ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

공인인증서 기반 인터넷 뱅킹의 구현, 보안성, 그리고 편의성 분석☆

Implementation, Security, and Usability Analysis of Accredited Certificate-based Internet Banking

박 혜 승[1] 이 재 협[1] 박 승 철[1*]
Hye-Seung Park Jae-Hyup Lee Seung-Chul Park

요 약

최근 우리나라에서 활발하게 도입되고 있는 공인인증서 기반의 오픈 뱅킹은 표준 통신 프로토콜과 웹 호환성 지원을 통해 기존 공인인증서 기반의 폐쇄형 뱅킹의 갈라파고스화 문제를 상당 부분 해소할 수 있을 것으로 기대되고 있다. 그러나 새로운 오픈 뱅킹이 기존 폐쇄형 뱅킹에 대해 제기되어온 안전성 문제와 사용자 편의성 문제를 어느 정도 해소할 지에 대해서는 의문으로 남아있다. 본 논문은 기존의 공인인증서 기반의 폐쇄형 뱅킹과 오픈 뱅킹의 구현 방식 차이를 분석하고, 오픈 뱅킹이 폐쇄형 뱅킹이 안고 있는 보안성과 편의성 문제를 어느 정도 해소하고 있는지 분석하는데 초점을 맞추고자 한다. 이 분석은 기존 폐쇄형 뱅킹이 15년 이상 서비스를 제공하는 과정에서 제기된 보안성 취약점, 보안성 강화를 위해 적용된 대응책, 대응책의 편의성에 대한 영향을 먼저 분석하고, 폐쇄형 뱅킹과 오픈 뱅킹의 구현 방식 차이를 통해 오픈 뱅킹의 보안성과 편의성을 추론하는 방식으로 진행되었다. 분석 결과 오픈 뱅킹이 여전히 안고 있는 보안성과 편의성 문제를 해소하기 위해 향후 오픈 뱅킹이 어떻게 개선되어야 하는지에 대해서도 간략하게 논의하고자 한다.

☞ 주제어 : 인터넷 뱅킹, 뱅킹 보안, NPKI 뱅킹, 오픈 뱅킹

ABSTRACT

We expect that the accredited certificate-based open banking, which is actively deployed in recent times, will solve the Galapagosization problem of the existing accredited certificate-based closed banking by supporting standard communication protocol and web compatibility. However, it is questionable how much the open banking will answer the security and usability problems of the existing closed banking. This paper is focused on analyzing the differences between the existing closed banking and the open banking, and then evaluates how much the security and usability problems of the existing closed banking are resolved by the open banking. The study firstly analyzes the security vulnerabilities raised in the process of providing closed banking services for the past 15 years or more, the countermeasures applied to enhance security, and the convenience impact of countermeasures. And then, the security and convenience of the open banking is inferred by analyzing the implementation difference between the closed banking and the open banking. The paper also briefly discusses how to improve the open banking to resolve the remaining problems of the open banking.

☞ keyword : Internet banking, banking security, NPKI banking, open banking

1. 서 론

1999년 PKI(Public Key Infrastructure) 기반의 전자서명법이 제정되면서부터 시작된 우리나라의 인터넷 뱅킹은 초기부터 인증서(certificate) 기반으로 구축되었다. 2002년 9월 금융 거래에서 사설인증서 대신 6개의 국가지정 인증기관(현재는 5개)으로 구성된 NPKI(National PKI)를 통해 발급하는 공인인증서 사용이 의무화된 이후, 인터넷 뱅킹에서 공인인증서는 절대적인 비중을 차지해 왔다 [1,2]. 2015년 3월 공인인증서 의무 사용 규정이 폐지된 이후에도 지금까지 인터넷 뱅킹은 대부분 공인인증서 기반으로 이루어지고 있다. 우리나라에서 인증서 기반의 인터넷 뱅킹이 시작된 2000년대 초반은 인증서를 포함하는 PKI 표준만 제정되어 있었을 뿐, 표준 웹 브라우저 환경에서 인증서 기반의 사용자 인증(user authentication), 128

1 School of Computer Science and Engineering, Korea University of Technology and Education, Cheonan, Chungnam-Do, 31253, Republic of Korea
* Corresponding author (scpark@koreatech.ac.kr)
[Received 10 March 2017, Reviewed 12 March 2017(R2 23 May 2017, R3 10 July 2017), Accepted 17 July 2017]
☆ 이 논문은 2017년도 한국기술교육대학교 교수 교육연구진흥과제 지원에 의하여 연구되었음.

http://dx.doi.org/10.7472/jksii.2017.18.4.69

비트 이상의 암호키를 사용하는 높은 수준의 암호화, 그리고 거래 인증(transaction authentication) 등을 지원하기가 어려운 실정이었다. 따라서 우리나라 정부기관과 은행들은 NPKI 기반의 인터넷 뱅킹 활성화를 위해 인증서 저장 및 개인키 보호 기술, 서명 및 암호화 기술, 통신 프로토콜, 그리고 관련 보안 기술들을 자체적으로 개발하여 적용하기로 하였다. 국제적 웹 표준 환경과 호환되지 않는 폐쇄형 뱅킹(closed banking)을 채택한 것이다. 폐쇄형 뱅킹 관련 기술들은 웹 환경과의 통합을 위해 그 당시 절대적인 시장 점유율을 확보하고 있던 마이크로소프트사의 인터넷 익스플로러(IE- Internet Explorer)의 웹 확장 언어인 ActiveX를 사용하여 구현되었으며, 공인인증서와 개인키는 사용자 편의를 위해 파일 시스템에 저장하고, 개인키 보호는 패스워드에 의해 생성되는 암호키로 암호화하였다[3]. 이렇게 구축된 인증서 기반의 인터넷 뱅킹은 공개키 암호 프로토콜에 근거한 강력한 보안 서비스, 개인키 소지와 패스워드 지식에 의한 2 요소의 강력한 인증 서비스, 그리고 전자서명에 의한 부인방지(non-repudiation) 서비스를 제공함으로써, 기존의 패스워드 기반의 보안 서비스와 확실하게 차별화되는 안전성을 제공하는 것으로 받아들여졌다. 이런 신뢰를 바탕으로 정부와 은행들은 공인인증서 보급을 강력하게 장려하였으며, 그 결과 2015년 말 현재 3,388만개의 공인인증서가 발급되어 인터넷 뱅킹을 포함한 다양한 인터넷 응용에 적용되고 있다[2]. 공인인증서 저장 매체는 HSM(Hardware Secure Module) 등으로 다양화되었으나 2015년 말 현재 여전히 90% 이상이 HDD와 USB 메모리를 사용하고 있다[4].

