電子商去來의 認證體系에 관한 考察

하 강 헌*

〈목 차〉

Ⅰ. 序 言

1997년 7월 1일 美國이 「지구촌 전자상거래 기본계획(A Framework for Global Electronic Commerce)」을 발표하고 EU에서 1997년 4월「전자상거래의 유럽선도(A European Initiative on Electronic Commerce)」案을 내놓고 그 해 7월「지구촌 정보네트워크(Global Information Network)」를 통한 Bonn선언을 채택한 이래, 바야흐로 전자상거래는 지구촌의 핫이슈로 등장하게 되었다.

이에 우리 정부에서도 電子去來基本法과 電子署名法을 제정하여 1999년 7월 1일부터 시행에 들어갔다. 전자적 정보매체를 통한 거래의 규모는 분석기관에 따

* 부경대학교 강사, 경제학 박사

라 다소 차이는 있지만 1998년 국내의 시장규모는 약 US$3.5억이며 2003년에는 US$96억으로, 세계적으로 1998년에 US$770억이며 2003년에는 US$1조 이상으로 폭증할 것으로 예상되고 있다.

이에 따라 향후에는 電子商去來 紛爭에 따른 商事仲裁도 급증할 것으로 예상된다. 전자상거래의 발전을 저해하는 위협 요소는 여러 가지가 있지만 이들 중 상당 부분은 본인 인증과 메시지 인증 등 認證體系로 방비할 수 있다. 이에 本稿에서는 전자상거래의 위협요소를 살펴본 후, 인증체계와 인증기관의 중요성을 論하여 장래의 商事仲裁에 대한 時事點을 제시하고자 한다.

Ⅱ. 電子商去來의 威脅要素

1. 電子商去來의 現況

電子商去來는 매우 다양하게 定義되고 있다. 많은 경우에 있어, 전자상거래는 인터넷을 통하여 제품과 서비스를 매매하는 것으로 정의되지만, 전자적 정보를 거래하는 것도 포함시키며 전자적 네트워크를 통하여 거래와 관련된 이행이나 자금이체 등도 이에 포함시킨다.[1] 電子去來基本法에서는 「'전자거래'라 함은 재화나 용역의 거래에 있어서 그 전부 또는 일부가 전자문서에 의하여 처리되는 거래를 말한다」라고 정의하고 있다.[2] 유엔 電子商去來모델法에서는 '상업적'이라는 용어의 범주에 재화나 서비스의 공급이나 교환을 위한 모든 거래를 포함시키고 있다.[3] 아무튼, 전자상거래는 인터넷[4]의 확산과 정보통신기술의 발전을 통하여 거래의 효율화 및 새로운 부가가치를 창출하는 대표적인 지식기반산업임에 틀림없

1) David Kosiur, Understanding Electronic Commerce, Microsoft Press, 1997, p.2.
2) 전자거래기본법 제2조 4항.
3) 이 개념에는 유통계약, 상사대리점, 팩토링, 리스, 건축계약, 컨설팅, 엔지니어링, 라이센싱, 투자, 금융, 뱅킹, 보험, 개발계약 또는 면허권, 합작투자 또는 다른 형태의 협조, 모든 형태의 물품이나 여객의 운송계약 등도 포함시킨다(UNCITRAL Model Law on Electronic Commerce(이하, UN 모델법) 제1조).
4) 인터넷이란 World Wide Web(www) browser라는 연결끈을 매개로한 디지털 정보의 운송메카니즘이다(Cary A. Jardin, Java Electronic Commerce Source Book, John Wiley & Sons, Inc., 1997, p.4).

다.[5]

98년 현재 한국의 전자상거래 규모는 약 3.5억불이지만[6] 2003년에는 약96억불로 급성장 할 것으로 예측되며 전세계적으로도 2003년에는 1조불 이상이 전자적 방식에 의해 거래될 것으로 분석되고 있다.[7] 향후 몇 년 내에 각 기업은 어떠한 형태로든지 電子商去來와 連繫된 방식[8]으로 기업을 經營할 것으로 예상되며,[9] 이에 따라 일반소비자도 전자상거래방식을 이용할 수밖에 없게 될 것이다. 반면에, 이렇게 갑자기 상거래 패러다임이 변화함에 따라, 안전한 거래질서를 위협하는 요소들이 곳곳에 도사리고 있다.

2. 電子商去來의 威脅要素

전자상거래를 하는 당사자는 거래상대방을 직접 볼 수 없기 때문에 상대방을 신뢰하기가 어렵다. 그러므로 상대방과의 거래내용 또한 믿을 수가 없는 것이다. 이에 따라 전자상거래시에는 네트워크상에서 상대방과 자신에 대한 신분을 확인할 수 있는 방법이 필요하며 또한 거래사실을 인증할 수 있는 신뢰할만한 제3자의 중재적 역할도 필요하게 되는 것이다. 네트워크상에서 안전(security)을 위협하는 공격의 유형은 ① 중요한 정보가 제3자에게 알려지는 機密性 (confidentiability) 공격,[10] ② 네트워크상에서 중요한 정보가 개조되는 無缺性(integrity) 공격,[11] ③

5) 産業資源部, '지식기반산업육성을 위한 전자상거래 활성화 정책방향', 99년 6월, (http://www.mocie.go.kr/new/990629~1.txt)

6) 우리 나라의 電子商去來 매출액 上位業體는 삼성인터넷몰, 한솔Csclub, 대한항공, 교보문고, 롯데인터넷백화점, 골드뱅크, 야후코리아, 아시아나항공, 유니플라자, 트윈피아 등이다. 제208회 국정감사자료, (재인용 ; 인터넷새소식, 1999년 9월 30일자 ; www.emag21.com/subscriber/mag-big.asp?catabig=B).

7) WEFA, 전자상거래 시장기획분석, 1999년 2월.

8) 기업의 전자상거래 구축은 유통이나 판매, 마케팅 및 소비자 경영과 같은 고부가가치 영역을 통합하는 기술이 필요하다. Ravi Kalakta, Andrew B.Whinston., Electronic Commerce-A Manager's Guide-, Addison-Wesley Longman, Inc., 1997, pp.25-26.

9) Intel社의 앤디 글로브회장은 앞으로 5년안에 인터넷과 연계되지 못한 기업은 도태될 것이라고 말한다. LA Times 99. 5. 22일자(재인용 ; 산업자원부, 전게보고서).

10) 가령, 카드 번호가 제3자에게 알려져 부정사용되는 경우.

11) 가령, 전자결제시 수신계좌가 개조되는 경우. S/W 공급자(Software Server)는 자신의 데이터가 접속자나 해커에 의해 개조되는 위험을 지니고 있다. Ravi Kalakota, Andrew B. Whinston, Frontiers of Electronic Commerce, Addison-Welsley Publishing Company, Inc., 1996, p.183.

