핀테크와 보안

박소영 (한국핀테크포럼)

목차

1. 서 론

2014년 중반을 기점으로 국내에서도 핀테크 산업이 큰 주목을 받고 있다. 금융서비스(Financial)과 IT기술(Technique)의 결합으로 만들어진 '핀테크'라는 신조어는 이제 신문지면에서 빠지지 않는 용어가 된 것이다. 더불어 국내의 다양한 핀테크 스타트업이 태생되면서 국내 핀테크 산업의 가능성에 대한 기대가 커지고 있다.

이 시점에서 글로벌 핀테크 기업들을 상대로 한국의 핀테크 기업이 경쟁력을 갖추기 위해 필연적으로 발전되어야 할 분야는 보안, 인증분야라고 본다. 이용자의 편의를 증대하기 위해, 이용자를 보호하기 위해, 더 나아가 핀테크 생태계의 지속적 성장을 위해 안정적 보안 체계가 따라야 하기 때문이다. 또한 국내의 경우 특정 보안인증 방식을 다년간 고수해온 탓에 글로벌 표준에서 멀어진 부분이 있어 특히나 글로벌 표준 형태의 보안 기술력이 시급하다.

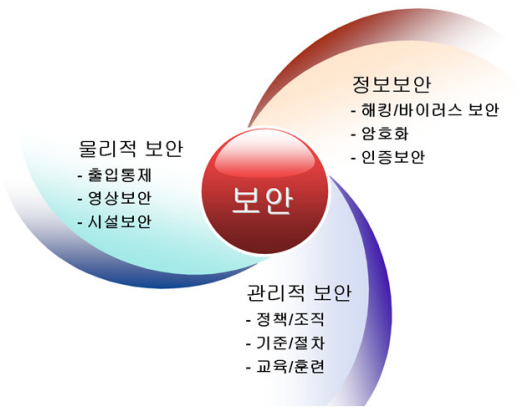
본 고에서는 국내의 표준 보안 기술 도입에 참고할만한 시사점을 도출하기 위해 핀테크 강대국들이 가지고 있는 보안법률을 살펴보고자 한다.

2. 미국, 유럽의 정보보안 관련 법안 현황

2.1 보안의 개념 및 정의

전통 금융산업에서 바라보는 보안영역은 관리적 보안, 기술적 보안, 물리적 보안 등 통상적으로 세가지 보안 영역으로 나뉜다. 최근 기업정보 유출, 개인정보 유출 사고 등으로, 기업에서는 정보보호 조직을 구성하고 비즈니스 환경에 따라 보안 위협의 양상과 사내 규정 요건에 적절히 대응하기 위해 정보 보안의 체계 수립 및 설정하고 있다.

정보보호는 "정보의 수집, 가공, 검색, 송신, 수신 도중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적 방법"혹은"악의적, 우연, 실수 등으로 발생하는 정보의 허가 받지 않



출처 : 한국정보보안학회, http://www.kiisc.or.kr/

(그림 1) 보안의 3가지 종류

은 유출, 전송, 변경, 파괴 등으로부터 정보를 보호하는 것"의 두 가지로 정의될 수 있겠다. 즉, 정보에 대한 허가 받지 않은 모든 행위를 통제하는 활동 모두를 정보보호라고 할 수 있는 것이다. 여기서 정보보호 활동은 관리적 보안, 기술적 보안, 정보보안로 분류할 수 있다.

현대 사회에서의 보안이란 개념은 하나의 영역으로 존재하기보다는 상호 영향을 끼치며 통합화(Convergence)되고 있는 추세이다. 출입통제(물리적보안)에 사용되는 RF카드의 정보는 선을 통해 서버로 저장되며 이를 해킹등으로부터 보호하기 위해 방화벽(정보보안)을 설치하게 되는 상

출처 : 디지털타임스, 최영배 차장 칼럼, 보안의 컨버전스화 오피니언

(그림 2) 보안의 컨버전스화

황이 일종의 물리적 보안과 정보보안의 간단한 협업체제라고 볼 수 있다.