2010년대에 들어오면서 웹 서비스 환경은 인터넷 뱅킹이 시작된 2000년대 초반과는 확연하게 달라지기 시작했다. IE 외의 크롬(Chrome)과 같은 다양한 웹 브라우저 사용이 활성화되고, 표준 웹 보안 프로토콜인 SSL/TLS의 기능이 확장되어 보다 강력한 보안 서비스를 제공하며, 웹 표준 보안 API(Application Programming Interface) 개발, 그리고 HTML5와 같은 웹 확장 기능을 지원하는 표준 웹 프로그래밍 언어 등이 개발되었다. 그에 따라 최근 들어, 국제 표준과의 호환성 결여로 글로벌 기술 발전 발전과 동떨어져 갈라파고스화 되었다는 지적을 받고 있는 기존의 공인인증서 기반의 폐쇄형 뱅킹(closed banking)을, 표준 통신 프로토콜 및 웹과 호환하는 개방형 인터넷 뱅킹을 오픈 뱅킹(open banking)이라는 이름으로 구축하는 작업이 활발하게 전개되고 있다[5,6,7]. 여기서는 개방형 뱅킹 대신 언론 등에서 이미 사용해온 오픈 뱅킹 용어를 사용한다.

NPKI 오픈 뱅킹은 웹 표준 및 표준 통신 프로토콜과 호환적인 구현으로 인해 기존의 폐쇄형 뱅킹이 가지고 있던 IE 의존성, 보안 기능 확장을 위한 ActiveX 프로그램 설치, 그리고 표준 통신 프로토콜의 고급 보안 기능 활용 불가 등의 문제점을 상당 부분 해소할 수 있을 것으로 기대된다. 그러나 기존 NPKI 폐쇄형 뱅킹은 호환성 결여 문제 외에도 다양한 유형의 보안 공격에 취약성을 드러내 왔으며, 이에 대한 대응 과정에서 추가적인 인증 수단 도입 등에 따라 사용자 편의성 저하 문제가 함께 제기되어 왔다[3]. 만약 현재 전환 작업이 추진되고 있는 오픈 뱅킹이 호환성 외에 안전성과 사용자 편의성 측면에서 기존 NPKI 폐쇄형 뱅킹을 충분히 개선하지 못한다면, FIDO (Fast IDentity Online)[8]와 같이 안전성과 편의성을 강조하는 새로운 핀테크 기술들과의 경쟁에서 생존이 어려울 것이다.

본 논문은 오픈 뱅킹이 기존 공인인증서 기반의 폐쇄형 뱅킹과 어떻게 다른지를 구체적으로 비교하고, 그 결과를 바탕으로 폐쇄형 뱅킹이 가지고 있던 보안성 문제와 사용자 편의성 문제를 얼마나 해소하고 있는지를 분석하는 데에 일차적인 목적이 있다. 그리고 현재의 오픈 뱅킹이 해소하지 못한 보안성 문제와 사용자 편의성 문제를 해결하기 위한 방안에 대해서도 간략하게 논의하고자 한다. 본 연구 결과가 오픈 뱅킹이 핀테크 시대에 더욱 경쟁력 있는 인터넷 뱅킹 솔루션으로 자리 매김하는데 도움이 되기를 기대한다.

2. 관련 연구

전 세계의 대부분의 은행들은 국제 표준인 SSL/TLS 보안 채널상에서 사용자 인증서가 아닌 패스워드 또는 OTP(One Time Password) 기반의 인증을 사용하고 있다. 그러나 우리나라의 NPKI 기반의 폐쇄형 뱅킹은 SSL/TLS가 아닌 자체적인 보안 통신 프로토콜을 사용하고 있으며, 기본적으로 공인인증서를 사용자 인증 수단으로 사용하고 있다[3]. 우리나라의 NPKI 기반 인터넷 뱅킹은 SSL/TLS 기반의 해외 인터넷 뱅킹에 비해 보안성이 높은 것으로 평가되고 있다. NPKI 최상위 인증기관인 한국인터넷진흥원(KISA, Korea Internet & Security Agency)은 세계적인 결제대행 업체인 PayPal의 부정결제 사고율이 0.3%인데 비해, 우리나라 NPKI 기반 결제시스템의 부정결제 사고율은 0.0002%에 불과함을 보고하고 있다[9]. 그럼에도 불구하고 자체 통신 프로토콜 사용과 ActiveX 기반의 구현에 따른 웹 및 프로토콜 호환성 부족 문제가 여

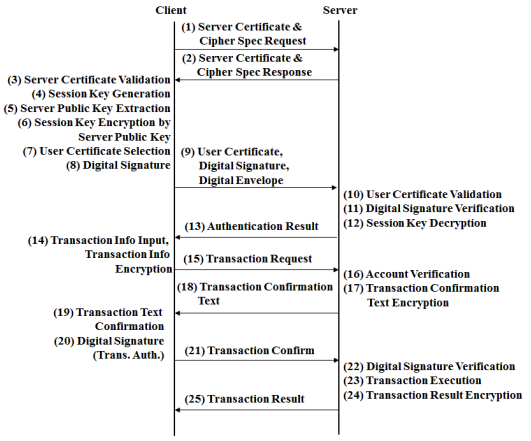
러 연구에서 지적되어 왔다[1,3]. 이런 지적에 따라 KISA는 기존 NPKI 기반의 폐쇄형 뱅킹을 표준 프로토콜인 SSL/TLS와 표준 웹 브라우저들과 호환되도록 구현하는 방법을 제시하고, 은행들의 오픈 뱅킹으로의 전환을 지원하고 있다[5]. 구체적인 구현 방법이 공개되고 있지 않지만 다른 대안에 대한 보고가 없는 점을 볼 때, 현재 대부분의 은행들이 도입하고 있는 오픈 뱅킹은 이와 같은 방식으로 구축되고 있는 것으로 믿어진다. 초창기 NPKI 공인인증서 기반의 인터넷 뱅킹이 시작될 때 패스워드와 개인키에 의한 디지털 서명의 2 요소 인증은 충분히 강력한 보안 서비스를 제공하는 것으로 믿어졌다. 그러나 현실은 여기에 보안카드 또는 OTP를 추가적으로 사용해야 하고, MITB(Man In The Browser) 공격을 방어하기 위해서는 2채널 인증을 추가로 수행해야 하는 등 불편함이 이어지고 있다[10]. 이는 NPKI 기반의 폐쇄형 뱅킹의 보안성이 기대와 달리 취약하여 보완이 필요하였음을 의미하고, 그에 따라 사용자 편의성도 함께 낮아졌음을 의미한다. 현재 도입이 추진되고 있는 NPKI 기반의 오픈 뱅킹이 이런 문제를 얼마나 해소할 수 있을 지에 대한 평가는 아직 거의 이루어지고 있지 않다. 만약 오픈 뱅킹이 충분한 안전성과 편의성을 제공하지 못한다면, FIDO 등 새로운 핀테크 기술들과 경쟁하기 위해 신속한 개선이 필요할 것이다. 이 점이 본 연구가 필요한 이유이다.

