법안 제안 상세이유

1. (전자)서명의 '법적 효력' ?

1. 육필 서명이나 날인도 우리 법체제 하에서는 문서의 진정성립을 뒷받침하는 '증거자료'에 불과하며, 증거자료를 믿을 것인지 여부는 법관의 자유심증에 따르는 것임. 서명되거나 날인된 문서라고 해서 그 기재내용 대로의 법적 효력을 반드시 인정받는 것은 아님.

2. 육필 서명이 법률상 요구되는 경우는 지극히 제한되어 있고(예를 들어 유언, 판결서), 유언은 현행법 하에서는 아예 전자적으로 작성될 수 없고, 판결서의 전자적 작성은 별도의 법률이 규율하고 있음(민사소송 등에서의 전자문서 이용 등에 관한 법률).

3. 육필 서명이나 날인의 법적 효력은 별도의 법규정 없이 법관의 자유로운 심증에 따르는 것이므로, 전자서명 역시 그와 동일하게 취급하는 것이 적절함. 육필 서명이나 날인에는 없는 '추정력 규정'(제 3 조 제 2 항)을 전자서명에 대해서만 둘 이유는 없음.

4. 실제로 추정력 규정이 문제로 되는 경우는 (전자)문서의 진정성립 여부에 다툼이 있는 경우인데, 공격자가 유저의 인증서 개인키와 인증서 암호를 입수하여 그것으로 전자서명을 하였다면, 그런 전자서명은 '공인전자서명'으로 인정받을 수 없으므로(개인키가 유저에게만 속하고, 유저가 서명할 때에도 그 상태가 유지되었다는 점을 입증해야 공인전자서명으로 인정받을 수 있으나, 이런 입증은 불가능함), '공인전자서명'의 '추정력'이라던가, '부인방지' 효력이란 것은 애초에 거론할 여지도 없음.

5. 현행 제 3 조는 '기명'에 대해서도 거론하고 있으나, 전자문서에서 이름을 입력하여 기재하면 종이문서에 '기명'하는 것과 동일한 것으로 보는 인식은 이미 널리 확산되어 있으므로, 전자서명의 효력과 관련하여 '기명'을 거론할 여지는 없음. '기명'에 대한 언급은 삭제함.

2. '공인전자서명' 관련 현행 규정의 법적 문제점

6. 현행 제 3 조 제 1 항은 당사자 간에 합의가 없어도 공인전자서명은 서명, 날인으로서 법적 효력을 인정받을 수 있다는 취지로 규정하고 있으나, 당사자의 합의에 기하여 이루어지는 전자거래에서 일방이 타방의 반대에도 불구하고 공인전자서명을 강요한다면, 과연 자유로운 의사의 합치로 계약이 성립되었는지 자체부터 의문시 됨.

7. 거래의 일방이 스스로의 의사에 기하여 전자서명을 자발적으로 하는 것을 금지할 이유는 물론 없지만, 일방이 상대방의 의사에 반하여 그 상대방으로 하여금 전자서명을 하도록 강요하는 것은 계약 자유의 근본 원칙에 반함.

8. 한미 FTA 제 15.4 조 제 1 항 가목은 "전자거래의 당사자가 그 거래를 위하여 적절한 인증 방법을 상호 결정하는 것을 금지하는 법령"을 채택하거나 유지할 수 없도록 규정하고 있음. 물

론 인증(authentication)과 전자서명(electronic signature)이 같은 것은 아니지만, 전자서명은 인증기술을 전제로 삼고 있으며, 공인전자서명을 일방이 강요할 경우 공인인증 또한 강요하게 되는 것이므로, 현행 전자서명법 제 3 조 제 1 항은 한미 FTA 에 어긋날 소지가 있음. 한미 FTA 와 전자서명법은 국내법상 동등한 지위에 있지만, 신법 우선의 원칙에 따라 한미 FTA 가 전자서명법의 해당 규정에 우선함.

9. 전자거래는 당사자의 합의에 기하여 이루어지는 것이고, 당사자의 합의에 따라서 전자서명이 사용되는 경우에는 현행 제 3 조 제 3 항이 적용되면 족함. 굳이 공인전자서명(제 3 조 제 1 항)과 전자서명(제 3 조 제 3 항)의 법적 효력을 구분하여 규정할 이유가 없음.

