정 보 보 호 학 회 지
제 30 권 제3호, 2020. 6

국내 인증 기술 및 서비스 현황

강 효 관*

요 약

사용자를 온라인에서 확인하는 인증 기술은 최근 코로나 19로 인한 비대면 서비스들의 확산으로 더욱 중요해졌다. 이러한 인증 기술로는 인터넷/모바일 뱅킹, 전자 정부 등에 널리 사용되고 있는 공인인증서부터 카카오 뱅크 등의 사설인증, 블록체인을 이용한 분산ID 기술, 사용자 편의성을 강조한 간편 인증 등으로 진화하고 있다. 본 기고에서는 여러 가지 형태의 인증 방식에 대한 특징과 동향을 살펴보고 이를 통한 발전 방향을 살펴보고자 한다.

Ⅰ. 서 론

사용자를 인증하는 것은 서로를 신뢰하기 위한 방안으로 이를 위해 오프라인에서 신분증을 확인하는 절차와 같은 방식에서부터, 여러 가지 기술을 사용하여 온라인에서 사용자를 확인하는 방식들이 있다. 서로 대면이 힘든 온라인의 경우 이러한 상호 신뢰를 형성하기 위해서 오프라인에 비해 기술적인 방안이 더욱 중요하다. 온라인으로 사용자를 인증하는 방법으로는 전자서명법에서 시작된 은행, 전자정부 등 사용자 인증이 필요한 거의 모든 분야에 사용되고 있는 공인인증서가 가장 대표적이다.

최근에는 기존 공인인증서의 여러 가지 불편함이나 문제점을 해결한 사설 인증, 간편 인증 등의 서비스가 출시되고 있다. 또한 블록체인, 생체인증 등 새로운 기술을 이용한 인증 방식이 개발 및 표준화 되고 있으며, 실제 사용가능한 제품으로 출시되고 있다. 본 기고에서는 여러 가지 형태의 인증 방식에 대한 특징과 동향을 살펴보고 이를 통한 발전 방향을 살펴보고자 한다.

Ⅱ. 기존 인증 방식

국내에서 사용 중인 기존의 인증 방식으로 대표적인 공인인증서는 1999년 전자서명법으로부터 시작되어 국내 인터넷/모바일 뱅킹, 전자 정부 등 본인인증과 전자서명이 필요한 대다수의 서비스에서 사용되고 있다. 하지만, 인증서 유출, Active-X 와 같은 보안 문제, 특정 플랫폼 지원 문제, 사용자 편의성 등에 대한 이슈가 지속적으로 제기되어 왔으며, 이에 대한 대응책으로 보안토큰, Non-ActiveX 지원 방식, 브라우저 인증서 등 여러 가지 개선 방안을 제시해왔다. 하지만, 2014년 일명 천송이 코트 회의로 알려진 “규제개혁 장관 회의”에서 공인인증서와 Active-X에 대한 대통령의 지적 이후, 이를 폐지하겠다는 대통령의 공약을 발표되었다. 이후 2015년 공인인증서 의무사용 조항 삭제와 2020년 공인인증서의 독점적 지위를 폐지하는 전자서명법 개정이 완료되었다[1].

본인 확인을 위한 다른 방법으로는 본인확인으로 지정된 이동통신사, 아이핀 서비스 업체, 신용카드사가 제공하는 방식이 있다.

2.1. 공인인증서

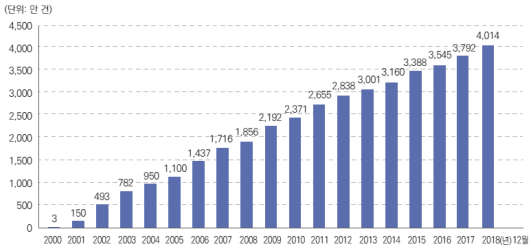
대표적인 인증방식인 공인인증서의 발전과 여러 가지 이슈에 대한 대응을 살펴보고, 의무사용 폐지로 대표되는 공인인증서 폐지 여론 이후 시장 동향 등에 대해서 살펴본다.

