Insight Report

2017. 12. 01. (2017-004호)

공인인증과 전자서명의 미래

- 카카오뱅크의 혁신과 은행권 블록체인 도입을 중심으로 -

강송희(Kang, Songhee)
(dellabee@spri.kr)

유호석(Yoo, Hoseok)
(hsy@spri.kr)

김준연(Kim, Junyoun)
(catchup@spri.kr)

SPRi 소프트웨어정책연구소

○ 본 보고서는 「과학기술정보통신부 정보통신진흥기금」을 지원받아 제작한 것으로 과학기술정보통신부의 공식의견과 다를 수 있습니다.

○ 본 보고서의 내용은 연구진의 개인 견해이며, 본 보고서와 관련한 의문사항 또는 수정・보완할 필요가 있는 경우에는 아래 연락처로 연락해 주시기 바랍니다.

- 소프트웨어정책연구소 산업·제도연구실 강송희 선임연구원(dellabee@spri.kr)

《 Executive Summary 》

2014년 당시, 대통령의 '천송이 코트' 언급으로 촉발된 공인인증서 논란은 언론의 조명을 받으며 사회적 이슈가 됐고, 결국 공인인증서의 의무적 사용은 폐지됐다. 이제 전자상거래와 인터넷뱅킹 등의 영역에서 공인인증서가 사용되는 것은 시장의 선택에 따른 것이고, 지금이 바로 공인인증서의 진가를 검증할 수 있는 시점이다.

공인인증서와 관련한 제도 변화에 대한 우리의 경험은 독특하다. 먼저 정부가 신기술의 등장 초기에 특정 기술을 선정해서 육성하고, 민간에서 역량이 축적되고 사회경제적 여건이 성숙되자 생체인증과 블록체인 등 또 다른 신기술을 활용한 다양한 인증방식을 인정하면서 기술 중립적 환경으로 회귀한 것이다. 이 보고서는 공인인증서의 도입과 의무화 폐지, 그리고 다양한 인증 방식 간에 상호 경쟁하는 과정을 참여자 간 전략선택의 게임이론을 활용하여 분석했다.

분석의 결과, 첫째, 공인인증서는 도입기에 금융거래를 안전하게 보호하고 전반적인 인증 수준을 높였으며, 최근에는 공인인증서 의무화가 폐지되어 인터넷 전문은행 등에서 간편 인증이 출현하고 공인인증에 신기술이 도입되는 긍정적 효과가 있었음을 밝혔다. 둘째, 금융 영역에서 인증과 전자서명 방식의 혁신이 늦어졌다는 논란에 대해, 일반적으로 보안인식이 낮은 사용자들에게 태생적으로 관리 책임이 일부 존재하여, 금융기관들이 공인인증서 의무화 제도를 최소한의 보안 기준으로 삼아 금융 사고가 발생했을 때 책임을 회피하는 근거로 활용할 수 있었으며, 새로운 인증 방식을 도입할 인센티브가 부재했음을 밝혔다.

신기술의 사회적 보급을 활성화하는 차원에서 정부의 제도적 개입은 가능하다. 그러나 이 사례가 시사 하는 바는 새로운 대안기술의 혁신이 빈번하게 발생하는 영역에서 자칫 추가적인 혁신을 저해하지 않게 하기 위해서는 민간에 역량이 축적되었을 때 시장 자율의 환경을 조성하도록 탄력적으로 제도를 운영할 필요도 있다는 것이다.

《 Executive Summary 》

The controversy over the accredited certificate triggered by the President's 'Chunsongyi Coat' in 2014 became a social issue under the light of the media and eventually led to the abolition of the mandatory use of the accredited certificate. Now, the use of the accredited certificate in the fields of e-commerce and Internet banking is in accordance with the market choice. Now is the time to verify the true worth of the accredited certificate.

Our experience with institutional changes related to the accredited certificate is unique. First, the government selected and fostered specific technologies at the beginning of the new technology adoption period. After firms accumulated competencies in the private sector and socioeconomic conditions matured, the government created a technology-neutral environment in turn. This report analyzes the dynamic changes in social consensus and competition of the whole process by using the game theory.

First, in the introduction phase of the accredited certificate, the financial transaction has been safely protected and the level of overall authentication technology has raised. In recent years, the abolition of the mandatory use of the accredited certificate has a positive effect such that the simple authentication method of the Internet bank has appeared and the new technologies(i.e. Blockchain) have been adopted into the accredited certificate. Second, the argument that the innovation of the authentication and digital signature system in the finance sector has been delayed is based on the assumption that the financial institutions interpreted the term of mandatory use of the accredited certificate as the minimum security standard. And also, we analyzed that there was no incentive for them to adopt new technologies.

This case suggests that the government is able to play a prime role in facilitating the introduction of a new technology. However, in order to foster further innovations in the area where innovation of new alternative technologies occurs frequently, it is also necessary to operate a flexible legal system such as a temporary policy after private firms accumulated capabilities.