가트너(Gartner Grp.) 보고서("What Convergence Really Means for Informaion Security", 2007.12)에서도 이와 맥락을 같이하는 내용의 보고서를 발표한 바 있다. 또한 뉴스를 통해 연일 타인의 사생활 영상을 열람하는 등의 사건 역시 허술한 패스워드 체계로 타 사용자가 인가되지 않은 채 타인의 영상을 볼 수 있었던 사고로, 물리적 보안의 사안이 정보보안의 문제로 전이되었음을 알 수 있다. 보안과 상호 연결되어 서로를 보완하는 관계에 있는 분야를 꼽자면 단연코 인증에 대한 논의가 빠지지 않게 되는데, 인증은 보안의 일부로 인식되기도 한다.

2.2 미국, 유럽의 정보보안 주요 법안 및 법안 관련 설명

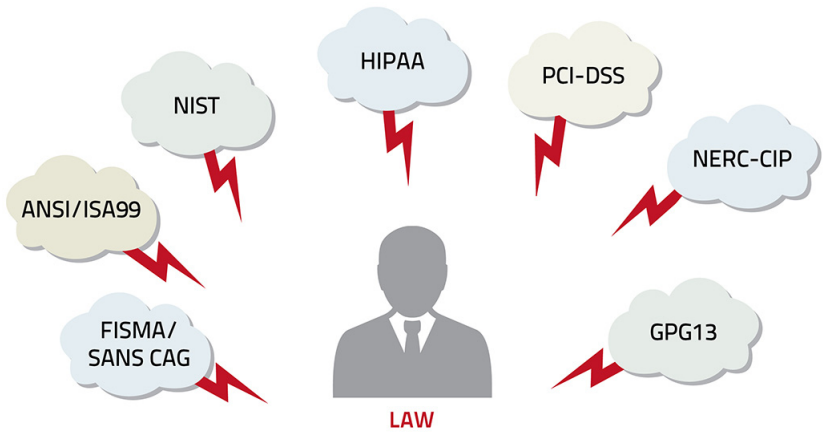
미국, 유럽의 정보 보안 관련 법안 중 가장 주요한 것으로 꼽히는 9가지의 법안 관련 상세 내용은 다음과 같다.

– FISMA : 미국 연방 정보 관리법 (Federal Information Security Management Act)

미국 연방정부는 연방 정부 정보시스템의 보안을 위하여 정부정보보안개혁법과 이를 승계한 연방정보보안관리법을 통하여 관리예산처를 중심으로 한 연방 정부 부처의 정보보안 개선을 위한 체계를 구축하였다.

– SANS CAG : 미국의 효과적인 사이버 국방에 대한 중요 보안 컨트롤. (SANS연구소 제작)

미국 및 국제 기관의 컨소시엄은 빠르게 성장한 민간 산업과 세계 각국의 전문가들에 의해 결



출처 : 구글

(그림 3) 미국, 유럽 주요 정보보안 법안

합된 것이다. SANS 연구소를 통해 궁극적으로 중요 보안 제어 법안이 되었다.

- ANSI : 미국 표준 협회 (American National Standards Institute, ANSI)

여기서 제정된 표준을 또한 ANSI라고 부르기도 한다. ISO에 가입되어 있다. 미국 내의 규격이지만, ISO에 앞서서 제정되는 경우도 많으며, ANSI 표준이 ISO 표준이 되기도 한다.

ANSI는 5 군데의 엔지니어링 회사와 3 군데의 정부 기관이 미국 엔지니어링 표준 위원회(AESC)를 창설한 1918년에 만들어진 것이다. AESC는 1928년에 미국 표준 협회 (ASA)가 되었다. 1966년에 ASA의 조직은 다시 정리되어 USASI(미국 표준 협회)가 되었다. 현재의 이름은 1969년에 채택되었다. 미국 내에서 기술표준 개발을 육성하기 위해 설립된 제1차 기관. ANSI는 산업계에 소속된 기술자 그룹들과 함께 일하며, 세계표준화기구인 ISO(International Organization for Standardization) 및 세계전자기술 위원회인 IEC(International Electro-technical Commission)의 일원이다. ANSI가 제정한 컴퓨터에 관한 표준 중 대표적인 것으로는 아스키가 있다.

- ISA99 : 산업 자동화 및 제어 시스템 보안(Industrial Automation and Control Systems Security)

ISA99 표준 개발위원회는 산업 자동화 및 제어 시스템 보안을 통한 ISA표준을 규격화하였다.

