Journal of the Korean Data & Information Science Society
2017, **28**(1), 163–171

http://dx.doi.org/10.7465/jkdi.2017.28.1.163
한국데이터정보과학회지

공인인증서의 암호학 활용에 관한 연구[†]

김대학[1]

[1]대구가톨릭대학교 수리정보과학과

접수 2016년 12월 30일, 수정 2017년 1월 18일, 게재확정 2017년 1월 19일

요 약

인터넷 뿐만 아니라 휴대용 컴퓨터라고도 불리고 있는 스마트폰의 기능이 향상되면서 인터넷상거래나 금융기관거래에서 인터넷이나 스마트폰을 이용한 거래가 활성화 되고 있다. 인터넷이나 스마트폰을 이용한 상거래나 금융기관 거래 (banking)에는 공인인증서 (authorized certificate, certificate)가 반드시 필요하다. 공인인증서는 지금도 중요시 되지만 미래사회에도 계속 중요하게 다루어질 중요한 안전장치이다. 공인인증서는 2015년 3월 현재 우리나라 국민 2,841만명이 이용할 정도로 생활 필수품에 가까운 위치를 점했다. 그러나 공인인증서의 사용자들이 상상이상으로 공인인증서에 대해 알고 있지 못하다는 점을 파악하여 본 논문에서는 공인인증서에 대한 중요사항들을 정리하고 암호학과 관련된 내용들을 설명하고자 한다. 각종 논문과 인터넷 자료 및 신문기사, 그리고 서적을 통하여 공인인증서의 본질적인 모습과 공인인증서가 어떤 암호체계를 기반으로 발전해 왔는지, 또 과거의 모습부터 근래의 모습에는 어떤 변화를 거쳐왔는지 살펴보고 다양하게 쓰이는 공인인증서의 장점과 그 속에 공존하는 단점, 그리고 취약점들에 대하여 언급하였다. 또한 앞으로 공인인증서가 어떻게 발전해 나갈지에 대해 비모수적 통계적 방법으로 예측하였다.

주요용어: 공개키, 공인인증서, 암호학, 암호화 함수, 의료정보서비스.

1. 서론

금융거래나 전자상거래에서 신원확인, 문서의 위조 및 변조, 거래사실 증명을 위해 사용하는 정보 중 하나가 전자서명 (digital signature)이다. 이 전자서명을 안전하게 사용하기 위해 만들어진 것이 공인인증서로, 실생활에서의 인감증명과 같은 역할을 한다. 이 공인인증서 안에는 발행기관 식별정보, 가입자의 성명 및 식별정보, 전자서명 검증키, 인증서 일련번호, 유효기간 등이 포함되어 있어 뱅킹이나 전자상거래에서 ID와 비밀번호만 입력하면 전자서명이 생성된다.

공인인증서는 전자서명의 검증에 필요한 공개키 (public key)에 소유자 정보를 추가하여 만든 일종의 전자신분증 (증명서)으로서 공개 키 증명서, 디지털 증명서, 전자 증명서 등으로도 불린다. 공인인증서는 개인 키와 함께 한 쌍으로 존재한다. 전형적인 공개 키 기반 구조 (public key infrastructure) 방식에서 서명은 인증 기관의 소유가 된다. 신뢰의 웹 방식에서 서명은 자신이 직접 서명하거나 다른 사람이 서명할 수 있다. 어떠한 경우든 인증서의 서명은 정보와 공개키를 함께 증명하는 인증 서명자의 증명이다.

공인인증서는 OpenSSL의 ssl-ca나 수세 리눅스의 gensslcert와 같은 도구를 포함한 유닉스 기반 서버용으로 작성되었다. 비대면 온라인 방식의 전자상거래에서 상대방과의 계약서 작성, 신원확인 등에

[†] 본 연구는 2014년 대구가톨릭대학교 일반연구비 지원에 의한 것임.
[1] (38430) 경상북도 경산시 하양읍 하양로 13-13, 대구가톨릭대학교 수리정보과학과, 교수.
E-mail: dhkim@cu.ac.kr

전자서명이 필요하며 동시에 공인인증서로 해당 전자서명을 생성한 자의 신원을 확인하게 된다. 전자금융 거래의 공인인증서 적용 흐름을 살펴보면, 1998년 은행들이 인터넷 뱅킹을 시작하면서 공개키 방식의 사설인증서를 발행하여 사용하기 시작하였다. 인증서의 서명을 디지털 서명이라 한다. 이때는 물론 국내 공인인증서 체계가 안정되지 않고 관련법의 정비도 미흡했던것이 원인이다. 그 후 공인인증기관의 공인인증서비스가 안정적으로 제공되고 전자서명법, 전자거래법 등 관련법이 정비가 되어 공인인증서의 사용상 문제점이 없다고 판단되어 2002년 3월 정보통신부 주관 은행 및 증권사 담당자들의 회의에서 전자금융거래에 공인인증서를 도입키로 합의 하였다. 그해 9월 인터넷 뱅킹의 인증서를 사설인증서에서 공인인증서로 전환하고 2003년 1월부터 사이버 증권거래에도 공인인증서를 사용하였다.

