http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.21, No.4, November 2016, pp.41-53
http://dx.doi.org/10.7838/jsebs.2016.21.4.041

전자금융 거래 시 생체인증을 전자서명에 활용하기 위한 기술 및 법률에 관한 연구

A Study on the Utilization of Biometric Authentication for Digital Signature in Electronic Financial Transactions: Technological and Legal Aspect

송재헌(Jae-Hun Song)*, 김인석(In-Seok Kim)**

초 록

요즘 각 스마트폰 제조사에서 플래그쉽(flagship) 스마트폰 모델에 지문, 음성, 홍채인식 기능을 기본적으로 탑재하면서 생체인증을 활용한 인증수단이 활성화 되고 있다. 이러한 생체인증(지문, 음성, 홍채 등)은 패턴이나, 비밀번호와 같이 스마트폰의 잠금 해제 기능뿐만 아니라 금융권을 중심으로 다양한 인증수단으로 확산되고 있다. 본 논문에서는 생체인증을 통해서 전자금융(인터넷뱅킹, 스마트뱅킹 등)거래 시 사용자를 인증하고, 거래 내역에 대한 전자서명을 통한 부인방지 기술에 대해 설명하고, 이러한 생체인증 기술이 금융서비스에 접목되기 위해 필요한 관련 기술적, 법률적인 요구사항을 연구하고자 한다.

ABSTRACT

Today, leading smartphone manufacturers offer biometric technologies such as fingerprints, voice recognition, and iris patterns in their flagship models. These biometric technologies are used for authentication. Biometric authentications are widely used in device security and even in financial transaction. This paper examines cases where a user uses biometric authentication during financial transaction (both online and smartphone banking), and explains biometric for non-repudiation by digital signature. Finally, the paper also explains technical and legal requirements for biometric authentication in the area of financial services.

키워드 : FIDO, 생체인증, 공개키 알고리즘, 전자서명, 부인방지
FIDO, Biometrics, PKI, Digital Signature, Non-Repudiation

* Department of Information Security Graduate School, Korea University(prayer21c@korea.ac.kr)
** Corresponding Author, Department of Information Security, Korea University(iskim11@korea.ac.kr)
Received: 2016-10-21, Review completed: 2016-11-17, Accepted: 2016-11-23

1. 서 론

금융과 IT기술이 융합된 핀테크 산업 활성화를 위해 금융위원회가 발표한 내용에 따르면, 보안성심의 제도, 인증방법평가위원회 제도를 폐지함으로써 금융 서비스의 보안규제 방식을 미국, 영국 등 핀테크 선진국처럼 '사전규제'보다 '사후 보안'을 강화하는 방향으로 규제 패러다임을 전환하고 있다[8].

이는, 글로벌 경쟁력을 갖춘 핀테크 서비스를 창출하고 핀테크 산업을 우리나라의 신성장 동력으로 육성하기 위함이다[8]. 이러한 정책의 일환으로, 인터넷을 주 채널로 모든 거래가 이루어지는 인터넷전문은행 출시에 앞서, 전자금융거래에서도 공인인증서 의무 사용 폐지(2015. 3. 18), 일회용비밀번호(보안카드, OTP) 의무 사용 폐지(2016. 6. 30) 등 각 종 규제가 순차적으로 완화되고 있다.

특히, 공인인증서는 공인인증기관(CA)이 발행하는 전자적 정보로서 신원확인, 무결성, 기밀성, 부인방지 등 많은 장점이 있어 국내 전자금융(인터넷뱅킹, 스마트뱅킹 등)거래 시 오랫동안 사용되어 왔다. 하지만, 공인인증서의 실제 사용 환경에서는 ActiveX 등 비표준기술로 구현되어 있어 설치에 따른 사용자의 편의성을 저해하고, 피싱, 파밍 등 악성코드를 통해 사용자 PC나 스마트폰의 NPKI 폴더에서 공인인증서 파일 탈취가 가능하다는 취약점이 지적되어 왔다[2].

공인인증서 의무 사용 폐지에 따라 금융 서비스 영역에서는 공인인증서 이외의 다양한 보안/인증 기술의 경쟁이 가능하게 되었으며, 공인인증서가 담당해 왔던 사용자 인증과 거래 내역 부인방지 기능을 대체할 수 있는 다양한 보안/인증 수단이 속속 출현하고 있다. 하지만, 아직까지도 공인인증서의 주요 기능 중 하나인 거래내역 부인방지 기능은 법률적/제도적 걸림돌이 남아 있는 현실이다.

본 논문의 제2장에서는 FIDO를 기반으로 하는 생체인증을 활용한 전자서명 기술에 대해서 설명하고, 제3장에서는 전자금융거래법과 전자서명법을 중심으로 생체인증을 전자서명에 활용하기 위한 관련 법률적・제도적 사항들을 검토하고, 제4장에서는 결론을 제시한다.