네트워크상에서 누군가로 위장하여 정보를 송신하는 認證性(authenticity) 공격,[12] ④ 전자적으로 메시지나 결제된 금액을 수령하고도 이를 수령치 아니하였다고 하는 否認(repudiation) 공격[13] 등이 주류를 이룬다.[14] 특히 인터넷에서는 타인의 정보에 접근할 기회가 사설망으로 구성된 컴퓨터망에 비해 훨씬 많고 그 방법도 다양하다.[15] 이러한 위험을 제거하기 위하여 암호기술을 이용한 디지털 서명과 같은 인증방식이 사용되고 있다. 그렇다고 하여 전자상거래 당사자의 불안요소가 모두 제거되는 것은 아니다.[16] 전자상거래당사자는 보안체계의 기술적인 면을 잘 이해할 수 없을 뿐만 아니라 전적으로 신뢰할 수는 없기 때문에[17] 누군가 믿을 만한 기관이 당해 거래를 인증하고 보장해 주길 원한다. 그러므로 認證機關의 역할은 매우 중요하며, 공신력 있는 인증기관이 제 역할을 수행할 때 전자상거래의 급속한 발전은 가능할 것이다. 국제전자상거래의 활성화를 위해서는 國際認證制의 도입이 절실히 필요하다.[18]

12) 가령, 전자결제시 명망있는 기업으로 가장하여 대금을 가로채는 경우.
13) 가령, 배송된 상품을 수령하고도 부인하는 경우.
14) Andrew B.Whinston, Dale O. Stahl, Soon-Yong Choi, The Economics of Electronic Commerce, Macmillan Technical Publishing, Indianapolis, Indiana, 1997, pp.46-47.
15) 송유진 外, 전자상거래가 세상을 바꾼다, i포스트, 1999, p.133.
16) 인터넷 자체가 단순하면서도 공개적으로 데이터를 전송하도록 고안되었기 때문에 인터넷망 자체는 데이커의 가로채기나 정보의 개조를 방지할 수 있는 시스템은 아니다. website를 威脅하는 要素로는 ① 외부적 위협, ② 내부적 위협, ③ 물리적 위협, ④ 데이터관련 위협 등이 있다(Martin Nemzow, Building Cyberstores-Installation, Transaction Processing, and Management-, McGraw-Hill, 1997, pp.295-296).
비록 Business to Consumer(기업 對 소비자) 거래에서의 조사이긴 하지만 한국소비자보호원의 조사결과 쇼핑몰에서 상품을 구입한 사람 중 15%가 피해를 입었다. 그 중 47%가 쇼핑몰사이트의 광고와 다른 상품을 받았으며, 피해를 입지 않은 소비자도 상당수불만을 가지고 있다('전자상거래 사기조심', 한국경제신문, 1999년 9월 30일자).
17) 국내전산망의 보안체계는 매우 허술한 것으로 평가되고 있다. "허술한 패스워드… 문열린 집", 문화일보, 1999년 9월 21일자. 대표적인 대칭키 암호방식인 DES방식이 2년전 해독방법이 알려졌으며 또한 대표적인 비대칭키 암호방식인 RSA방식도 2000년으로 특허시효가 종료된다. '암호전쟁', 조선일보, 1999년 9월 8일자.
18) 전자상거래 '국제인증제' 시급, 내외경제신문, 1999년 9월 11일자.

Ⅲ. 電子認證시스템

1. 電子認證의 意義

전자상거래에는 많은 위협요소가 내재되어 있다. 전자상거래 당사자는 정보시스템을 통해서 정보교환을 하고 있는 상대는 누구인지, 자신이 전송한 자료나 정보는 상대방에게 정확히 전달되었는지, 자신이 전송한 정보는 자신이 전달하고자 하였던 상대에게 전달되었는지, 혹시 제3자가 불법적으로 자신의 정보를 수정하지나 않았는지 불안해하지 않을 수 없다. 수신자가 수령한 내용의 위조 또는 삭제 여부와 상대방의 신분을 확인하는 방법이 電子的 認證이다. 前者의 인증을 메시지 認證 (message authentication), 後者의 인증을 本人認證 (entity authentication)이라 한다.[19] '認證'이라 함은 전자서명검정키가 자연인 또는 법인이 소유하는 전자서명키에 합치한다는 사실을 確認·證明하는 행위를 말한다.[20] 이러한 인증을 수행하는 데에는 암호기술을 이용한 디지털 서명이 효과적이다.[21] 비록 電子認證은 전자상거래의 보완수단으로 호평 받고 있지만 기술적인 면이나 실제 이용하는 측면에서는 初期段階를 벗어나지 못하고 있다.[22]

2. 暗號시스템

(1) 意義와 目的

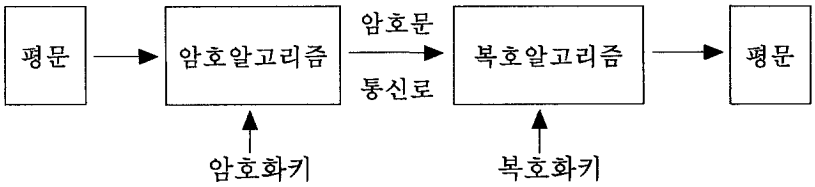
네트워크로 연결되어 있는 거래데이터는 일정한 프로그램을 사용한다면 누구나 판독할 수 있는 형태로 구성되어 있기 때문에 제3자가 데이터를 가로채거나 내용

19) 이만영 外, 전자상거래보안기술, 생능출판사, 1998, p.21.
20) 電子署名法 제2조 제6항.
21) Thomas F.Rebel, Wolfgang Koening., "Key Issues in Ensuring Security and Trust in Electronic Commerce" ; Edited by Jae Kyu Lee, Steven H. Kim, Andrew B. Whinston, Beat Schimid, Proceedings of The International Conference on Electronic Commerce '98, International Center for Electronic Commerce(http://icec.net), 1998, pp.327-328.
22) 최경진, 전자상거래와 법, 현실과 미래, 1998, p.156 참조.

을 변경할 가능성도 있다. 그러한 제3자의 접근을 통제하거나 또는 電子商去來 환경의 安全性을 보장하는 수단으로서 暗號化시스템은 必須的인 요소이다.

暗號(cryptography)란 메시지를 제3자가 해독 불가능한 형태로 변형하거나 암호화된 통신문을 해독 가능한 형태로 변환하기 위한 원리, 수단, 방법[23] 등을 취급하는 기술을 말한다. 암호화시스템은 평문(plain text)을 제3자가 이해할 수 없는 암호문(cipher text)으로 변환하는 暗號化(encryption)단계와 암호문을 정당한 수신자가 정당한 절차를 통해 본래의 평문으로 바꾸는 復號化(decryption)단계로 구성된다.[24] 이때 부당한 제3자[25]가 다른 수단을 통해 암호문을 평문으로 구하는 것을 解讀(cryptanalysis)이라고 하는데 암호기술은 이 해독의 위험으로

부터 벗어나야만 그 고유의 기능을 수행할 수 있다.



메시지에 대한 인증은 데이터의 무결성(integrity) 보장 및 상대방의 부인방지(non-repudiation) 등의 효과가 있다. 否認防止를 목적으로 하는 경우에 훗날 紛爭 發生시 證據的 效力을 갖춘 法的 文書의 역할을 하게 된다.[26]

(2) 暗號方式

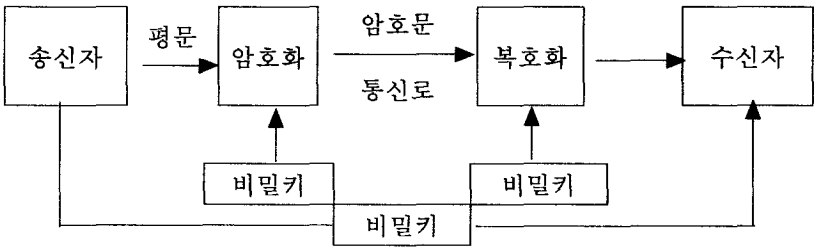
데이터를 暗號化하는 方式은 크게 대칭키 암호방식(symmetric crypto-systems)라 비대칭키 암호방식(asymmetric crypto-systems)로 구분한다. 대칭키 암호방식은 암호화하는 키와 복호화하는 키가 동일하기 때문에 대칭키 암호방식이라고 하는데 이 방식은 키가 동일하므로 만큼 암호화, 복호화키가 모두 비밀키

23) 이를 암호 알고리즘(algorithm)이라 한다.
24) Ravi Kalakota, Andrew B. Whinston, 'Electronic Commerce', op. cit., p.138.
25) 정당한 복호화키를 소지하지 아니한 자. 이를 해독자(hacker)라 한다.
26) Benjamin Wright, The Law of Electronic Commerce, 2nd edition, Aspen law & Business, Inc., 1996, §8.4-§8.5 참조.