공인인증서는 개인 키와 공개 키로 구성된 비대칭 키 암호화 시스템을 사용한다. 즉 공인인증서와 암호화 알고리즘과는 절대적인 연결관계가 유지될 수 밖에 없다. 암호학과 암호알고리즘의 구체적 내용에 대해서는 Forouzan (2008)과 Trappe와 Washington (2006)을 참고하기 바란다. 대칭키 알고리즘은 미국 암호화 표준 방법으로 공표된 DES (data encryption standard)와 AES (advanced encrytion standard) 등의 방법이 있다. 최근 들어 Kim (2012)은 암호학의 영역에서 DES의 라운드 키 생성 엑셀 매크로를 개발한 바 있고 Kim과 Oh (2015)는 확장 유클리드 알고리즘에 대한 컴퓨터 집약적 방법에 대하여 연구한 바 있다. 비대칭 키 암호화란 데이터를 암호로 만들 때와 풀 때 각각 다른 키를 사용하는 방식이다. 대표적인 비대칭키 암호화 알고리즘으로 Rivest 등 (1978)에 의한 RSA 알고리즘을 들 수 있다. 예로서 인터넷쇼핑몰에서 물건을 구매하고 공인인증서를 사용 할 때, 구매자는 자신만이 소유한 개인 키로 공인인증서를 암호로 바꾸어 송신한다. 판매자는 구매자가 제공한 공개 키를 이용해서 암호를 해제해 원래대로 바꾼다. 이를 원래의 서명과 비교해보면 위조 여부를 판독할 수 있게 된다. 공인인증서는 해당 공개 키의 주인이 누구인지 인증해주는 역할을 한다. 공인인증기관 (certification authority; CA)은 전자서명법에 의해 규정된 자격요건을 갖추여 미래창조과학부로 부터 지정된 기관으로서 현재 국내 공인인증기관으로 지정된 곳은 한국인터넷진흥원 (KISA)를 최상위인증기관으로 하여 하위 공인인증기관으로 금융결제원 (`http://www.yessign.com`), 한국정보인증 (`http://signgate.com`), (주)코스콤 (구 한국증권전산, `http://www.signkorea.com`), 한국전자인증 (`http://www.crosscert.com`), 한국무역정보통신 (KTnet, `http://www.tradesign.net/`) 등 5곳이며 미래창조과학부는 공인인증정책 수립 및 인증체계를 관리하고 외국정부화 인증서 연도에 대한 협약등을 추진하며 최상위 인증기관인 한국인터넷진흥원은 외국의 최상위기관과 상호인증, 하위 공인인증기관에게 공인인증서 발급, 공인인증서 검사 및 안전운영지원, 전자서명인증기술 개빌 및 보급 등의 역할을 하고 있으며 은행과 증권회사 등은 공인인증서를 직접 발급하지 않고 접수 및 등록만 대행해준다.

공인인증서는 금융기관의 서버에 저장하고 있는 것이 아니라 고객 개인이 직접 들고 있기 때문에, 해킹을 통해 금융기관의 정보를 빼내갈 수는 있더라도 공인인증서를 빼내 갈 수는 없다. 즉 금융기관에 저장된 정보만 해킹해서는 고객의 재산에 대한 영향력을 행사할 수 없다.

2. 암호화와 공인인증서

공인인증서는 전자 서명의 검증에 필요한 공개 키 (전자서명법에는 전자서명검증정보로 표기)에 소유자 정보를 추가하여 만든 일종의 전자 신분증 (증명서)이다.

공인인증서에는 두 방식의 암호화가 사용된다. 공개키 암호화 방식과 일방향 (해시함수) 암호화 방식이다. 송신자는 공인인증서와 전자문서를 전송하고, 이와 함께 개인키로 암호화된 전자서명을 전송한다. 수신자는 송신자의 공인인증서를 공개키로 복호화하여 전자서명을 검증하고 전자문서를 이용해 해시값을 도출하여 비교한다. 이를 통해 전자문서가 송신된 이후 변질되었는지, 전자서명이후 전자서명에 변화가 있었는지 알 수 있다. 이 과정에서 가장 중요한 요소가 각각의 암호시스템의 신뢰성이다. 이에

대해 알아보자.