- NIST : NIST 미국 국립기술표준원 (National Institute of Standards and Technology)

NIST는 미국의 전반적인 산업 경제를 향상시키기 위해 업계와 협력하여 기술,기준, 표준을 개발, 적용 및 지원을 목적으로 설립되었다. 특히, 민간 자본으로 달성하기 어렵고, 경제적인 측면에서 중요하다고 판단되는 기술의 선행 연구를 수행하였다. 즉, 연방정부에서는 현재 업계에서 수용할만한 표준이나 해결방안이 없고, 시스템의 보안과 상호운영성에 대한 필요성 및 요구사항이 클 경우에, NIST에 해당표준의 개발을 요청한다. 고객과 사용자 측면을 고려한 품질 관리 가이드를 제시하고 있다.

– HIPAA
:건강보험의양도및책임에관한법률(Health Insurance Portability and Accountability Act)

의료기록에 관한 프라이버시 보호를 위한 법률이다. 여러 의료기관에 보호되는 환자 의료 기록에 환자가 쉽게 접근할 수 있게 한다. 기록의 공개 여부도 환자가 결정할 수 있게 한다.

공정정보규정원칙 내용은 다음과 같다.

공지, 인식 데이터 수집 대상에게 데이터를 수집하는 것에 대한 공지를 해야한다.

선택, 동의 데이터 수집 대상이 자신의 데이터가 이차적으로 사용되는 것을 선택하고 동의할 수 있어야 한다.

접근, 참가 데이터 수집 대상이 수집된 데이터에 쉽게 접근할 수 있어야 한다.

보안, 데이터 수집 기관은 데이터에 대한 보안을 책임져야 한다.

시행, 공정정보규정원칙을 시행하기 위한 여러 법률과 규정이 필요하다.

– PCI-DSS : 결제 카드 산업 데이터 표준(Payment Card Industry Data Security Standard)

PCI DSS는 JCB, 비자, 마스터, 아멕스(아메리칸 익스프레스), 디스커버 카드 등 글로벌 카드사들이 참여하고 있는 지불카드 정보보안표준위원회에서 만든 보안 표준으로 결제대행(PG)사, 카드가맹점 및 관련 서비스 업계에서 이를 따르고 이행하고 있다. PCI DSS는 카드 소지자들을 위해 데이터 보안을 높이고, 일관적인 데이터 보안 조치들을 전 세계적으로 채택할 수 있도록 2004년 12월 개발되었다. 글로벌 카드회사가 협업해서 만든 보안 표준이기 때문에, 신뢰성도 높고 PCI-DSS를 준수한 대부분의 업체들은 데이터 침해사고의 비율이 현저하게 줄어드는 효과가 있다.


ControlCase
Managed Compliance

CERTIFICATE OF COMPLIANCE

Paygate Inc.
- SeokChonBuilding 602, BangiDong 66-7, SongPaGu, Seoul, Korea
- Data Center: LG Dacom KIDC Building, NonHyunDong 261-1, KangNamGu, Seoul 135-010, Korea
- Disaster Recovery Center: SeoChoDong, 1423-1, SeoChoGu, Seoul, Korea

has been audited by **ControlCase** and found to be in compliance with requirements of **PCI Data Security Standard Version 2.0** as per **Report on Compliance** issued on **September 16, 2013.**

The **PCI Data Security Standard** is used by all major card brands as the common security standard for their compliance programs. Brands and programs include,

- **VISA USA** - (CISP - Cardholder Information Security Program)
- **VISA International** - (AIS - Account Information Security)
- **MasterCard Worldwide** - (SDP- Site Data Protection)
- **American Express** - (DSOP - Data Security Operating Policy)
- **Discover Network** - (DISC - Discover Information Security and Compliance)
- **JCB** - Fully supports the PCI DSS mandate

Please note that this certificate does not substitute for the need to register with the card brands directly in order to be listed on their websites and for them to confirm you as compliant per their individual programs.

Level of Certification: **Level 1**
Reference no.: **091620131CNPG1**
Expiration Date: **September 15, 2014**
Assessed by: **ControlCase**

PAYMENT CARD INDUSTRY STANDARD

출처 : 페이게이트

(그림 4) (주)페이게이트 사에서 발급받았던 Level1의 Compliance 증명서

– NERC-CIP :
북미전력신뢰성위원회(NERC)의 CIP 표준 규제

고객들이 진화하는 보안 문제에 대처하는데 도움을 주기 위해 제정된 표준규제법. 최근 들어 사이버 위협의 빈도와 복잡성은 계속해 증가하고 있으며, 수도·전기·가스 등 공공 사업체들이 북미전력신뢰성위원회(NERC)의 CIP 표준 규제를 준수하기 위해 보다 많은 노력을 기울이고 있다.