3. '공인인증제도' 개선 방향

10. 국지적이고 고립된 방식으로 한국내에서만 운영되는 공인인증제도는 전세계를 기반으로 작동하는 '인터넷'의 근본 전제에 반함.

11. 정부가 인증기관을 지정하고(제 4 조), 인증기관이 수행하는 업무의 안전성을 정부가 검사(제 14 조)하도록 규정하는 현행법은, 정부가 그러한 안전성 검사를 실제로 수행할 전문성과 역량이 없으므로 형식적 검사에 그칠 수 밖에 없음.

12. 현행 전자서명법은 공인인증기관에 대한 안전성 점검을 KISA 가 수행하도록 규정하고 있을 뿐(제 19 조 제 2 항 과 제 3 항), KISA 에 대한 안전성 점검을 누가 수행하는지에 대한 규정은 없음. 현행 전자서명법 일부 조항의 적용에 있어서는 KISA 역시 '공인인증기관'으로 간주되기는 하나, 공인인증기관에 대한 안전성 점검에 관한 규정(제 19 조 제 2 항 및 제 3 항)은 KISA 에게는 준용되지 않고(KISA 가 KISA 를 스스로 점검할 수는 없기 때문), 정부가 형식적으로나마 수행하는 제 14 조의 '검사'조차도 KISA 에게는 준용되지 않음(정부에게 인증업무를 검사할 전문성이나 역량이 없기 때문; 제 25 조 제 2 항 참조). 요컨대, KISA 는 누구도 검증하거나 검사하지 아니하는 인증기관임. 글로벌 기준에 비추어 볼때, 전문성을 구비한 독립적 제 3 자에 의하여 정기적으로 점검받지 않는 인증기관은 그 신뢰성을 인정받을 수 없음.

4. 공공기관 등이 사용하는 전자서명

13. 현재, 행정기관 내부에서 사용되는 '행정전자서명'은 안전행정부의 '행정전자서명 인증관리센터'를 정점으로 구축되어 있음(전자정부법 제 29 조). 본 개정안은 행정전자서명 체계를 변경하는 내용을 담고 있지 않음.

14. 개정안은 공공기관 등이 민원거래에서 민원인에게 교부하는 전자문서에 전자서명을 하고자 할 경우, 미래창조과학부 장관이 정하는 인증업무수행기준을 충족하는 인증기관이 발행하는 인증서를 사용하도록 규정함(개정안 제 4 조). 공공기관 등이 민원거래에 전자서명을 반드시 사용하여야 한다는 의미는 아니고, 사안 별로 판단하여 전자서명이 유용하고 적절할

경우에 공공기관이 자신의 전자문서에 전자서명을 하여 민원인에게 교부할 수 있다는 의미임.

15. 민원인으로 하여금 그 의사에 반하여 전자서명을 하도록 공공기관 등이 강요하는 것은 적절하지 않음(개정안 제 3 조 제 2 항). 사적 주체들 간의 거래에서 전자서명을 사용할지 여부, 어떤 인증기관이 발행하는 인증서를 사용할지 등은 당사자의 자유로운 선택에 맡기는 것이 적절하고, 한미 FTA 제 15.4 조에도 부합됨. 사인들 간의 거래의 경우, 서비스 제공자에 따라서는 약관으로 고객의 전자서명이 요구된다는 취지를 정하고 그러한 이용조건에 기하여 고객의 전자서명을 요구하는 것은 물론 가능하며, 개정안 제 3 조 제 1 항은 이점을 확인하는 것임(현행법 제 3 조 제 3 항도 같음). 이 경우 전자서명을 원하지 않는 고객은 다른 서비스 제공자를 선택하면 될 것임. 그러나, 공공기관 등이 약관 조항에 기하여 민원인에게 전자서명을 요구할 경우, 민원인은 다른 서비스 제공자를 선택할 여지가 없어지므로 전자서명을 자신의 의사에 반하여 강요당하게 되는데, 이런 상황은 적절하지 않음.

5. 인증업무수행기준

16. 개정안은 인증기관 업무수행의 기술적, 관리적 측면에 대한 점검을 정부가 하는 것이 아니라(정부는 실질적 점검 역량이 없음), (1)정부는 '인증업무수행기준'을 제정하고 (2)실제 점검은 전문성을 구비한 보안점검 업체가 정기적으로 수행하도록 하고 있음.

가. 인증업무수행기준

17. 인증업무수행기준은 미래창조과학부장관이 제정하되, 인증 업무에 관하여 국제적으로 통용되는 업무수행기준을 반영하도록 규정함.