2.1. 공개키 암호화 방식

공개키 암호화 방식은 공개키와 개인키의 키 쌍이 존재하며 평문을 암호화, 복호화 하는데 서로 다른 키를 사용하는 방식으로 비대칭키 암호화 방식이라고도 불린다. 공개키 암호화 방식은 데이터 암호화 속도가 대칭키 암호화 방식에 비해 느리기 때문에 일반적으로 대칭키 암호화 방식의 키 분배나 전자서명 또는 카드번호 같은 작은 크기의 데이터 암호화에 사용되고 있다. 또한 대칭키 방식에 비해 키 관리의 어려움이 적다는 장점이 있다. 대표적인 공개키 암호 알고리즘으로는 국내에는 KCDSA (한국인터넷진흥원, 2011b)가 있으며 국외에는 RSA, ELgamal (1985), Blake (1995) 에 의한 ECC (elliptic curve cryptography) 등이 있다.

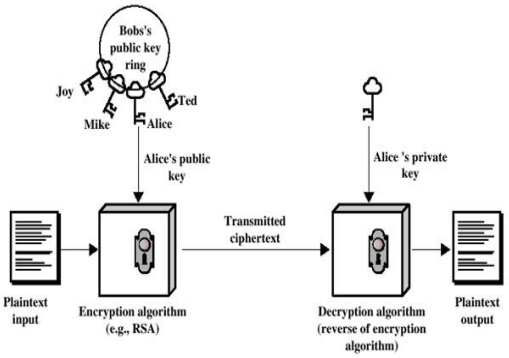

Figure 2.1 Public key encryption/decryption

현재 공인인증서에 사용되는 공개키 암호 알고리즘은 RSA 방법이다. RSA는 1983년에 미국 매사추세츠 공과대학교 (MIT)에서 개발한 공개키 암호 알고리즘의 하나로 소인수분해의 어려움에 안전성의 기반을 두고 있다. RSA 알고리즘을 활용한 암호시스템은 대칭키의 안전한 분배 및 관리문제를 해결하기 위해 널리 이용되며, 메시지 암호화 및 복호화, 전자서명 등에 사용된다. RSA는 두 개의 키를 사용한다. 여기서 키란 메시지를 열고 잠그는 상수 (constant)를 의미한다. 일반적으로 많은 공개키 알고리즘의 공개키는 모두에게 알려져 있으며 메시지를 암호화하는데 쓰이며, 암호화된 메시지는 개인키를 가진 자만이 복호화하여 열어볼 수 있다. 하지만 RSA 공개키 알고리즘은 이러한 제약조건이 없다. 즉 개인키로 암호화하여 공개키로 복호화할 수 있다. 공개키 알고리즘은 누구나 어떤 메시지를 암호화할 수 있지만, 그것을 해독하여 열람할 수 있는 사람은 개인키를 지닌 단 한 사람만이 존재한다는 점에서 대칭키 알고리즘과 차이를 가진다. RSA는 소인수분해의 난해함에 기반하여, 공개키만을 가지고는 개인키를 쉽게 짐작할 수 없도록 디자인되어 있다. 보다 이해하기 쉬운 예를 들자면, A라는 사람에게 B라는 사람이 메시지를 전하고자 할 때 B는 A의 열린 자물쇠를 들고 와 그의 메시지를 봉인 (공개키 암호화 과정에 해당)하고, 그런 다음 A에게 전해 주면, 자물쇠의 열쇠 (개인키에 해당)를 가지고 있는 A가 그 메시지를 열어보는 (개인키 복호화 과정에 해당) 식이 된다. 중간에 그 메시지를 가로채는 사람은 그 열쇠를 가지고 있지 않으므로 메시지를 열람할 수 없다. Figure 2.1은 공개키 방식에 의한 구조를 나타내고 있다.

2.2. 해시함수를 활용한 일방향 암호화 방식

일방향 암호화 방식은 해수 해시 함수를 이용하여 암호화 된 값을 생성하여 복호화 되지 않는 방식이다. 해시함수는 임의의 길이를 갖는 메시지를 입력으로 하여 고정된길이의 해시 값 또는 해시 코드라고 불리우는 값을 생성하며, 동일한 입력메시지에 대해 항상 동일한 값을 생성하지만 해수 값만으로 입력 메시지를 유추할 수 없어 전자서명체계와 함께 데이터 무결성을 위해 사용된다. 비밀번호와 같이 복호화 할 필요가 없지만 입력 값의 정확성 검증이 필요한 경우에 사용한다. 대표적인 해시함수로는 SHA-2 (SHA-224/256/384/512), RIPEMD-160과 국내에서 개발한 HAS-160이 있다.