로 구성된다. 그래서 이를 비밀키(private key) 암호방식이라고도 한다. 비대칭키 암호방식에선 공개된 키가 암호화 또는 복호화 기능을 수행하게 되므로 공개키(public key) 암호방식이라고도 한다.[27]

① 秘密키 암호방식

데이터를 암호화, 복호화하는 키가 모두 비밀키(공통키, 대칭키)로 동일한 암호방식이다.[28] 이 방식은 1970년대 초부터 상업적인 통신망에서 이용되어 있다. 그러나 이 방식은 송신자와 수신자가 동일한 키를 사용하기 때문에 키를 안전하게 전송하거나 키가 너무 많기 때문에 보관하는데 있어 문제점[29]을 드러내기 시작하였다.[30] 비밀키 암호알고리즘은 DES방식이 많이 사용된다.[31]



② 公開키 암호방식

공개키 암호방식은 개인이 소지한 비밀키와 일반에 공개된 공개키가 이용되는 방식이다. 이 방식은 데이터 송·수신자간에 다른 암호키를 사용하므로 수신자가

27) Peter Wayner, Digital Cash Commerce on the Net, AP Professional, 1996, p.19.

28) 최초로 상업적으로 이용된 공통키 암호방식은 DES(Data Encryption Standard)이다. DES는 1974년 미국 상무성으로부터의 공식적인 요청에 따라 IBM이 개발하였고, 1977년에 미국 연방 표준으로 채택되었다. M.E. Smid, D.K. Baranstad, "The Data Encryption Standard : Past and Future", Proceedings of the IEEE(Vol. 76), 1988.5, pp.550-559(재인용 ; 최경진, 전게서, 1998, pp.216-217).

29) 가령, 100명이 통신하는 경우 각자가 모두 비밀키를 가지고 있으므로 100x99x1/2=4,950개의 키가 필요해진다.

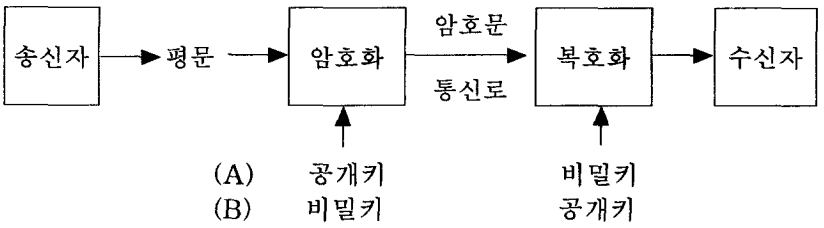
30) 전자상거래에서 비밀키 암호방식이 주도적 역할을 하기는 어렵다. Ravi Kalakota, Andrew B. Whinston, 'Electronic Commerce', op. cit., p.139.

31) 비밀키 방식의 암호알고리즘으로는 DES, FEAL, RC5, IDEA 등이 있다. 이 중 DES (Data Encryption Standard)방식이 가장 많이 사용된다. 이민섭, 현대암호학, 교우사, 1999, pp.144-146 참조. DES방식도 2년전 해독방법이 알려졌다(앞의 註17 참조).

송신자에게 비밀키를 분배하지 않아도 되며, 자신의 공개키만 공개하면 되므로 편리하다. 이 방식은 공개된 키가 암호화 기능을 수행하는 경우(A)와 복호화 기능을 수행하는 경우(B)로 구분된다.[32]

ⓐ 공개키의 暗號化 기능

송신자는 공개키로써 문서를 암호화하고 비밀키는 수신자는 소지하고 있는 비밀키로써 암호문서를 평문으로 복호화 한다(A).



ⓑ 공개키의 復號化 기능

송신자는 암호화할 때 자신의 비밀키로써 암호화하고 수신자는 공개된 공개키로써 복호화하는 방식을 말한다.

공개키 암호방식은 비밀키만 안전하게 유지하면 되므로 키관리가 비밀키 방식보다 훨씬 간편[33]한 이점이 있다.[34] 공개키 방식의 암호알고리즘으로는 RSA방식이 많이 사용된다.[35] 하지만 암호화속도가 비밀키 방식보다 떨어지는 단점이 있다. 秘密키 암호방식과 公開키 암호방식을 比較하면 다음과 같다.[36]

32) Ravi Kalakota, Andrew B. Whinston, 'Electronic Commerce', op. cit., p.139.

33) 가령 100명이 통신하는 경우 100개의 공개키와 100개의 비밀키만 필요해 진다.

34) 공개키 방식은 특히 디지털 서명에 많이 활용된다(Ravi Kalakota, Andrew B. Whinston, 'Electronic Commerce', op. cit., p.140).

35) 공개키 방식의 암호알고리즘으로 RSA, RABIN, ElGalmal 등이 사용되고 있다. 공개키 방식의 RSA, 비밀키 방식의 DES, IDEA방식이 오늘날 시장에서 가장 좋은 암호알고리즘(Peter Wayner, Digital Cash 2nd Edition-Commerce on the net, Academic Press Limited, 1997, p.261)이라고 평가된다. RSA는 암호방식은 매우 큰 정수의 소인수분해가 어렵다는 가정하에서 설계된 암호체계이며, ElGalmal 암호방식은 이산대수문제를 이용한 암호방식이다(Peter Wayer, 'Digital Cash Commerce…', op. cit., p.25).

36) Ravi Kalakota, Andrew B. Whinston, 'Electronic Commerce', op. cit., p.141 참조 수정작성.

비밀키 암호방식과 공개키 암호방식의 비교

구 분	비밀키 암호방식	공개키 암호방식
키의 관계	암호화 키 = 복호화 키	암호화 키≠ 복호화 키
키의 수	단일키	복수키(Pair of Keys)
키의 유형	비밀키	비밀키, 공개키 한개
키의 관리	키관리 복잡	디지털 인증서와 제3의 신뢰자(인증기관) 필요
키의 전송	필요	불필요
관리대상키의 수	많음	적음
인증·서명의 용이성	곤란	용이
암호화 속도	빠름	늦음
대표적인 암호	DES	RSA, ElGalmal 등

부가가치통신망(VAN : Value Added Network)을 이용한 EDI문서의 송·수신에는 송신자의 암호화키와 수신자의 복호화키가 대부분 동일하다.[37] 국제간의 전자상거래를 증진시키기 위해서는 글로벌 정보 인프라체제를 구축과 함께 국제적인 비즈니스 공동체에게 암호키의 위탁 관리를 시켜야 할 것이다.[38]

3. 電子署名

(1) 電子署名의 定義

전자상거래의 위협요소나 詐欺(fraud)로부터 벗어나기 위한 방법으로는 전자서명[39]이 효과적이다. 전자서명과 디지털서명의 개념이 혼동되고 있다. 유엔 전자서명법 초안에서는 電子署名을 「데이터 메시지에 부가되거나 논리적으로 결합된 전자적 형태의 서명 또는 자료로서 사람의 신원을 확인하고 데이터 메시지의 내

37) Phyllis K. Sokol, From EDI to Electronic Commerce - A Business Initiative-, McGraw-Hill, Inc, 1995, pp.107-108.

38) Dorothy E. Denning, "International Encryption Policy", edited by Ravi Kalakota, A. B. Whinston., Reading In Electronic Commerce, Addison Wesley Longman, Inc., 1997, p.116.

39) 전자인감이라고도 한다(송유진 外 共譯, 현대암호, 생능출판사, 1999, p.7).

용에 대한 그 당사자의 승인을 나타낼 목적으로 사용된 것」[40]이라고 정의하고, 디지털 署名은「어떤 당사자가 변환되지 않은 원래의 데이터와 함께 서명인의 공개키에 대응하는 비밀키로 변환 되었는 지의 여부 및 원래의 데이터 메시지가 변환 된 후 변형 되었는 지의 여부를 정확하게 결정할 수 있는 서명인의 공개키를 갖는 비대칭 암호방식과 메시지 압축함수를 이용하여 데이터 메시지를 변환하는 전자서명의 한 유형」[41]이라고 보고 있다.