목 차

Ⅰ. 연구배경 ····· 1

Ⅱ. 국내 공인인증의 역사와 국제비교 ····· 2

Ⅲ. 공인인증서 의무화 폐지 ····· 7

Ⅳ. 새로운 사설인증의 출현 : 카카오뱅크 ····· 9

Ⅴ. 기존 인증서의 변화 : 은행권 블록체인 도입 ····· 12

Ⅵ. 결론 ····· 14

참고문헌 ····· 17

Ⅰ. 연구배경

□ 2006년 이후 보안 취약점 등의 문제로 인해 공인인증서를 구현하기 위해 사용한 플러그인(Active-X) 방식의 폐지 및 대체 논란이 증대됨

○ 종이문서 인감도장과 유사하게 전자문서의 본인확인·원본여부를 공증하기 위해 개발된 공인인증서의 '전자서명' 기능이 인터넷의 확산으로 온라인 행정·금융·상거래에 까지 광범위하게 활용됨

- 전자서명법 상 '전자서명생성정보를 가입자가 지배·관리해야 한다'라는 요건을 충족하기 위해 사용자가 직접 공인인증서를 발급하고 관리함

○ 공인인증서의 전자서명 기능을 구현할 때 필요한 인증서 관리와 보안문제를 해결하고자 채택한 플러그인 방식(Active-X)은 1996년에 등장한 기술로 제작사인 마이크로소프트사조차 보안 취약성을 이유로 사용하지 않을 것을 2006년에 권고함

<표 1> 공인인증의 제도적, 기술적 구분

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

□ 2014년 3월, 박근혜 前대통령은 규제개혁장관회의 및 민관합동 규제개혁점검회의에서 "공인인증서와 Active-X 때문에 외국인이 '천송이 코트'를 살수 없다"고 지적함

□ 2017년 3월, 문재인 대통령은 ICT 현장 리더 간담회에서 "불필요한 인증절차를 과감하게 없애고 다양한 인증방식이 시장에서 차별 없이 경쟁할 수 있도록 하겠다"고 공인인증서와 Active-X 폐지를 공약함

□ **(찬·반 의견)** 공인인증서 대체가 어려우므로 유지하자는 찬성 의견과, 사용자 불편과 기술혁신 저하를 이유로 폐지하자는 의견이 있었음

<표 2> 공인인증서 찬·반 의견

구분	공인인증서 찬성[1]	공인인증서 반대[2]
이유	○ 국제표준 PKI(공개키)방식의 전자서명을 지원하는 수단은 당시로서는 공인인증서 뿐이었음	○ 계약이 번거롭고 국내 보안시장 경쟁력도 훼손 ○ 공인인증만 효력을 인정하는 경우 유엔국제상거래법위원회(UNCITRAL) 전자계약협약 제9조[3]에 위배
대안	○ Active-X없는 공인인증서 확산 ○ PKI(공인인증서) 기반 보안토큰 활성화와 지문·홍채인식 등 간편결제 강화	○ 자율인증이 경쟁하면 오히려 더 안전

Ⅱ. 국내 공인인증서의 역사와 국제비교

□ **(공인인증서의 정의)** 공인인증서는 온라인 거래 시, 법적으로 '공인'된 인증으로 어떤 문서에 가입자가 직접 서명했으며, 서명한 이후 위·변조되지 않았음을 증명하는 전자 정보

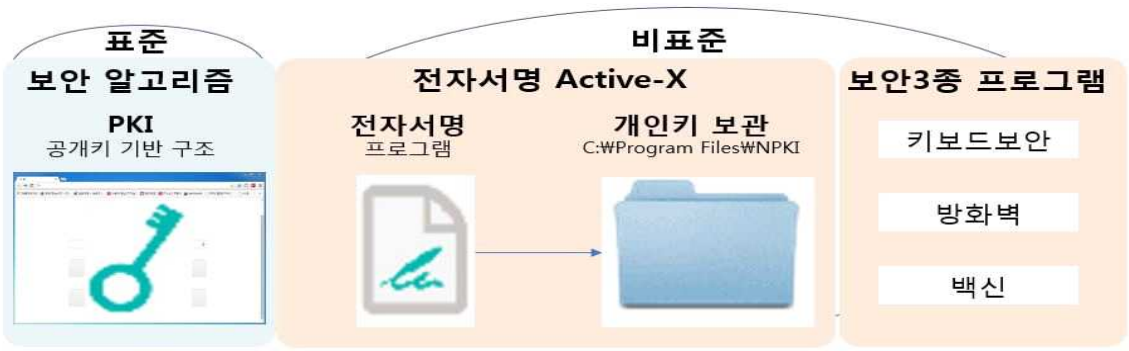
○ **(공인인증서의 사용)** 공인인증서는 본인확인과 전자서명 기능을 위해 플러그인(Active-X) 방식으로 구현[4]되었으며, 공공과 민간부문 모두 사용 중

* 공인인증서는 일종의 인터넷 인감 증명서로서 신뢰할 수 있는 제3자(인증기관)가 거래 당사자들의 신원을 확인해주기 때문에 안전한 거래뿐 아니라 거래 당사자가 계약 내용을 부인하는 것도 방지
* 인터넷진흥원(KISA)을 최상위인증기관(Root Certificate Authority)으로 5개 기관이 발급(정보인증, 코스콤, 금융결제원, 한국전자인증, 한국무역정보통신)

1) 출처 : 인터넷진흥원 매일경제 기고 '15.4.5 '공인인증 기술력이 핀테크의 핵심'
키뉴스 인터뷰 기사 '17.4.12 '블록체인, 공인인증서 대체논란 가열'
2) 출처 : 공인인증서 문제해결을 위한 이용자 모임 주최 국회정책 토론회
3) 국제적으로는 서명방법이 여러 정황에 비추어 신뢰할 수 있는 경우 서명 요건을 충족한 것으로 간주 (정진명, "UNCITRAL 전자계약협약의 국내법에의 수용" p70-71 참조)
4) 2014년 이후 Active-X 없는 공인인증서가 개발되었으나, 아직 대부분 사용자가 Active-X 인증서를 사용 중