2.1.1. 공인인증서 도입과 확산

공인인증서는 온라인 거래에서 안전성과 신뢰성을 확보하기 위해 1999년 전자서명법을 제정·시행하면서 시작되었다. 이후 2000년 공인인증기관을 지정하고, 공

* ㈜에티소프트 (부사장, river88@gmail.com)

인인증서 활성화를 위해 금융 분야(2002년 인터넷 뱅킹, 2003년 증권거래, 2005년 카드를 포함한 30만 원 이상 전자상거래)에 공인인증서 사용을 의무화 하였다. 이러한 활성화 방안을 통해 공인인증서는 2005년 천백만 건으로 처음으로 천만 건 이상 발급이 진행되었으며, 이후 2018년 12월 4천만 건 이상이 발급[2]되며, 인터넷 뱅킹, 증권거래, 전자민원, 인터넷 쇼핑, 주택 청약, 연말정산, 전자세금계산서, 나라장터 전자입찰 등 본인인증이 필요한 거의 모든 서비스에 도입되어 신원 확인 및 전자서명 수단으로 이용되고 있다.



〔그림 1〕 연도별 공인인증서 이용자 수 변화 (누적)

2.1.2. 공인인증서 관련 주요 이슈와 대응

공인인증서는 사용자 개인키 및 패스워드 유출, Active-X로 대표되는 다양한 플랫폼 지원이 대표적인 이슈[1]이다.

공인인증서 최초 도입 시기에 확산을 위해서 인증서와 개인키를 하드디스크의 특정 폴더에 저장하는 정책을 도입했다. 이를 통해 2005년 천만 건 이상 발급을 하는 정책적 성공을 거두었지만, PKI에서 가장 중요한 개인키 보관에 관해 안전보다는 확산에 중점을 두었기에 개인키가 유출되는 사고가 발생하였다. 이에 대응하기 위해서 개인키를 안전한 하드웨어에 저장하는 보안토큰 사용을 의무화를 위해 2015년 전자서명법 시행규칙 개정을 진행하였으나[3] 개정이 이루어지지 못했다.

공인인증서는 도입 시기에 별도의 프로그램이 아닌 웹브라우저에서 서비스를 제공하기 위해 마이크로소프트사의 IE(Internet Explorer)에서 동작하는 Active-X와 Netscape에서 동작하는 Plug-in을 사용했다. 이후 IE의 압도적인 시장 점유율로 인해 전자정부, 인터넷 뱅킹 등이 Active-X로만 서비스가 되고 2006년 오픈웹[2]에서 웹표준 준수 및 다양한 플랫폼 지원을 요청하게 되었다. 해당 요구 사항에 대응하기 위해 2006년 이후 공인인증서비스는 최소 OS 3종 (windows, mac, linux)와 브라우저 5종 (IE, Chrome, Firefox, safari, opera) 이상을 지원하는 것이 기본이 되었다.

2.1.3. 공인인증서 의무화 폐지 이후 환경 변화

여러 가지 보안 문제, 시장의 요구사항에 대응하였음에도 불구하고, 공인인증서는 브라우저와의 연동기술인 Active-X와 동일한 것으로 인식되고, 규제 개혁의 대상이 되어 2014년 규제개혁 장관 회의에서 해외 소비자가 불편 없이 국내 온라인 쇼핑몰을 사용하도록 하라는 지시 이후, 2005년 의무화 되었던 30만원 이상 전자상거래 시 공인인증서 사용이 폐지되었고, 2015년 전자금융감독규정에서 인터넷뱅킹 공인인증서 의무 사용이 폐지되었다.

공인인증서는 발급 건수가 2018년 4천만 건이 넘었으며, 여전히 생활에 밀접한 많은 서비스에서 이용되고 있다. 2014년 웹 표준 방식을 활용한 공인인증서 이용 기술 개발, 2016년 간편 공인인증서 기술 등 의 방안을 제시하고 있으며, 이를 통해 사용하고 있는 서비스의 불편을 해소하기 위한 노력을 진행하고 있다.

하지만, 의무사용 폐지 후 사설 인증서와 동일한 법적 효력을 가지게 되면서 기술적으로 공인인증서와 동일한 다양한 사설 인증 서비스가 출현하게 된다.

이후, 2020년 5월 20일 공인인증서의 독점적 지위를 폐지하는 전자서명법 개정이 완료되어 1999년에 시작된 공인인증서 제도가 21년 만에 역사 속으로 사라졌다.

2.2. 기타 본인확인 수단

"정보통신망 이용 촉진 및 정보보호 등에 관한 법률", "개인정보보호법"에 따라 정보통신서비스 제공자가 주민번호 등을 수집·이용할 수 없으며, 방송통신위원회에서 본인인증기관으로 지정된 업체만이 본인확인을 진행할 수 있도록 되어 있다. 지정된 본인확인 기관으로는 공인인증기관(5개사), 아이핀 서비스 업체 (3개

1) 양자 암호 발달에 따라 공인인증서의 기반이 되고 있는 공개키 암호의 무력화 이슈는 본 기고에서 다루지 않는다.

