International Commerce and Information Review
Volume 9, Number 1, Mar. 2007: pp. 297~312
통상정보연구 제9권 1호 (2007년 3월 27일)

논문투고일자 : 2007. 02. 04
게재확정일자 : 2007. 03. 15

국제상업회의소 GUIDEC Ⅱ의 전자인증관행의 내용 검토

Electronic Authentication and Certification Practices Under GUIDEC Ⅱ

강원진(Won-Jin Kang)
부산대학교 무역국제학부 교수
장 청(Chung Jang)
부산대학교 대학원 무역학과 박사과정

목 차

Abstract

The GUIDEC Ⅰ was published in November 1997 by the International Chamber of Commerce (ICC) and then the GUIDEC was published in October 2000 in the name of GUIDEC Ⅱ. The GUIDEC Ⅱ is the next version of GUIDEC Ⅰ.

This paper examines the electronic authentication and certification practices under GUIDEC Ⅱ in detail. Therefore, this paper can help parties concerned to understand electronic authentication and certification practices of electronic commerce.

GUIDEC Ⅱ maintains the content of GUIDEC Ⅰ, but GUIDEC Ⅱ adds some new definitions such as authenticating a message and explains the rights and responsibility of subscribers, certifiers, and relying parties in detail. The aim of the GUIDEC Ⅱ is to enhance the ability of international business community to execute trustworthy digital transactions utilizing legal principles that promote reliable digital authentication and certification practice.

Key Words : GUIDEC Ⅱ, electronic commerce, electronic signature, electronic certification, authenticating a message

Ⅰ. 서 론

종이문서에 기반을 둔 상거래에서는 수기서명 또는 기명날인 방식으로 문서의 진정성 및 거래당사자의 신원을 확인하여 왔다. 그러나 인터넷을 통한 전자상거래에서는 전자서명과 전자인증을 통하여 거래의 진정성과 거래당사자의 신원을 확인하고 있다. 특히 전자상거래에서는 전자문서의 위조, 변조 및 제3자의 메시지 도용과 메시지 전송실패 등 보안위험이 발생하게 된다.

전자인증 관련 입법은 그동안 미국, 국제연합(United Nations : UN) 그리고 유럽연합(European Union : EU) 등이 선도적으로 마련되어 왔다. 한국에서도 전자서명법과 전자거래기본법을 제정하여 거래당사자들에게 전자서명과 전자인증에 대한 법적 기반을 제공하고 있다.

국제상거래관행에 대한 통일규칙을 제공하고 있는 국제상업회의소 (International Chamber of Commerce : ICC)에서는 1997년 전자서명의 사용 및 인증, 인증기관에 관한 일반적인 지침의 필요성을 감안하여 상업적 적용의 보장 및 확인을 목적으로 디지털로 보장되는 국제전자상거래의 일반관례(General Usage for International Digitally Ensured Commerce : GUIDEC Ⅰ)를 제정하였다.[1] 그 후 ICC는 새로운 개념의 보완과 적용범위의 확장을 시도하기 위하여 디지털로 보장되는 국제전자상거래의 일반관례의 개정판(General Usage for International Digitally Ensured Commerce : GUIDEC Ⅱ)[2]을 제정하였다.

전자상거래의 핵심기반이라 볼 수 있는 전자서명과 전자인증에 관한 주요국들의 법제들에 대한 연구는 활발히 이루어져 왔다. 그러나 ICC의 GUIDEC Ⅱ에 반영된 전자인증관행 내용에 대하여 검토한 선행 연구는 거의 이루어지지 아니 하였다. 오현석(2004)[3]의 연구에서는 전자무역에서 전자인증제도의 문제점을 검토하면서 국제기구별 전자인증 제도의 법률기반으로 ICC의 GUIDEC Ⅰ,Ⅱ의 기본원칙 및 의의에 대해 검토한 바 있고, 김종칠・이진우(2000)[4]의 연구에서는 전자서명 인증 제도를 비교 검토하며 국제적 법제 동향을 살피는 시각에서 GUIDEC이 검토되었다.

미국의 윌리엄(William, 2001)[5]은 GUIDEC의 법적・기술적 배경 등을 검토하며 GUIDEC의 원칙 및 발전 방향을 다루고 있으나, GUIDEC의 전자인증 관행에 대한 검토는 이루어 지지 않았다. 그러나 본 연구는 위와 같은 연구들에서 다루어 지지 않았던 GUIDEC Ⅱ상의 전자인증관행 내용을 검토한다는 점에서 차별성이 있다. 또한 국제거래당사자는 ICC가 제시하는 전자인증관행을 적절히 활용하기 위하여 GUIDEC 상의 전자인증관행 내용을 검토하여야 할 필요가 있다.

---

1) International Chamber of Commerce, General Usage For International Digitally Ensured Commerce, 1998(이하, GUIDEC Ⅰ이라 한다).

2) International Chamber of Commerce, General Usage For International Digitally Ensured Commerce, 2001(이하, GUIDEC Ⅱ라 한다).

3) 오현석, “전자무역에서 전자인증제도의 문제점에 관한 연구”, 성균관대학교 박사학위논문, 2004.

4) 김종칠・이진우, “전자상거래에서 전자서명 인증제도에 관한 비교연구”, 「국제상학」, 제15권 제1호, 한국국제상학회, 2000.

5) William F. Fox, “The International Chamber of Commerce’s GUIDEC Principles : Private-sector Rules for Digital Signature,” *International Lawyer,* 2001.

따라서 본 연구는 전자상거래에서의 위험관리를 최소화 할 수 있는 전자서명과 전자인증에 대하여 미국 등 선도국의 법제를 참조하고 ICC의 디지털로 보장되는 국제전자상거래의 일반관례의 개정판인 GUIDEC Ⅱ에서 제시되고 있는 전자인증 관행의 내용을 검토하고자 하는데 목적이 있다.

연구의 범위는 GUIDEC Ⅰ에 기초를 두어 GUIDEC Ⅱ에 반영된 전자인증 관행을 중심으로 검토하고, 미국의 E-Sign법, UNCITRAL 표준법, 유럽전자서명지침, 그리고 한국 전자서명법을 비교 검토하고자 한다. 연구방법은 GUIDEC Ⅱ상에 규정된 관행과 관련 문헌연구 및 웹사이트를 활용한다.

Ⅱ GUIDEC Ⅱ의 제정배경과 제정목적

1. GUIDEC의 제정배경

전자상거래가 널리 확산됨에 따라, 세계 여러 각국에서 전자서명 관련 입법을 마련해왔다. 미국은 1995년 유타주에서 전자서명에 관한 입법을 한 이래 50개 주에서 전자서명에 관한 법률이 제정되었다. 2000년 6월 30일 클린턴 대통령이 서명한 '전 세계 및 국내 상거래의 전자서명법'(Elctronic Signature in Golbal and National Commerce Act : E-sign Act)이 제정되고 2000년 10월 1일자로 발효되었다. 미국변호사협회(American Bar Association : ABA)는 전자서명에 대한 세계 최초의 규범이라 할 수 있는 '디지털 서명 가이드라인'(Digital Signature Guideline)을 제정하였고,[6] 미국의 여러 주 뿐만 아니라 세계 여러 나라에서도 전자상거래의 제도적 핵심 기반인 전자서명에 대한 법제를 마련하였다.