1 **(적용기술)** 보안성을 높이기 위해 PKI(Public Key Infrastructure)[5] 기술에 기초하였으나, 전자서명 기능을 플러그인(Active-X)로 구현하면서 특정 웹브라우저에서만 작동하여 호환성 없는 비표준 기술이 됨

<그림 1> 공인인증서 관련 비표준 Active-X 기술



* 전자서명을 Internet Explorer에서만 작동하는 Active-X로 구현하고, 개인키를 브라우저가 아닌 이미 알려진 PC 특정폴더에 저장하며, 공인인증서 암호입력 등을 보호하기 위해 보안3종 Active-X를 추가설치

2 **(기능구성)** 공인인증서는 법적으로 **온라인 서비스의 전자서명**과 **본인확인**의 두 가지 기능으로 구성됨

* (전자서명) 자필 서명과 동일한 기능을 수행하는 전자적 수단
* (본인확인) 온라인 서비스의 거래 당사자의 명의와 실제 사용자가 일치하는지 확인하는 기능으로써 11개 본인확인 기관에 5개 공인인증기관이 포함

<표 3> 인증 기능별 담당 기관

인증기능		인증방식	담당 기관
본인확인	전자서명	공인인증서	금융결제원, 한국정보인증, 한국전자인증, 코스콤, 한국무역정보통신(5개)
		아이핀	서울신용평가정보, 나이스평가정보, 코리아크레딧뷰로(3개)
		휴대전화	SK텔레콤, KT, LG유플러스(3개)
		신용카드	KB국민카드, 신한카드, 하나카드, 현대카드, 삼성카드, 롯데카드, BC카드, 한국NFC(시범사업자, '17.7월)

5) public key infrastructure : 암호화 내용을 아무나 열어볼 수 없도록 공개키와 개인키로 나누어 해독하는 암·복호화 알고리즘

□ 공인인증서의 도입과 확산

○ **(공인인증서의 도입)** 온라인 거래의 안전성·신뢰성을 확보하기 위해 1999년 2월 국내 전자서명법을 제정하고, 국제적으로는 유엔 국제상거래법위원회(UNCITRAL)가 2001년 전자서명모델법'을 채택 후 인증기술의 중립성 원칙을 수용하여 국내 전자서명법을 개정함

○ **(공인인증서의 확산)** 「공인인증서 활성화 TF」에서 공인인증서 확대에 따른 문제 및 대응방안을 검토하고(2002.5.~6.), 부처 간 협의 후 금융분야 사용 확대 방안을 발표함(2002.7.)

<표 4> 도입초기 공인인증서 발급 건수 추이 (단위: 천 건)

연도	2000	2001	2002	2003	2004	2005	2006	2007
발급건수	27	1,502	4,934	7,824	9,498	11,000	14,375	17,155

* 자료: 정통부(2007), 국가정보보호백서
* 은행, 비은행의 인터넷뱅킹은 2002.9.1.부터 공인인증서를 발급
* 증권, 보험은 2003.1월부터 공인인증서를 사용해옴

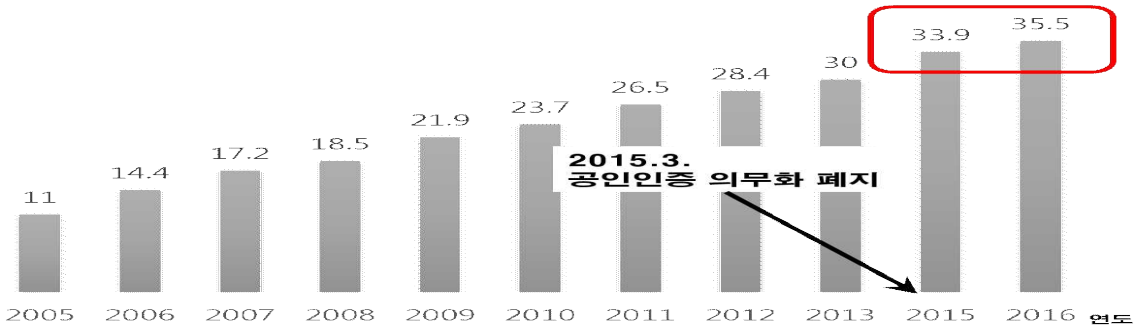
<표 5> 공인인증서 추진 경과

시기	추진 내용
1999년 2월	전자서명법 시행
7월	한국인터넷진흥원, 최상위인증기관 전자서명인증관리센터 개설
2000년 2월	6개 공인인증기관 지정(한국정보인증, 코스콤, 한국정보사회진흥원(2008년 지정 종료), 금융결제원, 한국전자인증, 한국무역정보통신)
2002년 9월	금융위, 인터넷뱅킹 공인인증서 사용 의무화
2003년 1월	금융위, 증권거래 공인인증서 사용 의무화
6월	(옛) 정통부, 모든 전자거래에서 사용가능한 범용 공인인증서 발급
2005년 11월	금융위, 전자상거래서 30만원 이상 결제시 공인인증서 사용 의무화
2014년 3월	대통령 주재 규제개혁 장관회의(해외소비자가 불편 없이 국내 온라인 쇼핑몰 이용)
8월	금융위, 전자상거래서 30만원 이상 결제시 공인인증서 의무사용 폐지 미래부, 웹표준방식 활용한 공인인증서 발급 및 이용기술 개발
2015년 3월	금융위, 인터넷뱅킹 공인인증서 의무사용 폐지(전자금융감독규정)
2016년 2월	액티브엑스 없는 간편 웹 표준 공인인증서 기술 발표
12월	KB국민 신한 씨티은행 등 총 14개 사이트에 간편 공인인증서 기술 적용

* 출처 : 머니투데이(2017.3.11.)