2) 다양한 환경에서 전자정부와 인터넷 뱅킹 서비스 제공을 요구하기 위해 만들어진 단체

사), 이통통신사(3개사), 신용카드사 (8개사)가 있다.

휴대폰 본인확인은 휴대폰 개통 시 오프라인 또는 (범용)공인인증서로 확인된 본인이 휴대폰을 소지하고 있는지 여부로 소유기반 본인확인 방법이다. 타인 명의의 휴대폰을 사용하는 경우 사용이 불가능한 단점이 있으며, 최근에는 PASS 앱을 통한 본인확인 및 전자서명 방식으로 발전되었다.

아이핀을 통한 본인확인은 오프라인, (범용)공인인증서, 휴대폰 본인 확인을 통해 본인 확인 후 가입절차를 진행하고, 이후 아이디와 패스워드를 확인하는 지식기반의 본인확인 방식이다. 주민번호 유출에 대응하기 위해 만들었으나 실제 서비스의 서비스의 효용도가 낮아 최근 공공 아이핀 발급은 중단하고 민간 아이핀으로 일원화가 진행되고 있다[4].

신용카드를 통한 본인확인은 신용카드 발급 시 카드 발급 상담사를 통한 오프라인 확인, (범용)공인인증서, 휴대폰 본인 확인, (旣 발급된)신용카드를 통한 본인확인 후 카드의 소유여부를 확인하는 방식이다. 간단히 카드 번호, 유효기간, CVC 번호를 입력하는 방식과 사설 인증서를 사용하는 방식이 제공된다.

Ⅲ. 새로운 인증 기술

기존 인증방식의 불편함이 지속적으로 제기되고 있으며, 이를 개선할 수 있는 새로운 기술을 기반으로 한 서비스가 출시되고 있다. 대표적인 기술로는 FIDO (Fast IDentity Online)와 블록체인 기반의 DID (Decentralized ID) 가 있다.

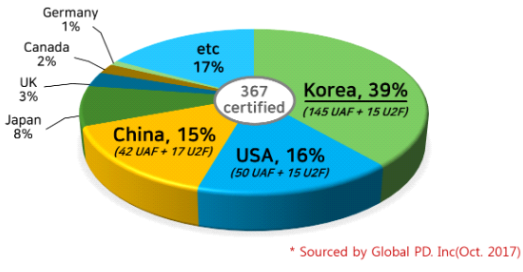
3.1. FIDO (Fast IDentity Online)

편하면서 안전한 인증 수단은 지속적으로 연구되어 왔지만, 편리하지만 보안 취약점을 가지는 지식기반 인증, 별도의 장치가 필요한 소유기반 인증, 인식을 위한 하드웨어와 처리할 소프트웨어가 필요한 생체기반 인증 등 각 방식은 각자 해결해야할 문제점을 가지고 있다. 생체 센서가 탑재된 스마트폰의 보급, TrustZone 등 안전한 실행영역, 지속적으로 발전되어온 PKI 등 각각의 기술이 결합되어 기존 방식의 문제점을 해결 할 수 있는 기반이 마련되고 이를 바탕으로 FIDO 기술이 등장하게 되었다.

FIDO는 2013년 FIDO Alliance가 공식 출범하고[5], 이후 구글, 마이크로소프트, 비자, 페이팔, RSA, 인텔, 삼성 등 글로벌 업체가 참여하여 시장을 키우게된다. 이후 2014년 FIDO UAF(Universal Authentication Framework), U2F(Universal 2nd Factor) 프로토콜을 완성하고 온라인 특히 생체 센서가 있는 모바일에서 FIDO가 사용자 인증 시장을 주도하게 된다. 특히 국내에서는 기존 공인인증서의 불편함이 지속적으로 제기되는 시점에 이를 해결해 줄 수 있는 새로운 기술인 FIDO가 생체 센서가 있는 스마트폰의 보급과 더불어 KB국민은행, 신한은행 등 많은 서비스에 도입되며 시장의 주목을 받게 되었다.