2. 생체인증을 활용한 전자서명 및 부인방지 기술

생체인증을 금융서비스에 적용하기 위해서는 해당 기술이 기존 공인인증서가 담당하던 사용자 인증과 거래 내역에 대한 부인방지 기능을 충족시킬 수 있는지 검토할 필요가 있다.

본 장에서는 생체인증의 기술 표준인 FIDO (Fast IDentity Online) 규격의 명세 범위와 부인방지 서비스의 요건을 살펴보고, FIDO 기반의 전자서명 및 부인방지 기술들을 고찰하고자 한다.

2.1 FIDO 기술 규격

FIDO 기술 규격은 온라인 환경에서 생체인식기술을 활용한 인증방식에 대한 개방형 기술 표준으로서, 안전한 사용자 인증을 위해 사용자의 디바이스에서 제공하는 보안 기능을 활용하고, 사용자가 암호, 인증서 등을 생성하고 외우는데서 발생하는 불편함을 해소하고자 FIDO Alliance에서 개발하였다.

FIDO 기술 규격은 크게 두 가지 방식으로 나뉘는데, 지문 및 음성, 얼굴인식 등 생체 정보에 기반한 사용자 인증 과정에 활용되는 표준인 UAF(Universal Authentication Framework) 방식과, 기존 ID/Password 인증 방식 및 추가의 보안 정보를 보관하는 USB(Universal Serial Bus) 방식, 스마트카드 등 별도의 인증 장치를 사용하는 U2F(Universal Second Factor) 방식으로 구분된다.

본 논문에서는 생체인증 기반의 부인방지에 초점을 맞추기 위하여 UAF를 중심으로 고찰하도록 한다.

2.1.1 FIDO 기술 규격 범위

FIDO UAF 기술 규격은 아키텍쳐, 프로토콜 및 각 구성 요소에 대한 상세 API에 대해 명시하는 10개의 세부 규격으로 구성된다. 각 세부 규격에 대한 명세 내용은 <Table 1>과 같다.

상기 표에서 보는 바와 같이 FIDO 기술 규격은 생체인증 프로토콜을 통한 사용자 등록, 인증, 전자서명 및 사용자 해지에 대한 규격을 주 내용으로 다루고 있다. 본 논문에서 관심있는 사용자 인증 및 거래 내역의 부인방지 측면으로 분석하면 사용자 인증과 거래 내역 전자서명 부분까지가 FIDO 기술 규격이 제공하는 범위로 판단할 수 있다.

2.1.2 FIDO 기술 규격의 거래 내역 전자서명

앞 절에서 검토한 것처럼 FIDO 규격은 사용자 식별/인증 및 거래 내역 전자서명 프로토콜

〈Table 1〉 FIDO UAF Specification

Detailed Technical Specifications	Details and Ranges
FIDO UAF ARCHITECTURAL OVERVIEW	FIDO UAF component and entire process flow (Registration, Authentication Transaction signature, Deregistration, etc)
FIDO UAF PROTOCOL SPECIFICATION	Registration, Authentication, Transaction signature, Deregistration messages details
UAF APPLICATION API AND TRANSPORT BINDING SPECIFICATION	FIDO Client API details (Registration, Authentication,Transaction signature, Deregistration, etc)
FIDO UAF AUTHENTICATOR- SPECIFIC MODULE API	FIDO ASM API details
FIDO UAF AUTHENTICATOR COMMANDS	FIDO Authenticator commands details
FIDO UAF AUTHENTICATOR METADATA STATEMENTS	Description for the method for representing the FIDO Authenticator for use in FIDO server
FIDO UAF AUTHENTICATOR METADATA SERVICE	Description for how to distribute FIDO Metadata
UAF REGISTRY OF PREDEFINED VALUES	A constant value used in the FIDO protocol description
FIDO APPID AND FACET SPECIFICATION	Authentication method description to FIDO Client, ASM, Authenticator from the client-side
FIDO SECURITY REFERENCE	FIDO Protocol security verification and security-related considerations stated