3. ActiveX에 의존적인 기존의 폐쇄형 뱅킹

3.1 동작 절차

그림 1은 기존 NPKI 공인인증서를 기반으로 하고 ActiveX로 구현된 기존 폐쇄형 뱅킹의 전형적인 거래 절차의 예를 보이고 있다[11]. 폐쇄형 인터넷 뱅킹은 서버 인증, 사용자 인증과 세션키 교환, 금융 거래 등의 순서로 이루어지는 것이 일반적이다. 만약 공인인증서 기반의 인증 서비스만 필요한 인터넷 거래의 경우 서버 인증과 사용자 인증 절차만 구현되고 나머지는 생략된다. 공인인증서 기반의 폐쇄형 뱅킹을 위한 메시지 교환 절차는 별도의 표준 프로토콜 없이 서비스 제공자의 서비스 요구에 따라 자체적으로 정의되는 프로토콜을 사용한다. 즉, 인터넷 뱅킹을 위한 별도의 표준 프로토콜을 사용하지 않고 HTTP의 웹 응용 프로그램(클라이언트, 서버)으로 개발된다.

인터넷 뱅킹은 클라이언트 응용 프로그램이 웹 브라우저를 통해 웹 서버 응용 프로그램에게 서버 인증서 및



(그림 1) 기존 폐쇄형 인터넷 뱅킹의 동작 절차
(Figure 1) Operational Procedure of Existing Closed Banking

암호 사양 요청 메시지를 전송함으로써 개시된다. 서버 응용 프로그램은 자신의 공인인증서와 자신이 지원하는 암호 사양(해시 알고리즘, 공개키 암호알고리즘, 대칭키 알고리즘 등)을 클라이언트 응용 프로그램에게 응답한다. 공인인증서 기반의 폐쇄형 뱅킹에는 SHA-1 해시 알고리즘, RSA(Ronald Rivest, Adi Shamir, and Len Adleman) 공개키 암호화 알고리즘, 그리고 자체적으로 개발된 SEED 대칭키 암호화 알고리즘이 사용되고 있다. 서버 인증서 및 암호사양 응답 메시지를 수신한 클라이언트 응용 프로그램은 서버 인증서를 검증함으로써 서버를 인증한다. 서버 인증서 검증은 인증서 유효기간 확인, 인증서에 포함된 인증기관 서명 확인, 폐기 여부 확인 절차를 포함하여 이루어진다. 서버 인증서 확인이 웹 브라우저가 아닌 클라이언트 프로그램에 의해 자체적으로 이루어진다.

서버 인증이 완료되면 클라이언트 응용 프로그램은 서버가 제안한 대칭키 암호화 알고리즘(SEED)에서 사용할 일회용 세션키(session key)를 생성한다. 그리고 세션키를 서버 인증서에 기술된 서버 공개키를 사용하여 공개키 암호화 알고리즘(RSA)으로 암호화한다. 서버의 공개키로 암호화한 세션키를 전자봉투(digital envelope)라 한다. 즉, NPKI 폐쇄형 뱅킹은 실제 데이터 암호화를 위한 세션키 교환을 전자봉투 방식으로 수행한다. 그리고 클라이언트 응용은 서버 응용 프로그램에 대해 사용자 인증을 수행하기 위해 사용자의 공인인증서를 선택하고, 패스워드로 개인키를 입수하여 교환된 메시지와 연계된

사용자 인증용 전자서명을 생성한다. 마지막으로 사용자의 공인인증서, 전자서명, 그리고 전자봉투가 서버 응용 프로그램에게 전송된다.

서버 응용 프로그램은 유효기간 확인, 인증서에 포함된 인증기관 서명 확인, 폐기 여부 확인 등을 통해 사용자 공인인증서를 검증하고 사용자의 공개키를 확보한다. 이 때 사용자의 공개키는 전자서명 검증키 역할을 수행한다. 즉, 사용자의 전자서명을 공인인증서의 공개키로 복호화함으로써 전자서명을 검증한다. 전자서명 검증이 완료되면 서버에 의한 사용자 인증이 성공적으로 완료되게 된다. 그런 다음 서버 응용 프로그램은 클라이언트 응용 프로그램과 암호화 통신에 사용할 세션키를 확보한다. 세션키는 서버의 공개키로 암호화된 전자봉투를 서버의 개인키로 복호화함으로써 확보된다. 그리고 서버 응용 프로그램은 사용자 인증 결과를 담은 메시지를 클라이언트 응용 프로그램으로 전달함으로써 인증과 키교환 절차를 완료한다.

인증과 키교환 절차가 완료되면 클라이언트 응용 프로그램은 조회 요청 메시지를 전송하여 거래 정보를 조회할 수 있고, 계좌 이체 정보를 전송하여 계좌 이체 등의 금융 거래를 요청할 수 있다. 계좌이체 금융 거래는 송금계좌, 수신계좌, 이체금액, 계좌비밀 번호 등을 입력하고, 안전한 거래를 위한 추가적인 인증 수단 선택과 선택된 수단에 따른 인증 정보를 입력함으로써 수행된다. 금융 거래는 일반적으로 거래를 요청하는 예비거래(transaction request)와, 거래내역을 확인하고 인증하는 본거래(transaction confirm)로 이루어진다. 클라이언트 응용 프로그램은 거래 요청 정보를 SEED 암호화 알고리즘으로 암호화하여 전달하되, 본거래 내역 인증은 웹 브라우저상에서 사용자의 거래내역 확인, 공인인증서의 개인키 추출, 그리고 거래내역에 대한 전자서명 생성으로 이루어진다. 본거래 내역에 대한 전자서명은 거래 인증(transaction authentication) 외에 사용자에 대한 부인방지(non-repudiation) 서비스를 추가적으로 제공한다.