유엔국제무역법위원회(United Nations Commission on International Trade Law : UNCITRAL)는 1996년 '전자상거래에 대한 표준법'(UNCITRAL Model Law on Electronic Commerce)을 제정한 이래 전자서명에 대한 통일규칙[7] 및 전자서명에 대한 표준법[8]을 제정하였다.

EU는 1999년 12월 13일 전자서명입법지침을 채택하였다. 이 지침은 2001년 1월 19일에 공표되었으며, 2001년 7월 19일 까지 회원국들이 이를 국내법으로 수용하도록 시한을 정한 바 있다. EU의 전자서명지침은 유럽연합회원국들이 자국의 전자 서명법제를 마련하거나 개정할 경우에 따라야 할 가이드라인을 담고 있다.[9] 이에 따라 EU 회원국들은 자국의 국내법을 제정하거나 개정함으로써 유럽연합 전자서명입법지침을 시행하고 있다.[10] 한국에서도 1998년 12월에 전자서명법을 제정하였으며, 1999년에 전자거래기본법을 제정함으로써 전자상거래에 대한 법규를 마련하였다.

---

6) American Bar Association, Digital Signature Guidelines, 1996.
7) UNCITRAL Uniform Rules on Electronic Signatures, 2001.
8) UNCITRAL Model Law on Electronic Signatures, 2001.
9) 정완용, "개정 전자서명법의 비교법적 고찰", 「비교사법」 제10권 제4호, 한국비교사법학회, 2003, 2면.
10) 정완용, 상게논문, 5면.

각 나라 및 국제기관의 전자상거래에 대한 입법 활동의 흐름에 발맞추어 ICC는 1997년 11월 전자상거래 프로젝트(Electronic Commerce Project : ECP)의 후원 하에 국제전자상거래의 보호에 대한 일반 사용이라는 명제로 초판을 발간하였으며, 미국변호사협회 과학 기술 분과 정보보안 위원회(Information Security Committee : ISC)의 디지털서명 가이드라인[11]을 기초로 GUIDEC Ⅰ을 제정하게 되었다.[12]

GUIDEC Ⅰ은 전자상거래에 관한 중요 사항을 모아 용어의 사용기준을 제시하고 관련문제들의 배경을 설명하고 있다. 세계적으로 널리 이용되는 공개키 암호화(Public Key Cryptography)기법에 대한 이해를 높이고, 서로 다른 법적 전통을 조화시키기 위해 대륙법과 영미법의 처리내용을 함께 소개하고 있다.

이 지침은 디지털 서명 장치를 통한 메시지의 보장 및 인증에 대한 일반적인 원칙들을 마련하고자 하였으며, 현존하는 법규 및 관행을 재정립하고 이들과의 조화를 시도하고 있다.[13]또한 디지털서명 기술의 국제적 활용을 위한 프레임을 제공하고 개념들을 확실히 정의함으로써 현존하는 가이드라인들을 보충하는 시도를 하였다.[14]

GUIDEC I은 최종 본문을 완성하기 위해 다수의 선행 법들을 검토한 후 선행 법을 제정한 나라들의 전문가들과 함께 GUIDEC을 전개하였고, 대부분의 중요 선행 법들과 전자상거래에 대한 UNCITRAL 표준법에 규정된 전자서명에 대한 현행 국제법상의 처리방식을 원용하고 확대한 것이다.[15]

ICC는 GUIDEC Ⅰ을 제정한 후 2001년 10월 전자상거래상의 새로운 용어 및 개념을 보완한 GUIDEC Ⅱ를 제정하게 되었다. GUIDEC Ⅱ는 GUIDEC Ⅰ을 기반으로 제정되었으며, 비즈니스 사회와 관련해 직접적인 범위로 확대하였다.[16] 상관습으로 보다 활성화된 전자계약에 대해 설명하며, UNCITRAL 표준법과 유럽연합지침과 같은 정책발전에 대한 인식의 결과로 GUIDEC Ⅱ는 신뢰할 수 있는 디지털 거래를 위하여 바이오메트릭(biometrics)[17]과 같은 추가적인 잠정기술을 포함하고 있다.

---

11) 이 가이드라인은 디지털 서명을 한 쌍의 키를 쓰는 방법, 즉 디지털 서명을 만들었는데 여기서 쓰이는 비밀키(Private Key)와 디지털 서명의 진정성을 확인하는 공개 키(Public Key)에 의한 방법을 제시하고 있다. 이 가이드라인에 따르면 적법한 디지털 서명은 통상의 서명과 동일한 효과가 있고, 디지털 서명에 첨부한 메시지가 문서성을 충족하고, 디지털 서명된 메시지의 사본은 원본으로써 유효하되, 다만 서명자가 특정한 한 개를 고유의 원본으로 할 것을 의도한 경우에는 원본만 유효하다.; ABA. op. cit. 1996.

12) 최석범, "글로벌전자무역에 관한 연구", 「국제상학」, 제14권 제1호, 한국국제상학회, 1999, 259면.

13) 강원진, "전자신용장 국제결제 인프라구축 동향과 해결과제", 「국제상학」, 제19권 제1호, 한국국제상학회, 2004, 146면.

14) Pamela N. Price, "Designing the Legal Infrastructure For Cyberspace Commerce : How much Regulation is too much?," *Suffolk University Law Review,* 1998, p.11.

15) William F. Fox, *op.cit.,* 2001. pp.4～5.

16) ICC, GUIDEC Ⅱ, Ⅰ-1.

17) 바이오메트릭스는 개인의 독특한 생체정보를 추출하여 정보화시키는 생체인식에 의한 인증방식을 말하지만 여기에서는 도판(template) 위에 서명한 것을 미리 식별용으로 만들어 놓은 서명감(specimen)과 대조함으로써 인증기관의 일부 기능을 수행하거나, 아니면 보장을 거쳐야 하는 파일에 첨부하기 위하여 만들어진 기호 열(string)을 이용하는 것을 의미 한다; GUIDEC Ⅰ, Ⅲ-5.

2. GUIDEC Ⅱ의 제정목적

GUIDEC Ⅱ의 목적은 상이한 법체계하에 존재하는 규범 및 관행에 대비하여 디지털 메시지의 인증에 대한 일반적인 틀을 제정하기 위한 것이다. GUIDEC Ⅱ는 전자인증에 관한 원칙에 대하여 상세한 설명을 제공하며, 특히 정보시스템의 보안문제와 관련해 공개키 암호화 기술과 디지털 정보의 프로세싱, 인증보호 관련 권고사항 및 간결한 표준관행을 제공하고 있다.[18]

GUIDECⅡ는 거래관행에 따른 당사자의 위험과 책임을 공평하게 분배하고 서명자, 인증기관 및 이에 의존하는 당사자들의 권리와 책임을 명확하게 기술하여 당사자의 책임한계를 제공하고 있다.[19] 이와 같이 GUIDEC Ⅱ의 목표는 신뢰할 수 있는 디지털 인증관행을 촉진하는 법적 원칙을 활용하고 신뢰할 수 있는 디지털 거래를 실행하여 국제거래사회의 역량을 강화시키는 것이다.