○ **(사용자 증가 지속)** 의무화 폐지 후에도 공인인증서 발급 건수는 오히려 증가하여 누적 3천 500만 건을 상회하는 중

< 연도별 공인인증서 발급 건수 추이(단위: 백만 건)>



* 자료: KISA(2017), 언론보도자료

□ 공인인증제도 국제 비교

○ **(행정용도 사례)** 정부·공공 행정 서비스 용도로 공인인증서를 활용하는 주요국은 생체인식 등 국내 공인인증서와 다른 방식으로 개발된 인증을 사용 중

<표 6> 주요국의 행정용 공인인증

국가		공인인증 용도	비고
유럽	영국	전자여권[6], 지문 등 생체인식 거주 허가[7](2012)	전자여권 관련 기술적 명세와 표준(2006)[8], 생체인식 거주 허가를 위한 기술적 명세와 표준 발표(2009)[9]
	벨기에	전자여권	
	그리스	전자여권, 행정 포털 접근용(2013)	
	리투아니아	전자여권, 전자거주허가증, 전자 운전 면허증 등 행정	
	오스트리아	온라인 세금신고, 전자주민증, 전자공증, 정부전자문서	
	핀란드	온라인 세금신고, 인구정보시스템	
	독일	전자정부, 소송서류 전송 등	
일본		전자민원, 상업등기	-
미국		행정업무 처리, 민원서비스	-
호주		전자세금조회, 전자 부동산 양도 증명, 의료서비스 등	-
대만		전자송장, 전자세금조회, 토지대장 발급	-
싱가포르		정부조달, 건설관련 전자문서, 법원 문서 제출 등	-
필리핀		전자정부, 행정 서비스	-

6) e-MTRD(Machine Readable Travel Document)
7) BRP(Biometric Residence Permits)
8) The EAC-PKI was developed under auspices of the EU to support free movement of citizens of the EU Schengen States. Commission Decision C(2006) 2909 of 28 06 2006 sets out the Technical Specifications on Standards for Security Features and Biometrics in Passports and Travel Documents issued by

○ **(금융거래 사례)** 인도 등 공인인증을 인터넷 뱅킹에 활용하는 일부 국가들도 공인인증기관을 지정하지는 않으며, 기술적·관리적 요건을 만족하는 인증기관에 한시적인 면허를 발급함

<표 7> 주요국의 공인인증기관 지정 및 관리 여부

국가	인증기관 지정 여부	법적효력 및 업무범위
한국	공인인증기관 지정	공인인증기관이 인증한 전자서명에 전자서명법상의 효력 부여
미국	규정 없음 * 초기 주법(州法)에서 허가제도를 규정하였으나 후발 주들은 등록제 등 완화된 제도 채택	모든 전자서명에 대해 법적 효력 인정 ※주법에서 제한
독일	인증기관 임의신고 * 법에서 정한 요건을 구비한 인증기관이 주무관청에 신고, 주무관청의 확인 후 확인 필증 수여	규정없음 * 개정민법에서 공인전자서명의 서명으로서의 효력을 인정(독일민법 제126조A)
영국	인증기관에 관한 규정 없음 * 자율적 비영리기구인 tScheme에 의한 자발적인 승인시스템	전자서명, 전자서명의 발생, 통신방법, 서명에 사용된 절차 등을 증명하는 선언을 한 경우, 개인의 경우에도 전자서명이 인증됨
인도	기술·관리적 요건을 만족하는 인증기관에 한시적인 면허 발급	정보기술법(2000)에 따른 법적 효력을 인정하며 보안 수준별 3종류의 전자서명이 존재

* 자료 : KISA(2002), 주요국가의 전자서명 인증제도 현황을 참조하여 수정

Member States.

9) European Regulations (EC) 1030/2002 and 380/2008 in relation to BRPs, therefore this Certificate Policy complies with Article 5.4.3 of the Technical Specifications on Standards for Security Features and Biometrics in Residence Permits issued by Member States, set out in Commission Decision C(2009) 3770 final of 20/05/2009. This requires participating Member States to publish a National CP based on the Common EU Certificate Policy. As a minimum, the National Policy must meet the standards of the Common EU Certificate Policy but MAY place further restrictions on the control and usage of certificates within that Member State

Ⅲ. 공인인증서 의무화 폐지

□ **(의무화 폐지)** 2015년 3월 공인인증서 의무사용 조항이 삭제되고 2017년 1월 금융사고 시 금융기관의 책임을 면해 주던 약관도 개정함

<표 8> 정부의 자율 인증 활성화 추진 경과

규정 개정 내용	시행일
전자금융감독규정 시행세칙 제 4조를 개정하여 전자상거래 지급결제에서 신용카드·직불카드 결제 또는 30만원 미만의 온라인 계좌이체를 공인인증서 의무사용 대상에서 제외	'14년 5월
전자상거래 결제 간편화 방안 발표[10]	'14년 7월
매체 분리 원칙[11] 폐지	'15년 2월
보안프로그램(3종) 설치 의무[12] 폐지	'15년 2월
2015년 3월 18일 관련법상 공인인증서 의무사용 폐지	'15년 3월
인증방법평가위원회[13] 폐지	'15년 3월
국가기관 인증 정보보호제품 사용의무 폐지	'15년 3월
금감원 사전 보안성심의 의무 폐지	'15년 9월
정보통신망법 제 47조, 금융분야 ISMS인증 의무화 대상 제외	'16년 6월
금보원 금융회사 자체 보안성 심의 가이드 발간	'16년 7월
2017년 1월 전자금융거래 표준약관을 개정하여 전자금융거래에서 발생한 피해를 은행이 원칙적으로 책임지도록 함	'17년 1월