3.2 시도된 공격과 적용된 대응책

NPKI 폐쇄형 인터넷 뱅킹은 다음의 2가지 특성으로 강력한 보안성이 유지되는 시스템이다. 첫 번째는 공개키 암호 통신 프로토콜이고, 두 번째는 개인키 소지와 패스워드 지식에 의한 개인키 보호라는 2요소 인증이다. 현재까지 우리나라 NPKI 폐쇄형 뱅킹에서 공개키 암호 통신 프로토콜에 대한 공격이 성공한 예는 보고된 적이 없다. 그러나 개인키 소지와 패스워드 지식의 2요소 인증 체계는 당초의 기대와 달리 많은 공격의 대상이 되어 왔으며, 다수의 피해 사례가 보고와 그에 따른 대응책 적용이 반복되어 왔다. 표 1은 그 동안 NPKI 폐쇄형 뱅킹에 대해 시도된 공격 유형과 해당 공격 방어를 위해 적용된 대응책을 요약하고 있다.

(표 1) NPKI 폐쇄형 뱅킹에 대한 공격과 대응책
(Table 1) Attacks on NPKI Closed Banking and their Countermeasures

attack types	countermeasures
offline phishing and disguised certificate issuance	additional iTAN/OTP_based authentication
malware-based password and iTAN cracking	anti-malware software installation, iTAN extension, OTP deployment, promotion of strong password usage
online phishing/pharming and disguised banking	promotion of OTP_based additional authentication, education/campaign, SMS notification
file system hacking to steal certificate/ private key/ banking info.	anti-malware software installation, promotion of OTP and HSM usage
web memory hacking to forge banking information	extension of end-to-end encryption, 2nd channel authentication

가장 먼저 시도된 공격 유형은 전화와 메일 등을 통해 보안에 취약한 사용자를 사회 공학적으로 공격하여 패스워드를 알아낸 다음(오프라인 피싱 공격), 해당 사용자를 가장하여 공인인증서를 온라인으로 재발급 받아 대출 등의 금융 거래에 사용하는 공격이다. 이 공격은 공인인증서 재발급이 개인키 보호 패스워드 입력으로 이루어지는 취약점을 이용한 공격이다. 이와 같은 온라인 공인인증서 위장 발급 공격에 대한 대책으로 온라인 공인인증서 재발급 시 패스워드 외에 보안카드(iTAN) 또는 OTP 확인을 의무화하였으며, 보안카드(또는 OTP)가 없는 사용자의 경우 대면 신원확인을 반드시 거치도록 하였다.

두 번째로 시도된 공격 유형은 키로거(key logger)와 같은 악성 소프트웨어를 사용하여 사용자가 입력하는 개인키 보호 패스워드와 보안카드 번호를 탈취하는 공격이다. 이 공격은 패스워드 기반의 개인키 보호 취약성과 작은 경우의 수의 보안카드 취약성을 이용하였다. 공격자는 획득한 피해자의 패스워드와 보안카드 번호를 사용하

여 공인인증서를 재발급 받고, 공인인증서와 보안카드를 대출 등의 금융 거래에 사용하는 공격이다. 이 공격에 대한 대응책으로 키보드 보안 소프트웨어 등 악성 소프트웨어 방어 도구들이 대폭 강화되었고, 당시 35개 내외의 보안카드 번호를 1000개 이상으로 대폭 확대하여 보안카드 번호 탈취를 어렵게 하였다. 그리고 보안카드 대신 OTP(One Time Password) 사용을 장려하여 보안카드 번호 유출 가능성에 대비하고, 강한 패스워드 사용으로 패스워드 크래킹 공격에 대비할 수 있게 조치하였다.

NPKI 폐쇄형 뱅킹에 대해 세 번째로 시도된 공격 유형은 온라인 피싱 및 파밍(online phishing and pharming) 공격이다. 보안에 취약한 사용자를 은행 사이트와 유사하게 위조된 사이트로 접속을 유도한 후, 보안상의 이유 등으로 사용자로 하여금 패스워드, 전체 보안카드 번호, 금융 계좌 번호 등을 입력하게 하고, 이 정보를 사용하여 공격자의 계좌로 계좌 이체를 함으로써 해당 사용자에게 금전적 피해를 입히는 공격이다. 이 공격은 NPKI 폐쇄형 뱅킹 소프트웨어가 위조 사이트를 구분하여 사용자에게 확실하게 경고하지 못하는 취약점과, 사용자가 경고 메시지를 무시하는 경향을 이용한다. 이 공격에 대한 대응책으로 보안카드 대신 위조 사이트에 노출이 될 수 없는 OTP 사용을 장려하고 있으며, 사용자를 대상으로 전체 보안카드를 입력하지 않도록 교육과 캠페인을 강화하였다. 그리고 금융 거래 후 내역을 SMS로 통보하여 확인할 수 있게 한다.

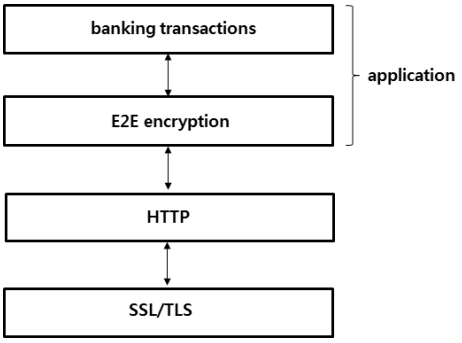
네 번째의 공격 유형은 파일 시스템을 해킹하여 공인인증서, 개인키, 파일에 기록된 패스워드, 사진으로 저장된 보안카드 등을 탈취하는 공격이다. 공격자는 탈취한 정보를 대출 등 금융 거래에 사용하여 해당 사용자에게 피해를 입힌다. 이 공격은 대부분의 사용자가 공인인증서와 개인키를 파일 시스템에 저장하는 점과, 보안에 취약한 사용자가 민감한 정보(패스워드, 보안카드 등)를 편의상 파일 시스템에 보관하는 취약점을 이용한다. 이 공격에 대한 대응책으로 악성 소프트웨어 방지 도구의 사용을 강화하고, 악성 소프트웨어에 의한 복제 공격이 불가능한 HSM(Hardware Security Module)에 공인인증서와 개인키 보관을 장려하고 있으며, 보안카드 대신 통째로 노출이 불가능한 OTP 사용을 장려하고 있다.