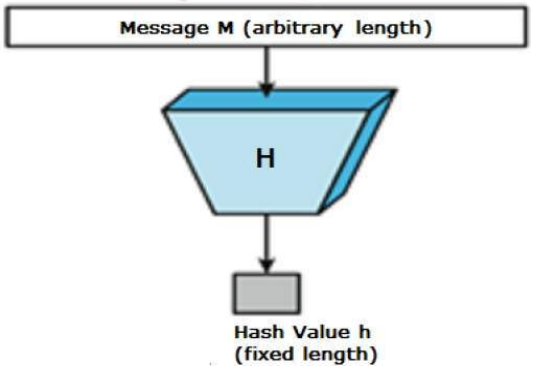

Figure 2.2 Hash oneway function encryption

Figure 2.2는 일방향 해시함수 암호화 과정을 나타내고 있다. 현재 공인인증서에 사용되는 일방향 암호화 방식은 SHA-256이다. 최초의 알고리즘은 1993년에 미국 국립기술표준원 (NIST; national institue of standards technoloty)에 의해 안전한 해시 표준 (Secure Hash Standard; SHA)으로 연방정보처리기준 (federal information processing standard; FIPS) PUB 180으로 출판되었으며, 다른 함수들과 구별하기 위하여 보통 SHA-0이라고 부른다. 얼마 안 있어 미국안전보안국 (national security agency; NSA)는 이 표준을 폐기했고, 1995년에 개정된 알고리즘 FIPS PUB 180-1을 새로 출판했으며 이는 SHA-1 이라고 불리운다. SHA-1은 SHA-0의 압축 함수에 비트 회전 연산을 하나 추가한 것으로, NSA에 따르면 이는 원래 알고리즘에서 암호학적 보안을 감소시키는 문제점을 수정한 것이라고 하지만 실제로 어떤 문제점이 있었는지는 공개하지 않았다. 일반적으로 SHA-1은 SHA-0보다 암호학적 공격이 힘든 것으로 알려져 있으며, 따라서 NSA의 주장은 어느 정도 설득력이 있다고 볼 수 있다. SHA-0과 SHA-1은 최대 비트의 메시지로부터 160비트의 해시 값을 만들어 내며, 로널드 라이베스트가 MD4 및 MD5 해시함수에서 사용했던 것과 비슷한 방법에 기초한다. NIST는 나중에 해시 값의 길이가 더 긴 네 개의 변형을 발표했으며, 이들을 통칭하여 SHA-2라 부른다. SHA-256, SHA-384, SHA-512는 2001년에 초안으로 처음으로 발표되었으며, 2002년에 SHA-1과 함께 정식 표준 FIPS PUB 180-2로 지정되었다. 2004년 2월에 삼중 DES의 키 길이에 맞춰 해시 값 길이를 조정한 SHA-224가 표준에 추가되었고 SHA-256과 SHA-512는 각각 32비트 및 64비트 워드를 사용하는 해시 함수로서 몇몇 상수들이 다르긴 하지만 그 구조는 라운드의 수를 빼고는 완전히 같다. SHA-224와 SHA-384는 서로 다른 초기 값을 가지고 계산한 SHA-256과 SHA-512 해시 값을 최종 해시 값 길이에 맞춰 잘라낸 것이다. 예로서 MD4 방식에 의한 입력문자열 “I love you.”에 대한 해시값은 “49dd22119f540d88aed7a97c5afc5947”로 되고 마침표가 없는 입력문자열 “I love you”에 대한 해시값은 “bfdb7e67ee0fcd82e624ee2d0ab3df68”로 전혀 다르게 나타난다. Table 2.1에는 다양한 방법에 따른 해시값을 예로 나타내었다.