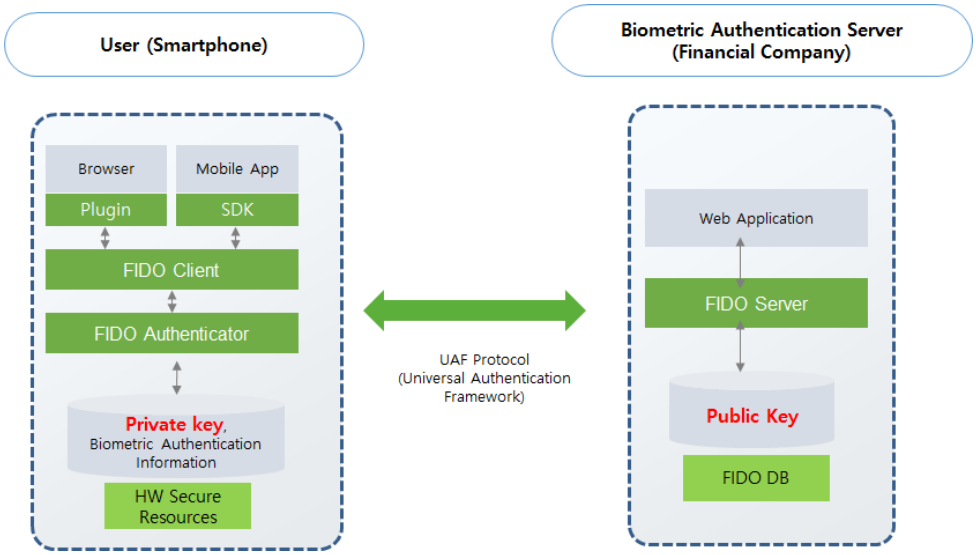
을 정의하고 있다. 기존 공인인증서가 금융서비스의 안전성을 위하여 제공하던 부인방지 요건 중 사용자와 트랜잭션 간의 바인딩 및 전자서명 절차를 설명하면 다음과 같다.

(1) 사용자의 등록을 위하여 사용자의 스마트폰 센서에서 생체정보(지문, 홍채, 음성 등)를 취득하여 스마트폰 하드웨어 보안영역에 공인인증서와 같은 PKI 키쌍(개인키, 공개키)을 생성한다. 이후, 공개키는 금융회사 FIDO 서버로 전송하고 개인키는 스마트폰 하드웨어 보안영역에 저장한다.

(2) 사용자의 스마트폰 디바이스에서 생체정보(지문, 홍채, 음성 등)를 인식 한 후, 개인키를 이용한 연산 결과를 FIDO 서버에 전송하여 FIDO 서버가 사용자의 공개키로 사용자를 인증한다.

(3) 인증된 사용자는 단말기 상의 개인키로 거래 내역에 대해 전자서명 연산을 수행하고 그 결과를 FIDO 서버로 전송하여 서버가 사용자의 공개키로 거래 내역 전자서명을 검증하는 프로토콜을 수행할 수 있다.

FIDO 기반의 생체인증 기술은 공인인증서와 동일한 공개키 알고리즘을 통한 암호화 및 전자서명을 제공하기 위한 PKI 기술을 사용하여 구현되기 때문에, 기술적으로는 공인인증서와 동등한 보안수준을 제공한다. 뿐만 아니라, 기존 공인인증서의 문제점으로 지적되고 있는 공인인증서 유출 문제와, 공인인증서 오남용 문제를 해소할 수 있는 장점이 있으며, 재발급 및 키 갱신으로 인한 PC, 스마트폰 간 인증서 이동 등의 불편함과 복잡한 패스워드를 기억하고 입력할 필요 없이 생체정보(지문, 음성, 홍채 등)스캔만으로 편리하게 이용할 수 있는 등 다양한 장점을 제공한다.



〈Figure 1〉 Biometric Structure Diagram

〈Table 2〉 Biometric Authentication vs Certificate Verification

Sections	Biometric Authentivation	Certificate Verification
Strength of cipher	2048-bit	2048-bit
Encryption algorithm	Public key algorithm (FIDO-based)	Public key algorithm
Save-private key	Smartphone hardware security zone	Kept on file in the location defined in the certificate verfication
Outflow-private key	The private key can not be outflow	Phishing apps, malware such as private keys outflow risk
Share with others	No biometric information sharing	Others to the certificate (private key, password, etc.) can be forwarded to abuse and non-repudiation issue certificates for use

하지만, <Table 1>에서 확인한 바와 같이 FIDO 기술 규격 자체로는 금융 서비스가 필요로 하는 부인방지 기능을 제공하는 데에 한계가 있다.

2.2 부인방지 서비스 요건

금융 서비스에서 요구되는 부인방지 서비스는 금융 거래 당사자와 금융회사 간에 분쟁이 생겼을 때에 금융 거래의 주체가 되는 사용자가 해당 금융 거래를 수행했다는 사실을 부인하지 못하도록 증거를 제시하는 서비스를 의미한다. 이러한 부인방지 서비스를 명확히 살펴보기 위해서 부인방지 서비스가 만족해야 하는 요건을 살펴보면 다음과 같다.

(1) 거래 내역과 고객 결합(Transactions and users must be tightly bound)
(2) 거래 내역 위조 불가(Transactions must be difficult to forge)
(3) 거래 내역 변경 불가(Transactions must be unalterable)
(4) 거래 내역 검증 가능(Transactions must be verifiable)

처음 두 가지 요건은 전자서명 제출(Submission) 시의 부인방지 요건이며, 나머지 두 가지 요건은 전자서명 수신(Receipt) 시의 부인방지 요건을 제시하는 것으로서, 상기 네 가지 요건을 모두 만족해야만 금융 거래의 부인방지 서비스로 사용이 가능하다.