GUIDEC Ⅱ는 국제 상거래 규범과 관행 중에서 핵심이 되는 개념, 모범이 되는 관행, 인증에 관한 문제를 다루는데, 거래당사자들은 전통적인 상법(lex mercatoria)에 따라 행동하는 전문적인 상인이라고 가정한다. 이 보고서는 소비자를 둘러싼 거래상의 권리와 의무를 논하는 것은 아니며, 공증 원칙에 관한 언급이 있기는 하지만 보다 중요한 국가 또는 공공의 이익을 위하여 공증이나 정부의 간섭 등 보안의 강화를 요하는 거래상의 관행에 대하여 설명하는 것도 아니다.[20] 이 점에서 GUIDEC II는 공증인에게 공증을 하는 권한, 법적 능력이 있어야 하듯이 이와 관련하여 정보의 인증을 위한 규칙을 마련하려는 것이 아니라는 점을 유의하여야 한다.

또한 GUIDEC Ⅱ가 디지털서명과 같은 시스템을 기반으로 한 공개키 방식을 포함한 당사자들을 위한 아웃라인을 구성하였지만, 디지털 서명을 포함한 이외의 기술에도 적용될 것이라는 것을 의미한다.

Ⅲ. GUIDEC Ⅱ에 반영된 전자인증관행의 내용 검토

1. 메시지 진정성 확인에 대한 관행

1) 메시지의 진정성 확인의 개념

진정성(authentication)은 누가 의사표시를 하였는가에 대하여 확증할 수 있는 것으로서, 거래당사자가 서로 상대방의 신원을 확인할 수 있도록 하는 기능으로 송신자와 수신자가 합법적인 사용자임을 증명할 수 있어야 한다. 이처럼 서명자의 신원을 확인하는 것은 사용자 인증이라고 할 수 있으며, 전송된

18) *Ibid.*
19) ICC, GUIDEC Ⅱ, Ⅰ-2.
20) *Ibid.*

메시지가 위조 및 변조되지 않았음을 증명하는 것을 메시지 인증이라 한다. 메시지 인증은 무결성으로 대치될 수 있는 것으로 의사표시의 내용적 완전성에 관한 것으로, 표의자의 의사표시가 애초에 발하여진 것과 동일한 내용으로 상대방에게 도달하였는지를 확증하는 것을 말한다.[21] GUIDEC Ⅱ상에서 서명자의 신원과 메시지가 진정성 확인 후 변조되지 않았다는 증거가 있으면 메시지는 진정성이 확인되는 것으로 보고 있다.[22]

GUIDEC Ⅱ에서는 의사표시를 한 상대방의 신분을 증명할 수 있는 진정성과 전송된 메시지의 위조 및 변조가 없음을 증명하는 무결성이 확보된 메시지를 진정성이 확인된 메시지라 정의하고 있다.

2) 메시지 진정성 확인의 법적 중요성과 귀속

UNCITRAL 전자상거래에 관한 표준법 제13조의 데이터 메시지의 귀속에 대한 조항에 따르면, 데이터 메시지는 작성자 자신에 의하여 전송한 경우에는 작성자의 것이 되며, 데이터 메시지에 관련하여 작성자를 대신하여 행동할 권한을 가진 자와 작성자 또는 작성자를 대신하여 자동적으로 운영되도록 설계된 정보시스템에 의하여 송신된 경우, 데이터 메시지는 작성자의 것으로 본다.[23]

GUIDEC Ⅱ상에서 진정성이 확인된 메시지는 실제로 메시지의 진정성을 확인한 사람에게 귀속되어야 하는 것으로 보고 있다.[24] 여기서 진정성을 확인한 사람은 메시지의 서명자를 뜻한다. 한국 전자서명법 제2조 11호에 따르면, 서명자[25]란 공인인증기관으로부터 그 자신의 전자서명 검증키를 인증 받은 자를 말한다. 즉, 디지털 서명을 직접 행하는 서명자이다.[26]

진정성이 확인된 메시지를 서명자에게 귀속시킨다는 의미는 진정성이 확인된 메시지를 갖고 있는 자인 서명자가 정직하게 행동하고, 확인된 메시지를 평가하는데 있어 상당한 주의를 기울여야 한다는 것이다. 또한 진정성이 확인된 메시지가 잘못되어 있다거나 의문이 유발될 경우를 인식해야 하며, 그 사실을 통지 한다는 것을 전제로 하고 있다. 누가 실제로 메시지의 진정성을 확인하였는지를 검토함에 있어 서명자가 메시지의 진정성을 확인했다는 확신이 있어야 한다.

위조되었거나 부정하게 변경된 메시지를 실수로 귀속시킴으로써 손해를 끼치고, 그러한 위조 또는 부정한 변경이 인증장치의 보관에 대한 서명자의 소홀함이나 서명자의 과오에 기인한 것이라면 서명자는 손해를 보상하여야 한다. 예컨대, 인증기관이 발행한 인증서에 포함된 내용이 잘못된 것임을 알고도 인증기관에 대해 통지하지 않은 경우, 이로 인하여 인증서상의 잘못된 정보를 신뢰한 제3자가 손해를 입는다면 서명자는 그 신뢰당사자와 인증기관 모두에 대해서 책임을 져야 할 것이다.[27]

---

21) 강원진, “전자무역거래 활성화를 위한 전자결제시스템의 요건과 과제”, 「국제상학」, 제17권 제3호, 한국국제상학회, 2002, 114면.
22) ICC, GUIDEC Ⅱ, Ⅸ-1.
23) UNCITRAL Model Law on Electronic Commerce, 1996, Article 13.
24) ICC, GUIDEC Ⅱ, Ⅸ-2.
25) 공인인증기관에 가입한 자로, ‘가입자’라고도 한다.
26) 최준선, “전자서명과 전자인증의 제문제”, 「무역상무연구」, 제15권 제3호, 한국무역상무학회, 2001, 228면.
27) 최준선, 상게논문, 229면.

또한 서명자에 대한 귀속의 효과는 진정성이 확인된 메시지의 내용, 거래에 관한 사실 및 상황, 준거법 및 당사자간의 거래방법과 거래관행에 따라 달라짐[28]을 명시하고 있다.

3) 대리인에 의한 메시지 진정성 확인 관행

대리인이 메시지의 진정성을 확인하고, 대리인이 본인의 권한으로써 진정성을 확인 하였다고 진술하였다면, 준거법에 따라 대리인이 메시지의 진정성을 확인할 수 있는 충분한 권한을 가지며 확인된 메시지는 본인이 한 것으로 효력이 있다.[29]

일반적으로 사람들은 대리인이 표시한 대리권을 믿게 되면 스스로의 위험 부담 하에 행동한다.[30] 따라서, 진정성이 확인된 메시지를 갖고 있는 사람은 대리인의 말을 그대로 받아들일 것이 아니라 진정성 확인된 인증서 또는 대리인임을 나타내는 보다 믿을 만한 증거를 요구할 것을 강조하고 있다.