마지막 공격 유형은 브라우저의 응용으로 동작하는 클라이언트의 메모리상의 정보(계정, 금액 등)를 악성 소프트웨어를 사용하여 변경하는 공격이다. 이 공격은 2013년 말에 처음 시도되었고, OTP를 사용하더라도 방어할 수 없도록 매우 지능적으로 이루어졌다[10]. 공격자는 사용자를 대기 상태로 만든 다음 몰래 수신 계좌 번호를 공격자 계좌로 변경하고, 이체 금액을 변경함으로써 사용자에게 금전적 피해를 준다. 사용자가 보는 화면은 정상인 것처럼 조작됨으로써 사용자는 거래 내역 변경 사실을 알아채지 못한다. 거래 서명 단계에서도 화면에 보이는 내용이 아닌 웹 메모리의 변경된 내용에 대해 서명하므로 사용자는 조작 사실을 인지할 수 없다. 이 공격은 암호화되기 전의 웹 메모리상의 거래 정보가 공격자에게 노출될 수 있는 취약점과, 웹 메모리상에서 거래 서명이 이루어지는 취약점을 이용한다. 이 공격에 대한 대응책으로 키보드에서 입력된 거래 정보를 즉시 암호화하고, 암호화된 정보를 웹 메모리에서 거래 서명이 이루어진 정보와 함께 전송한 후 서버가 비교할 수 있게 하는 종단간 확장 암호화(end-to-end encryption extension) 기능을 구현하였다. 또한 거래 과정에서 수신 계좌 등이 변경될 때 2채널 인증을 통해 재확인하는 방법을 도입하였다[10].

4. 웹 표준을 준수하는 새로운 오픈 뱅킹

4.1 프로토콜 구조

갈라파고스화된 기존의 NPKI 공인인증서 기반의 폐쇄형 뱅킹을 표준 보안 통신 프로토콜 및 웹과 호환되도록 개선한 오픈 뱅킹은 그림 2와 같은 프로토콜 구조를 가진다[5]. 자체적인 보안 통신 프로토콜을 채택한 폐쇄형 뱅킹과 달리, 오픈 뱅킹은 웹 보안 통신을 위한 표준 프로토콜인 SSL/TLS를 사용한다. SSL/TLS는 기본적으로 웹 브라우저와 웹 서버 간에 교환되는 HTTP 메시지의 안전한 교환을 위해 보안 채널을 제공한다. 그러나 오픈 뱅킹은 응용과 SSL/TLS 프로토콜 사이 구간에서 이루어

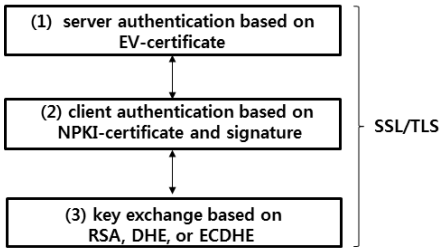


(그림 2) NPKI 오픈 뱅킹의 프로토콜 구조
(Figure 2) Protocol Architecture of NPKI Open Banking

질 수 있는 악성 소프트웨어에 의한 메모리 조작 공격(MITB 공격)을 최대한 방어하기 위해, 종단간(E2E, end-to-end) 암호화 기능을 추가적으로 구현하도록 권고되고 있다[5]. 결과적으로 오픈 뱅킹 응용은 2중의 보안 채널을 사용하게 된다.

4.2 동작 절차

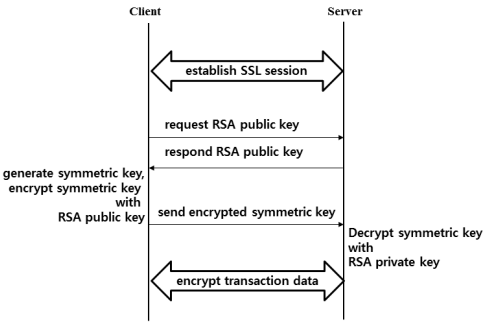
그림 3은 오픈 뱅킹의 SSL/TLS 활용 방법을 보이고 있다.



(그림 3) NPKI 오픈 뱅킹의 SSL/TLS 활용
(Figure 3) SSL/TLS Utilization by NPKI Open Banking

기존 폐쇄형 뱅킹이 자체적인 응용에 의해 서버 인증이 이루어지는데 비해, 오픈 뱅킹은 표준 웹 브라우저가 SSL/TLS의 서버 인증 기능을 사용하여 서버 인증을 수행한다. 서버 인증서는 EV(Extended Validation) 인증서[12]를 사용하고, 표준 웹 브라우저의 사용자 인터페이스를 통해 피싱 또는 파밍 사이트와 구별을 보다 용이하게 한다. 즉, 정상적인 EV 인증서로 인증된 서버는 웹 브라우저가 주소창을 초록색으로 표시한다. 오픈 뱅킹의 사용자 인증은 SSL/TLS의 클라이언트 인증 기능을 활용하여 수행되고, 사용자의 NPKI 인증서와 서명을 확인함으로써 인증이 이루어진다. 따라서 NPKI 인증서와 개인키가 웹 브라우저가 접근 가능한 웹 저장소에 저장되고, 개인키 보호는 폐쇄형과 동일하게 패스워드를 사용한다. NPKI 폐쇄형 뱅킹이 암호키 교환을 위해 RSA를 사용하는데 반해, 오픈 뱅킹은 SSL/TLS가 지원하는 RSA, DHE (Ephemeral Diffie-Hellman), ECDHE(Elliptic Curve DHE) 등에서 선택하여 키를 교환할 수 있다.

MITB 공격 방어를 위한 오픈 뱅킹의 응용 레벨의 종단간 암호화 절차는 그림 4와 같이 권고되고 있다[5]. 종단간 암호화를 위한 암호키 교환은 NPKI 폐쇄형 뱅킹과 같이 RSA 방식을 채택하고 있다. 먼저 클라이언트 응용은 인증서 다운로드를 통해 서버의 공개키를 획득한다.



(그림 4) NPKI 오픈 뱅킹 응용의 종단간 암호화 절차
(Figure 4) End-to-End Encryption Procedure of NPKI Open Banking Application

그런 다음 클라이언트는 암호키(symmetric key)를 생성하고, 서버의 공개키로 암호키를 공개키 암호화 방식으로 암호화하여 서버에게 전달한다.

5. 분석과 제언

5.1 구현 방식 분석

오픈 뱅킹은 기존 NPKI 폐쇄형 뱅킹의 갈라파고스화 문제를 해결하기 위해 철저하게 표준과의 호환성에 유지에 초점을 맞춰 개발되었다. 표 2는 오픈 뱅킹의 구현 방식을 기존의 폐쇄형 뱅킹과 비교하여 보여주고 있다. 오픈 뱅킹은 보안 통신 프로토콜을 SS/TLS를 채택함으로써 표준 웹의 보안 통신 기능을 사용하고 있다. 그리고 응용 구현을 위해 ActiveX를 배제하고 표준 언어인 HTML5와 Java Script를 사용함으로써 다양한 브라우저와의 호환성을 보장한다. 서버 인증은 응용이 아닌 SSL/TLS의 서버 인증 기능을 활용하고, NPKI 공인인증서 대신 SSL/TLS용 EV 인증서를 사용함으로써 표준 웹 브라우저의 서버 인증 표시 인터페이스를 사용한다.