한국 전자서명법에서는 電子署名이란「전자문서를 작성한 자의 신원과 전자서명의 변경여부를 확인할 수 있도록 비대칭키 암호화방식을 이용하여 전자서명 생성키로 생성한 정보로써 당해 문서에 고유한 것을 말한다」[42]라고 정의하고 있다. 유엔초안에서는 디지털 서명은 전자서명의 일종으로서 비대칭키 암호화방식이라고 보는 반면, 한국 전자서명법에서는 전자서명 자체를 비대칭키 암호화방식에 의한 것으로 보고 있어 약간의 차이가 있다. 이는 전자서명의 암호화 방식으로 대칭키 방식은 사용되지 않기 때문이다. 따라서 전자서명과 디지털 서명[43]의 개념을 사실상 同一한 개념으로 이해하여도 별다른 무리는 없다.

(2) 電子署名의 機能과 效果

전자상거래에서 가장 중요한 점은 데이터의 무결성을 확보하고, 사용자를 인증할 수 있어야 하는 것이다. 이를 해결하기 위한 기술적 대책[44]이 디지털 서명인 것이다. 전자거래기본법에서는 '電子署名'의 定義를「전자문서를 작성한 작성자의 신원과 당해 전자문서가 그 작성자에 의하여 작성되었음을 나타내는 전자적 형태의 서명을 말한다」[45]라고 정의하고 있어, 전자서명은 본인인증과 메시지인증 기

40) UN전자서명법초안 제1조 b.
41) UN전자서명법초안 제4호.
42) 전자서명법 제2조 제2항.
43) 디지털서명은 최근에 개발되었지만 문서(메시지)의 인증과 당사자의 부인방지에 있어서 보다 효과적인 기능을 수행한다. Ravi Kalakota, andrew B. Whinston, 'Frontiers of Electronic Commerce', op. cit., p.202.
44) 기술적 대책은 암호화시스템을 이용한 전자서명(디지털서명)이 효과적이지만 제도적 대책은 후술할 認證機關制度가 효과적이다. 디지털서명은 거래당사자 자신이 인터넷상에서 전자적으로 인증행위를 하는 것이며, 認證書는 인증기관으로부터 전자 운전면허를 발급받는 것이다. 국제전자상거래에서는 인증서를 판독하지 못하는 言語問題가 대두된다(David Kosiur, op. cit., p.39).

능을 수행한다는 것을 알 수 있다.

비밀키를 보유한 일방당사자는 그 비밀키에 대응하는 복호화키를 공개한 후 비밀키를 이용해서 디지털 서명을 한 문서를 상대방에게 보내면 이 계약서를 수령한 상대방은 공개키를 이용해서 디지털 서명의 확인과정을 거친 후 문서를 신뢰하게 되는 것이다.[46] 이때 디지털 서명이 본인의 것임을 확인시켜주는 역할은 인증기관이 수행하게 되는 것이다.[47] 그런데 대리인이 디지털 서명을 한 경우 효력이 있는지의 여부가 문제된다. 電子的 代理人에 의한 署名의 效力에 관하여, 유엔 電子署名法 草案 제6조에서는 전자적 대리인에 의한 전자서명의 유효성을 인정하는 것으로 검토하고 있다.[48] 美國 統一商法典에서도 전자적 대리인에 의해서 전자서명이 유효하게 작성되며, 계약이 유효하게 성립하는 것으로 보고 있다.[49] 한국 전자서명법에서는 이에 관한 규정을 두고 있지 아니하다. 아무튼 대리인의 서명이라도 서명의 효력은 본인에게 귀속되는 것으로 보아야 할 것이다. 전자상거래에서는 상대방을 확인할 수 있는 수단이 제한되어 있기 때문에 매번 거래시마다 상대방을 확인하여야 한다면 전자상거래의 효과를 발휘할 수 없을 것이며[50] 또한 유엔 전자상거래 모델법에서도 이러한 취지로 규정하고 있기 때문이다.[51] 하지만 분쟁발생시 법정이나 중재원에서 디지털 서명이 증거적 효력을 부여받기 위해서는 認證機關으로부터 공개키를 배부 받는 것이 가장 좋은 방법이다.[52]

---

45) 전자거래기본법 제2조 5.

46) David Kosiur, op. cit., pp.73-74.

47) 전자상거래를 발전시키기 위해서는 인증기관의 설립이 선결요건이다. 현재는 디지털 서명을 거의 이용하고 있지 아니하다. 고작 접근관리를 위한 암호화시스템 정도가 이용될 뿐이다. 암호시스템을 이용한 디지털서명이 활성화되려면 인증기관의 존재가 필수적이다. David Kosiur, op. cit., p.75, p.251 참조.

48) UNCITRAL Working Group on Electronic Commerce(Thirty-second session), Draft Uniform Rules on Electronic Signatures, 1998.1, Remarks 45. 참조.

49) Uniform Commercial Code Part2B, Article 203, 402.

50) 윤광운 外, 전자상거래론, 삼영사, 1999, p.215 참조.

51) UNCITRAL 모델법 제13조(3) (a)에서는 "데이터 메시지가 작성인이 송신한 것인지 확인하기 위해서 수신인이 미리 합의된 방법으로 적절한 수단을 사용한 경우에 수신인은 데이터 메시지를 작성인의 것으로 보고 그에 기초하여 행동할 권한이 있다"고 규정하고 있다. 또한 同法 제13조 (5)는 "데이터 메시지가 작성인의 것이거나 작성인의 것으로 추정되어 수신인이 그러한 추정에 의하여 행동할 경우에 작성인과 수신인 간에서 수신인은 데이터 메시지가 작성인의 의도대로 수신되었음을 추정할 수 있고, 그러한 추정에 기하여 행동할 권리를 갖는다"고 규정하고 있다.

52) 인증기관을 통하여 공개키를 배정받은 사용자가 행한 디지털서명은 증거적 효력이 보다 확실하다(David Kosiur, op. cit., pp.76-77). 그는 Verisign, Cybertrust, Nortel 등

(3) 電子署名의 方式

디지털서명에는 공개키 서명방식을 이용하고 있으며 대표적인 것이 RSA서명방식이다.[53]

① RSA 署名方式

디지털 서명에는 암호알고리즘(RSA)과 함께 메시지를 압축(digest)시키기 위하여 해쉬함수(hash function)를 이용한다. RSA[54] 서명방식에서 공개키와 비밀키를 생성하는 과정은 RSA 암호방식과 같다.[55] 서명자는 메시지와 그 메시지에 대한 서명을 검정자(수신인)에게 전송하면 검정자는 서명자의 공개키를 사용하여 전송받은 메시지와 검증자가 그 공개키로서 검증한 메시지가 같으면 유효한(동일한) 서명으로 판정한다.[56]

메시지를 압축시키기 위하여는 해수함수를 사용한다. 임의의 길이를 가진 메시지라도 해쉬함수를 사용하면 초기값에 대하여 換字와 轉置를 반복하여 일정 길이로 압축된 해쉬값을 구할 수 있다.[57] 즉 메시지가 압축되는 것이다. 이러한 해쉬함수로는 MD5, SHA 등이 많이 사용되고 있다.[58]

RSA 署名方式을 살펴보면,[59]

이 발급한 디지털 인증서를 예로 들고 있다.

53) Peter Wayner, Digital Cash 2nd edition, op. cit., p.16.

54) 개발자인 Ronald Rivest, Adi Shamir, Leonard Ademen의 머리글자를 따서 RSA라 부른다. RSA는 인터넷상에서 사용되는 공개 암호화 기술의 하나로서 가장 많이 이용되고 있고, 사실상의 표준이다(고명국, 인터넷과 전자상거래, 도서출판 글로벌, 1999, p.189).