Table 2.1 Recommendation algorithm and minimum key sizes

method	input value	hash value
MD4	cryptography algorithm	ab019d42c8b52d539a33f781599800a2
MD5	cryptography algorithm	410994f88ca57a488375296b0df9a8b3
SHA-1	cryptography algorithm	7115d3dd709dd5aa70d22e4ab30149bc2eb364b7
SHA-256	cryptography algorithm	ab2d8fa5c726d9e8e012b1ea90217616f82874d6d115b98e149ff29cb31a536f

3. 공인인증서 고도화를 위한 노력

공인인증서의 기명날인으로서의 기능과 무결성을 전자서명법이 인정하는 만큼 공인인증서의 안전성과 신뢰성의 확보와 발전을 위한 정부의 일이 법규화 되어있다. 공인인증서 암호체계 고도화 계획 (한국인터넷진흥원, 2011a)은 2009년 9월 수립되어 2012년 1월 시행되었다. 분산 컴퓨팅 기술의 급속한 발달로 인해 기존 암호 알고리즘의 안전성은 저하되어 보다 고도화된 암호 알고리즘이 요구되었다. 이에 관하여 NIST, ECRYPT등 국외 암호전문기관은 기존 공인인증서의 암호체계 (RSA-1024방식의 전자 서명키, 160비트 SHA-1방식의 해시 암호)는 2013년 까지 사용하지 않을 것을 권고했다. 그러므로 공인인증서 자체에 대한 해킹 (불법복제, 위조생성 등)을 방지하고 공인인증서 신뢰성 보장을 위해 전자서명키 길이 상향 조정, 해시 알고리즘 교체 등 공인인증서 암호체계의 고도화 추진이 필요하게 되었다. 2012년 1월 이전의 전자서명 알고리즘에 사용되는 전자 서명키 길이는 최상위 인증기관 및 공인인증기관은 2,048비트를, 가입자는 1024비트를 이용했다. 이는 공인인증서 암호체계 고도화 기본계획의 수립시기인 2009년 당시 NIST권고에 의하면 기존 가입자공인인증서의 전자 서명키 (1024비트)의 안전도는 78비트로 2011년 이후에는 유효기간 1년 내에 전자 서명키가 노출될 위험이 있다고 하였으나 모든 공인인증서가 그런 것은 아니었다. NIST나 ECRYPT의 권고를 기준으로 할 때 기존 최상위인증기관의 전자 서명키 (2048비트)의 안전성은 108비트로 2010년에 발급한 경우 유효기간만료일인 2030년 까지 안전하게 사용 할 수 있다. (Rivest, 1992) 이들 관계를 표로 정리하여 Table 3.1에 나타내었다.

Table 3.1 Recommendation algorithm and minimum key sizes

Life time	No.of bits	Algorithm	FFC-DSA	FFC-DH	IFC	ECC	H	HMAC
through 2010	80	2TDEA	1024	1024	160	160	SHA-1	SHA-1
thorugh 2030	112	3TDEA	2048	2048	224	224	SHA-224	SHA-1
beyond 2030	128	AES-128	3072	3072	256	256	SHA-256	SHA-1
beyond 2030	192	AES-192	7680	7680	384	384	SHA-384	SHA-224
beyond 2030	256	AES-256	15360	15360	512	512	SHA-512	SHA-256

Table 3.1에서 Lifetime은 알고리즘의 안전성 보장기간을, No. of bits 는 비트단위의 보안강도를, Algorithm은 대칭키 알고리즘을, FFC-DSA는 비대칭키 알고리즘 (FFC; finite field cryptography)중 DSA (data encryption standard)를, FFC-DH는 Diffie-Hellman 알고리즘을, IFC (integer factorization cryptography) 는 인수분해에 기반한 RSA 암호화 방법을, ECC (elliptic curve cryptography)는 타원곡선 암호화 방법 ECDSA를, H는 해시함수가 전자서명 및 해쉉전용 어플리케이션으로 사용되는 경우 (digital signatures and hash-only applications)를 그리고 마지막으로 HMAC (keyed-hash message authentication code)는 해시함수가 키 유도 및 난수 생성 기능을 위해 사용되는 경우를 의미한다.

공인인증서 암호체계 고도화 계획은 전자 서명키 길이 상향과 해시함수의 알고리즘의 고도화를 향해 추진되었다. 가입자 공인인증서의 길이를 1024비트에서 2048비트로 상향하면서 해커가 전자 서명키를 알아내기 위해 처리해야할 연산량이 2^1024에서 2^2048번으로 증가되어 2030년까지 안전성을 확보했고 만약 그 기간 사이 예상을 상회하는 컴퓨터의 성능발전이나 기술발전이 있을 경우 2030년 이전에도 공

인인증서의 암호체계는 다시 고도화 될 수 있다. 해시 알고리즘은 160비트 해시 (SHA-1)에서 256비트 해시 (SHA-256)로 교체되었다.

