

프랑스의 본인서명확인증명제도

정보신청기관 : 한국법제연구원 법제교류지원센터

법률행위에 있어서 당사자는 당해 법률행위로부터 발생하는 채무관계에 대한 내용을 문서 등에 기재하고, 이에 관한 합의가 있었음을 나타내기 위하여 서명을 하며, 이 서명을 함으로써 법률행위는 완성된다. 이러한 서명에 대하여, 프랑스는 「정보기술 및 전자서명에 관련된 입증권의 적용에 관한 2000년 3월 13일자 법률 제 2000-230호」(Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique)¹⁾의 제정 이전에는 서명에 관한 법적 정의 및 기능에 대하여 법률이 명

확히 규정하고 있지 않았고, 서명이 존재하여야 하는 분야에 따라 이를 규정하고 있었다.²⁾ 따라서 서명에 관한 자세한 내용은 판례를 통하여 형성되었다. 즉, 형식에 있어서는 서명은 어떠한 형식이나 도안으로도 할 수 있고,³⁾ 서명의 본질인 증서의 내용에 동의한다는 의사 표현에 있어서는 제3자가 조력할 수도 있음을 인정하고 있다.⁴⁾ 그리고 서명이 없거나 침삭된 서명은 그 증서의 증명력을 상실시키고, 증서의 내용이 부정되는 경우 그 증서는 서명 없는 문서(commencement de preuve par écrit)로 된다.⁵⁾



- 1) 이하 '2000년 전자서명법'이라 한다.
- 2) 즉 민법 제970조에서, 자필유언장에 대해서는 자필로 서명되어야 한다는 지적만 되어 있다.
- 3) Cass. req., 8 juill. 1903 : DP 1903, 1, p. 507 ; Cass. 1^{re} civ., 12 Juill. 1956, 1, no 302.
- 4) Cass. 1^{re} civ., 19 juin 1951 : Bull. civ. 1951, 1, no 190.
- 5) 침삭된 서명 : Cass. 1^{re} civ., 16 juin 1993 : Bull. civ. 1993, I, no 219 ; 서명이 없는 증서 : Cass. 1^{re} civ., 17 janv. 1961 : Bull. civ. 1961, I, no 41

1. 서명의 법적 정의

2000년 전자서명법에 의해 추가된 민법 제 1316-4조 제1항은 “법률행위의 완성을 위하여 필요한 서명은 서명자의 신원을 확인한다. 서명은 당해 법률행위로부터 발생하는 채무에 대한 당사자의 합의를 나타낸다. 서명이 공무원에 의하여 이루어진 경우, 그 서명은 당해 증서에 공증력을 부여한다.”고 규정함으로써, 서명의 정의와 기능에 관하여 법적 근거를 마련하고 있다. 2000년 전자서명법은 “서명은 문서가 서면증거로서 가치가 있는 ‘증서(instrumentum)’가 되기 위하여, 문서의 ‘주요 부분’을 차지하고 있는 부분으로서 문서 그 자체라는 관념”을 확고히 하고 있다.⁶⁾ 또한 이 법은 서명의 신원확인 기능을 규정하고 있다.

2. 서명의 신원확인 기능

민법 제1316-4조 제1항에서 “서명자의 신원을 확인한다.”고 규정함으로써, 서명의 신원확인 기능을 명문화하고 있다. 서명은 서명을 한 자에게만 관련되며, 이 서명은 그 서명을 한 자와 표시 사이의 관계를 형성하게 되는 것이다. 그러므로 서명은 신원확인 방법을 구성하는 것이지, 서명자의 신원을 바로 형성케 하는 어떠한 표지를