– GPG13 : 영국 정부 제공 리스크보호 모니터링 기준 지침.

CESG 보호 모니터링 방식. 기업의 리스크 프로파일을 개선하기 위해, 사람과 비즈니스 프로세스 및 기술에 대한 리스크 보호 모니터링 기준 지침을 제공한다. 영국내각부는 보안 정책 프레임 워크지침을 제공한다. 기술위험 평가에 대한 지침은 12개의 감시제어로 구성되어있다.

지금까지 미국과 유럽의 정보보호인증심사 관

련 법안을 알아보았다. 현재 국내 통용되는 정보보호인증심사는 오직 ISMS방식 하나뿐이라는 점을 비교해보았을 때 국내 정보보호인증심사의 다양화가 시급한 문제임을 알 수 있다.

3. 주목받는 신인증기술, 생체인증

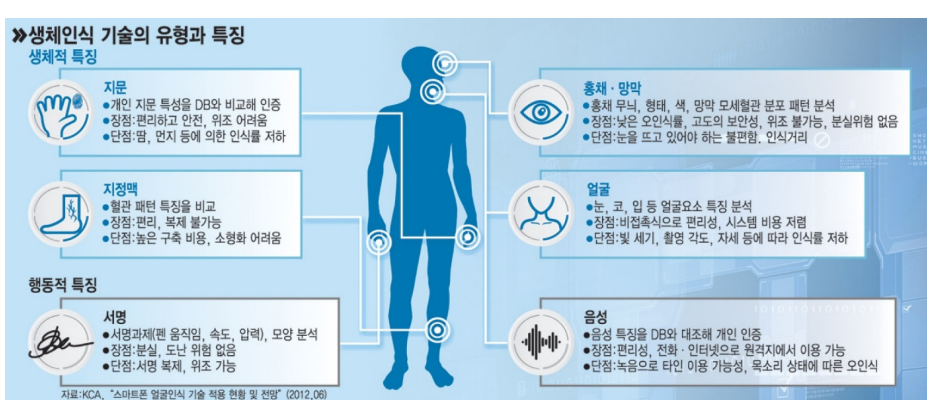
최근 다양한 핀테크 업계에서 공인인증서를 대체하기 위한 인증 수단으로 바이오인식을 주목하고 있다. 핀테크 산업의 최대 걸림돌인 보안 문제에서 비교적 자유롭고 사용이 편리하기 때문이다. 인증을 위해 별도의 도구를 구비할 필요가 없고, 분실할 위험이 없다는 게 가장 큰 장점이다.

'바이오인식'이란 사람이 자기 몸에 갖고 있는 정보를 이용한 보안 인증을 말한다. 사람의 신체적·행동적 특징을 자동화한 장치로 추출하고 분석해 개인의 신원을 정확하게 확인하는 기술로, 개인의 특성인 지문이나 홍채, 망막, 정맥, 손의 형태, 얼굴, 목소리 등을 판별해 본인 여부를 확인한다.

바이오인식은 열쇠나 카드 등 소유물을 이용한 방식이나 비밀번호 등 지식을 이용하는 방식을 넘어서는 차세대 기술로 점점 지능화하고 고도화하는 금융 범죄를 차단할 새로운 방안으로도 거론되고 있다. 금융권이 바이오인증에 기대하는 가장 큰 효과는 보이스피싱 같은 금융사기를 차단할 수 있다는 점이다. 바이오인식 기술이 적용되면 타인의 명의를 도용한 대포 통장을 매개로 벌어지는 금융사기를 방지할 수 있다. 바이오인식은 지불결제 편의성도 높일 수 있다. 애플의 '터치아이디'처럼 지문만으로 결제가 이뤄지면 더 편리하게 모바일 쇼핑을 할 수 있다.

미국·유럽 등 해외 일부 초등학교에서는 어린이들의 급식 결제에도 지문인식을 사용하고 있다. 식당 직원이 돈을 만질 필요가 없어 위생적이고, 아이들이 돈을 가지고 다닐 필요가 없어 안전해서다. 또 무상 급식의 수혜자인지 옆에서 확인할 수 없어 프라이버시도 보호되는 장점도 있다.