18. 현재, 인증 업무의 안전성과 신뢰성에 관하여 전세계적으로 통용되는 점검 기준은 다음과 같음:

    - WebTrust Program for Certification Authorities[1]
    - ETSI TS 101 456 v1.4.3
    - ETSI TS 102 042 V2.1.1
    - ISO 21188:2006

19. 주요 웹브라우저들 역시 인증 기관의 안전성에 대하여 누구보다도 지대한 관심을 기울이고 있으며, 웹브라우저들은 인증 기관이 충분한 전문성을 가진 독립적 제 3 자에 의하여 국제적으로 통용되는 이러한 인증업무수행기준을 준수하는지를 정기적으로 점검 받는다는 증빙이 없으면 그러한 인증 기관은 신뢰하지 아니함.

1 http://www.webtrust.org/principles-and-criteria/item27818.pdf

- Microsoft Root Certificate Program[2]
- Mozilla CA Certificate Maintenance Policy (Version 2.1)[3]
- Apple Root Certificate Program[4]
- Specification for X.509 root certificates to be included in the Opera browser[5]

20. 미래창조과학부는 국제적인 기술 경향을 반영하는 적절한 인증업무수행기준을 마련하여 공표함으로써 국내의 인증 기술 및 인증 서비스를 국제 수준으로 끌어올리고 보안 감사 서비스 시장의 활성화를 지원할 수 있을 것임.

나. 보안 점검(보안 감사, security audit) 서비스 시장 활성화

21. 현행법은 '정부'가 공인인증기관의 안전운영 여부를 '검사'하고(제 14 조), 공인인증기관의 안전성 점검을 KISA 가 수행하도록 규정하고 있으나(제 19 조 제 2 항, 제 3 항), 이런식의 '관주도' 접근 방식은 보안 감사 서비스 시장의 등장을 원천 봉쇄하는 결과를 낳음.

22. 미래창조과학부 장관이 제정한 인증업무수행기준에 따라 점검을 '실제로' 내실 있게 수행할 수 있는 전문성을 구비한 자(competent auditor)를 어떻게 양성할 것인지가 핵심적 중요성을 가지는바, 관련 업계의 의견을 반영하여 '민간 주도'의 accredition 프로그램이 등장할 수 있도록 적절히 지원하는 것이 바람직함(WebTrust 가 운영하는 자격 취득 프로그램 참조).[6] 만일 정부가 '인허가' 방식으로 이 문제를 접근할 경우, 보안 감사 서비스 시장의 경쟁과 활발한 성장을 저해하고, 기득권 업자를 양산하는 등 기존 공인인증제도가 안고 있는 문제를 고스란히 반복하게 될 우려가 있음.

23. 공인인증기관을 '정부'가 지정하고, '정부'가 검사하고, 정부 산하기관인 KISA(누구도 검증하지 않는)가 '점검'하도록 해둔 '관치 보안'으로 일관한 지난 13 년간 국내 보안 업계는 세계에서 고립되는 결과로 되어, 인증업무의 안전성 점검을 제공할 전문성을 세계 시장에서 인정받는 보안 감사(security audit) 업체가 단 한 곳도 생겨나지 못했음을 반성할 필요 있음.

24. 인증 서비스 및 보안 감사 서비스의 활성화 및 선진화를 위한 미래창조과학부의 바람직한 역할은 보안 감사 서비스에 필요한 적절한 교육과 훈련 및 보안 감사 서비스의 품질관리 프로그램이 민간 영역에서 활발하게 등장하고 가동될 수 있도록 지원하는 것이지, 정부 인허가 체제를 도입하는 것이 아님.

---

2 http://technet.microsoft.com/en-us/library/cc751157.aspx#EGAA
3 http://www.mozilla.org/projects/security/certs/policy/MaintenancePolicy.html
4 http://www.apple.com/certificateauthority/ca_program.html
5 http://www.opera.com/docs/ca/
6 http://www.webtrust.org/signing-up-for-the-trust-services-program/item64422.aspx

6. 벌칙

25. 개정안은 정부가 인증기관을 지정하는 것이 아니라, 누구든지 인증 서비스를 제공할 수는 있지만, 정부가 정한 인증업무수행기준을 충족하는 업체는 그 점을 표시하도록 하는 것임 (제 5 조 제 1 항). 과연 그 업체가 인증업무수행기준을 실제로 준수하는지 여부는 '사전 통제'가 아니라, 사후 통제로 전환하는 것이 개정안의 골자임.