NPKI 폐쇄형 뱅킹이 인증서와 개인키를 주로 파일시스템에 저장하는데 비해, 오픈 뱅킹은 브라우저의 접근이 용이한 웹 저장소(web store)에 저장한다. 패스워드에 의한 개인키 보호 방법은 폐쇄형 뱅킹과 동일하다. 오픈 뱅킹의 사용자 인증 방법은 NPKI 공인 인증서와 서명을 확인하는 폐쇄형 뱅킹과 동일하고, 서명 생성 역시 동일하게 웹 응용에서 이루어진다. 이는 거래 내용에 대해 서명하는 거래 서명(transaction signature)의 경우도 마찬가지이다.

(표 2) NPKI 폐쇄형 뱅킹과 오픈 뱅킹의 구현 방식 비교
(Table 2) Implementation Comparison of NPKI Closed Banking and Open Banking

items	closed banking	open banking
security communication protocol	proprietary	SSL/TLS
language	activeX	HTML5, JavaScript
server certification	application	browser
server certificate	NPKI certificate	EV certificate
storage for certificate and private key	file system	web store
private key protection	password	password
user authentication	NPKI certificate & signature	NPKI certificate & signature
signature generation	web application	web application

5.2 보안성 비교 분석

본 연구에서 오픈 뱅킹의 보안성 분석은 기존 NPKI 폐쇄형 뱅킹의 보안성 평가와, 폐쇄형 뱅킹 대비 오픈 뱅킹의 보안성 개선 정도 비교를 통해 이루어졌다. 표 3은 3.2절에서 정리한 사이버 공격 유형에 대한 NPKI 폐쇄형 뱅킹과 오픈 뱅킹의 보안성을 요약하여 보이고 있다. 결론부터 기술하면, 기존의 NPKI 폐쇄형 뱅킹에 대한 공격을 방어하기 위해 다양한 대응책들이 적용되었지만 여전히 각 유형의 공격으로부터 자유롭지 못한 상태에 있고, 새로운 오픈 뱅킹은 일부 공격 유형에 대해 부분적으로 보안성을 개선하는 정도에 그치고 있다.

오프라인 피싱 공격은 기존 폐쇄형 뱅킹에서 NPKI 공인인증서의 위장 발급을 목적으로 처음 시도되었지만, 보안카드와 SMS 등으로 추가적인 인증이 보완된 지금도 여전히 유효한 공격이다. 전화와 이메일 등으로 피해자를 속여 패스워드와 보안카드 등을 피싱하여 공인인증서를 온라인으로 위장 발급받을 수 있는 여지가 여전히 존재하는 것이다.

오픈 뱅킹도 NPKI 공인인증서 기반의 사용자 인증에 기초하고 있고, 공인인증서 발급 과정에 대한 특별한 개선을 포함하고 있지 않으므로 오프라인 피싱 공격에 대해 동일한 취약점을 안고 있다. 키로거(key logger) 등의 악성 소프트웨어에 의한 패스워드와 보안카드 크래킹(cracking) 공격은 키보드 보안 강화와 보안카드 번호 확장 등을 통해 상당 부분 개선이 되었다. 그러나 키보드 보안이 키보드 입력을 완벽하게 보호할 수 없고, 해킹 기술의 발전에 따라 많은 수의 보안카드 번호도 유출될 수 있다. 따라서 기존 NPKI 폐쇄형 뱅킹은 여전히 이 유형의 공격에 취약성을 안고 있으며, 동일한 사용자 입력 인터페이스와 보안 정책을 사용하는 오픈 뱅킹도 동일한 취약점을 안고 있다. 오픈 뱅킹의 경우 사용자 편의성 개선을 위해 키보드 보안 소프트웨어 설치 의무화를 완화하는 추세이므로, 이 유형의 공격에 오히려 더 취약할 수도 있다.

(표 3) NPKI 폐쇄형 뱅킹과 오픈 뱅킹의 보안성 비교
(Table 3) Security Comparison of NPKI Closed Banking and Open Banking
(◑ : vulnerable, ◕ : improved but still vulnerable)

security vulnerability	closed banking	open banking
offline phishing	◑	◑
password and iTAN cracking	◑	◑
online phishing/pharming	◑	◕
certificate/private key hacking	◑	◕
web memory hacking	◑	◑

온라인 피싱/파밍 공격은 기존의 NPKI 폐쇄형 뱅킹에서 지금까지 가장 활발하게 시도되어온 공격이다. 오픈 뱅킹은 온라인 피싱/파밍 공격을 방어하기 위해 SSL/TLS와 연계된 EV 인증서를 사용하고, 자체적인 응용이 아닌 표준 웹 브라우저의 사용자 인터페이스를 통해 서버 인증 결과를 표시할 수 있게 한다. 따라서 서버가 보다 정확하게 검증된 인증서를 사용하게 하고, 표준 웹 인터페이스에 익숙한 사용자들이 위조 사이트 구별을 좀 더 쉽게 할 수 있게 함으로써, 오픈 뱅킹의 피싱/파밍 공격에 대한 보안성이 상대적으로 개선될 것으로 판단된다. 그러나 공격자가 위조 사이트에 대해 EV 인증서를 발급받을 수 있고, 인증 사이트 표시를 위한 브라우저의 표준 인터페이스가 사용자들의 완벽한 위조 사이트 구분을 보장할 수는 없기 때문에, 오픈 뱅킹이 피싱/파밍 공격으로부터 완전히 자유롭기는 어려울 것으로 보인다.

기존 NPKI 폐쇄형 뱅킹은 기본적으로 공인인증서와 개인키를 파일시스템에 저장하고 사용해 왔다. 따라서 악성 소프트웨어 공격을 통해 비교적 쉽게 공인인증서와 개인키 해킹이 이루어져 왔고, 이런 공격은 현재까지도 여전히 성행하고 있다. 이 공격이 패스워드 크래킹 공격과 결합될 경우 인터넷 뱅킹에 실질적인 피해를 입히는 공격으로 발전할 수 있다. 오픈 뱅킹은 공인인증서와 개

인키를 파일시스템 대신 상대적으로 안전한 웹 저장소(web store)에 저장한다. 그러나 역호환성(backward compatibility) 보장을 위해 기존 파일시스템 저장을 여전히 지원하고 있고, 웹 저장소도 해킹으로부터 완전히 자유롭지 않으므로, 이 공격에 대한 오픈 뱅킹의 보안성이 개선되기는 하겠지만 여전히 취약성이 남아있다.