4. 공인인증서의 이용 현황과 사용자 통계적 추정

공인인증서는 1999년 제도도입 후, 2000년에는 전자입찰, 2001 2005년에는 인터넷 뱅킹, 온라인 증권, 2006년 2009년에는 주택청약, 연말정산, 2010년에는 스마트 폰 뱅킹, 2011년에는 전자세금계산서 분야까지 공인인증서의 이용이 도입되었다. 2000년 만 7세 이상 인구의 인터넷 이용률 (최근 1개월 이내 인터넷 사용자 비율) 은 44.7%, 사용자수는 1,904만 명으로 나타났다. 시간이 지나 2011년 7월에는 만 3세 이상 인구의 인터넷 이용률 (최근 1개월 이내 인터넷 사용자 비율)은 78%로 집계되었고 인터넷 사용자수는 3,718만 명으로 증가했다.

인터넷사용자 중 64.5%가 최근 1년 이내 인터넷을 통해 상품이나 서비스를 구매한 것으로 나타났다. 2011년 7월 인터넷 사용자수를 기준으로 환산하면 약 2,400만 명이다. 인터넷 뱅킹의 경우 이용률 (최근 1년 이내 인터넷 뱅킹 사용자의 비율)은 42.4%, 마찬가지로 환산하면 약 1,576만 명이다. 인터넷 주식거래의 경우 만18세 이상사용자의 9.9%가 최근 1년 이내에 인터넷을 통해 주식거래를 한 것으로 나타났다. 여기서 특이점은 인터넷 사용자 중 주식거래자의 경우로 따져보면 89.4%가 인터넷으로 주식거래를 한 것이다.

이처럼 공인인증서의 이용분야는 증가하였고, 공인인증서 발급 수 역시 증가하였다. 공인인증서의 발급 수는 2006년에 1,440만 건, 2007년에 1,720만 건, 2008년에 1,860만 건, 2009년에 2,190만 건, 2010년 12월에는 2,370만 건을 기록하였다. 그리고 마침내 2011년 2월 경제활동인구의 95%이상인 2,441만 명이 이용할 정도로 생활필수품에 가까운 위치를 점했다. 한국은행 보도자료에 의하면 2015년 3월말 현재 인터넷뱅킹서비스 등록고객수는 1억 861만명으로 증가하였고 인터넷뱅킹 공인인증서 발급건수는 2841만 건으로 나타났다. 일평균 인터넷뱅킹 이용건수는 7,694만 건, 일평균 이용금액은 37조 5910억 정도의 규모를 점하고 있는 실정이다. 한편 PC 기반 인터넷뱅킹 이용건수는 2011년 이후 정체상태를 보이고 있으나 모바일뱅킹 이용건수는 지속적으로 증가하여 2014년 4/4분기부터 PC기반 인터넷뱅킹 이용건수를 추월하고 있다. Figure 4.1은 비모수적 회귀곡선 추정기법인 국소가중회귀평활법 (locally weighted scatter smoothing)으로 추정된 공인인증서 발급건수를 나타내고 있다.

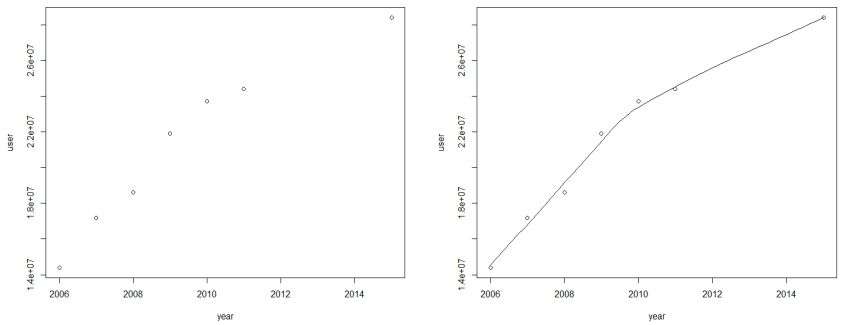

Figure 4.1 Number of issued authorized certificate. (left: data, right: loess fitted)

우리나라는 1980년대 이후 체계적인 국가정보화 정책을 수립하고 인프라 구축, 국가정보화 고도화 및 활용·확산을 전략적으로 추진해 온 결과, 2010년과 2012년 연속으로 UN 전자정부 평가에서 1위를 차지

하는 등 세계적으로 인정받는 정보화 강국으로 발돋움 하였다. 이처럼 우리나라는 전자정부라는 목표를 향해 좋은 성적으로 나아가고 있으며, 일반인이 민원인으로서 전자정부시스템을 이용하기 위해서는 신원을 증명할 필요가 있고 이때 사용 되는 것이 공인인증서이다. 이처럼 공인인증서는 금융 분야뿐만 아니라 행정 분야에도 널리 이용되고 있다. 이외에도 보험가입이나 대출서비스, 인터넷을 통한 세금납부, 항공권이나 열차표 예약, 화물운송물류시스템, 대학의 학사업무, 의료업무, 인터넷 청약 등에도 사용되고 있다.