FIDO는 바이오인식 국제 표준을 마련하기 위한 협의체로, 삼성전자·구글·마이크로소프트·페이팔·알리바바 등 핀테크 기업을 포함한 200여개 기업이 회원사로 가입돼 있다. KB금융지주 경영연구소는 바이오인식과 관련한 세계 시장규모가 2016년에 96억달러(약 10조 4,467억원), 2019년



출처 : 전자신문 정민영 기자

(그림 5) 생체인식 기술의 유형과 특징

에는 150억달러까지 커질 것으로 예상했다. 국내에서도 연간 2억 6,000만달러 수준의 시장이 형성될 것으로 전망했다. 모바일 바이오인식 시장도 급속도로 성장할 전망이다. 시장조사업체 AMI는 올해 23억 7,300만달러(약 2조 1,182억원)에 이르는 모바일 바이오인식 시장이 2020년에는 333억 2,900만달러(36조 4,152억원)로 커질 것으로 예상하고 있다.

국내 기업들도 발빠르게 나서고 있지만, 아직 바이오인식에 필요한 주요 기술은 해외 업체들이 주도하고 있다. 애플은 2012년 어센텍을 인수하면서 지문인식 센서를 공급받고 있고, 다른 업체들도 미국의 시냅틱스와 스웨덴의 FPC 등의 제품을 활용하고 있다. 국내의 업체들이 기술력으로 승부하여 잠재력을 발휘해야할 것으로 보인다.

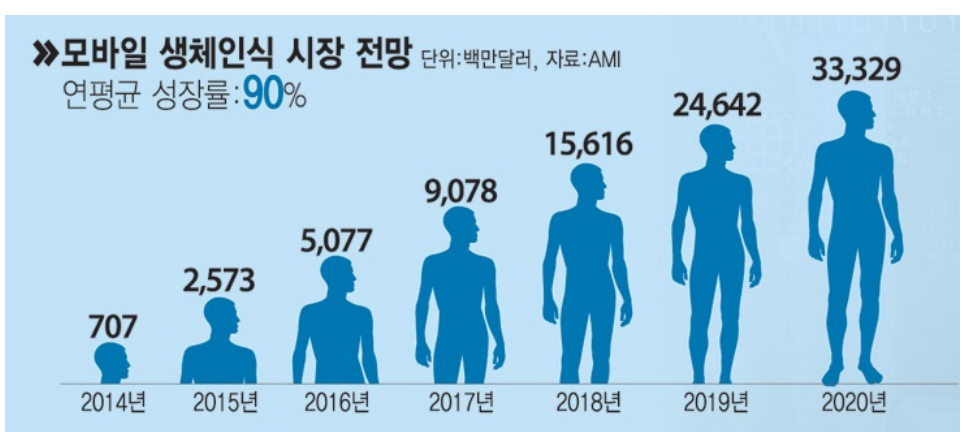
4. 시사점

핀테크 강대국으로 꼽히는 미국과 영국 등은 핀테크 산업 육성에 발맞춰 보안 강화를 위한 감사 법률 체계 수립을 통해 성장하는 핀테크 산업에 대응하기 위한 노력을 지속적으로 추진하고 있다. 또한 미국의 경우 특히 사이버보안뿐만 아니라, 고객의 의료정보 등이 유출되지 않도록 다양한 분야에서 정보보안에 대한 법안을 마련해 두고 있다. 이러한 사전 준비로 인해 앞서 설명한 바이오 인증 등의 신 인증기술의 등장 시에도 미리 구축된 보안감사를 통한 인증과정을 거쳐 안전하고 편리한 서비스를 빠르게 도입할 수 있는 것으로 보인다.

이와 같이 핀테크 강대국의 보안감사 추진, 이행하는 과정을 통해 우리에게 주는 시사점을 도출해 보면 다음과 같다.

첫째, IT기술이 나날이 발달하고 있는 현 시점에서 시장출시에 앞서 알맞은 보안성을 평가할만한 제도적인 기반이 있다는 것은 큰 이점이다. 국내도 나날이 발전하는 핀테크산업에 알맞은 다양한 보안감사를 강화하는 것이 시급하다고 본다.