<표 9> 의무화 폐지 전후의 공인인증과 사설인증의 효력 비교

구분	개정 전 전자서명법	개정 후 전자서명법
공인인증의 효력	·자필서명과 동일한 효력(전자서명법 제3조)	좌동
사설인증의 효력	·효력없음	공인인증 외 전자서명은 당사자 간의 약정에 따른 서명, 서명날인 또는 기명날인으로서의 효력을 가짐
공인인증의 요건	·전자서명 생성정보가 가입자에게 유일하게 관리 ·서명 당시 가입자가 전자서명생성정보를 지배·관리 ·전자서명 후 해당 전자서명이 변경되었는지 확인 ·전자서명 한 전자문서가 변경되었는지 확인	좌동

10) 30만원 이상 결제 시 대체 인증수단 도입 및 PG(Payment Gateway)사의 카드정보 저장 허용
11) 전자금융감독규정 제34조, '매체 분리' 원칙은 금융 거래 매체와 같은 매체를 인증 수단으로 쓰면 안 된다는 것
12) 금융사는 전자금융거래 보호 차원에서 이용자가 보안프로그램을 다운로드 받도록 해야 한다는 것
13) 공인인증서 이외의 인증방법의 안전성을 평가하기 위한 위원회

□ 공인인증 의무화 폐지 결과 분석

게임이론을 활용해서 공인인증서 생태계 참여자들의
'인증수단 선택'간 전략적인 균형상태로 설명

① 공인인증서 도입·확산기 (2003년 ~ 2015년 3월)

- 공인인증서 의무화로 인해 기업(1)와 기업(2)가 모두 공인인증서를 채택하는 것이 가장 큰 이득을 얻을 수 있는 균형 상태(3,3)를 보이며 **사설인증을 선택하면 투자조차 회수하기 어려움**

<그림 2> 공인인증서 도입시기의 게임 설정

		금융기업 2	
		사설	공인
금융기업 1	사설	(2, 2)	(1.7, 3)
	공인	(3, 1.7)	**(3, 3)**

* **(가정1)** 보안 투자와 상관없는 영업활동으로 얻는 기업의 이득은 기업(1)과 (2) 모두 2로 초기 기대값은 동일하고, 기업이 사설인증을 도입하면 추가비용이 0.5만큼 소요되나, 기존 공인인증을 유지할 경우 추가비용은 없음
* **(가정2)** 두 기업이 동일한 보안 전략을 선택하는 경우, 사설 인증의 경우 기업의 이득은 0.5, 공인 인증의 경우 기업의 이득은 1이며, 두 기업의 전략이 다를 때 사설인증을 선택한 기업이 0.3만큼의 추가 손실이 있음

② 공인인증서 의무화 폐지이후 (2015년 3월 ~ 현재)

- 의무가 아니기에 사설인증과 공인인증 중 어느 것을 선택하더라도 무방하므로, **공인인증서과 사설인증이 시장에서 경쟁할 수 있는 환경이 마련됨**

<그림 3> 공인인증서 의무화 폐지 이후의 게임 설정

		금융 기업 2	
		사설	공인
금융기업 1	사설	**(3, 3)**	**(3, 3)**
	공인	**(3, 3)**	**(3, 3)**

* **(가정1)** 보안투자와 상관없는 영업활동으로 얻는 기업의 이윤은 2로 동일하고, 기업이 사설인증을 도입하면 추가비용이 0.5만큼 소요되나, 기존 공인인증을 유지할 경우 추가비용은 없음
* **(가정2)** 사설인증의 경우 편의성이 제고되어 사용자의 유입이 더 많고, 따라서 사설인증을 선택한 기업의 이득은 1.5, 공인 인증을 선택한 기업의 이득은 1이지만, 사설 인증을 선택한 기업과 공인 인증을 선택한 기업이 경쟁할 때 사설인증으로 인한 추가 이득$(\epsilon = 0)$은 특별히 없는 상태

Ⅳ. 새로운 사설인증의 출현 : 카카오 뱅크 사례

□ 카카오뱅크의 출현

○ 카카오뱅크는 케이뱅크에 이은 국내 두 번째 인터넷 전문은행*으로, 모바일 비대면 영업을 통한 낮은 금리와 간소한 메뉴·인증이 특징임

* 인터넷 전문은행은 개좌개설이 쉽고 대출 금리가 낮아 소액 위주의 금융거래에 특화되어 있으며, 중신용자에게 적합한 신용대출을 제공하고 언제나 거래가 가능

○ 2017년 7월 27일 서비스 개시 이후 영업 5일 만에 100만 계좌를 넘어섰고, 한 달 동안 300만 계좌가 개설되는 등 금융시장에 활력이 됨

* 시중은행의 반년 실적은 10만 계좌 개설 수준(이코노뉴스, 2017.9.15.)