55) Peter Wayner, ibid, pp.25-26 참조.

56) David Kosiur, op. cit., pp.72-73.

57) Peter Wayner, 'Digital Cash 2nd edition, op. cit., pp.35-36 참조.

58) MD5(Message Digest Algorithm5)는 MD4를 개선한 IETE(Internet Engineering Task Force) RFC(Request for Comments)의 표준이긴 하지만 충돌메시지가 발견되는 등 약간의 흠이 있다. SHA-1(Secure Hash Algorithm1)은 RIPEMD-160(Race Integrity Primitive Evalution Message Digest 160)과 함께 ISO CD(Committee Draft)의 표준이다. 1999년 개정 후 깨어지지 않는다. 암호화 방식은 송유진 外, 전게서, p.49, p.58, Peter Wayner, ibid, pp.36-39 참조.

59) David Kosiur, op. cit., pp.73-74, Figure4-4 참조 수정정리.

A사의 비밀키

↓

A사 → 평문 → 해쉬함수 → 압축문1 → 암호화(RSA) → 디지털서명 →

B사 → 디지털서명 → 복호화(RSA) → 압축문1.

↑

A사의 공개키

A사 → 평문 → B사 → 평문 → 해쉬함수 →압축문2.

이때 압축문1과 압축문2가 同一하다면 평문(원문)이 개조, 수정되지 않았을 뿐(메시지 인증)아니라 송신자가 A사임이 증명(본인 인증)되는 것이다. 한가지 問題點은 平文으로 수신자에게 송부할 때, 문서의 안전성이 완전하지 못하다는 것이다.[60]

② DSS 署名方式

DSS(Digital Signature Standard) 서명방식은 NIST(National Institute of Standards and Technology)에서 1991년에 발표한 표준 디지털서명案으로, 1994년 5월 19일 美國에서 標準으로 발표하였다. 이는 소인수분해를 바탕에 둔 공개키 방식의 암호방식을 이용하여 오직 電子署名만을 提供하는 방식이다. RSA와는 달리 암호화나 키교환에는 이용되지 않으며, RSA에 비해 수행속도가 늦다는 批判을 받고 있다.[61] 이 밖에 1985년 ElGalmal이 이산대수에 바탕을 둔 공개키 암호방식과 전자서명을 제안하였는데 키값의 안전성은 거의 완전하지만 그 활용도는 높지 않다.[62] 현재는 RSA 암호방식에 의한 RSA 서명방식의 활용도가 높으며, RSA 암호방식은 전자화폐의 보안을 위한 Blind(묵지)서명에도 활용되고 있다.[63]

---

60) 그렇다고 하여 평문 송부시 공개키 방식이 아닌 비밀키 방식을 이용하면 더 복잡한 문제가 발생한다(David Kosiur, op. cit., p.75).

61) 공개검토의 결과 검토자의 90%가 問題點이 있다고 답하였다. 또한 특허권 문제도 걸려있다. 이만영 外, 전자상거래보안기술, 前揭書, p.69 참조.

62) 암호화방식은 이만영 外, 上揭書, pp.44-46, Peter Wayner, ibid, pp.30-31 참조.

63) 전자화폐의 보안을 위해 Blind 署名方式이 활용되고 있다. 전자화폐의 거래시에는 전자화폐에 고유의 식별정보(전자화폐 데이터에 부가하는 지폐의 일련번호와 같은 정보)를 부여하여도 은행이 해독하지 못하도록 할 필요가 있다. 은행은 전자화폐에 대한 식별정보를

Ⅳ. 認證機關

1. 認證機關의 意義

전자상거래 당사자는 당해 거래의 安全性을 확보하기 위해 암호기술을 이용한 전자서명을 이용하여 문서를 전송하게 된다. 그런데 수신자는 이러한 기술적 측면에 대한 완전한 신뢰를 가지지 못하는 것이 일반적이다. 실제, 기술적으로도 완전한 신뢰를 보장할 수는 없다.[64] 이러한 전자상거래 당사자의 심리적 불안을 제거해 주는데 있어 가장 바람직한 방법이 제3의 신뢰된 기관(TTP : Trusted 3rd Party)이 당해 거래의 인증을 해주는 것이다.[65] 바로 이 기관이 認證機關(CA : Certification Authority)[66]이다. 그러나 인증기관도 해당국가의 법에 따라 인증기

모르는 상태에서 가치를 보증할 기술이 필요하다. 이러한 은행의 디지털 서명기술로는 Blind 서명기술이 가장 많은 호응을 받고 있다. 전자화폐의 사용자는 먼저, 고유의 식별정보(일련번호)를 묵지 봉투(Blind Factor)속에 넣고 은행으로 보내면 은행은 그 묵지 봉투 속의 식별정보는 모르는 상태에서 사용자가 요구한 전자화폐의 묵지봉투위에 서명을 하게 되고, 사용자는 그 전자화폐를 자신의 지급처에 보내게 된다. 이때 상대방은 묵지봉투속에 든 Blind 서명으로부터 전자화폐를 획득하게 되는데, 은행의 디지털서명으로써 그 전자화폐의 위조여부를 확인할 수 있게 된다. 즉, 전자화폐의 거래에는 사용자의 Blind 서명과 은행의 디지털서명 등 두 가지의 서명이 필요하다. 사용자가 일련번호를 생성할 때에도 RSA 암호화방식을 사용한다. Ravi Kalakota, Andrew B. Whinston, 'Forntiers of Electronic Commerce', op. cit., p.202.

64) 현재 국제적인 표준암호체계인 '512비트 암호'체계는 대용량 컴퓨터로 해독하면 1주일 내에 해독가능 하므로 더 복잡하고 난해한 암호체계의 사용이 필요하다고 미국 샌프란시스코의 컴퓨터 보안업체인 RSA社가 1999년 8월 27일 발표한 바 있다. 현재 인터넷 전자상거래의 95%이상이 '512비트 암호체계'를 사용하고 있다(내외경제신문, 1999년 8월 30일자). 우리 나라 인터넷 상점중 '침입방지시스템'을 갖춘 곳은 10개중 3개에 불과하다('인터넷 상점 보안 허술하다', 조선일보, 1999년 10월 7일자).

65) David Kosiur, op. cit., p.75.

66) 인증기관은 공개키 기반을 구조로 한다. 공개키 기반 구조(PKI, Public Key Infrastructure)는 두 가지 방식으로 구성되는데, 이는 최상위 인증기관인 Root CA에 바탕을 둔 ① 순수계층 구조방식과, 모든 인증기관이 평면적으로 구성되는 ② 네트워크 구조 방식이 있다. ①의 구조에서는 최상위 계층의 루트 CA는 전반적인 PKI 정책을 수립하고 제2계층 CA가 인증하며, 제2계층 CA는 루트CA에 의해 설정된 정책하에 자신의 정책을 수립하고, 제3계층 CA를 인증한다. 제3계층 CA는 사용자를 인증하는 구조로 형성되어 있다. 이 구조는 최상위 인증기관간의 상호인증은 허용하지만 하부의 CA간의 상호인증은 원칙적으로 배제한다. 이 방식은 루트 CA간의 상호인증을

관으로 인정된 公認認證機關과 인증기관 스스로의 신뢰를 바탕으로 인증업무[67]를 행하는 私設認證機關으로 구분하여야 할 것이다.[68] 정보통신부장관은 인증업무를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정되는 자를 공인인증기관으로 지정할 수 있는데,[69] 정부통신부 장관에 의하여 지정을 받아 인증업무를 제공하는 자가 公認認證機關이다.[70] 우리 나라는 공인인증기관제도만을 택하고 있다. 그러나 유엔 전자서명법 초안에서는 면허를 받지 못한 기관(사설 인증기관)의 경우에도 인증기관으로서의 기능을 수행할 수 있도록 규정하고 있다.[71]

