달리 블록체인을 이용 은행 간 인증서 정보 공유함

나. 블록체인을 통한 은행 간 인증서 공유



- 국내 1 개 증권사는 2017 년 10 월에 블록체인 인증 시범서비스를 개시했고, 은행권은 2018 년 7 월부터 시범서비스를 개시할 예정임

"끝"

[참고문헌]

1) 인사이트리포트_2017-004호, 공인인증과 전자서명의 미래(2017.12), SPRI
2) 스마트 환경에서의 공인인증서 활용과 문제점(2013.03), KISA