구성하는 것은 아니다.⁷⁾

서명만으로 본인임을 추정하고 있지 않으므로, 당사자 일방이 증서의 서명을 부인하거나 증서 작성자의 상속인 또는 승계인이 그 증서의 서명을 알지 못한다고 주장하는 때에는 법원은 이에 관한 사실조사를 명하여야 한다(민법 제1324조). 즉, 당사자의 서명에 대한 부인의 결과는 신민사소송법 제287조 이하의 증서의 검증 절차에 따르게 된다. 이는 보통의 채무관계 부인에 관한 입증방법과 동일하다. 이러한 확인 절차는 소송과정에서 사실 확인에 관한 부대소송(신 민사소송법 제287조~제295조) 또는 본소(신 민사소송법 제296조~제298조)에서 행해질 수 있다. 서명에 관한 사실 확인의 경우, 법관은 기술 전문가의 조력을 받을 수 있다(신 민사소송법 제292조).

3. 전자서명의 인정

2000년 전자서명법에 의한 민법 제1316-4조는 전자서명에 대하여 자필서명과 같은 가치를 부여하고 있다. 그러나 2000년 전자 법률이 채택될 때, 전자서명의 인정을 규정하는 민법 제1316-4조는 증명할 수 있는(ad probationem) 서면에만 적용될 수 있었다. 특히 ‘디지털 경제에서의 신용’에 관한 2004년 6월 21일 제2004-275호 법



6) Luc Gryubaum, JurisClasseur ; Civil Code/Art. 1316 à 1316-4 ; no 36, 2006.

7) *ibid.*, no 37.

를(Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique)⁸⁾ 이전에는 유효성(ad validitatem)이 요구되는 서명은 필요적으로 자필서명이었다. 그런데, 2004년 디지털 경제에서의 신용에 관한 법률 제25조는 서면이 법률행위의 유효성을 위하여 요구되는 경우에 관하여, 민법 제1108-1조를 추가하였다. 유효한 서면이 민법 제1316-1조와 제1316-4조에 따라 제정되고 유지되는 이상, 그 서면은 전자적 형식하에 작성되고 보존될 수 있다고 규정한다. 그러므로 유효성이 요구되는 서면은 전자서명을 갖출 수 있게 된 것이다.⁹⁾

서명자의 신원확인 과 문서내용의 동의에 관한 서명의 기능을 완수하기 위하여, 전자서명은 안전절차에 기초를 두고 있다(민법 제1316-4조 제2항). 이는 필수적인 요건이기 때문에, 문서의 주요 부분에 첨부되는 전자서명은 전자문서를 유효하게 만든다. 또한 전자서명에 대하여 발생할 수 있는 이의제기에 대비하기 위하여 전자서명의 신뢰성에 관한 기술적 요구가 필요하다.

4. 전자서명의 신뢰성 요건

2000년 전자서명법은 서명이 기재된 경우 “반대의 입증이 있을 때까지, 서명자의 확보된 신원

과 보장되는 증서의 완전성에 대해서는 국사원령이 정하는 요건에 따른다(민법 제1316-4조 제2항).”고 규정하고 있으므로, 전자서명이 (민법 제1316-4조의 적용을 위한) 2001년 국사원령¹⁰⁾이 정한 기준에 따라 실행된 경우, 증명력이 부여될 것이다. 이와 같은 2001년 국사원령 제2조는 “전자서명방식의 신뢰성은 안전성이 보장되고, 이 방식이 전자서명생성안전장치에 의하여 전자서명을 실행하고, 이러한 전자서명의 확인이 공인전자인증서의 사용에 근거하는 경우, 반대의 입증이 없는 한 그 신뢰성은 추정된다(제2조).”고 규정하고 있다.

(1) 안전전자서명의 이용

입법자는 ‘진보된’ 전자서명에 관하여, 유럽 공동체가 취한 높은 수준의 안전을 채택하였다. 즉, 전자서명은 ‘오직 서명자에게만’ 관련된다(서명자의 신원을 확인한다). 전자서명은 서명자가 자신의 배타적인 관리하에 이를 보장할 수 있고, 차후 정보의 모든 변경이 검출될 수 있도록 서명에 관계되는 정보에 연결할 수 있는 방법으로 생성된다. 신뢰성 추정은 유럽공동체 공보에 공표된 리스트에 언급된 제품명이나 또는 ‘인증 서비스제공자’ 인 제3자에게 전자서명을 신청하는 자에 대하여 발생한다.