□ 카카오뱅크의 인증 전략

○ 카카오뱅크는 거래안전성과 사용편의성을 보장하기 위해 일원화된 기술구조로 직접 개발하고 다중 보안전략을 적용하여, 단순하면서도 보안성이 뛰어난 간편 인증 수단을 제공함

<그림 4> 카카오뱅크 인증 전략

* 일원화된 기술구조 : 자사의 모바일 앱 기반으로 백신, 키보드 보안, 방화벽 등 타사의 보안모듈을 추가로 설치할 필요 없음

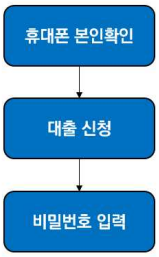
* 다중보안(Multi-Layering) : 거래의 준비부터 완료까지 모든 과정에서 각 단계별로 필요한 보안기술·방식·솔루션들을 적용함으로써 중첩된 보안 체계가 전체적인 거래 안정성을 유지

<표 10> 카카오뱅크 다중보안의 특성

구분	카카오뱅크 다중보안	일반은행 다중보안
개념	거래 안전성을 보장하기 위해 보호 장치를 계층화하고, 각 단계별 보안 요소를 정의하여 해당 단계 요건을 충족 시에만 다음 단계로 진행할 수 있음	
프로세스	이전 단계 보안 절차의 반복이 없음	다중보안 요소를 충족시키기 위한 다양한 조합이 있으며 고객의 반복 입력이 잦음 (예: 공인인증으로 로그인한 경우 이체 등의 거래 시에 다시 공인인증 비밀번호 입력)

○ 서비스 가입으로 전자서명 환경 설정을 완료하고, 1인 1 휴대폰 정책 하에서 매체(기기)→ 로그인→ 거래인증(인증비밀번호, 본인확인, 추가 인증수단 등)의 순서로 서비스를 이용함

<표 11> 간편하면서도 다중보호된 인증절차

용도		인증방식 설명	예시
서비스 가입	회원가입	❶휴대번호로 본인확인 ❷카카오계정이 있는 경우 약관 동의로 바로 회원가입	
	계좌개설	❶ 휴대폰 본인인증, 거래목적 및 자금출처 등 ❷정보입력과 ❸신분증 촬영, ❹타행계좌인증의 과정을 거침	
서비스 이용	로그인	❶패턴(기본인증수단) ❷지문	
	이체	❶카카오톡이나 계좌번호 입력 ❷인증 비밀번호 입력 후 완료	
	대출	❶비상금 대출: 약관·약정서에 동의 → 주민번호 입력(실명인증)→ 완료 (60초 이내) ❷마이너스·신용 대출: 공인인증으로 관련 서류제출 대행	

□ 공인인증은 아니지만, 정부가 요구하는 비대면 실명확인 요건을 충족함

ㅇ 금융위원회 비대면 실명확인 요건의 필수·권고 사항을 모두 구현함

* 아래 표에서 카카오 채택 사항을 굵은 테두리로 하이라이트

<표 12> 국내 허용 비대면 실명확인 요건 충족여부

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

* 자료: 금융위원회, 계좌 개설시 실명확인 방식 합리화방안

□ 이체 거래 시 카카오뱅크 사설인증을 일반은행 공인인증 방식과 비교하면, 모바일 환경에 집중, 간소한 단계로 편의성을 높임

<표 13> 카카오 사설인증의 다중보호 기술을 이용한 편의성

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

* 모바일 보호 영역 : Hardware Backed Key Store(Android), Secure Enclave(iOS)

* 양방향 TLS : 현재 TLS 스펙에서는 단방향만이 필수임

Ⅴ. 기존 공인인증서의 진화 : 은행권 블록체인

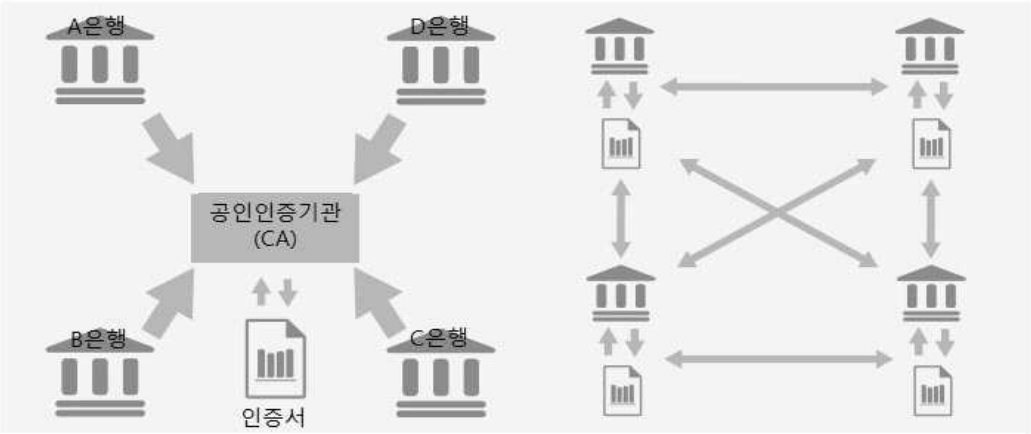
□ 블록체인과 인증

○ 정보를 블록 단위로 쪼개 인터넷으로 연결된 다수의 컴퓨터에 분산저장한 후, 상호 검증하는 방식으로 온라인 거래의 위·변조를 방지하는 기술인 블록체인을 인증서에도 적용하는 방안이 개발됨