(1) 거래 내역과 고객의 결합 요건의 확인을 위해서는 우선 대면인증 등 금융기관 책임 하에 고객 신원을 확인하여야 하며, FIDO 인증기(Authenticator)는 신뢰할 수 있는 실행 환경에서 동작해야 한다. 또한, 거래 내역의 전자서명은 안전하게 관리되는 개인키로 수행되어야 한다.
(2) 거래 내역의 위조를 불가능하게 하기 위해서는 신뢰할 수 있는 공개키 알고리즘 및 일방향 해시 알고리즘으로 전자서명을 수행해야 한다.
(3) 거래 내역의 변경을 불가능하게 하기 위해 서버에 안전하게 등록된 공개키로 전자서명을 검증해야 하며, 금융기관 서버 내에서 거래 내역과 전자서명을 안전하게 보관하여야 한다.

상기 세 가지 요건들은 FIDO 기술 규격과 금융 서비스 시스템이 자체적으로 지원 가능한 영역으로 판단된다. 하지만, 마지막 요건인 (4) 거래 내역 검증 기능은 전자서명 검증을 통한 거래 내역 무결성 검증과 함께 전자서명 생성정보(개인키 등)의 유효성 검증을 포함하는 요건으로서 FIDO 기술 규격만으로는 제공할 수 없는 요건으로 파악된다[10].

2.3 FIDO 기반 부인방지 기술

생체인증을 금융 서비스에 적용 시 거래 내역 부인방지 요건을 충족시키기 위한 기술이 다양하게 개발되고 있다. FIDO 규격과 국내 공인인증 기술을 연계하는 모델, 공인인증기관의 시점확인 서비스를 이용하는 모델, 그리고 KSI(Keyless Signature Infrastructure) 기술 연계 모델 등이 그것이며 해당 기술들은 국내 금융회사 서비스에 적용되어 활용되고 있다.

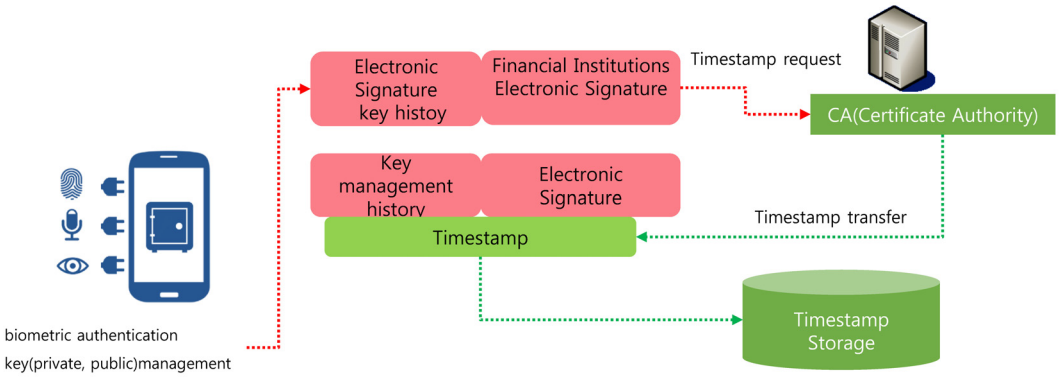
2.3.1 FIDO-공인인증 기술 연계 모델

한국인터넷진흥원은 국내 공인인증기관의 최상위 인증기관으로서 기존 공인인증 체계와 FIDO 기술 규격을 기술적으로 접목시킬 수 있도록 “바이오정보 연계 등 스마트폰 환경에서 공인인증서 안전 이용 구현 가이드라인”을 작성하여 공표했다. 이 가이드라인의 부록에서는 FIDO 인증기술과 공인인증서 연계 기술로서 지문 등 생체 정보를 이용하여 비밀번호를 입력하지 않고 공인인증서를 이용할 수 있는 방법을 제시하고 있다.

해당 가이드라인은 FIDO 프로토콜 수행 시점에 공인인증서 개인키 연산을 추가함으로써 기존 공인인증서의 주요 기능이었던 거래 내역 부인방지 기능을 제공할 수 있다는 장점이 있는 반면, 최근 규제 개혁 대상인 공인인증서를 생체인증 서비스에서도 사용해야 한다는 문제점을 가지고 있다.

2.3.2 TSA 기술 연계 모델

타임 스탬프(Time Stamp) 서비스는 전자서명법에 명시된 공인인증기관 서비스로서 전자문서가 제시된 시점에 존재했었음을 확인해 주는 시점확인 서비스이다. 또한, 시점확인 서비스를 제공해 주는 공인인증기관을 시점확인 서비스 기관(TSA: Time Stamp Authority)이라 부른다.