하지만, 시장에 확산된 FIDO는 모바일 환경에서, UAF, U2F 프로토콜만으로 인증을 처리해야하기 때문에 PC를 포함한 다양한 환경에서 적용이 힘든 단점이 있다. FIDO Alliance는 표준화를 통해 플랫폼 제약 없이 브라우저, OS 등에서 사용할 수 있도록 하기 위해 FIDO2의 규격화를 진행하여, W3C에서 2018년 CR(Candidate Recommendation), 2019년에 최종 규격으로 선정되었으며, 윈도 10, 안드로이드, 구글 크롬, 파이어폭스, 마이크로소프트 에지 등에 적용되어 플랫폼으로서의 역할을 제공하게 되었다.

국내에서는 FIDO2의 규격화가 진행되자 FIDO의 성공을 바탕으로 전체 인증 제품의 39%를 차지할 만큼 적극적으로 추진하였으나, 개인 사용자가 별도의 토큰을 개인의 비용으로 구매하는 것에 익숙하지 않은 문화로 기존 FIDO에 비해서 큰 성과를 내고 있지 못한 상황이다.



〔그림 2〕 국가별 FIDO 인증 실적

3.2. DID (Decentralized ID)

국내외의 각종 개인정보 유출 사고[6,7]로 인해 중앙에서 관리되는 개인정보가 공격의 타깃이 될 수 있다는 인식 변화에 따라 개인의 신원 증명을 직접 관리하고 공개 대상 범위를 스스로 선택할 수 있는 자기주권 신원 (Self sovereign identify / SSI) 증명 개념이 생겨나게 되었다.

블록체인은 대중들에게 가상화폐로만 알려져 있지만, 암호 기술을 기반으로 합의알고리즘 등으로 분산원장을 관리하여 기존 중앙 집중적으로 관리되던 데이터를 분산하여 관리하고 무결성을 제공하는 기술이다. 블록체인의 이러한 특징은 자신의 정보를 스스로 관리하고자하는 요구를 시스템으로 구현할 수 있는 기반이 되었다.

DID에서는 개인의 신원정보를 여러 신원정보 발행자가 발급하고 검증할 수 있는 발행자 ID 정보를 블록체인을 사용한 신뢰된 ID 저장소에 저장한다. 이후 서비스 제공자가 신원정보를 요청하는 경우 기존에 발급된 정보 중 제공할 정보를 선택적으로 제공하며, 서비스 제공자는 신뢰된 ID 저장소를 통해 신원 정보를 검증할 수 있다. 중앙화된 시스템에서 개인정보 유출에 대한 피해와 자신의 개인정보가 자신의 동의 없이 임의로 활용되는 것을 방지할 수 있는 장점이 있다.

하지만, 본인이 제공하는 신원정보가 신뢰성을 가지기 위해서는 신원정보 발행자가 신뢰성을 가져야한다. 개인의 신원정보들이 탈중앙화 되었다고 하더라도 신뢰할 수 있는 신뢰기관이 필요하게 된다. 국내에서는 앞서 언급한 공인인증서, 휴대폰 등 본인확인 기관이 이를 담당하게 되고 새로운 본인인증 기술을 사용하기 위해 기존의 본인확인이 사용되는 상황이 발생할 수 있다.

DID 시장을 주도하기 위해 많은 컨소시엄이 만들어지고 있으며, 국내에서도 마이아이디 얼라이언스, 이니셜 컨소시엄, DID 얼라이언스 등이 경쟁하고 있다.

Ⅳ. 새로운 인증 서비스

2015년 공인인증서 우월적 지위 폐지 후 국내에는 2017년 카카오뱅크를 시작으로 은행권의 KB 모바일 인증서, 증권 업계의 통합인증 서비스인 오픈패스, 통신사 공통 서비스인 PASS 앱, 웹 표준 기반 간편인증 서비스까지 다양한 형태의 사설 인증 서비스가 도입되고 있다.

4.1. 카카오뱅크

카카오뱅크는 2017년 국내 두 번째 인터넷 전문은행으로 거래를 안전하고 사용자의 편의성을 극대화 하는 방향으로 사설 인증 방식으로 서비스를 시작하였다[8]. 기존 공인인증서의 경우 사용과 보안을 위해 여러 보안 모듈(PKI, 키보드 보안, 방화벽 등)을 설치하던 방식을 일원화하여 자체 개발하고, 보안성 강화를 위해 중요 정보를 모바일 보호 영역에 저장하는 방식을 사용하였다. 또한 기존 공인인증서가 사용하는 PKI 방식의 보안 수준을 제공하는 사설 인증서를 사용하면서도 복잡한 UX(User eXperience)를 직관적인 UX로 변경하는 것을 목표로 생체인증, PIN번호 등의 기술을 적용하여 고객 편의성을 극대화 했다. 보안성을 유지하면서도 고객의 편의성을 도모하는 혁신은 이후 많은 업체가 사설인증서를 도입하는데 벤치마킹되었다.