4) 메시지의 진정성 확인에 적합한 방법

서명자는 그 상황에서 가장 적합한 방법으로 메시지의 진정성을 확인하여야 한다.[31] 메시지의 진정성이 제대로 확인되지 못한다면 그 메시지는 무시될 수 있으며, 두 당사자간의 합의사항에 따라 선택된 인증방법에 따르지 않은 경우와 진정성이 확인된 메시지가 법적 효력을 발휘하지 못할 경우에도 메시지는 무시될 수 있다. 그러한 해결점으로 GUIDEC Ⅱ는 메시지의 진정성을 확인하는 가장 합리적인 방법으로 인증기관을 통하는 방식을 제시하고 있다.[32] 인증기관은 공개키와 공개키 제공자 사이의 관계의 진정성을 확인하고 공개키의 저장소 역할을 하는 신뢰할 수 있는 제3자인 것이다. 인증기관은 그 사람에게 속하는 비밀키와 공개키 한 쌍을 증명하고 서명자의 신원확인을 해야 한다.[33]

인증기관이 개입된 전자서명은 일반적으로 공개키 암호화방식을 이용하며, 공개키 암호화방식을 이용한 서명을 디지털서명이라고 한다. 디지털서명 방식은 현재까지 개발된 전자서명 방법 중에서 가장 안전하고 유력한 수단으로 인식되고 있다.

5) 진정성이 확인된 메시지의 범위

진정성이 확인된 메시지의 작성자는 무엇이 확인되고 있는지 분명히 밝혀야 한다.[34] 메시지의 진정성 확인은 메시지가 변조된 경우에는 적용되지 않으므로 진정성이 확인된 메시지의 수신인은 메시지

28) ICC, GUIDEC Ⅱ, Ⅸ-2, Commentary.
29) ICC, GUIDEC Ⅱ, Ⅸ-3.
30) ICC, GUIDEC Ⅱ, Ⅸ-3, Commentary.
31) ICC, GUIDEC Ⅱ, Ⅸ-4.
32) ICC, GUIDEC Ⅱ, Ⅸ-4, Commentary.
33) Lupton W. Evrett, "The digital signature : Your Identity by the numbers," *Richmond Journal of Law and Technology,* 1999, p.6.
34) ICC, GUIDEC Ⅱ, Ⅸ-5.

가 변조되지 않고 그대로 도달하였는지 판단하여야 한다. 이러한 판단은 메시지가 인정될 때 메시지의 범위가 명확히 정하여지고 수신이 가능할 때 이루어진다.

서명자는 진정성이 확인된 메시지를 수신 시스템이 제대로 표현할 수 있도록 법을 요구하거나 서명자와 수신인이 합의한 방법으로, 아니면 거래관행, 적용 가능한 기술표준, 또는 동종 메시지의 공통된 관행에 따른다.[35] 통상적으로 매체의 크기, 활자, 줄 간격, 여백, 이와 유사한 특성의 사소한 변형은 중요하지 않다. 그러나 메시지의 논리구조를 변화시키는 등 그 의미내용에 상당한 영향을 주는 변화는 변조로 취급될 수 있다.

6) 메시지 진정성 확인 장치의 보호 관행

어떠한 장치를 이용하여 메시지의 진정성을 확인하는 경우에는 그 장치가 무단 사용되는 것을 방지하기 위하여 최소한의 합리적인 주의를 기울여야 한다.[36]

메시지 진정성 확인 장치는 물리적으로 접근이 제한되고 주의 깊게 통제되는 장소에 보관되어야 한다. 신뢰할 수 있는 사람들과 통상적으로 진정성 확인 서비스를 이용하여야 할 필요성이 있는 사람들을 기준으로 접근을 허용해야 한다. 장치에 대한 접근이 허용되는 사람들은 비밀번호나 비밀 문구(pass phrase), 바이오메트릭 정보, 기타 안전한 방법으로 신원이 확인될 수 있어야 한다. 진정성 확인 장치에 대한 통제는 상실되었지만 구제조치가 가능한 경우, 지체 없이 구제조치를 취하여야 한다.[37]

GUIDEC Ⅱ상에서 권고하고 있는 디지털 서명 방식인 공개키 암호법은 개인키의 소유자가 안전하고 기밀하게 보관해야 한다. 이것은 하나의 비밀키를 두 사람이 보관하는 전통적인 암호해독법보다 쉽다. 그럼에도 불구하고, 비밀키의 보안이 문제이다. 예를 들어, 키가 분실되거나 손상된 경우 부득이하다.[38] 비밀키를 분실한 경우에는 공개키 인증서를 취소하거나, 이를 취소될 수 있을 때까지 즉시 그 효력을 정지시켜야 한다.

2. 인증에 대한 관행

1) 유효한 인증서의 효력

인증서는 신원이 확인된 당사자와 공개키 사이의 관계 확인으로 인증기관에 의해 발행된다.[39] 인증서는 공개키와 서명자 사이의 관계를 증명하는 전자기록이며, 서명자의 공개키를 포함하고 키의 유효

35) ICC, GUIDEC Ⅱ, Ⅸ-5 Commentary.
36) ICC, GUIDEC Ⅱ, Ⅸ-6.
37) ICC, GUIDEC Ⅱ, Ⅸ-6 Commentary.
38) Thomas J. Smedinghoff., "Electronic Contracts and Digital Signatures and Overview of Law and Legislation," *Practising Law Institute,* 1999, p.19.
39) Thomas J. Smedinghoff, *Online Law, The SPA's Legal Guide to doing busimess on the Internet,* Addison-Wisley Developers Press, 1997. p.47.

기간, 크기 또는 서명 생성 소프트웨어의 확인을 포함할 것이다.[40]

UNCITRAL 통일규칙 초안에 의하면, 인증서라 함은 인증기관이 특정키를 보유한 사람의 신원을 확인하기 위하여 발행한 데이터 메시지 기타 전자문서를 말한다. 통일규칙 초안에서는 공개키와 그 보유자를 연결시켜주는 신원인증서 및 고급인증서의 두 가지로 규정하고 있다. 나열된 인증서의 최소요건을 갖추지 못한 인증서는 무효로 간주되어야 하는지 또는 인증서에 대한 규정을 흠결보완규정으로 보아 당사자간의 합의로 요건을 갖추지 못한 인증서도 유효로 할 것인지에 대해 논의되었다. ABA의 디지털서명 가이드라인에 따르면, 인증기관은 서명자가 인증서를 출력하여 제시하거나, 서명자가 인증서 내용을 온라인상에 볼 수 있도록 허락하거나 메일과 같은 방법으로 서명자에게 인증서의 내용을 전달함으로써 인증서의 내용을 생성 통지를 할 수 있다고 정의하고 있다.[41]

전자서명법 제2조에 따르면, 인증이란 전자서명 생성정보가 가입자에게 유일하게 속한다는 사실을 확인하고 이를 증명하는 행위라고 말하고,[42] 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보를 인증서라 한다.[43] 인증서는 인터넷상에서 사용되는 신분증으로서 '신뢰할 수 있는 제3자'인 '인증기관'이 전자문서를 작성한 자가 그 본인이 맞고, 수신된 전자문서가 전송되는 과정에서 제3자에 의해서 변형되지 않았다는 것 등을 입증하기 위하여 발급해주는 증명서를 의미한다.