공인인증서는 가입자를 기준으로 개인용 공인인증서와 법인/단체용 공인인증서로 나누어 발급하고, 그 안에서 다시 용도 제한 정도에 따라 범용과 용도제한용으로 구분한다. 가장 많이 사용되는 공인인증서는 개인용도제한용 공인인증서이다. 대부분의 사용자들이 인터넷을 통한 상품이나 서비스 구매와 인터넷뱅킹에 사용하는 인증서이다. 인증서 발급 초기에는 공인인증서의 용도별 발행에 대한 인식이 미비해 은행이용을 위해 각 은행별로 공인인증서를 발급 받거나, 특정 용도별로 공인인증서를 다수 발급받는 등 다수의 공인인증서를 사용하는 경우가 많았으나 현재는 금융기관에서도 특정 금융기관용 공인인증서는 잘 발행하지 않기에 사용자가 최초로 신청하여 발급받는 공인인증서의 경우 대개 은행업무용으로 용도 제한된 공인인증서이다. 그렇기에 한 금융기관에서 발급받으면 동종의 모든 금융기관에서 사용이 가능하다. 공인인증서 발급기관과 금융기관은 공인인증서를 발급하기 위해 가입자의 정보를 수집한다. 이는 인증서 발급 및 관리, 인증서비스 관련 각종 공지, 인증서 부정발급 확인 및 사용방지 등의 목적을 위함이다. 그 내용은 아래와 같다.

Yessign 공인인증서비스에서는 인증서 발급 및 관리, 인증서비스 관련 각종 공지, 인증서 부정발급 확인 및 사용방지 등의 목적을 위해 전자서명 법령에서 규정한 정보로서 최소한의 개인정보를 수집하고 있다. 수집하는 개인정보는 성명, E-mail주소, 주소, 전화번호, 휴대전화번호 등이며 수집하는 고유식별정보는 주민등록번호이다. 그리고 기기정보 항목으로서 IP및 MAC주소, HDD Serial, USB Serial, OS버전, 웹브라우저버전 등을 수집한다. 기기정보를 확보함으로서 공인인증서가 임의로 복사되거나 이동 되었을 때 작동을 막는다. 위의 경우는 PC의 HDD의 Serial 번호, IP, OS버전과 USB의 Serial 번호를 채집한다. 스마트폰을 저장매체로 사용하는 경우 PC의 공인인증서를 스마트폰으로 복사하는 과정을 거치는데 지정된 절차에 따라 진행되어야만 공인인증서가 작동한다.

5. 결론 및 토의

각종 여론조사나 설문조사에서 나타나듯이 공인인증서의 안전성에 대한 국민들의 불신은 점점 커져간다고 볼 수 있다. 불신의 이유로는 최근 PC해킹에 의한 공인인증서 유출사고 관련 언론보도가 가장 큰 것으로 나타났으며 공인인증서 이용을 위한 프로그램의 안전/신뢰성 순으로 나타났다. 대부분의 사용자는 공인인증서가 안전하다고 느끼며, 공인인증서의 안전성에 의문을 표시하는 사용자도 공인인증서 자체의 안전성에 의문을 표시하는 경우는 반의 반 정도였다. 공인인증서는 현대사회에서 첨단을 달리고 있는 분야라고 해도 과언이 아니다. 공인인증서가 사용자의 요구조건에 충족하려 노력하는 만큼 공인인증서의 이용분야는 급속도로 늘어날 것으로 보인다. 최근 새로이 등장한 스마트폰 공인인증서의 경우 공인인증기관의 공인인증서 어플리케이션을 다운 받은 후 신규로 공인인증서를 신청하거나 PC에 저장되어있던 공인인증서를 스마트폰으로 이동시키는 방법으로 사용이 가능하다. 여러 어플리케이션이 있으나 공인인증서는 동일하며 각각의 목적 역시 개별적인 금융기관의 스마트폰뱅킹의 기능과 연동되거나 KICA 공인인증서 어플리케이션처럼 공인인증서 보관과 관리에 중점을 두는 형태이다. KICA 공인인증서 어플리케이션은 스마트 폰에서 인증서 신청/발급/갱신/폐지/재발급 등의 공인인증서 서비스 기능을 제공하고, PC 또는 스마트 폰에서 발급받은 공인인증서의 이동저장 및 전자서명, 암호화 등 보안기능 제공을 제공한다. 현재의 공인인증서 어플리케이션의 경우 금융기관별로 공인인증서 보관기능이