메모리 해킹 공격은 웹 메모리상의 내용을 조작하기 때문에 방어하기가 매우 어려운 공격이다. 확장된 암호화 기능 적용과 2채널 인증 등의 대응책으로 2014년 이후 이 공격에 의한 피해 사례가 보고되고 있지 않다. 그러나 확장된 암호 모듈에 의해 암호화되기 전에 금융 정보가 공격자에 노출될 가능성이 여전히 존재한다. 이 공격에 대한 방어를 위해 오픈 뱅킹은 SSL/TLS의 보안 채널 사용 외에 응용 단계에서 종단간 암호화 기능을 추가로 구현하고 있다. 그러나 폐쇄형 뱅킹의 경우와 마찬가지로 종단간 암호화 기능이 금융 정보의 노출을 완전히 차단할 수 없기 때문에, 오픈 뱅킹 역시 메모리 해킹 공격에 여전히 취약성을 안고 있음을 알 수 있다.

5.3 편의성 분석

표 4는 편의성 측면에서 NPKI 폐쇄형 뱅킹과 오픈 뱅킹을 비교하고 있다. 편의성 측면에서 오픈 뱅킹의 가장 큰 장점은 웹 브라우저 확장을 위한 ActiveX 플러그인 소프트웨어 설치가 불필요하다는 것이다. 이는 폐쇄형 뱅킹과 달리 오픈 뱅킹은 표준 웹 브라우저와 호환되게 구현되기 때문이다. 오픈 뱅킹의 SSL/TLS EV 인증서를 통한 서버 사이트 인증과 웹 브라우저 주소창 색깔을 통한 인증 결과 표시 인터페이스는 피싱/파밍 사이트 구분을 상대적으로 용이하게 할 것으로 판단된다. 그러나 오픈 뱅킹에서도 패스워드 기반의 개인키 보호 정책을 기본으로 채택하고 있기 때문에, 기존의 NPKI 폐쇄형 뱅킹의 편의성 문제의 핵심인 개인키 보호 패스워드 관리의 불편함 문제는 오픈 뱅킹에서도 여전히 안고 가야할 문제로 남는다.

앞의 표 3에서 보는 것처럼 오픈 뱅킹이 기존 NPKI 폐쇄형 뱅킹의 보안성을 크게 개선하고 있지 못하고 있다. 따라서 NPKI 인증의 취약점을 보완하기 위해 도입된 보안 카드, OTP, 2채널 인증 등은 여전히 오픈 뱅킹에서도 유지될 수밖에 없고, 그에 따른 편의성 문제도 여전히 숙제로 남게 될 것이다. 또한, 오픈 뱅킹 역시 NPKI 공인인증서 기반으로 구축되므로 공인인증서 관리 불편함도 여전히 남는 문제이다.

(표 4) NPKI 폐쇄형 뱅킹과 오픈 뱅킹의 편의성 비교
(Table 4) Usability Comparison of NPKI Closed Banking and Open Banking
(◑ : inconvenient, ◕ : improved but still inconvenient, ● : fully improved)

usability	closed banking	open banking
plug-in software installation	◑	●
distinguishing phishing/pharming site	◑	◕
password management	◑	◑
additional authentication	◑	◑
certificate management	◑	◑

5.4 오픈 뱅킹의 보안성과 편의성 개선을 위한 제언

오픈 뱅킹의 안전성과 편의성 문제의 근원과 이를 개선하기 위해 본 논문이 제언하는 내용을 요약하면 표 5와 같다. 만약 개인키와 패스워드 해킹 가능성이 없다면 패스워드 등 민감 정보 수집에 초점을 맞춘 온/오프라인 피싱/파밍 공격이 원천적으로 불가능하다. 또한 악성 소프트웨어에 의한 해킹 공격도 걱정할 필요가 없을 것이다. 따라서 피싱/파밍 사이트 구별의 불편함이 사라지고, 개인키와 패스워드 노출에 대비하여 도입된 보안카드와 OTP 등의 추가적인 인증의 불편함도 사라지게 될 것이다. 그러나 메모리 해킹 공격은 개인키와 패스워드와 무관하게 수행될 수 있으므로 개인키와 패스워드 해킹에 대한 대책과 별도의 대책이 필요함을 알 수 있다. 메모리 해킹 공격은 서명 내용에 대한 조작이 불가능하게 만드는 것이 근본적인 대책이 된다.

공인인증서의 주기적인 갱신에 따른 불편함은 개인키 유출 위험성이 낮아지면 자연스럽게 갱신 주기를 널려서 해결할 수 있다. FIDO는 개인키를 해킹이 불가능한 신뢰 플랫폼(trusted platform)인 인증 장치(authenticator device)

(표 5) 오픈 뱅킹의 취약요소와 개선방향
(Table 5) Vulnerabilities of Open Banking and Future Improvement

vulnerabilities	future improvement
hacking possibility of private key and password	① store private key within trust platform ② biometrics-based private key protection
signature creation on web browser where signature content can be falsified	③ utilize trust platform of smartphone as security token

에 저장하고, 개인키 보호를 패스워드 대신 지문 또는 홍채 등과 같이 해킹이 매우 어렵고 관리는 매우 편리한 생체 인증(biometrics)으로 보호한다. FIDO는 기본적으로 서명 생성도 인증 장치에서 이루어지도록 함으로써 서명 내용에 대한 조작을 불가능하게 하고 있다[8].

오픈 뱅킹이 FIDO 등과 같은 새로운 핀테크 기술과 경쟁하기 위해서는 유사한 수준의 보안성과 편의성을 제공할 수 있어야 할 것이다. 공인인증서와 개인키를 HSM, USIM등 해킹 염려가 없는 신뢰 플랫폼에 저장하고, 생체 인증을 통해 개인키를 보호하는 기술은 다양하게 개발되고 있다[5]. HSM은 별도로 하드웨어를 소지해야 하는 불편함과 서명 내용을 출력하기 위한 디스플레이 탑재가 어려운 점 등의 이유로 대안이 되기 어려울 것으로 판단된다. 그러나 대부분의 사용자가 보유하고 있고, USIM 등 신뢰 플랫폼을 지원하고 있으며, 지문 인식, 홍채 인식 등 생체 인증 인터페이스 활용이 가능한 스마트폰은 오픈 뱅킹을 위한 인증서 및 개인키 저장, 보호, 그리고 서명 생성 장치로 충분히 활용 가능할 것이다. 무엇보다도 스마트폰의 USIM 등에서 서명이 생성되면, 사용자가 스마트폰 화면을 통해 서명 내용을 쉽게 확인할 수 있으면서도 서명 내용 조작 방지가 가능한 장점이 있다. 이 경우 개인키 소지와 생체 인증을 통한 개인키 보호 외의 추가적인 인증이 불필요하게 되어 오픈 뱅킹의 편의성 문제를 함께 해결할 수 있다.