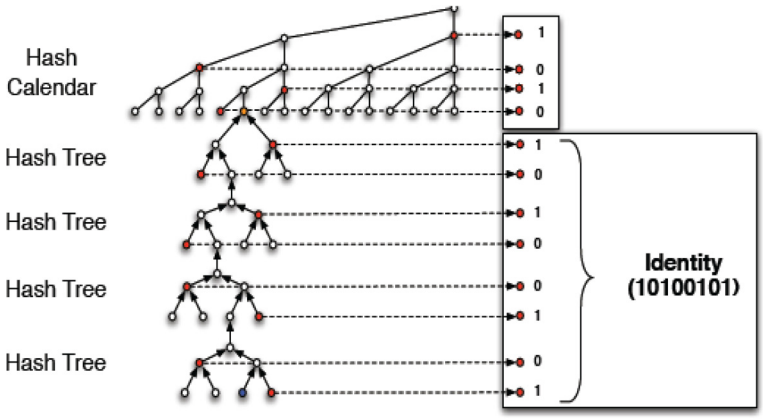


〈Figure 2〉 TSA-Based Non-Repudiation Service

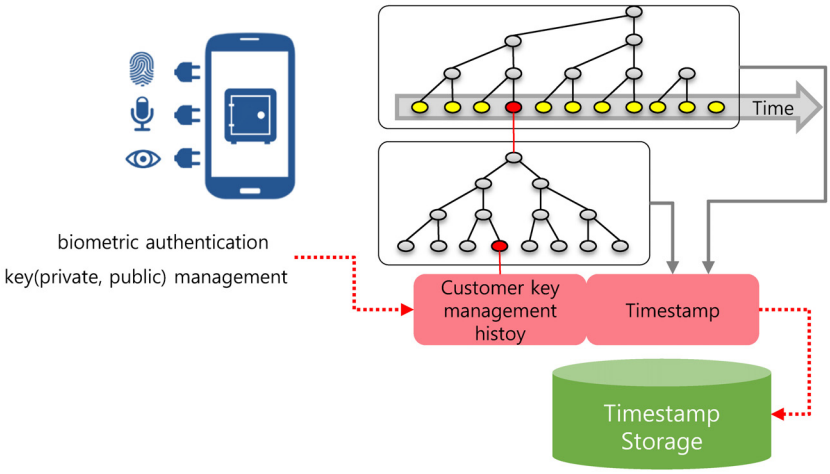
NH농협은행은 FIDO 기반 생체인증을 이용한 거래 내역 부인방지 기능 구현을 위해 TSA의 시점확인 서비스를 연계하여 적용했다. 사용자는 FIDO 규격에 따라 안전한 실행 환경 및 저장소를 통해 사용자 인증을 수행한 후, 주요 금융 거래(자금이체 등) 시 생성된 키쌍 중 공개키를 해당 금융회사 서버에 등록하는 시점에 공인인증기관의 시점확인을 요청한다. 금융회사 서버는 사용자의 키 등록 및 관리 내역과 함께 공인인증기관의 시점확인 서명 정보와 함께 별도의 저장소에 보관하여 추후 발생할 수 있는 분쟁에 대한 증거 데이터로 활용하게 된다.

2.3.3 KSI 기술 활용 모델

KSI(Keyless Signature Infrastructure)는



〈Figure 3〉 Keyless Signature Infrastructure



〈Figure 4〉 KSI-Based Non-Repudiation Service

공인인증기관과 같은 별도의 TTP(Trusted Third Party) 없이 해당 데이터가 해당 시점에 존재했었다는 사실을 증명해 주는 부인방지 기술이다. 이 기술은 미 공군, NSA를 비롯하여 중국, 말레이시아, 필리핀 정부에서도 사용하고 있으며, 중요 문서의 존재 여부 및 진위 여부를 보증하는데 이용되고 있다.

KSI에서는 중요 정보들의 존재 여부 및 진위 여부를 보증하기 위해 해당 문서들의 해시값을 신문, SNS 등에 공표하거나 변경 불가능한 저장장치(WORM Storage)를 이용하게 되는데, 이 절차의 효율성을 위해 해시트리 구조를 사용한다.

FIDO 기반 생체인증에 KSI 기술을 연계시키기 위하여 일정 시간 동안 등록된 사용자의 키 쌍 관리 내역을 해시트리 블록으로 묶은 후, 해당 블록의 최상위 해시값을 다시 시간 정보를 추가한 해시 캘린더로 체인화함으로써 부인방지 서비스를 구현할 수 있다.

3. 생체인증관련 제도 및 법률적 사항

핀테크의 상징을 의미하는 간편결제 방식이 출현한 이후, 오랫동안 안전한 인증기술로 평가 받던 공인인증서가 편의성을 저해하는 대표적인 규제의 대상으로 인식되면서 최근에는 다양한 인증기술과 간편결제 서비스가 금융 서비스 시장의 판도를 바꾸고 있다[2].