따라서, 인증서는 공개키가 누구의 소유라는 것을 증명하는 것으로서, 이러한 역할을 담당하는 것이 인증기관이다. 인증기관은 사용자의 신원을 철저히 확인하고 신원이 확인된 신청자에게 공개키에 관한 정보가 담긴 인증서를 발급하고 증명한다. 이에 인증기관은 자신의 비밀키로 사용자의 인증서를 전자서명함으로써 사용자 인증서의 무결성 및 기밀성 등을 보장하여 준다.[44]

GUIDEC Ⅱ상에 인증기관이 인증된 메시지가 실무관행상 필수요건을 갖추지 못하였다는 통지[45]를 받지 못한 경우에는 유효한 인증서에 기재된 사실들이 정확하게 진술되어 있으며 이를 신뢰할 수 있다고 규정하고 있다.[46] 정보의 일부가 검증되지 않았다는 사실이 인증서에 명백히 나타나 있지 않다면 인증기관은 유효한 인증서에 기재되어있는 모든 사실의 정확성을 반드시 확인하여야 한다고 규정하고 있어[47] 메시지의 수신자가 인증된 메시지를 그대로 받아들일지 아니면 그 이상의 증거를 요구할 것인지에 대해 상업적인 위험을 평가를 할 수 있게 된다.

---

40) American Bar Association, Digital Signature Guidelines, 1996.
41) *Ibid.*
42) 한국 전자서명법 제2조 제6호.
43) 한국 전자서명법 제2조 제7호.
44) 전순환, "전자서명과 인증기관에 관한 연구", 「상품학연구」, 제26호, 한국상품학회, 2002, 203면.
45) 1994년 UNIDROIT의 국제상사계약 원칙(제1.9조)에서는 통지란 선언, 요구, 요청, 기타의 의사표시를 포함한다고 규정하고 있다.; ICC, GUIDEC Ⅱ, Ⅸ-1 Commentary.
46) ICC, GUIDEC Ⅱ, Ⅹ-1.
47) ICC, GUIDEC Ⅱ, Ⅹ-2 Commentary.

2) 인증기관의 신뢰도에 대한 관행

GUIDEC Ⅱ상의 인증기관[48]의 신뢰도에 대해 규정된 관행을 살펴보면, 인증기관은 반드시 기술적으로 신뢰할 수 있는 정보 시스템과 처리방법만을 사용하고, 인증서의 발급, 공개키 인증서의 효력정지 또는 취소, 비밀 키의 보호에 있어서 믿을 만한 사람을 고용하여야 한다. 또한 인증서의 발급, 효력정지, 취소에 있어서 인증기관을 신뢰할 수 없게 만드는 이익의 충돌이 없어야 하며, 서명자가 의무를 위반하는 원인을 제공하지 않도록 한다.[49]

인증기관은 기본적으로 전자서명 사용자의 신원을 확인하는 일과 이와 관련된 시점확인 등의 부수적 업무를 수행한다. 신원인증업무의 일환으로서 인증기관은 사용자의 신원을 확인하여 인증서를 발급하고 전자서명 키를 관리하고 인증서를 확인하고 인증서 및 인증서의 효력변경사항을 공개하며 사후분쟁에 대비하여 인증서 관련기록을 보존하는 등의 업무를 수행한다. 또한 네트워크상에서 전송되는 메시지의 안전성을 확보하기 위하여 암호화 기술을 사용하여 인증하는 기능을 수행함으로써 위험을 회피하기 위한 구조를 제공한다. 이를 위하여 가입자 자신을 확인하고 가입자의 공개키를 보관하여 가입자로부터 전자서명을 한 문서를 수취한 사람에 대하여 그 공개키를 '전자증명서'로서 발행한다.

전자서명을 이용한 문서의 교환 및 전자거래에 있어서 당사자를 인증하는 일은 전자메시지의 이용에 있어 거래의 기반을 이룬다. 따라서 일정한 자격이나 요건을 구비한 인증기관이 이를 수행함으로써 이용자들로부터 신뢰를 받을 수 있게 된다.[50] 인증기관의 신뢰도는 인증 전체의 개념에 있어서 중심이 되고 있으며 그만큼 인증기관의 신뢰도의 중요성이 인식된다. UNCITRAL의 전자서명에 대한 통일 법 제10조에서도 인증서비스 제공자, 즉 인증기관의 신뢰도에 대해 명시되어 있다.[51] 인증서는 인증서비스 제공자가 신뢰도가 있느냐에 따라 활용되어지며, 인증기관은 재정적으로 인적자원이 풍부해야 하며, 하드웨어와 소프트웨어 시스템의 높은 질 등이 신뢰할 수 있는 인증기관의 조건이다.

3) 인증기관의 의무와 책임에 관한 관행

인증기관이란 가입자 개인의 신원을 확인해주고 전자서명을 생성하기 위해 필요한 전자서명검증정보와 전자서명 생성키의 조합이 그 가입자의 것임을 증명해주는 신뢰할 만 한 제3자를 말하며 네트워크상에서 이루어지는 모든 상업적, 비상업적 거래에 있어서 신뢰의 중심이 된다.[52]

---

48) 인증기관이란 전자거래에서는 양 당사자는 상호 직접 접촉하지 않고서도 또 서류를 직접적으로 전달하지 않고서도 불특정 다수의 상대방과 계약이 체결될 수 있다. 이 때문에 거래당사자간에서 체결된 전자계약행위가 안전하고 확실하게 되기 위해서는 전자문서의 신뢰성이 확보되어야 한다. 이러한 문제는 비대칭 암호화 방식을 통한 전자서명을 사용하여 극복될 수 있다. 따라서 전자서명의 검증 키가 전자서명을 행한 당사자의 것이라고 확인·증명하거나, 불특정 다수의 전자서명 키 인증을 효율적으로 수행하거나 또는 전자서명 키의 인증의 공신력을 제고하여 전자문서 이용 관련 분쟁을 최소화하기 위해서 거래당사자 이외의 공정한 제3자의 개입이 요구된다. 이러한 역할을 담당하는 것이 인증기관(certification authority : CA)이다.; 강원진, 전게서, 292면.

49) ICC, GUIDEC Ⅱ, X-3.

50) 강원진, 전게서, 292~293면.

51) UNCITRAL Uniform Rules on Electronic Signatures, 2001, Article 10.