둘째, 단순히 국가 주도적인 보안감사 시스템보다 국가간, 기관 및 민간 부문간 협력이 필요하다. 국가 주도적인 보안감사 시스템은 천편일률적인 형태로 분야별 다양성이 배제될 수밖에 없다. 핀테크와 같이 신기술의 등장에 민감한 산



출처 : 전자신문 정민영 기자

(그림 6) 모바일 생체인식 시장 전망

업일수록 이러한 협력이 필수적이라고 본다. 특히 국내의 경우 과거 특정 인증방식에 갇혀 수년간 글로벌 표준으로부터 멀어진 보안인증을 시행한 바 있다. 이를 글로벌 표준의 형태로 개선해야만 글로벌 시장에서 경쟁력을 가질 수 있다. 이를 위해서도 범국가적인 협력이 필요하다.

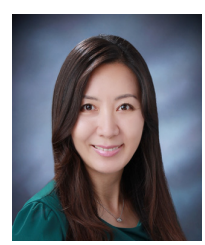
셋째, 핀테크 신기술 도입에 국가차원의 다양한 지원이 필요하다. 한국은 전 국민의 지문을 소유하고 있는 특수한 국가이다. 이를 잘 활용한다면 바이오인식 산업 발전에 큰 도움이 될 수 있다. 최근 글로벌 시장에서 핀테크-바이오인식이 급부상했지만 사실상 전세계의 시장은 아직 초기 단계이다. 선진국과 비교할 때 우리나라가 다소 늦은 것은 사실이지만 강력한 IT인프라를 갖고 있는 이점을 볼 때 향후 해외 추진 속도를 추월할 가능성도 높다고 본다. 강력한 IT인프라를 갖고 있기 때문이다. 바이오인식기업들에게 핀테크는 새로운 기회다. 이를 주목하고 국가차원에서 적극적으로 대응하여 글로벌 시장에서 성공하는 한국기업을 육성하는 집중력이 필요한 시기이다.

현재 국내에서도 핀테크와 보안에 관련해 다각도로 노력을 기울이고 있음을 안다. 다만본 고에서 살펴본 해외의 사례에서 핀테크 산업의 발달과 함께 보안성 강화를 위해 지속적으로 다양한 정책들을 실행해 가고 있음을 알 수 있었다. 우리의 경우에도 다양한 벤치마킹 사례를 발굴, 적용하여 핀테크 서비스 보안의 중요성 인식 확산을 위해 노력해 다양한 인증체계의 자유로운 시장경쟁 구도가 형성되길 기대한다.

참 고 문 헌

[1] 임석재 한국인터넷진흥원 IoT 보안산업팀 선임연구원, 핀테크 보안 동향 - 한국정보통신기술협회
[2] 장상수 한국인터넷진흥원 정책연구단TF 수석연구 위원, 핀테크(Fintech)가 정보보호산업에 미치는 영향에 대한 고찰
[3] 노상규(Sangkyu Rho), 핀테크가 해결해야 할 3가지 과제: 신뢰, 보안, 사용자 경험 (Trust, Security & UX in Financial Service Innovation) ,March 11, 2015
[4] 해당링크: http://organicmedialab.com/2015/03/11/trust-security-ux-in-financial-service-innovation/
[5] 정유신 서강대학교 경영학부 교수, 핀테크의 확대 추세와 금융투자회사의 대응방안
[6] 김영린 금융보안원장, 핀테크 활성화와 금융사 자율보안 전자신문기고문

저 자 약 력



박 소 영

이메일: shyeong@paygate.net

- 1996년 서강대학교 경영대학원 석사 학위 취득
- 1998년 페이게이트 창업
- 2000년 국내 최초 모바일 결제 서비스 X-pay 출시
- 2003년 페이게이트 재팬 설립
- 2006년 일본 시중은행의 계좌 입금 서비스런칭
- 2007년 중국 알리바바 알리페이 중화권 외 최초런칭
- 2009년 페이게이트 홍콩, US설립
- 2010년 중국 은행 연합 CUP카드 서비스 한국런칭
- 2010년 중국 텐센트 텐페이 서비스 한국런칭
- 2010년 기업호민관실과 함께 인증방법평가 위원회 설치 제안
- 2011년 공인인증서 대체 기술 정부 제안으로 국무총리 훈장 수상
- 2012년 금액인증 보안나군 평가 승인
- 2014년 홍콩 HSBC 은행 협업 '오픈페이' 서비스 출시
- 2015년 현재 한국핀테크포럼 의장, 한국 인터넷기업협회 특별부회장, 기업은행 핀테크