나 사용기능이 겹치는 경우가 많은 만큼 향후 정부공인의 공인인증서 어플리케이션에서 보관과 보안기능이 강화되어 독립되고, 개별금융기관의 스마트폰뱅킹 어플리케이션 역시 공인인증서 보관기능은 분리되어 자사의 업무를 처리하는데 특화된 어플리케이션으로 발전할 가능성을 조심스레 예측해본다. 추정되는 공인인증서의 사용처는 의료부문이다. 가까운 미래에 개발 될 것으로 기대되고 있는 인터넷 의료서비스와 연동하여 활용될 가능성이 충분하다 여겨진다. 의료 서비스에 있어 환자의 정보는 아주 중요하다. 환자의 진료기록과 처방전, 입원기록과 경과보고 등등 환자의 프라이버시와 더불어 환자의 생명을 좌우할 수 있는 정보이기 때문이다. 공인인증서가 사용된다면 환자의 정보를 보호함은 물론 서비스를 제공받음에 있어 착오를 줄일 수 있을 것이라 예상된다.

References

Blake, I., Seroussi, G. and Smart, N. (1999). *Elliptic curves in Cryptography*, London Mathematical Society, lecture note series 265, Cambridge University Press, Cambridge.

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, **31**, 469-472.

Forouzan, B. A. (2008). *Introduction to cryptography and network security*, The McGraw-Hill Companies, New York.

Kim, D. (2012). On the development of DES round key generator based on Excel Macro. *Journal of the Korean Data & Information Science Society*, **23**, 1203-1212.

Kim, D. (2015). Computer intensive method for extended euclidean algorithm. *Journal of the Korean Data & Information Science Society*, **25**, 1467-1474.

Korea Electronic Certification Authority (Crosscert). `http://www.crosscert.com`.

Korea Financial Telecommnications & Cleanings Institute (Yessign, KFTC). `http://www.yessign.com`.

Korea Information Certificat Authority (Signgate). `http://signgate.com`.

Korea Internet & Security Agency (2011a). Development of improved certificate encryption system, Korea Internet & Security Agency, Seoul.

Korea Internet & Security Agency (2011b). Development of improved korean digital signature algorithem and standard, Korea Internet & Security Agency, Seoul.

Korea Trade Nnetwork (Tradesign). `http://www.tradesign.net/`.

Koscom (Signkorea). `http://www.signkorea.com`.

Rivest, R. L. (1992). *The MD4 message digest algorithm, RFC 1320*, MIT and RSA Data Security, Cambridge.

Rivest, R. L., Shamir, A. and Adleman, L. (1978). A method of obtaining digital signature and public-key cryptosystem. *Communication of the Association for Computing Machinery*, **21**, 120-126.

Trappe, W. and Washington, L. (2006). *Introduction to cryptography with coding theory*, Prentice Hall, Upper Saddle River.

Journal of the Korean Data & Information Science Society
2017, **28**(1), 163–171

http://dx.doi.org/10.7465/jkdi.2017.28.1.163
한국데이터정보과학회지

On the application of authorized certificate for cryptology[†]

Daehak Kim[1]

[1]Department of Mathematical Sciences, Catholic University of Daegu

Received 30 December 2016, revised 18 January 2017, accepted 19 January 2017

Abstract

With the advance of function of smart phone system and internet services, mobile trade grows more popular in the area of e-business or banking. These environmental changes, it makes the needs of authorized certificates. Authorized certificate is not only important in these days but also future society. In 2015, 27 millions of Korean people used public key certificate, but most of them does not know the details on the public key certificate. Therefore, in this paper, we explain and investigate the characteristics on the public certificate and explain the relation ship between authorized certificate and public key encrytion. By investigating several papers, internet data, newspapers and books, we found the historical changes, substantial aspects, the encryption systems on the authorized certificate. Also we study the pros and cons of authorized certificate. Finally we predict the number of issued authorized certificate for the future society based on nonparametric statistical method.

Keywords: Bio-medical services, certificate, cryptology, hash function, public key.

[†] This research was supported by Catholic University of Daegu research grant in 2014.
[1] Professor, Department of Mathematical Sciences, Catholic University of Daegu, Kyungsan 38430, Korea. E-mail: dhkim@cu.ac.kr