8) 이하 2004년 디지털 경제에서의 신용에 관한 법률이라 한다.

9) Luc Gryubaum, op. cit., no 41.

10) 민법 제1316-4조의 적용과 전자서명에 관한 2001년 3월 30일 제2001-272호 령(Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique). 이하 2001년 국무원령이라 한다.

(2) 전자서명성장장치

전자서명성장장치¹¹⁾는 ‘기술적 방법 및 적절한 절차’에 의해 보장되는 경우에만 안전한 것으로 인정된다. 전자서명생성에 관한 정보는 (a) 한 번 이상 생성될 수 없고, 데이터의 비밀성이 보장되어야 하며, (b) 추론에 의하여 발견될 수 없고, 전자서명은 일체의 변조로부터 보호되어야 한다. (c) 제3자에 의한 모든 사용으로부터, 서명자가 만족하는 방법으로 보호될 수 있어야 한다(2001년 국사원령 제3조 제1항). 또한 이 장치들은 “서명하는 문서의 내용에 어떠한 변경도 가져오지 않고, 서명자가 서명 전에 이에 대해 정확하게 인식하였다는 것에 장애가 되지 않아야 한다(2001년 국사원령 제3조 제2항).

위에 열거된 요구에 대한 전자서명성장장치의 적합성은 정보시스템 안전을 담당하는 수상에 의하여, 또는 유럽공동체 회원국에 의해 지정된 조직체에 의해 인증되어야 한다. 2002년 4월 18일 국사원령¹²⁾은 전자서명시스템을 인증하기 위한 절차를 상세히 규정하고 있다. 이 절차는 3개의 단계로 규정되어 있다 : (1) 서비스제공자는 국가정보시스템안전기구(ANSSI)에게 신청서를 제출하여야 한다. (2) 그 다음 수상이 승인한 센터가 서비스제공자의 시스템을 평가한다. (3) 이 평가 후 인증서가 인정될 수 있다.



11) 전자서명 생성에 관한 정보를 적용하기 위해 마련된 하드웨어 또는 소프트웨어 등.

12) 정보기술 제품과 시스템에 의해 제공되는 안전 평가와 인증에 관한 2002년 4월 18일 제2002-535호 령(Décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information).

13) CHRISTIANE Féral-Schuhl, CYBERDROIT; Le droit à l'épreuve de l'internet, 5e édition, Dalloz, 2008, no 92.43.

(3) 전자서명확인

전자서명의 확인은 인증서비스제공자에 의해 교부된 공인전자인증서의 이용에 기초를 둔다. 우선 전자서명확인에는 다음의 요건을 충족한 경우 공인인증의 대상이 될 수 있다. (a) 전자서명확인 정보는 전자서명확인장치를 실행하는 확인자가 알고 있는 것이어야 한다. (b) 전자서명확인요건은 전자서명의 정확성을 보증하고, 이 확인의 결과는 변조됨이 없이 확인자가 알고 있어야 한다. (c) 확인자는 서명된 정보의 내용을 확실하게 결정할 수 있어야 한다. (d) 전자서명확인 시에 사용된 전자인증서의 효력요건 및 기간은 변조됨이 없이 확인자가 알아야 한다. (e) 서명자의 신원은 변조됨이 없이 확인자가 알아야 한다. (f) 가명을 사용한 경우, 그 가명의 사용을 확인자가 명확히 알도록 하여야 한다. (g) 전자서명확인요건에 대해 영향을 미치는 모든 변경은 탐지될 수 있어야 한다(2001년 국사원령 제4조).