간편결제 방식은 복잡한 세부정보 입력이나 소프트웨어 추가 설치 없이 지급결제에 필요한 개인정보와 신용정보를 서버에 등록하고 거래 발생 시 설정된 인증수단(아이디/패스워드, SMS/ARS인증 등)으로 본인인증을 완료하는 서버형 결제방법[2]으로 미국의 페이팔과 중국의 알리페이가 대표적이다.

본 장에서는 거래의 단순화와 편의성을 향상시킨 시대적 흐름에 따라 개정된 전자금융거래법 등 관련법을 살펴보고, 금융 서비스의 관점에서 생체인증을 활용한 전자서명의 신원확인 효력과 거래 내역 부인방지 효력 및 한계점을 검토해 보고자 한다.

3.1 전자금융거래법 및 관련 규정 개정

전자금융거래법은 컴퓨터, ATM, 전화기 등 전자적 장치로 이루어지는 금융거래를 규율하는 거래법이면서 동시에 전자금융업의 영위와 감독에 대한 사업법이다. 공인인증서와 관련하여 기존 전자금융거래법 제21조 제3항에서 “금융위원회는 전자금융거래의 안전성과 신뢰성을 확보하기 위하여 전자서명법 제2조제8호의 공인인증서의 사용 등 인증방법에 대하여 필요한 기준을 정할 수 있다.”고 명시하여 금융회사들은 공인인증서를 사용할 수밖에 없는 상황이었다. 하지만, 개정된 전자금융거래법에서는 “금융회사 등은 전자금융거래의 안전성과 신뢰성을 확보할 수 있도록…(중간생략)…인증방법에 관하여 금융위원회가 정하는 기준을 준수하여야 한다.”(전자금융거래법 제21조 제2항)고 하였고, “금융위원회는 제2항의 기준을 정할 때 특정 기술 또는 서비스의 사용을 강제하여서는 아니 되며, 보안기술과 인증기술의 공정한 경쟁이 촉진되도록 노력하여야 한다.”(전자금융거래법 제21조제3항)고 개정하였다.

이에 따라 전자금융감독규정 또한 개정이 되었는데, 기존 전자금융감독규정 제37조에서는 “모든 전자금융거래에 있어 전자서명법에 의한

공인인증서 또는 이와 동등한 수준의 안정성이 인정되는 인증방법(이하 '공인인증서 등')을 사용하여야 한다."는 내용을 개정하여 "전자금융거래의 종류, 성격, 위험 수준 등을 고려하여 안전한 인증방법을 사용하여야 한다"고 명시하면서 공인인증서 의무사용에 대해 폐지하였다. 따라서, 생체인증을 통한 전자서명 기술이 공인인증서를 대체하여 전자금융거래에 사용하는 데에 따른 규정 또는 법률적으로는 특별한 장애물이 없는 것으로 판단된다.

3.2 생체인증을 활용한 전자서명의 신원확인 효력

전자금융거래법 제2조(정의)의 제10호에서는 이용자의 생체정보를 전자금융거래에 있어서 거래지시를 하거나 이용자 및 거래내용의 진실성과 정확성을 확보하기 위하여 사용되는 수단 또는 정보가 되는 "접근매체"로 명시하고 있다. 즉, 공인인증서와 동일한 수준에서 정의된 이용자 신원확인 매체로 이해할 수 있다.

또한, 앞장에서 생체인증의 전자서명 기술에서 언급 했듯이, 생체인증을 통한 전자서명 생성정보(개인키)로 전자문서에 전자서명하여 이를 수신자에게 보내고, 수신자는 그것을 서명자의 전자서명검증정보(공개키)로 복호화한 후 그 내용을 확인해 맞으면, 수신자는 그 전자문서를 보낸 사람을 확인할 수 있다. 전자서명 된 전자문서(즉 개인키에 의하여 암호화된 전자문서)를 복호화 하였을 때, 그 내용이 되도록 암호화를 할 수 있는 사람은 공개키의 짝이 되는 개인키를 가지고 있는 서명자뿐이기 때문이다[4].

따라서, 생체인증 방식은 본인이 없으면 사용할 수 없는 고정형 정보이고, 본인만이 사용할 수 있기 때문에 유일무이한 신원확인의 효력[6]이 있는 것으로 판단된다.

3.3 생체인증을 활용한 전자서명의 부인방지 효력과 한계

생체인증에 기반한 전자서명에 부인방지 효력이 인정되는지에 관하여는 전자서명법을 검토할 필요가 있다. 전자서명법에서는 전자서명의 종류를 공인전자서명과 공인전자서명외의 전자서명(이하 "비공인전자서명")으로 분류하고 있다. 공인전자서명은 공인인증서에 기초하고 일정한 요건을 갖춘 서명으로 정의하고 있다(전자서명법 제2조 제3호).

또한, 공인전자서명은 당해 전자서명이 서명자의 서명, 서명날인 또는 기명날인이고 당해 전자문서가 전자서명된 후 그 내용이 변경되지 않았음이 추정된다고 명시하고 있다(전자서명법 제3조 제2항).