인증기관은 전자적으로 인증서를 발송할 때. 인증서에 디지털 서명을 첨부해야 한다.[53] 서명자는 인증서의 내용을 검토해야 하고 공개적으로 인증서가 사용되기 전에 정확성을 확인해야 한다.[54] 서명자는 정확성과 타당성 확인을 위해 인증서를 받아들여야 하고 서명자가 인증서의 내용을 재검토 한 후 인증서의 정확성을 확인하고 인증서를 발행하거나, 인증기관이 바로 발행할 것이다.[55] 인증기관이 인증서를 발행할 때, 인증서는 서명자에 의해 받아 들여 진다고 나타낼 것이고, 그 인증서는 유효성이 주어진다.[56]

인증기관은 인증기관의 영향을 받을 것으로 예상되는 모든 사람들에게 중요한 인증실행 설명서 및 인증기관이 발급한 인증서의 신뢰도 또는 인증기관의 서비스 수행 능력에 중요한 사실들을 통지하기 위한 상당한 노력을 기울여야 한다. 또한 인증기관은 그의 사업에 필요한 충분한 재정 자원을 보유하고 그가 발급한 인증서에 기인하는 합리적인 위험을 부담하여야 한다[57]고 규정하고 있다.

인증기관은 인증 관련 업무를 수행함에 있어서 인증기관이 공표한 정책, 관습 및 관련 법률에 규정된 절차에 따라 행위를 하여야 할 책임이 있고,[58] 그와 같은 의무를 이행하지 못한 경우에는 책임을 진다.[59] 한국 전자서명법에서는 “공인인증기관이 인증업무 수행과 관련하여 가입자 또는 인증서를 신뢰한 이용자에게 손해를 입힌 때에는 그 손해를 배상하여야 한다. 다만, 그 손해가 불가항력이나 이용자의 고의 또는 과실로 인하여 발생한 경우에는 그 배상책임이 경감 또는 면제 된다”고 규정하고 있다.[60]

따라서, 공증인과 같은 현행의 전문 인증기관은 가입자가 인증기관을 신뢰한 결과로 입을 수 있는 손해를 배상하기 위해 전문손해보험에 가입할 의무가 있다.[61] 그러한 보험은 인증기관에 대한 배상청구가 있을 때까지 그 자원에 접근할 수 없는 것이지만 인증기관의 재정자원에 추가되는 것으로 볼 수 있다. 인증기관은 인증사업에 필요한 충분한 재정 자원을 보유하고 그가 발급한 인증서에 기인하는 합리적인 위험을 부담하여야 한다.

4) 인증기관의 업무에 관한 관행

한국의 전자서명법에 따르면, 인증 업무는 인증서의 발급 및 인증관련 기록의 관리 등 인증역무를 제공하는 업무를 뜻하며,[62] 이는 인증기관의 의무이기도 하다. 인증기관은 가입자의 신원확인, 인증서

52) 최영봉, “전자거래에 있어서 인증관련당사자의 책임에 관한 연구”, 「국제무역연구」, 제8권 제2호, 국제무역학회, 2002, 306면.
53) Thomas J. Smedinghoff, *op. cit.,* p.47.
54) ABA, *op. cit.*
55) *Ibid.*
56) Lupton W. Everett, *op.cit.,* p.6.
57) ICC, GUIDEC Ⅱ, Ⅹ-4.
58) UNCITRAL Model Law on Electronic Signatures, 2001, Article 9(1).
59) UNCITRAL Model Law on Electronic Signatures, 2001, Article 9(2).
60) 한국 전자서명법 제26조.
61) ICC, GUIDEC Ⅱ, Ⅹ-5.

의 발행, 인증사실의 공시,[63] 기타 업무[64] 등을 담당하고 있다.

GUIDEC Ⅱ상에서 인증기관의 업무에 관한 관행을 보면, 상당한 기간 동안 인증기관이 발급한 인증서에 모든 사실의 기록을 보유하여야 하며 인증기관의 업무를 종료시킬 때 반드시 서명자들과 그가 발급한 유효하고 사용 중인 인증서를 신뢰하는 사람들에게 최소한의 혼란을 주는 방식으로 처리하여야 하며, 그의 기록을 적당한 자격을 갖춘 후임자[65]에게 인계하여야 하는 것으로 규정하고 있다.[66] 즉, 인증기관이 업무를 종료하여야 하는 경우, 이를 이용자에게 통지하고 등록관청에 신고할 의무가 있으며 다른 인증기관과 협의하여 그 인증업무를 인계할 의무가 있다.[67] 이러한 인계를 할 수 없는 경우에는 등록 내지는 감독관청으로 하여금 인증업무의 인수인계를 위해 필요한 조치를 할 수 있도록 하여야 할 것이다.[68] 인증기관의 업무를 승계하겠다는 사람이 나타나지 않는다면 장래에 인증기관이 인증서를 관리할 수 없기 때문에 기존의 유효한 인증서를 모두 취소할 필요가 있다.

5) 요청에 의한 공개키 인증서의 효력정지에 대한 관행

인증서는 신원인증서(identifying certificate; identify certificate), 권한인증서(authorizing certificate; authority certificate), 거래인증서(transactional certificate) 등이 있다.[69] 한국의 전자서명법과 UNCITRAL 전자서명에 대한 표준법의 인증서에 관한 규정들은 공개키와 그 보유자를 연결시켜주는 첫째 범주의 신원인증서만을 규율대상으로 하고 있다.[70]

한국 전자서명법 제15조 제2항에 따르면, 공인인증기관이 발급하는 인증서에 포함되어야 할 최소한의 내용으로, 가입자의 이름, 가입자의 전자서명 검증키, 가입자와 공인인증기관이 이용하는 전자서명 방식, 인증서의 일련번호, 인증서의 유효기간, 공인인증기관의 명칭, 인증서의 이용범위 또는 용도를 제한하는 경우 이에 관한 사항, 가입자가 제3자를 위한 대리권 등을 갖는 경우 이에 관한 사항 등을 규정하고 있다.[71] 이는 UNCITRAL 표준법 제9조 제1항 (c) 및 (d)와 유사한 규정이다. ABA가이드라인 제1.5조, 일리노이즈 주 전자상거래안전법 제 5-105조 제2항도 거의 같은 내용의 규정을 두고 있다.

---

62) 한국 전자서명법 제2조 제8호.
63) 공인인증기관은 자신이 발급한 인증서가 유효한지의 여부를 누구든지 정보통신망을 통하여 항상 확인할 수 있도록 인증관리체계를 안전하게 운영하여야 한다.; 한국의 전자서명법 제19조.
64) 일시증명, 기록증명 및 보관, 키 생성과 보관 등의 업무.
65) 적당한 자격을 갖춘 후임자(qualified successor)란 다른 인증기관은 일반적으로 퇴출하는 인증기관을 승계할 수 있는 자격이 있다. 책임감이 투철한 우수한 문서보관업자, 전문단체 또는 감독기관 등도 적임이라고 할 수 있다. 그 후임자는 새 인증서를 발급할 필요는 없지만, 적어도 인증서의 효력정지, 취소 및 검색 서비스는 계속 운영하여야 한다.; ICC, GUIDEC Ⅱ, X-7 Commentary.
66) ICC, GUIDEC Ⅱ, X-7.
67) 강원진, 전게서, 297면.
68) ICC, GUIDEC Ⅱ, X-7 Commentary.
69) A.M. Froomkin, “The Essential Role of Trusted Third Parties in Electronic Commerce,” *Readings in Electronic Commerce,* 1997, p.119.
70) 최준선, 전게논문. 223면.
71) 한국 전자서명법. 제15조 제2항.