(4) 공인전자인증서

공인전자인증서는 개인과 그의 공적 열쇠(clé publique) 사이를 연결하여야 하는 전자 신원확인카드이다.¹³⁾ 인증서 발급에 관하여 권한 있는 인증서비스제공자에 의해 교부된 인증서만이 공인전자인증서로서 유효하다. 그리고 전자인증서

가 권한을 부여받기 위해서는 다음과 같은 의무적 사항을 포함하고 있어야 한다. (a) 전자인증서가 공인전자인증서로서 교부되었다는 것을 표시하는 문구, (b) 전자인증서서비스제공자의 신원확인, (c) 서명자의 이름 또는 가명(가명 역시 신원이 확인되어야 한다), (d) 전자서명생성 정보에 부합하는 전자서명확인 정보, (e) 전자인증서의 유효기간의 시작시점과 종료시점의 표시, (f) 전자인증서의 신원확인 코드, (g) 전자인증서를 교부하는 전자인증서서비스제공자의 안전성이 보장된 전자서명 등이다.

5. 전자인증서서비스제공자

2001년 국사원령 제6조는 전자인증서서비스제공자의 직무 및 의무에 관하여 규정하고 있다.¹⁴⁾ 그 주요 내용은 재판에서 전자인증의 입증을 하기 위하여 필요하다고 판단될 수 있는 전자인증서에 관한 모든 정보를 전자적 형태하에서의 보존하여야 하고, 정보의 입력 및 변경은 인증서서비스제공자에 의해 이러한 목적을 위하여 권한을 부여 받은 자에게만 유보되어 있고, 시스템의 안전성을 위태롭게 하는 성질의 변경은 모두 검출될 수 있다는 것을 보장하는 인증서보전시스템을 이용하여야 한다. 이와 같이 전자인증서서비스제공자의 요건을 충족한 자는 공인된 전자인증서서비스제공자가 될 수 있다. 이 공인은 산업부장



14) 자세한 법률 규정은 다음과 같다.

- a) 전자인증서서비스제공자가 제공하는 전자인증서서비스의 신뢰성을 가져야 한다.
- b) 전자인증서가 교부되는 자를 위하여 신청을 한 자의 전자인증서를 대조하는 명부서비스의 운영을 보장하여야 한다.
- c) 그 전자인증서가 교부되었던 자가 기간의 제한 없이 확실하게 취소할 수 있도록 하는 서비스의 운영을 보장하여야 한다.
- d) 전자인증서의 교부 일자와 취소 일자가 정확하게 정해져야 한다.
- e) 전자인증서서비스제공에 필요한 지식, 경험 및 자격을 가진 직원을 고용하여야 한다.
- f) 적절한 안전절차를 적용하여야 한다.
- g) 전자인증서서비스제공자가 보장하는 직무의 기술상 안전과 암호상 안전을 보장하는 시스템 및 제품을 사용하여야 한다.
- h) 전자인증서의 위조 및 변조를 예방하기 위하여 적절한 조치를 취해야 한다.
- l) 전자인증서서비스제공자가 서명자에게 전자서명생성정보를 제공하는 경우, 전자서명생성 시 이들의 정보에 관한 비밀을 보장하고, 이 정보를 보존하거나 재생산하는 것을 자제하여야 한다.
- j) 전자서명생성정보와 전자서명확인정보가 동시에 제공될 경우에, 생성정보가 확인정보에 상응하도록 하여야 한다.
- k) 재판상 전자인증의 입증을 위하여, 필요하다고 판단될 수 있는 전자인증서에 관한 일체의 정보를 저작적 형식으로 보존하여야 한다.
- l) 다음의 경우, 보증하는 전자인증서보존시스템을 사용하여야 한다 ;
 - 정보를 입력하고 변경하는 권한이 제공자에 의해 이를 위하여 허가된 자에게만 주어져야 한다.
 - 전자인증서에 대한 공중의 접근은 인증서보유자의 사전 동의 없이는 가능하지 않아야 한다.
 - 시스템의 안전성을 위태롭게 할 성질의 변경은 모두 탐지될 수 있어야 한다.

관의 명령에 의해 이를 위하여 지정된 심리절차로 교부되는 자격을 받은 조직체에 의해 교부된다(2001년 국사원령 제7조).