카카오뱅크는 보안성 및 편의성 증대를 위해서 1인 1기기 정책과 카카오뱅크 앱에서만 서비스를 제공하고 있다. 고객이 서비스 이용추세가 PC에서 모바일로 넘어가는 시점에서의 선택과 집중의 결과로 PC, 브라우저 등 범용적인 환경에서는 서비스가 제공되지 않는다.

4.2. KB모바일 인증서

2019년 KB국민은행은 기존 공인인증서의 불편함을 개선한 사설인증서 시스템인 “KB모바일 인증서”를 서비스하기 시작했다[9]. 최초 발급 절차의 간소화, 인증서의 안전한 저장과 생체인증, 간편 비밀번호를 포함한 편리하고 다양한 인증 방식 제공 등을 주요 특징으로 하고 있다. 특히 매년 갱신해야하는 공인인증서의 불편함을 해소하기 위해 인증서를 폐기하거나 장기간 사용하지 않는 경우를 제외하면 계속 사용할 수 있다. 연말정산, 전자정부 민원서류 등과도 연계하여 공인인증서가 필수였던 서비스에도 사용가능하다.

KB모바일 인증서 또한 KB국민은행 앱에서만 사용가능하며, PC, 브라우저 등 범용적인 환경에서는 사용이 불가하다.

4.3. 오픈패스(OpenPass)

2019년 안랩과 코스콤은 안랩의 “안랩 V3 모바일 플러스 2.0”에 코스콤의 통합인증기능을 이식한 서비스를 오픈하였다[10]. 약 2,800만대의 모바일 기기에서 이용 중인 앱에 인증기능을 통합하여, 각 사용자의 추가 설치에 대한 부담을 줄였다. 인증서의 안전한 저장과 생체 인증, 간편 비밀번호 등 편리한 인증 방식 역시 제공하고 있다. 다른 사설 인증 방식과는 다르게 공인인증서를 통한 인증을 같이 제공하고 있으며, PC에 인증서를 가지고 있지 않은 경우에도 앱을 통해 인증서비스를 사용할 수 있다.

4.4. PASS 앱

2018년 통신 3사는 각각 운영해온 본인인증 서비스(SK텔레콤 ‘T인증’, KT ‘KT인증’, LG유플러스 ‘U+인증’)를 ‘PASS’라는 브랜드로 통합하였다[11]. 이후 2019년 PASS 앱 기반의 사설인증서인 ‘패스 인증서’를 출시했다[12]. 패스 인증서는 본인 인증만 제공하던 PASS 앱에 전자서명 기능을 추가하였으며, 인증서를 WBC (White-Box. Cryptography, 화이트박스 암호)를 통해서 보호하고, 백신, 위변조 방지 등의 보안 기술을 적용하였다. 생체 인증, 간편 비밀번호 등 편리한 인증 방식을 제공한다.

4.5. 웹 표준 기반 간편인증 서비스

2019년 중 인터넷 뱅킹 이용 실적 중 모바일 뱅킹이 차지하는 비중은 건수 및 금액 기준으로 각각 61.9%, 13.1%을 차지하고 있다. 모바일의 비중이 높지만, 모바일이 아닌 인터넷 뱅킹은 아직도 건수 기준으로는 38.1%를 차지하고 있으며, 금액은 오히려 더 높은 86.9%를 차지하고 있다[13]. 이러한 통계를 볼 때 PC 웹, 모바일 웹에서 별도의 설치 없이 사용할 수 있는 사설인증 서비스 역시 필요하다고 볼 수 있다. 앱이 반드시 필요한 다른 서비스와 달리 예티소프트와 한컴시큐어(現 한컴위드)는 웹 표준 기반으로 사설인증 서비스를 제공하고 있다[14,15].

웹 표준 형태의 서비스는 다른 앱과의 연동이 필요한 경우 사용자에게 보다 나은 UX를 제공해준다. 예를 들어, SMS, 카카오톡 등으로 상품 광고를 보낸 경우 별도의 앱으로 서비스하는 경우 앱 설치, 전환 등을 거쳐야 하지만, 웹 표준 형태의 서비스는 In-App 브라우저 등을 통해 별도의 설치나 전환이 없어 고객의 중간 이탈을 최소화 할 수 있는 장점이 있다.