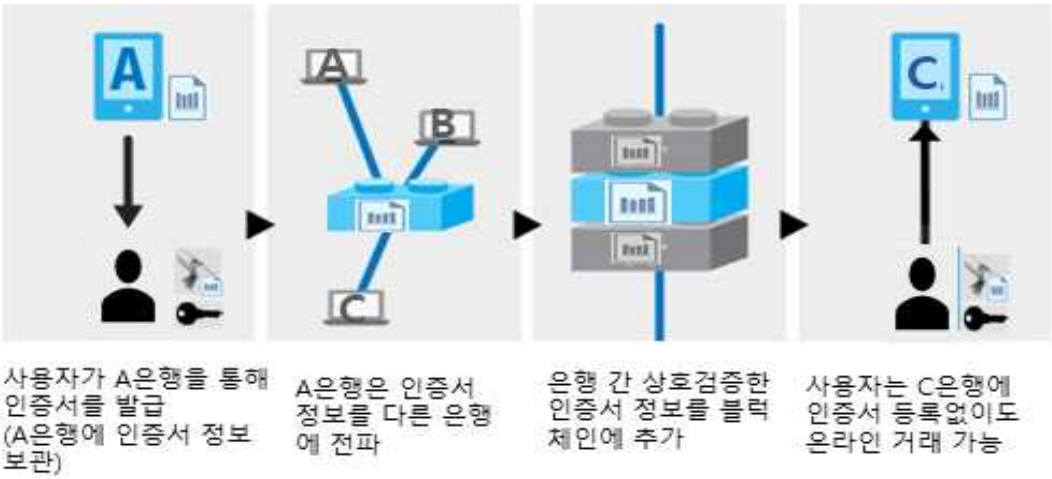
- 인증기관의 중앙서버에 인증서 정보를 보관하는 기존 방식과 달리 블록체인을 이용하여 은행 간 인증서 정보를 공유함

<그림 5> 기존방식과 블록체인 비교

< 기존 방식 : 중앙집중 > < 블록체인 방식 : 분산 >



<그림 6> 블록체인을 통한 은행 간 인증서 공유



* 美필라델피아 연방준비은행 총재인 패트릭 T. 하커는 '17.4.3. 펜살베니아 주립대에서 "블록체인의 진정한 가치는 가상화폐(비트코인)를 유통하는 것이 아닌 인증에 있다"고 연설

□ 기존 공인인증서의 불편함을 블록체인으로 개선

○ 국내 11개 증권사는 2017년 10월에 블록체인 인증 시범서비스를 개시했고, 은행권은 2018년 7월부터 시범서비스를 개시할 예정임

- 기존 공인인증은 한 곳에서 발급한 인증서를 금융기관마다 별도로 등록하는 과정이 필요했는데, 블록체인으로 인증서 정보를 공유하면 이러한 등록절차가 필요 없어짐

  * 블록체인 기술의 대표 사례로 많이 알려진 비트코인의 경우 누구나 접근이 가능한 공공(Public) 블록체인이나, 금융권의 경우 일부 사용자만 접근해 정해진 권한을 이용하는 사설(Private) 블록체인을 적용할 것으로 분석[14)]

- 종전 공인인증서는 중앙시스템 장애나 공격으로 서비스가 중단되면 모든 업무가 중단됐으나, 블록체인 시스템에서는 한 기관에 장애가 발생해도 다른 기관의 업무에 지장이 없음

14) 디지털데일리 '17.6.30 보도참조 (http://www.ddaily.co.kr/news/article.html?no=157636)

Ⅵ. 결론

□ 최근 제4차 산업혁명으로 기존 산업과 새로운 기술과의 융복합이 가속화되고 있어 기존의 제도관행이 지속적인 혁신을 저해하지 않도록 보다 탄력적인 정부의 개입과 제도 운영이 요구됨

* 예시) 국산 피처폰의 미들웨어를 특정 SW로 규정한 WIPI는 국산 핸드폰의 표준화에는 기여했으나 국제화에는 실패한 사례이며, 헬스케어에서 정부가 특정 방식에만 보험수가를 인정하는 바람에 새로운 측정방식의 도입을 저해한 당화혈색소 측정의 사례가 있음

□ 이 보고서가 분석한 공인인증이라는 제도 역시 최초에는 금융거래를 안전하게 보호하는 등 전반적인 인증 수준을 높이는 역할을 담당했었지만 의무화 폐지를 통해 사설인증과 공인인증이 경쟁적으로 진화하고 있는 상황임

○ 인증 제도의 경우, 과거 특정 기술에 종속된 공인인증의 도입을 의무화하는 방식에서 보안의 요건을 만족한다면 새로운 기술의 선택은 기업의 자율에 맡기는 기술 다양화의 방향으로 추가적인 혁신 인센티브를 제공하는 것이 필요함

- 카카오뱅크가 대표적인 사례인데, 공인인증서 없이 지문과 인증비밀번호 만으로 금융거래가 간편하게 이뤄지고 있음

□ 보다 일반화한 결론은 신기술의 사회적 보급을 활성화하는 차원에서 정부의 제도적 개입은 가능하나 새로운 대안기술의 혁신이 빈번하게 발생하는 영역에서 자칫 추가적인 혁신을 저해하지 않게 하기 위해서는 '일몰제'와 같은 탄력적 제도 운영도 필요함

○ 특히, 최근의 경우와 같이 다양한 신기술이 출현하고 혁신의 속도가 점점 빨라지는 추세*에서는 기술 생태계 변화에 부합하는 탄력적 제도운영이 중요

* 1876년 벨(Bell)이 발명한 유선 전화기의 보급률이 10%에서 90%로 도달하는 데 걸린 기간은 73년이었으나, 1990년대에 상용화된 인터넷이 확산되는데 걸린 시간은 20년에 불과했고, 휴대전화가 대중화되는 기간은 14년에 불과(KISTEP, 2017)

[별첨1] 공인인증서 게임의 일반식

1 기업 간 전략 선택 게임의 조건 설정

○ 기업(1)과 기업(2)는 금융 또는 전자상거래 서비스를 제공하는 게임 참여자로서, 이들은 온라인 서비스를 제공하기 위해 인증 방식을 선택할 수 있다. 인증 방식에는 사설인증(a)와 공인인증(b)가 있다. 이때 기업(1)과 기업(2)가 각 인증 전략을 선택함에 따라 얻게 되는 이득은 다음과 같다.