(1) 전자인증서비스제공자의 감독

전자서명 및 인증서비스제공자의 평가·감독 기구는 국방총사무국(SGDN; Secrétaire général de la défense nationale)산하 ‘국가정보시스템안전기구(ANSSI; Agence nationale de la sécurité des systèmes d’information)¹⁵⁾이다. 이 기관은 암호화기술의 평가와 인증 등 정보시스템안전분야에서 국가권한에 관한 임무를 수행한다. 특히 ANSSI는 2009년 령에 의하여 전자서명인증서 감독기구이었던 ‘정보시스템안전중앙국(DCSSI; Direction centrale de la sécurité des systèmes d’information)을 승계하였다.

(2) 전자인증서비스제공자의 책임

2004년 디지털 경제에서의 신용을 위한 법률에 따라, 전자인증서비스제공자는 (a) 인증서를 교부한 날짜로부터 인증서의 정보들이 정확하지 않은 경우, (b) 인증서가 공인된 것으로 보여질 수 있게 하기 위한 정보들이 불충분한 경우, (c) 인증서의 교부가 ‘서명자가 이 인증의 공적 합의에 따른 사적 합의를 가지고 있다는’ 확인을 수행하지 않는 경우, (d) 인증서비스제공자가 인증서의 철회기록을 행하지 않거나 제3자에게 이 정보를 자유로이 쓰이게 한 경우에는 제공자가 증과실 또는 태만을 행하지 않았음을 입증하지 않아도, 인증서를 신뢰한 자에게 손해배상 책임을 진다(제33조).



- m) 전자인증서가 교부되는 자의 신원을 그에게 공식신원증명서의 제출을 요구하여 확인하고, 다른 한편, 이 자가 제시하는 자격을 확인하고, 이러한 신원과 자격을 입증하기 위하여 제출된 문서의 특징 및 참조사항을 보존하여야 한다.
 - n) 전자인증서를 교부할 때에 그가 보유하는 정보가 정확하다는 것과 그렇게 신원이 확인된 서명자가 이 인증서에 포함된 전자서명확인정보에 상응하는 전자서명생성정보를 보유하고 있다는 것을 확인하여야 한다.
 - o) 전자인증서비스제공에 관한 계약 체결 전에 전자인증서교부를 신청한 자에게 서면으로 다음 사항을 통지하여야 한다.
 - 인증서 사용방식과 사용조건
 - 제7조에 언급된 전자인증서비스제공자의 의도적인 인증과정에 종속되거나 종속되지 아니한다는 사실
 - 분쟁의 불복방법과 해결방법
 - p) 전자인증서에 근거하는 자에 대한 그에게 유용한 o)에서 규정된 정보의 요소들을 제공하여야 한다.
- 15) ‘국가정보시스템기구’라 칭한 국가관할기구 창설을 위한 2009년 7월 7일 제2009-834호 령(Décret n° 2009-834 du 7 juillet 2009 portant création d’un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d’information »)에 의해 설립되었다. 이 기구의 웹 사이트는 <http://www.ssi.gouv.fr>.

6. 신뢰성의 추정

전자서명에 의한 전자 사서증서의 소지자는 일반 종이 매개체에 의한 증서의 소지자보다 우월한 지위에 놓인다. 즉, 앞에서 기술한 전자서명의 신뢰성에 관한 요건을 충족한 경우, 반대의 증거가 있기 전까지 이러한 전자서명에 관한 신뢰성은 추정된다(민법 제1316-4조 제2항). 서면이라는 매개체에 의한 증서 소지자에게 존재하지 않는 추정의 이익이 전자서명의 소지자에게 부여되는 것이다. 따라서 전자서명의 신뢰성에 대한 추

정을 번복하기 위해서는 전자증서의 내용을 부인하는 자가 전자서명 신뢰성에 관한 확인절차의 결함을 입증하여야 한다.

백 명 선

(프랑스 주재 해외법제조사원)