GUIDEC Ⅱ상의 인증서의 효력정지에 관한 규정을 살펴보면, 인증서를 발급한 인증기관은 자신이 공개키 인증서에 서명자라고 기재되어 있다거나, 또는 대리인·피용자·사업상의 동료 또는 서명자의 직계가족과 같이 서명자의 비밀키[72]의 안전에 손상이 가해진 것을 알 수 있는 사람이라고 신원을 밝힌 사람의 요청이 있으면 즉시 그 효력을 정지시켜야 한다[73]고 규정한다.

효력의 정지는 일시적으로 공개키 인증서를 무효화시키기 때문에 인증서에 기재되어 있는 공개키의 서명자와의 관계도 사실상 일시적으로 단절된다. 그러한 관계가 없다면 당해 공개키[74]로 검증될 수 있는 전자서명은 서명자에게 귀속될 수 없을 것이다. 따라서 서명자는 그의 전자서명 효력을 정지시킬 수 있다.

인증기관은 그 요청을 하는 사람의 권한을 확인할 의무는 없지만, 그러한 요청을 즉시 확인하기 위한 일정한 절차를 마련해 두어야 한다. 이러한 절차가 없다면, 인증기관으로서 서명자에 대한 의무를 위반한 것이 되고, 서명자가 전자서명을 사용하지 못하는 데서 오는 손해를 보상할 책임이 있다. 중요한 공개키 인증서의 효력을 정지시킴으로써 전자서명의 귀속을 일시 배제하는 것은 서명자가 비밀 키의 소지에 따른 위험을 관리하는 주요 수단 중의 하나이다. 인증서를 신뢰할 수 있는 사람이 인증서 효력의 정지에 대한 제한이나 배제에 관하여 통지를 받은 경우에는 인증기관과 서명자 사이의 약정으로 그 효력의 정지를 제한하거나 배제할 수 있다. 이러한 제한이나 배제는 인증실행 설명서에 포함시킬 수 있다.[75]

6) 동의 없는 공개키 인증서의 효력정지 또는 취소 및 통지

공개키 인증서를 발급한 인증기관은 인증서상의 서명자 또는 그의 수권대리인으로부터 취소 요청을 받은 때 및 취소를 요청한 사람이 서명자이거나 취소를 요청할 수 있는 권한을 가진 그의 대리인임을 확인한 때에는 즉시 인증서를 취소하여야 한다.[76] 공개키 인증서를 발급한 인증기관은 인증기관이 인

72) 비밀 키 방식은 송신자에 의한 암호화와 동시에 수신자에 의한 복호화를 위한 공유 키의 사용에 의하여 문서교환의 안전을 도모하는 방식으로서, 대칭적 암호화 방법이라고도 한다. 이 방식은 암호화 및 복호화 변형에 동일한 키가 사용된다는 것이 특징이다. 그러나 이 방식 하에서 송수신자는 비밀 키가 노출되거나 도난당하지 않도록 항상 키의 관리에 주의를 기울여야 한다는 단점이 있다. 특히 송수신자가 지리적으로 멀리 떨어져 존재하고 있다면 메시지를 전달하는 사람으로서는 제3자가 알 수 없도록 전화나 전송시스템 등을 통하여 비밀 키를 전송할 필요가 있다. 또한 이 방식 하에서는 송수신자간에 데이터 교환에 앞서서 미리 신뢰관계를 구축하고 비밀 키를 분배하고 있어야 하기 때문에 불특정 다수인을 상대로 하는 전자상거래에서는 사용되기 어려운 측면이 있다.; 강원진, 전게서, 271면.

73) ICC, GUIDEC Ⅱ, X-8.

74) 공개키 방식은 암호화를 위한 키와 복호화를 위한 키 라는 한 쌍의 키를 사용하는 방법으로서 1976년에 스탠포드대학의 다이피와 헬만에 의하여 도입되었다. 공개 키 방식을 비대칭적 암호화 방법이라고도 한다. 이 방식에서 암호화된 정보는 이에 대응시키는 키에 의하여만 복호화 될 수 있다. 한 쌍의 키 중 비밀 키는 사용자의 시스템에 비밀히 보관되고, 공개 키는 공개되어 보관기관에 보관되면 누구나 검색할 수 있다. 또 한 쌍의 키를 동일한 시스템에 관련시킬 수도 있는데, 비밀 키는 시스템 내에 비밀히 보관하고 공개 키는 공개하는 것이다. 공개 키 방식은 디지털 서명에 이용된다. 비밀 키는 그 보유자만이 보관하고 있고, 이에 의하여 암호화된 문서는 이에 대응하는 공개키에 의하여만 복호화 될 수 있기 때문에 문서 작성자의 신원을 증명하고 메시지의 진정성과 무결성을 확보할 수 있기 한다. 이러한 공개 키 기법에는 공개키가 해독키로 사용 되는가 암호 키로 사용되는가에 따라 인증모드와 암호화모드로 구분된다.; 강원진, 전게서, 272면.

75) ICC, GUIDEC Ⅱ, X-8 Commentary.

증서에 진술되어 있는 사실이 허위임을 확인하였을 때 인증기관이 그의 신뢰도에 중대한 영향을 줄 정도로 인증기관의 정보 시스템의 신뢰성이 손상되었음을 확인하였을 때 이를 취소하여야 한다. 만일 인증기관이 인증서를 취소하지 않거나, 적어도 조사를 수행하는 동안 인증서의 효력을 정지시키지 않고 위에서 말한 어느 이유에 대한 통지를 받은 것으로 밝혀진 경우에는 당연히 이로 인한 손해에 책임을 져야 한다. 이러한 행위를 하지 아니한 것은 제3자에 대한 인증기관의 '신뢰도'에 의문을 가져올 수 있기 때문이다.[77]

인증기관은 이 조항에 따라 효력정지의 원인을 규명하기 위한 조사를 수행하는 데 필요한 기간 동안 의심이 가는 인증서의 효력을 정지시킬 수 있다. 또한 인증기관이 동의 없이 인증서의 효력을 정지시키거나 취소할 수 있는 정확한 변수는 인증기관과 서명자 사이의 약정을 통하여 정할 수 있다. 따라서, 인증기관에 의한 공개키 인증서의 효력의 정지나 취소가 있는 즉시 인증기관은 그 효력의 정지 또는 취소에 대하여 적절한 통지를 하여야 한다고 규정하고 있다.[78] 만약 공개키의 분실이나 손상이 있었다면, 키의 유효기간이 지나기 전에 폐기할 필요가 있다. 하나의 키는 인증서를 폐기함으로써 취소되지만, 문제는 통지방법이다. 그 문제에 대한 대책으로 인증서 폐기목록(Certificate Revocation List : CRL)이 있다. 인증서폐기목록은 유효기간 이전에 인증서가 폐기되었다는 간단한 자료이다. 인증서폐기목록은 인증기관에 의해 유지되는 저장소의 일부분일 것이다. 만약 비밀 키가 분실되거나 손상되었다면, 그 상대 공개키와 인증서는 인증서폐기목록에 작성되어져야 한다. 공개키를 인증하기 전에, 신뢰당사자는 인증서폐기목록을 검토하여 그 상황을 확인해야 한다.[79] 만약 인증기관이 통지를 하지 않은 경우에는 인증기관은 서명자와의 계약을 위반한 것이 되거나, 최악의 경우 서명자가 무효화된 키를 이용한 결과 발생한 손해배상을 하여야 한다.