< 기업 1과 기업 2 간의 게임 설정 >

		기업 2	
		사설(a)	공인(b)
기업 1	사설(a)	$(E_1 + R_a\ ,\ E_2 + R_a)$	$(E_1 + R_a + \epsilon\ ,\ E_2 + R_b)$
	공인(b)	$(E_1 + R_b\ ,\ E_2 + R_a + \epsilon)$	$(E_1 + R_b\ ,\ E_2 + R_b)$

- *기업(1)과 기업(2)는 인증 방식에 대한 보안투자와 상관없이, 금융 또는 전자상거래 서비스 영업 활동으로 E_i = 기업 i(i=1, 2)의 이득을 얻는다.*
- *사설인증과 공인인증에 대한 투자비용은 기업의 상황과 관계없이 C_a = 사설인증에 대한 투자비용, C_b = 공인인증에 대한 투자비용으로 동일하다.*
- *사설인증과 공인인증으로 인한 이득은 기업의 상황과 관계없이 I_a = 사설인증으로 인한 이득, I_b = 공인인증으로 인한 이득으로 동일하다.*
- *사설인증으로 인한 투자비용 대 이득, 즉 투자회수율(RoI, Return on Investment)는 $R_a = I_a - C_a$가 되고, 공인인증으로 인한 투자비용 대 이득은 $R_b = I_b - C_b$가 된다.*
- *두 기업의 인증 전략이 다를 때 사설인증을 선택함으로써 얻게 되는 추가 이득을 ϵ라 할 것이며, 이는 양의 값이나 음의 값을 갖는다.*

2 기업의 기대 이득의 계산

○ 만약 기업(2)가 사설 인증을 선택할 확률을 p라 하면, 기업(1)이 사설인증을 선택하는 경우의 기대 이득은

$(E_1 + R_a)p + (E_1 + R_a + \epsilon)(1-p) = E_1 + R_a + \epsilon(1-p)$이고,

기업(1)이 공인인증을 선택하는 경우 기대 이득은

$(E_1 + R_b)p + (E_1 + R_b)(1-p) = E_1 + R_b$ 이 된다.

○ 한편, 기업(1)이 사설인증을 선택할 확률을 q라 하면, 기업(2)의 사설인증 선택 시 기대 이득은

$(E_2 + R_a)q + (E_2 + R_a + \epsilon)(1-q) = E_2 + R_a + \epsilon(1-q)$

공인인증 선택 시 기대 이득은

$(E_2 + R_b)q + (E_2 + R_b)(1-q) = E_2 + R_b$ 가 된다.

[별첨2] 외부자문위원 리뷰 현황

자문위원	소속	자문일시	자문분야
안성진 대표	블록체인 팩토리	2017.4.27.	인증 기술
김종현 교수	아주대학교 사어버보안학과	2017.5.21	인증 기술
윤기찬 교수	고려대학교 행정학과	2017.5.18.	이론 및 구성
박지환 변호사	사단법인 오픈넷	2017.5.19.	제도적 대안
하태기 담당	카카오 뱅크	2017.9.28.	사설 인증 사례

[참고문헌]

1. 국내문헌

- KISA(2002), 주요국가의 전자서명 인증제도 현황
- 정통부(2007), 국가정보보호백서
- 정진명, “UNCITRAL 전자계약협약의 국내법에의 수용” 70-71면
- KDI(2015), 공인인증서 규제 논란의 교훈과 향후 전자상거래 정책방향 제언
- 금융보안원(2017), 인증기술 도입을 위한 선정 프로세스, 美 NIST 가이드라인 재인용
- KISA(2016), 대국민 전자서명실태조사
- 미래부, KISA(2017), 2016년 정보보호실태조사(기업부문) 최종보고서

2. 국외문헌

- Katz, M. L., & Shapiro, C. (1985). Network externalities, competition, and compatibility. The American economic review, 75(3), 424-440.

3. 기타

- 공인인증서 문제해결을 위한 2차 정책토론회: “4차산업혁명시대, ‘새마을운동식 IT정책’에서 ‘시장경쟁’으로”
- law.go.kr
- 인터넷진흥원 매일경제 기고 ‘15.4.5
- 매일경제 ‘17.3.10
- 동아일보, ‘14.4.4.
- 동아일보, ‘17.4.10
- 뉴스토마토, ’ 17.4.9
- 허핑턴포스트코리아, ‘17.3.2.
- 머니투데이 ‘17.3.11.
- 키뉴스 인터뷰 기사 ‘17.4.12

주 의

1. 이 보고서는 소프트웨어정책연구소에서 수행한 연구보고서입니다.
2. 이 보고서의 내용을 발표할 때에는 반드시 소프트웨어정책연구소에서 수행한 연구결과임을 밝혀야 합니다.

OPEN 공공누리 출처표시 상업용금지 변경금지 공공저작물 자유이용허락

[소프트웨어정책연구소]에 의해 작성된 **[SPRI 보고서]**는 공공저작물 자유이용허락 표시기준 제 4유형**(출처표시-상업적이용금지-변경금지)**에 따라 이용할 수 있습니다.

(출처를 밝히면 자유로운 이용이 가능하지만, 영리목적으로 이용할 수 없고, 변경 없이 그대로 이용해야 합니다.)