6. 결 론

현재 활발하게 도입되고 있는 NPKI 오픈 뱅킹은 기존 NPKI 폐쇄형 뱅킹의 IE에 대한 의존성, ActiveX 프로그램 설치 등과 같이 호환성 결여로 인한 사용자 편의성 문제를 해결하고 있는 것으로 판단된다. 그러나 기존 NPKI 폐쇄형 뱅킹이 안고 있던 개인키와 패스워드 유출 위험성과 웹 메모리 해킹 공격의 위험성에는 오픈 뱅킹도 여전히 노출되어 있음을 알 수 있었다. 따라서 오픈 뱅킹 사용자는 개인키 소지와 패스워드 지식 외에 보안카드 또는 OTP를 추가 인증 수단으로 사용해야 하는 불편함을 여전히 감수해야 하고, 그러고도 웹 메모리 해킹 공격 등 지능화된 해킹 공격으로부터는 자유롭지 못한 상황에 있음을 알 수 있었다. FIDO와 같은 새로운 핀테크 기반의 뱅킹 솔루션들은 생체 인증과 공개키 암호 프로토콜 결합 등을 통해 높은 보안성과 편의성을 동시에 제공하고 있다. 따라서 오픈 뱅킹이 새로운 핀테크 솔루션들과의 경쟁에서 생존하기 위해서는 가까운 장래에 보안성과 편의성을 획기적으로 높일 필요가 있다. 충분한 처리 능력과 안전성을 지원하는 USIM 등을 갖추고 있고, 지문인식, 홍채인식 등 생체 인증 기능을 지원하며, 표준 웹 브라우저와의 통합 수단을 제공하고, 대부분의 사용자들이 소지하고 있는 스마트폰을 NPKI 인증서와 개인키의 저장 및 보호, 서명 내역 확인, 그리고 서명 생성을 위한 신뢰 플랫폼으로 활용하는 방안을 적극 고려할 필요가 있다.

참고문헌(Reference)

[1] J. H. Lee, "Usability and Problems of Accredited Certificate in Smart Environments," *Internet & Security Focus*, March 2013, pp. 23-53 http://www.kisa.or.kr/uploadfile/201306/201306121702079155.pdf

[2] National Information Agency, and et. al, "2016 National Information Security White Paper," *White Paper,* p. 345, April 2016. http://isis.kisa.or.kr/ebook/download_pdf/2016.pdf

[3] H. S. Kim, J. Mun, J. H. Huh, and R. Anderson, "On the Security of Internet Banking in South Korea," *Oxford Univ. Computing Laboratory Research Report(CS-RR-10-01)*, p. 19, Oct 2010. https://www.cs.ox.ac.uk/files/2916/RR-10-01.pdf

[4] Korea Internet & Security Agency, "Research on the Actual Condition of Electronic Signature System Usage," *KISA Research Report (KISA-WP-2015-0032)*, p. 122, Dec. 2015. https://www.kisa.or.kr/public/library/report_View.jsp?regno=022108

[5] Ministry of Science, ICT and Future Planning and Korea Internet & Security Agency, "Technology Guideline for Improving Internet Usability Environment," *MSIFP and KISA Special Publication*, p. 259, Sept. 2014. https://www.kisa.or.kr/notice/press_View.jsp?mode=view&p_No=8&b_No=8&d_No=1302

[6] H. S. Yeom, “Banks, Enforce Internet Banking without Active X”, *Daehan Finance News*, Nov. 2015. http://www.kbanker.co.kr/news/articleView.html?idxno=57708

[7] S. I. Lee, “Open Banking Service of Banks, Enforce Integration into Main Page”, *Digital Daily,* March. 2017.
http://www.ddaily.co.kr/news/article.html?no=154198

[8] FIDO Alliance, "Specifications Overview," https://fidoalliance.org

[9] KISA RootCA, “Secure and User-friendly Accredited Certificate,” http://www.rootca.or.kr/

[10] Financial Services Commission, “Memory Hacking Related Press Release,” *FSC Press Release*, Jan. 2014.
https://www.fsc.go.kr/downManager?bbsid=BBS0030&no=88525

[11] Financial Security Agency, “A Management Guide for Financial Part Encryption Technologies,” *FSA Special Publication*, p. 105, Jan. 2010.
cfile1.uf.tistory.com/attach/2677683B5407CCEF088377

[12] CA/Browser Forum, “Guidelines for the Issuance and Management of Extended Validation Certificates Version 1.5.5,” *CA/Browser*, p. 44, March. 2015.
https://cabforum.org/wp-content/uploads/EV-SSL-Certificate-Guidelines-Version-1.4.6.pdf

◐ 저 자 소 개 ◑

박 혜 승
2012년 한양대학교 컴퓨터공학과 졸업(학사)
2014년 한양대학교 전자컴퓨터통신공학과 졸업(석사)
2016~현재 한국기술교육대학교 컴퓨터공학과 박사과정 재학 중
관심분야 : 플래시 메모리, 운영체제, 네트워크 보안, 핀테크 보안
E-mail : hs2000park@koreatech.ac.kr

이 재 협
1984년 홍익대학교 화학공학과 졸업(학사)
1987년 일리노이공대 전산학과 졸업(석사)
1992년 일리노이공대 전산학과 졸업(박사)
1993～현재 한국기술교육대학교 컴퓨터공학부 교수
관심분야 : 컴퓨터 그래픽스, 가상현실, 컴퓨터 네트워크
E-mail : jae@koreatech.ac.kr

박 승 철
1985년 서울대학교 계산통계학과 졸업(학사)
1987년 KAIST 전산학과 졸업(석사)
1996년 서울대학교 대학원 컴퓨터공학과 졸업(박사)
2004년～현재 한국기술교육대학교 컴퓨터공학부 교수
관심분야 : 컴퓨터 네트워크. 네트워크 보안, 멀티미디어 네트워크. 핀테크 보안
E-mail : scpark@koreatech.ac.kr