26. 인증업무수행기준 준수 여부를 정부가 '사전에' 통제하겠다는 발상은 결국 인허가 제도와 마찬가지의 '관 주도' 보안 정책으로 또다시 귀결할 뿐 아니라, 인증업무수행기준을 준수하는지 여부는 훈련된 보안 감사 전문가(competent auditor)가 판단 할 사안이지, 전문성을 기대할 수 없는 공무원이 판단할 사안이 아님.

27. 미국 캘리포니아 주의 전자서명 관련 규정[**첨부자료 참조**]에서도, 정부는 인증업무 수행 등에 관한 '기준'만을 제정할 뿐, 그 준수 여부를 정부가 '검사'하거나, '점검'한다는 규정은 없음. 그 이유는 어느 나라의 '정부'도 그런 검사를 하거나 점검을 할 전문성은 없기 때문이고, '정부'가 섣불리 그런 시도를 할 경우, 민간에서 그러한 점검 서비스가 활발하게 성장할 기반이 박탈되기 때문임.

28. 정부가 제정, 공표한 인증업무수행기준을 충족하거나, 국제적으로 통용되는 인증업무수행기준을 충족하는 인증기관은 그 사실을 표시하게 함으로써, 그러한 기준을 충족하지 못하는 인증업체와의 실질적 차이를 소비자들이 스스로 파악할 수 있을 것임.

29. 반면에, 정부가 인증기술이나 특정 인증 업체의 '안전성'을 보증, 보장, 선전하는 것은 바람직하지 않음. 일반적으로 어떤 보안 기술에 대하여서도 그것이 '안전하다'는 주장을 정부가 공식적으로 내세우는 것은 상식에 어긋나는 것임. 특정 보안 기술이 '안전한지'는 그 기술을 적용한 거래로 인하여 피해를 입은 소비자가 보상을 받을 수 있는지, 얼마나 받을 수 있는지에 당장 영향을 미치는 첨예한 쟁점이므로, 이 문제에 대하여 정부가 "그 기술은 안전하다"면서 사업자(금융기관) 편을 드는 모습을 보이는 것은 소비자 보호에 막대한 지장을 초래하게 됨. 자신이 제공하는 서비스의 안전성을 마치 정부가 보장하는 듯 선전하는 인증기관은 처벌할 필요가 있음.

30. 정부가 특정 보안 기술을 강제하거나, 후원하거나, 그 안전성을 보장하는 듯한 모습을 보일 경우,

    - 해당 기술의 '안전성'이 과장되게 인식되고
    - 법관 마저도 그 기술이 매우 안전할 것이라는 예단을 가지게 되어, 사고거래의 책임을 고객에게 지우는 쪽으로 판단하게 될 위험이 생김.

- 사례 1: <전화사기 피해자 잇단 패소…'본인인증'이 발목>

- “타인이 정씨 명의를 사용해 계약을 체결했더라도 정씨가 본인 인증을 해줬다면 대리권을 준 것으로 봐야 한다” “공인인증서 인증은 전자상거래상 본인 여부를 확인하기 위한 충분한 수단이다” 서울중앙지법 민사 45 단독 이영선 판사
- http://www.yonhapnews.co.kr/bulletin/2013/04/01/0200000000AKR20130401197000004.HTML?input=1179m

- 사례 2: <보이스피싱 피해자도 일부 패소>: 2012 가단 5088900 판결
  - 사기범이 보이스피싱을 통해 피해자의 공인인증서 재발급에 필요한 정보를 획득한 다음, 공인인증서를 쉽게 재발급받아 피해자 명의로 저축은행에서 인터넷 대출을 받고 그 돈을 대포통장으로 이체시키는 수법을 사용한 사례에서 법원은 피해자들(모두 6 명이 유사한 범죄의 피해자였음)에게 발생한 손해의 40%를 피해자들에게 부담시킴. 서울중앙지법 민사 49 단독 안희길 판사

첨부 문서:

1. Microsoft Root Certificate Program (발췌)
2. Mozilla CA Certificate Maintenance Policy (Version 2.1) (발췌)
3. Apple Root Certificate Program (발췌)
4. Specification for X.509 root certificates to be included in the Opera browser (발췌)
5. California Code of Regulations, Title 2, Division 7, Chapter 10 (Digital Signatures) (전문)