즉, 당해 전자문서를 송부한 사람이 추후 그러한 전자문서의 진정성립, 송부사실 또는 그 내용의 진정 성립을 부인할 때 당해 전자문서가 진정 성립된 것이 법률상 추정되므로 이를 부인하는 자가 당해 전자문서가 위·변조되었다는 등 진정 성립되지 않았음을 증명하여야 한다.

하지만, 비공인전자서명은 이러한 법률상의 추정력이 없고, 당사자의 약정에 따른 서명, 서명날인 또는 기명날인으로서의 효력(전자서명법 제3조 제3항)만을 가지므로, 그 전자서명의 진정 성립 및 내용의 부인여부에 대한 분쟁 발생 시 에는 당해 전자서명이 당사자의 서명이고 전자서명 후 그 내용이 변경되지 않았다는 점은 민사소송법의 일반원칙에 따라 증거로

제출하는 자(예: 은행)가 입증해야 한다[7]. 즉, 공인인증서와 같이 당사자가 아닌 제3자에 대하여 배타적으로 효력[9]을 인정받을 수는 없다는 한계점이 있다.

따라서, 생체인증을 통한 전자 자금이체성 업무와 관련하여 분쟁이 발생할 경우, 생체인증을 통한 전자서명은 전자서명법상의 부인방지에 관한 추정적 효력을 받지 못하므로 해당 금융기관이 전자서명이 당해 이용자의 서명이고, 당해 전자문서가 전자서명된 후 그 내용이 변경되지 아니하였다는 점을 직접 입증해야하는 한계가 있다[7].

〈Table 3〉 The Legal Analysis on Applying Biometric Authentication in Financial Service

Category	Related Laws	Analysis
Whether law enables the use of biometric authentication for e-financial transactions	ELECTRONIC FINANCIAL TRANSACTIONS ACT Article 21 ③ The Financial Services Commission shall not compel the use of any specific technology or service when determining the standards referred to in paragraph (2) and shall endeavor to promote the fair competition of security technologies and certification technologies.	The law allows various authentication technologies (including biometrics) for electronic financial transactions
	REGULATION ON SUPERVISION OF ELECTRONIC FINANCIAL ACTIVITIES Article 37 Financial Institution or Electronic Financial Business Company shall be able to secure appropriate authentication methods by considering the type, character, and risk-level, etc of electronic financial transaction.	As the mandatory use of certificate is no longer applied, the use of biometric authentication for electronic financial transaction is available
Whether law enables the use of biometric authentication as means to identify users	ELECTRONIC FINANCIAL TRANSACTIONS ACT Article 2 The term “means of access” means any of the following means or information which is used to issue a transaction request in electronic financial transactions or to secure the authenticity and accuracy of users and the details of such transaction: (d) Biological information of users;	Biometric information of users are means to identify users in electronic financial transactions
Whether law enables the use of biometric authentication as digital signature/non-repudiation	DIGITAL SIGNATURE ACT Article 3 (3) A digital signature other than a certified digital signature shall have such an effect of a signature, signature and seal, or name and seal, as is agreed between the parties concerned.	A digital signature other than a certified digital signature has an effect of a signature, signature and seal, or name and seal. In case of dispute, however, the financial institution must prove the authenticly of user’s signature and confirm the electronic document is not altered after the digital signature

4. 결 론

최근 핀테크의 활성화에 따라 혁신적인 기술과 간편함을 차별성으로 내세우는 인터넷전문은행의 출현에 따라 기존 시중 은행들은 다양한 금융 서비스 개발을 위해 신기술 도입을 서두르고 있다.

특히, 전체 금융거래의 89.7%를 비대면(인터넷/스마트폰뱅킹, 자동화기기 등)거래가 차지하고 있는 상황에서, 비대면 거래에 대한 안전성과 고객의 신뢰성을 확보하기 위한 가장 핵심적인 요소는 '신원확인'과 '부인방지' 기술이며, 본 논문에서는 FIDO로 대표되는 생체인증 기술을 금융서비스에 적용하기 위한 기술적/법률적 사항을 살펴보았다.

그러나, 앞에서도 고찰해 보았듯이 생체인증을 통한 혁신적이고 안전한 신원확인 및 부인방지 기술이 존재함에도 불구하고 법적/제도적 한계로 인해 공인전자서명의 요건에 해당하지 않는 것으로 판단된다. 따라서, 생체인증 분야의 기술적인 발전만으로는 국제적 흐름에 따른 혁신적 금융서비스의 활성화에 기여하기 어려우며, 관련 정책 및 법・제도의 제정이 반드시 병행되어야 할 것이다.