2. 認證書 發給節次

먼저, 사용자(A)가 인증기관에 인증서발급을 요청하면 인증기관은 등록기관(RA ; Registration Authority)에게 인증서의 심사를 의뢰하게 된다. 이때 登錄機關은 보안확인과 여신체크 후 인증서 발행의 가부를 판정한다. 등록기관이 인증서 발행이 가능하다고 판정하면 認證機關은 자신의 디지털서명을 부가한 인증서를 발행하여 사용자에게 인증서를 발급하게 된다.[72] 그러면 사용자(A)는 자신의 비밀키로 암호화한 메시지를 전자인증서와 함께 상대방(B)에게 전송하고 상대방(B)은 (A)의 공개키로 복호화하여 메시지가 본인에 의한 것임을 확인하게 된다.[73]

통한 국제간 상호 동작을 원활하게 하는 장점이 있다. ②는 모든 CA가 평면적으로 구성되어 있으며 모든 CA간에 상호인증을 허용한다. 그러나 모든 CA간의 상호인증이 허용되면, 상호인증의 수가 대폭 증가하는 단점이 있다(이만영 外, 전자상거래보안기술, 전게서, pp.163-164).

67) 인증서의 발급 및 인증관련 기록의 관리 등 인증역무를 제공하는 업무를 말한다(전자서명법 제2조 8항).

68) 현재 인증업무를 하고 있는 I사, B사 등은 물론 미국의 Verisign社도 사설인증기관(정확히 사설인증회사)일 뿐이다. 현재 우리 나라에 공인된 인증기관은 없다. 금년 내에 공인인증기관의 지정이 있을 것으로 예상된다.

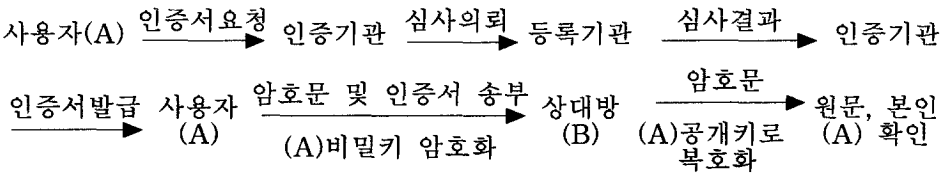
69) 전자서명법 제4조 1호.

70) 전자서명법 제2조 9항.

71) UN전자서명법 제7조 1.b.「디지털 서명을 목적으로 사용되는 암호키에 관한 인증수행을 정규업무로 하는 자 또는 단체」도 인증기관에 포함시킨다.

72) 디지털 인증서는 보통 ① 사용자의 이름, 기구(단체), 주소 ② 인증기관의 서명 및 ID 정보 ③ 사용자의 공개키 ④ 디지털 ID의 유효기일 ⑤ 인증서의 종류 ⑥ 디지털 ID의 인증서 번호 등으로 구성된다(David Kosiur, op. cit., p.76 Figure 4-5).

73) David Kosiur, op. cit., pp.74-75.



즉, 사용자는 認證機關으로부터 認證書를 발급받지만 그 인증서의 發給與否는 登錄機關에서 결정하게 된다. 사용자는 통상 사이버몰에서 영업을 하는 자이며 이를 加入者[74]라 한다. 공인인증기관은 인증업무를 개시하기 전에 한국정보보호센터[75]로부터 전자서명검정키를 인증받아야 한다.[76] 공인인증기관은 인증받은 전자서명검정키[77]에 합치하는 전자서명생성키[78]를 이용하여 인증업무를 수행하여야 한다.[79]

3. 公認認證機關의 役割

인증기관이란 認證役務를 제공하는 자를 말한다. 인증업무란 인증서의 발급 및 인증관련 기록의 관리 등 인증역무를 제공하는 업무를 말한다. 인증기관의 주요 업무는 ① 인증서 발급 ② 인증관련 기록관리로 구분할 수 있다.

---

74) 공인인증기관으로부터 그 자신의 전자서명검정키를 인정받은 자.

75) 우리 나라의 최상위 인증기관. 최상위 인증기관을 Root CA라 한다. SET認證의 경우 하부에 Brand CA(예, Visa, MasterCard, Discover, Amex 등)를 두고 있다. Peter Wayner, 'Digital Cash 2nd edition', op. cit., p.161.

76) 인증기관을 이용한 키 관리방법에 대해서는 ITU(International Telecommunication Union)라는 通信관련 國際標準機構에서 발표한 X.509 勸告案(동일한 규격이 ISO/IEC 9594-8임)이 표준이다. 이 X.509권고에는 인증기관을 계층적으로 구성하는 것이 정해져 있다. 단독의 인증기관이 지구상 모든 이용자를 인증하는 것은 불가능하므로 지역이나 응용에 따라 많은 인증기관이 존재하고 각 인증기관의 서명검증용 공개키를 상위의 인증기관에 확인하는 구조로 한다(송유진 外 공역, 현대암호, 전게서, pp.211-212).

77) 전자서명을 검증하기 위하여 이용되는 전자적 정보를 말한다(전자서명법 제2조 4).

78) 전자서명을 생성하기 위하여 이용하는 전자적 정보를 말한다(同條3).

79) Warwick Ford, Michael S. Baum., Secure Electronic Commerce, Prentice Hall PTR, 1997, pp.339-342(재인용 ; 윤광운 外, 전자상거래론, 삼영사, 1999, pp.230-231). 인증기관의 주요기능으로는 공개키의 인증, 신분(당사자)확인, 시간 날인(Time-Stamping), 증거보유(Evidence Retention), 배달매개(Delivery Intermediation), 분쟁해결 기능 등이다.

(1) 認證書

① 認證書의 發給

공인인증기관은 인증서를 발급 받고자 하는 자에게 인증서를 발급한다. 이 경우 公認認證機關은 인증서의 이용범위 및 용도 등을 고려하여 그 身元을 確認하여야 한다.[80] 공인인증기관이 인증서를 발급하는 때에는 인정받은 전자서명검증키에 합치하는 전자서명생성키를 이용하여 당해 인증서에 電子署名을 하여야 한다.[81] 인증서를 발급할 때 공인인증기관은 인증서의 이용범위 및 용도, 이용된 기술의 안전과 신뢰성 등을 고려하여 인증서의 有效期間[82]을 정하여야 한다.[83]

② 認證書의 效力

認證書의 效力이 消滅되는 경우로는[84] 첫째, 인증서의 유효기간이 경과한 경우 둘째, 그 인증서를 발급한 공인 인증기관의 지정이 취소된 경우[85] 셋째, 가입자 또는 그 대리인이 인증서의 효력 정지를 요청한 경우[86] 넷째, 인증서의 폐지사유가 발생한 경우[87] 다섯째, 한국정보보호센터가 공인인증기관에게 발급한 인증서가 폐지된 경우 등이다. 이러한 사유가 발생하지 아니하는 한 공인인증기관으로

80) 전자서명법 제15조 ①.
81) 同條. ③.
82) ITU는 인증서에 대한 기본 형식을 정하고 있는데 이를 X.509형식이라 한다. X.509는 1988년 발표된 이래 현재 X.509 v3에 이르고 있다. 주요 구성형식은 X.509의 버전, 일련번호, 인증기관 서명문, 발급자 이름, 유효기관, 인증서 소유자 이름, 공개키 정보, 발급자 서명 등인데, v3에서는 키 및 정책확장자, 발급자와 소유자에 대한 속성정보, 인증서 경로규제 정보 등의 표준확장자 영역을 도입하고 있다. 이만영 外, 전자상거래 보안기술, 전게서, pp.173-176 참조.
83) 同條. ⑤.
84) 전자서명법 제16조.
85) 공인인증기관의 지정이 취소되는 경우로는 허위 기타 부정한 방법으로 공인인증기관으로 지정된 경우, 정지명령을 받고도 인증업무를 정지하지 아니한 경우, 공인인증기관으로 지정 받고도 6개월 이내에 인증업무를 개시하지 아니하거나 인증업무를 休止한 경우 등이다. 同法 제12조 제1항 참조.
86) 인증서 효력회복 신청은 효력이 정지된 날로부터 6月 이내에 하여야 한다. 동법 제17조 참조.
87) 인증서의 폐지사유는 ① 가입자 또는 대리인이 인증서의 폐지를 신청한 경우, ② 사기 또는 기타 부정한 방법으로 인증서를 발급 받은 경우, ③ 가입자의 전자서명생성키가 분실·훼손 또는 도난, 유출된 사실을 공인인증기관이 인지한 경우 등이다. 이때 공인인증기관은 인증서를 폐지하여야 한다. 동법 제18조 참조.