Ⅴ. 결 론

공인인증서는 여러 사설인증의 출시에도 불구하고 국가적인 인프라와 오랜 기간 서비스 경험과 같은 여전히 매력적인 장점이 있다. 지속적으로 제기되어 왔던 불편함 등을 편의성으로 바꿀 수 있다면 보다 더 큰 경쟁력을 가질 수 있을 것으로 보인다.

사설인증은 카카오뱅크의 사례에서 보듯 당연하다고 생각되는 것들을 다시 생각하는 혁신과 기술 만능 주의가 아닌 실제 시장에서 원하는 기능을 제공해야지만 무한 경쟁 시장에서 살아남을 수 있을 것이다.

2020년 공인인증서의 의무화 및 독점적 지위가 폐지되었다. 이제 시장에서 새로운 인증기술의 선택은 더 이상 법의 영역이 아니라 보안성, 성능, 편의성 등 기술의 질에 따라 결정될 것이다. 즉, 특정 기술 만능주의가 아니라 필요한 분야에 적절한 기술을 사용할 수 있는 토대가 마련되었다고 볼 수 있다.

공인인증서도 서비스를 사용자가 보다 편하게 개선하여 법 때문이 아닌 실제로 좋은 서비스임을 확인 시키고, 사설 인증도 각 서비스의 장점을 기반으로 전 분야에 사용되고 있는 공인인증서와 많은 분야에서 선의의 경쟁을 한다면, 사용자는 더욱 편하고 안전한 인증서비스를 받을 수 있게 될 것으로 보인다.

참 고 문 헌

[1] 원병철, “전자서명법 국회 본회의 통과, ‘사설인증서’의 시대 온다”, 보안뉴스, 2020년 5월 20일

[2] 국가 정보원, 과학기술정보통신부, 행정안전부, 방송통신위원회, 금융위원회, 국가정보보호백서 , pp.128, 2019

[3] 김동욱, “은행 공인인증서 ‘보안토큰’ 저장 의무화한다”, 이데일리, 2015년 6월 22일

[4] 양정우, “7월부터 ‘공공 아이핀’ 발급 중단 민간 서비스로 일원화”, 연합뉴스, 2018년 2월 1일

[5] History of FIDO Alliance, https://fidoalliance.org/overview/history/
[6] 홍재원, “카드 고객정보 사상 최대 1억400만건 유출”, 경향비즈, 2014년 1월 8일
[7] 이현수, “또! 페이스북. 2억 6천만명 개인정보 유출”, 전자신문, 2019년 12월 22일
[8] 손경호, “공인인증서 없는 카카오뱅크, 보안 괜찮을까?”, ZDNet, 2017년 8월 1일
[9] 김연숙, “국민은행, 유효기간 따로 없는 ‘KB모바일 인증서’ 출시”, 연합뉴스, 2019년 7월 15일
[10] 홍하나, “코스콤, 안랩과 손잡고 ‘통합인증 서비스’ 출시한다”, 디지털데일리, 2019년 5월 22일
[11] 김인순, “통신3사 공동인증브랜드 ‘PASS’ 사설 전자인증 시장 ‘태풍’ 되나”, 전자신문, 2018년 5월 22일
[12] 황준호, “‘PASS 인증서’출시, 공인인증서 비켜”, 아시아경제, 2019년 4월 25일
[13] 이정국, 이동민, “2019년중 국내 인터넷뱅킹서비스 이용현황”, 한국은행, 2020년 4월 1일
[14] 임민철, “예티소프트, 웹기반 간편인증·전자서명 솔루션 출시”, ZDNet, 2018년 2월 23일
[15] 노동균, “한컴시큐어, 간편인증 솔루션 ‘애니핀’으로 공인인증 대체시장 공략”, IT 조선, 2018년 4월 17일

〈저자소개〉

강 효 관 (Kang,HyoKwan)
1998년 2월 : 경희대학교 컴퓨터 공학과 졸업
2000년 2월 : 경희대학교 컴퓨터 공학과 석사
2002년 2월 : 경희대학교 컴퓨터 공학과 박사 수료
2003년 5월~2009년 5월 : ㈜한컴위드(舊 ㈜소프트포럼)
2009년 5월~2011년 5월 : ㈜코스콤
2011년 9월~현재 : ㈜예티소프트
<관심분야> 사용자 인증, 공개키 암호, 차세대 암호