Ⅳ. 결 론

전자상거래에서는 거래당사자가 메시지의 진정성 확인과 신원확인을 위하여 전자서명과 전자인증을 통하여 거래의 신뢰성을 확보하고 안전을 도모하여야 한다. 유엔 국제무역법위원회에서는 전자상거래와 전자서명에 대한 표준법, 유럽에서는 전자서명지침, 미국에서는 E-Sign법을 제정하여 전자서명과 전자인증에 대한 제도적 기반을 구축하였다.

ICC는 이와 같은 상이한 법제들과의 조화를 위하여 전자인증에 관한 새로운 가이드라인인 GUIDEC Ⅰ 및 Ⅱ를 제시하였다. GUIDEC Ⅱ, 즉 디지털로 보장되는 국제전자상거래의 일반관례의 개정판상에

76) ICC, GUIDEC Ⅱ, X-10.
77) ICC, GUIDEC Ⅱ, X-10 Commentary.
78) ICC, GUIDEC Ⅱ, X-11.
79) Thomas J. Smedinghoff, *op.cit.,* p.19.

반영된 전자인증관행은 메시지의 진정성 확인과 인증이 핵심 내용이다.

먼저, 메시지의 진정성 확인은 첫째, 거래당사자의 진정성확보와 전자문서의 무결성을 보장한다는 의미로써 진정성이 확인된 메시지의 조건을 명시하는 것이다. 둘째, 진정성이 확인된 메시지는 실제 메시지의 진정성을 확인한 사람에게 귀속되어야 하며, 사기 및 위조의 경우라도 메시지는 실제로 진정성을 확인한 사람의 것이 된다. 셋째, 대리인이 본인의 권한으로 메시지의 진정성을 확인한 경우에는 메시지의 진정성 확인을 본인이 한 것과 동일한 효력을 가지게 된다. 넷째, 메시지의 진정성을 확인하는 가장 적합한 방법으로 인증기관을 통하는 방법을 권장하고 있다. 다섯째, 진정성이 확인된 메시지의 범위 및 진정성 확인을 위한 장치의 보호에 대한 인증기관의 의무에 대한 가이드라인을 제시하고 있다.

다음으로, 인증에 대한 관행 내용은 첫째, 인증기관이 인증된 메시지의 실무관행상 중요한 요건을 충족하였을 경우에는 유효한 인증서에 기재된 사실들이 정확하게 진술되어 진 것으로 신뢰할 수 있다. 둘째, 신뢰할 수 있는 인증기관이 갖추어야 할 조건들을 나열하고 있다. 셋째, 인증기관의 의무와 책임에 관해 규정하고 있다. 넷째, 인증기관이 업무를 종료시킬 때 서명자와 인증기관이 발급한 인증서를 신뢰하는 사람들에게 혼란을 주지 않는 방식으로 처리하며, 인증기관이 보유한 기록을 적당한 자격을 갖춘 후임자에게 인계하도록 한다. 다섯째, 요청에 의한 공개키 인증서의 효력정지에 대한 관행과 동의 없는 공개키 인증서의 효력정지 또는 취소에 대한 규정과 효력정지 또는 취소에 따른 통지관행을 제시하고 있다.

이와 같이 국제상업회의소의 GUIDEC Ⅱ는 상이한 법체계하에 존재하는 규범 및 관행에 대비하여 디지털 메시지의 인증에 대한 일반적인 틀에 대한 지침이며 전자상거래에서 발생할 수 있는 규범의 조화를 위하여 거래당사자들의 의무와 책임을 제공함으로써 전자상거래 상에서 발생 가능한 분쟁을 예방할 수 있는 유용성 있는 표준관행의 소재로 제공되고 있다 할 것이다.

참 고 문 헌

강원진, 「전자결제시스템」, 삼영사, 2000.

_____, “전자신용장의 국제결제 인프라구축 동향과 해결과제”, 「국제상학」, 제19권 제1호, 한국국제상학회, 2004.

_____, “전자무역거래 활성화를 위한 전자결제시스템의 요건과 과제”, 「국제상학」, 제17권 제3호, 한국국제상학회, 2002.

김정회, 「전자무역」, 두남, 2004.

김종칠 · 이진우, “전자상거래에서 전자서명 인증제도에 관한 비교연구”, 「국제상학」, 제15권 제1호, 한

국국제상학회, 2000.

오현석, “전자무역에서 전자인증제도의 문제점에 관한 연구”, 성균관대학교 박사학위논문, 2004.

전순환, “전자서명과 인증기관에 관한 연구”, 「상품학연구」, 제26호, 한국상품학회, 2002.

정완용, “개정 전자서명법의 비교법적 고찰”, 「비교사법」, 제10권 제4호, 한국비교사법학회, 2003.

최석범, “글로벌전자무역에 관한 연구”, 「국제상학」, 제14권 제1호, 한국국제상 학회, 1999.

최영봉, “전자거래에 있어서 인증관련당사자의 책임에 관한 연구”, 「국제무역연구」, 제8권 제2호, 국제무역학회, 2002.

최준선, “전자서명과 전자인증의 제문제”, 「무역상무연구」, 제15권 제3호, 한국무역상무학회, 2001.

American Bar Association, Digital Signature Guidelines, 1996.

Everett Lupton W., "The Digital Signature : Your Identity By the Numbers," *Richmond Journal of Law and Technology*, 1999.

Fox William F., "The International Chamber of Commerce's GUIDEC Principles : Private-sector Rules for Digital Signature," *International Lawyer*, 2001.

Froomkin, A. M., "The Essential Role of Trusted Third Parties in Electronic Commerce," *Readings in Electronic Commerce*, 1997.

ICC, *General Usage For International Digitally Ensured Commerce* (GUIDEC) - version I, 1998.

___, *General Usage For International Digitally Ensured Commerce* (GUIDEC) - version II, 2001.

Price Pamela N., "Designing the Legal Infrastructure For Cyberspace Commerce : How much Regulation is too much?," *Suffolk University Law Review*, 1998.

Smedinghoff Thomas J., *Online Law, The SPA's Legal Guide to doing business on the Internet,* Addison-Wisley Developers Press, 1997.

_____, "Electronic Contracts and Digital Signatures and Overview of Law and Legislation," *Practising Law Institute*, 1999.

The European Union Directive on Electronic Signatures, 1999.

The Electronic Signature in Global and National Commerce Act. 2001.

UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996.

UNCITRAL Draft Uniform Rules on Electronic Signatures, 2000.

UNCITRAL Report of the Working Group on Electronic Commerce on the Work of its thirty-seventh session, 2000.

UNCITRAL Model Law on Electronic Signatures, 2001.

UNCITRAL Uniform Rules on Electronic Signatures, 2001.

International Chamber of Commerce, http : //www.iccwbo.org/

United Nations Commission on International Trade Law, http : //www.uncitral.org/