부터 발급된 인증서는 有效期間까지 그 효력이 유지된다.

③ 認證業務에 관한 記錄의 管理

공인인증기관은 가입자의 인증서와 인증업무에 관한 기록을 안전하게 보관, 관리하여야 하며 가입자인증서 등을 당해 인증서의 효력이 消滅된 날로부터 10년 동안 保管하여야 한다.[88]

4. 公認認證機關의 推進現況

우리 나라는 1999년 7월 1일부터 전자서명법이 시행[89]됨에 따라 공인인증기관의 지정을 추진하고 있다. 몇 몇 회사가 행하고 있는 인증은 공인인증은 아니다. 현재 美國의 Versign社는 각국에 자신의 2차 CA를 두고 활발히 인증기관으로서의 역할을 하고 있다. 하지만 이 또한 사설 인증기관일 뿐이다.[90] 하지만 공인인증기관이 없는 상황에서 이러한 인증회사의 신뢰마저 부가하지 아니한다면 이는 더욱 전자상거래의 위험을 안고 거래할 뿐이다.[91] 美國은 몇 개 州를 제외하고는 공인(License)제도를 채택하지 않고 있다.[92] 유엔 전자서명법 초안에서도 私設認證機關을 포용하고 있다.[93] 日本에서는 2001년 4월 이전에 전자인증제도를 시행할 방침이다. 일본 법무, 통산, 우정성은 전자상거래 활성화 방안의 하나로 전자인증제도를 공동 입안하고 있는데 관련법안은 내년 정기의회에 상정될 예정이다.[94] 英國에서도 97년 통상부가 발표한 "전자인증서비스 제공을 위한 신뢰받는 제3기관의 허가"라는 자문보고서를 통해 전자인증 관련 입법을 추진하고 있다.[95]

88) 동법 제22조.

89) 우리 나라는 세계에서 6번째로 전자서명법을 갖춘 국가가 되었다. 전자신문, 1999. 7. 13일자.

90) Verisign社외에도 IBM, Intel社 등이 디지털 인증사업을 추진하고 있다. 2000년 인증시장규모(S/W 및 인증서비스)는 US$9,200만불로 전망된다. 전자신문, 1998년 7월 13일자).

91) SETCo, Verisign, CyberTrust, Nortel 등이 私設認證機關으로 활동하고 있지만 전자인증서의 배부와 검정업무는 아직 초기단계를 벗어나지 못하고 있다. 또한 이들 인증기관도 국가간에는 상호운영되지는 못하고 있다(David Kosiur, op. cit., pp.250-251).

92) 유타, 캘리포니아, 플로리다州 등을 제외하고는 공인인증기관에 관한 입법활동이 거의 없다. Benjamin Wright, op. cit., § 16·7·3 참조.

93) UN전자서명법 초안 제7조. 1·b 참조.

94) 일본경제신문, 1999년 8월 4일자(재인용 ; 내외경제신문 1999년 8월 5일자).

우리 나라는 공인인증기관의 지정요건을 자본금 100억 이상, 50억 이상의 시설투자, 20여명의 전문인력 확보 등 엄격한 자격요건을 두고 있으며 공인 인증기관으로 등록되기 위해서는 6개월 이상의 서류심사 및 기술심사를 거쳐 정보통신부장관의 허가를 받아야 한다.[96] 最上位 認證機關인 한국인증관리센터는 이미 1999년 7월 7일 개원되어 있는 상태이다.[97] 우리 나라 공인인증기관의 인증서비스는 내년 초에나 시행될 것으로 예상된다.[98]

우리 나라에서 공인인증기관의 인증서비스가 개시되면 SET Co,[99] GTE[100] 등 민간 인증기관과의 치열한 경쟁이 예상된다. 이러한 인증기관의 기능이 국제 전자상거래에서 그 역할을 다하려면 國際的인 公認認證機關이 설립되어야 한다.[101] 그러나 현실적으로 국제공인인증기관을 설립하는 데에는 어려움이 있으므로[102] 우선은 정부간 兩者協定(bilateral agreement)을 통하여 주요 교역국과 국가간 相互認證體系를 갖추도록 노력해야 할 것이다.[103]

---

95) www.new.nca.or.kr/data/trend/1998/5-13/f2.html.

96) 이는 인증사고 발생시 배상책임을 질 수 있어야 하기 때문이다(전자신문, 1999년 4월 12일자).

97) 同 新聞. 1999. 7. 13일자.

98) 同 신문, 1999. 6. 15일자. 가장 준비가 활발한 기업은 한국정보인증(주)이다. 법인설립절차를 마치고 공인 CA등록을 10월경 할 예정이다. 同 신문 1999. 7. 13일자.

99) SET(Secure Electronic Transaction) Co는 Visa와 Master Card가 네트워크(인터넷 포함)상에서 신용카드 결제시 공개키 기반구조(PKI)하에 인증업무를 수행한다. 상인의 인증을 위한 MCA(Merchant Certificate authority), 결제 인증을 위한 PCA (Payment gateway Certificate Authority) 등의 인증기관이 있다. Peter Wayner, 'Digital Cash 2nd edition', op. cit., p.159, pp.161-162 참조.

100) GTE(Global Trust Enterprise)는 설립 추진중인 세계적인 超大型 認證會社이다. Abn-Amoro, Bankers Trust, Barclay Bank, City Bank, Deutsch Bank 등이 향후 5년간 140개 은행, 자본금 3조달러 확보계획을 수립하고 설립추진 중이다. GTE가 설립되면 Verisign과 같은 작은회사들은 유인력을 상실할 전망이다(www.crosscert.co.kr/rep-subo3.ntml)

101) 國際電子商去來를 활성화시키기 위해서는 國際暗號標準과 協定을 바탕으로 국제비즈니스 공동체가 키 위탁관리에 참여하여야 한다. Dorothy E. Denning, op. cit., pp.115-116 참조.

102) UN, EU, OECD 등에서도 모델법이나 가이드라인을 제시하고 있는 정도이다. www.new.nca.or.kr/data/trend/1998/5-13/£2.html 참조.

103) 전자서명법 제27조에서는 정부가 전자서명의 상호인정을 위하여 외국정부와 협정을 체결할 수 있도록 규정하고 있으며, 상호인증협정이 체결되는 경우에는 外國의 認證機關 또는 외국의 승인기관이 발급한 증명서에 대하여 공인인증기관이 발급한 인증서와 同一한 법적 지위 또는 法的 效力을 부여할 수 있도록 규정하고 있다.
정보통신부와 일본우정성은 2000년 1월부터 한·일 양국간 전자상거래를 시범 실시

끝으로, 전자상거래의 인증체계가 완전하지 못한 사정하에서, 전자상거래당사자는 매매계약체결시 훗날에 있지도 모를 분쟁해결을 위하여 契約書상에 仲裁條項을 挿入하여야 할 것이다.[104] 중재조항을 삽입하지 아니한다면 분쟁해결을 위해 訴訟을 해야하는 불편이 뒤따르게 된다.[105] 이는 특히 기업간 전자상거래에서 중요하다.