본 논문에서 제안하는 사항은 첫째, 공인인증서에 기초한 전자서명만을 공인전자서명으로 인정하고 있는 전자서명법의 개정이 이루어져야 한다. 공인전자서명에만 부여된 법적 추정력을 일정한 요건을 갖춘 비공인전자서명으로 확대하면 금융회사와 ICT 기업들이 공인인증서에 대한 절대적인 의존에서 벗어날 수 있을 것으로 판단된다. 이에 따라 생체인증 등 안전하고 편리한 인증 및 부인방지 기능을 활용한 혁신적인 금융서비스[2]가 연구/개발될 수 있을 것이다.

둘째, 새로운 신원확인 및 전자서명 서비스의 활성화를 위해서는 혁신적인 보안/인증 기술을 보유한 업체들이 인증기관으로서 서비스를 제공할 수 있어야 할 것이다. 생체인증 등의 기술을 전자서명에 활용하기 위해서는 개인의 신원을 확인하여 개인키를 부여하고, 전자서명을 위한 공개키를 누가 사용할 것인가를 확인해주는 메커니즘을 제공해 주는 인증기관(CA: Certificate Authority)[3]이 중심이 된다. 미래창조과학부에서는 2016년 전자서명법 시행령 제2조의2(공인인증기관 지정에 대한 사전심사)를 신설하여, 자신이 보유한 전자서명기술이 공인인증기관의 지정기준 요건을 모두 충족하는지 여부에 대한 사전심사를 미래창조과학부장관에게 신청할 수 있도록 하여, 생체인증기술 등 다양한 인증기술을 보유하는 공인인증기관을 지정할 수 있도록 문을 열어 놓았다. 하지만, 전자서명법 및 관련 법령상의 공인인증기관 설립 요건 문제와 공인인증 규격이 PKI 인증서 규격에 국한되어 있는 등 해결해야 하는 과제가 남아 있는 실정이다. 많은 핀테크 기업들이 새로운 비즈니스 모델로 공인인증서에 준한, 생체인증을 활용한 공인인증 서비스 기관으로 지정될 수 있도록 관련 법규가 개정되어야 하며, 중소규모의 핀테크 기업들이 공인인증기관으로 지정되기 위한 요건(자본금 50억 이상, 시설 및 장비 등)을 완화할 수 있도록 관련 규격의 정비를 위한 연구가 진행되어야 할 것이다.

끝으로, 금융회사는 핀테크의 활성화에 따른 기술발전 속도에 맞추어 안전한 금융서비스 제공을 위해 선제적 사전 위험평가예방 활동(취약점 분석・평가 강화, 정보보호 관리체

계(ISMS)구축 등)[2]를 더욱 강화해 기술 혁신 과정에서 유발되는 리스크를 합리적으로 통제하고 소비자 권익을 보호할 수 있도록 노력하길 제안해 본다.

References

[1] Cha, B. R. and Ko, F. I. S., "An OTP(One Time Password) Generation Method Using the Features of Fingerprint," The Journal of Society for e-Business Studies, Vol. 13, No. 1, pp. 33-43, 2008.

[2] Jang, S. S., "A Study on the Effect Fintech on the Information Security Industry," Internet & Security Focus, pp. 4-32, 2015.

[3] Jeong, C. H., "Electronic signature based authentication," Seoul Association For Public Administration, pp. 185-215, 2003.

[4] Jeong, W. Y., "A Comparative research on the revised electonic signature Act," Compare Justice, Vol. 10, No. 4, pp. 1-49, 2003.

[5] Kim, J. D., "The Legal Analysis on the Electronic Signature," Jungang Law Academy, Vol. 6, No. 3, pp. 353-376, 2004.

[6] Lee, H. J., "Biometrics began accelerate in the mobile security authentication means," Digieco, pp. 1-10, 2016.

[7] Lee, J. H., "The biometric authentication technology and financial transactions and its future," etnews, 2016.

[8] Park, J. G., "Understanding and Responding to Fintech services in the information security point of view," Payment and Information Technology, Vol. 61, pp. 70-100, 2015.

[9] Shim, C. S. and Chung, H. W., "A Study on the Improvement in Legal Issues for Related Electronic Signature Acts in Korea Focusing on the Legal Issues Connected with e-Signature and e-B/L," Korea Internet Electrornic Commerce Association, Vol. 10, No 2, pp. 59-75, 2010.

[10] Tsai, C. R., "Non-repudiation In Practice," Second international Workshop for Asian Public Key Infrastructure, pp. 1-2, 2002.

저 자 소 개

송재헌 (E-mail: prayer21c@korea.ac.kr)
2015년~현재 고려대학교 정보보호대학원 금융보안학과 석사과정
NH농협은행 IT본부 기획역
관심분야 생체인증, 웨어러블디바이스 보안

김인석 (E-mail: iskim11@korea.ac.kr)
2008년 고려대학교 정보경영공학과 (박사)
2009년~현재 고려대학교 정보보호대학원 교수
FDS산업포럼 회장, 한국사이버정보전학회 운영위원