V. 結 言

전자상거래가 全지구촌의 화제가 되고 있다. 안전한 電子商去來를 위해서는 공개키 暗號시스템을 바탕으로 한 電子署名 방식과 인증기관에 의한 認證書 발급제도가 前提되어야 한다. 공인인증제도의 도입은 전자상거래의 발전을 가속화시킬 것이다. 이러한 認證體系가 갖추어지지 아니하거나 또는 이런 방식을 이용하지 않고 전자상거래를 한다면 전자상거래상의 紛爭은 急增할 수밖에 없다.

전자서명에는 공개키 방식의 암호기술을 이용한 RSA방식이 많이 사용될 것이다. 대금결제와 관련하여서는 Blind서명을 함께 사용하는 것이 효과적일 것이다. 물론, 인증체계와 제도를 이용한다고 하여도 새로운 상거래 패러디임은 많은 분쟁을 유발할 것으로 예상된다.

우리 나라에서 내년에 公認認證機關이 인증서비스를 시작하는 것은 상당히 고무적이다. 우리 나라의 認證機關構造는 X.509勸告에 기초한 純粹階層構造가 바람직하며, 認證書 形式도 이를 기초로 하여야 한다. 공인인증기관의 등장으로 국내

키로 5월 14일 합의하였고, 전자상거래 인증 및 결제시스템을 연내에 구축하기로 하였다. 내외경제신문, 1999년 5월 15일자.

104) 전자상거래의 인증체계가 완전하다고 하더라도 모든 상거래시에는 분쟁이 발생하기 마련이다. 紛爭이 發生한 경우, 당사자간에 자주적으로 해결이 되지 않으면 第3者에 의한 解決을 추진하는데, 일반적으로 소송보다는 商事仲裁方式이 상거래 당사자에게 選好되고 있다. 한주섭외, 국제상사중재론, 동성사, 1997, pp.27-32 참조.

105) 분쟁이 발생한 후 당사자간 합의에 의해 仲裁付託을 할 수도 있지만, 분쟁이 발생한 후 중재계약을 체결한다는 것은 일반적으로 불가능에 가까우므로(강이수, 국제거래분쟁론, 삼영사, 1999, p.367), 事前에 계약체결시 仲裁條項(계약)을 合意하는 것이 바람직하다.

분쟁은 어느 정도 방지할 수 있으리라 기대하지만 국제 공인인증기관의 설립은 요원하므로 國際 電子商去來는 여전히 危險에 노출되어 있다. 인터넷을 주도하고 있는 미국의 인터넷 사이트 중 90%가 1년 내에 도산한다고 한다.

國際 電子商去來가 발전하기 위해서는 ① 국제적인 認證機關의 설립(2차 CA는 각 국가별로 둠) ② 국제적인 認證標準의 개발 ③ 국제간에 적용할 수 있는 電子署名法의 입법(협약의 형태라면 더욱 바람직함) 등이 시급히 필요하다. 하지만, 국제적인 공인인증체계의 구축은 단기간 내에는 불가능하다. 어쩌면 오랜 세월동안 불가능할지도 모르므로, 전자상거래 당사자는 국제적 체계를 갖춘 私設인증기관을 이용하여야 할 것이다.

政府는 공인인증기관의 국가간 연대를 위해 주요 교역국과의 兩者協定을 지속적으로 체결해 나가야 할 것이다.

전자상거래 당사자는 암호 및 전자서명 등 電子認證體系를 이해하고 거래에 임하는 것이 바람직하다. 아니면, 최소한 가상공간에서 만나는 상대방이 인증서를 가졌는지 확인하고, 인증기관을 통하여 거래하여야 할 것이다. 또한 전자상거래 당사자는 훗날의 紛爭解決을 위하여 계약서상에 仲裁條項을 挿入하는 것이 바람직하다.

商事仲裁에 임하는 중재인도 향후의 분쟁은 전자상거래의 認證과 관련된 분쟁이 증가할 것으로 예상되는 바, 암호 및 서명인증체계, 인증기관의 구조와 역할 등에 관하여 충분한 理解와 對備를 하는 것이 바람직하다.

ABSTRACT

A Study on the Certification System in Electromic Commerce

Kang Hun Ha

The basic requirements for conducting electronic commerce include confidentiality, integrity, authentication and authorization. Cryptographic algorithms, make possible use of powerful authentication and encryption methods. Cryptographic techniques offer essential types of services for electronic commerce : authentication, non-repudiation. The oldest form of key-based cryptography is called secret-key or symmetric encryption. Public-key systems offer some advantages. The public key pair can be rapidly distributed. We don't have to send a copy of your public key to all the respondents. Fast cryptographic algorithms for generating message digests are known as one-way hash function. In order to use public-key cryptography, we need to generate a public key and a private key. We could use e-mail to send public key to all the correspondents.

A better, trusted way of distributing public keys is to use a certification authority. A certification authority will accept our public key, along with some proof of identity, and serve as a repository of digital certificates. The digital certificate acts like an electronic driver's license. The Korea government is trying to set up the Public Key Infrastructure for certificate authorities. Both governments and the international business community must involve archiving keys with trusted third parties within a key management infrastructure. The archived keys would be managed, secured by governments under due process of law and strict accountability. It is important that all the nations continue efforts to develop an escrowed key in frastructure based on voluntary use and international standards and agreements.

참 고 문 헌

강이수, 국제거래분쟁론, 삼영사, 1999

고명국, 인터넷과 전자상거래, 도서출판 글로벌, 1999

송유진 外 共譯, 현대암호, 생능출판사, 1999

송유진 外, 전자상거래가 세상을 바꾼다, i포스트, 1999

이만영 外, 전자상거래보안기술, 생능출판사, 1998

이민섭, 현대암호학, 교우사, 1999

윤광운 外, 전자상거래론, 삼영사, 1999

최경진, 전자상거래와 법, 현실과 미래, 1998

한주섭 外, 국제상사중재론, 동성사, 1997

Andrew B. Whinston, Dale O. Stahl, Soon-Yong Choi, The Economics of Electronic Commerce, Macmillan Technical Publishing, Indianapolis, Indiana, 1997

Benjamin Wright, The Law of Electronic Commerce, 2nd edition, Aspen law & Business, Inc., 1996

Cary A. Jardin, Java Electronic Commerce Source Book, John Wiley & Sons, Inc., 1997

David Kosiur, Understanding Electronic Commerce, Microsoft Press, 1997

Dorothy E. Denning, "International Encryption Policy", edited by Ravi Kalakota, A. B. Whinston., Reading In Electronic Commerce, Addison Wesley Longman, Inc., 1997

Martin Nemzow, Building Cyberstores - Installation, Transaction Processing, and Management-, McGraw-Hill, 1997

Peter Wayner, Digital Cash 2nd Edition-Commerce on the net, Academic Press Limited, 1997

————————, Digital Cash Commerce on the Net, AP Professional, 1996

Phyllis K. Sokol, From EDI to Electronic Commerce - A Business Initiative-, McGraw-Hill, Inc., 1995

Thomas F.Rebel, Wolfgang Koening., "Key Issues in Ensuring Security and Trust in Electronic Commerce" ; edited by Jae Kyu Lee, Steven H. Kim, Andrew B. Whinston, Beat Schimid, Proceedings of The International Conference on Electronic Commerce '98, International Center for Electronic Commerce(http://icec.net), 1998

Ravi kalakota, Andrew B. Whinston, Frontiers of Electronic Commerce, Addison-Wesley Publishing Company Inc., 1996

———————————————, Electronic Commerce-A Manager's Guide, - Addison-Wesley Longman Inc., 1997

기타, 언론보도 및 Web site 자료 다수.