법안 제안 상세이유

1. 공인인증서의 문제점

비표준적 위치(NPKI 폴더)에 저장되고 있으므로,

- 이용자들이 별도 프로그램을 자기 컴퓨터에 설치 해야하는 번거로움과 보안상 위험이 따르고
- 단순히 copy & paste 함으로써 이용자의 인증서 개인키가 쉽게 복제, 유출되며
- 다양한 운영체제이나 디바이스, N-스크린 환경에 대응하기가 어렵고
- 글로벌 표준과 동떨어진, 고립된 인터넷 환경을 조성하고 있음.

국내 최상위 공인인증기관 KISA 는 국제적으로 인정받거나 신뢰받지 못하고 있으므로,

- 서버인증에 사용될 수가 없고,
- 국내 공인인증업체의 외국 진출이나 세계 인증 시장 진출은 불가능
- 13 년간의 정부 지원과 보호주의 정책에도 불구하고 국제경쟁력을 구비하지 못하는 상황

공인인증서 99% 이상은 파일 형식(soft token)인바,

- 미국 국립표준기술 연구소(NIST)가 2006 년 4 월에 발간한 전자인증 가이드라인(Electronic Authentication Guideline)에 의하면, 이렇게 전자파일 형태로 배포된 인증서(Soft crypto token)의 보안 강도는 높게 평가되지 않음. 단순암호(Password)보다는 우월하나, OTP(일회용 암호)생성기보다 우월하지도 않음.

Table 2. Token Types Allowed at Each Assurance Level

Token type	**Level 1**	**Level 2**	**Level 3**	**Level 4**
Hard crypto token	√	√	√	√
One-time password device	√	√	√	
Soft crypto token	√	√	√	
Passwords & PINs	√	√		

Electronic Authentication Guideline, p. 39 (위 표에서 Level 1 은 초보적 수준의 보안강도를 말하며, Level 4 는 가장 고도의 보안강도를 뜻함. Hard crypto token 은 하드웨어 토큰임)

- 실제로, 2000 년대 초반까지는 공인인증서 만으로 거래하다가, 도저히 사고를 막을 수 없어서 그 보다 강력한 일회용 암호수단(보안카드 또는 OTP 생성기)을 도입한 것임. 공인인증서로 막을 수 없는 상황에서, 그 보다 "저급한" 수준의 보안조치를 추가할 이유는 없음.
- 하드웨어 토큰(HSM) 방식의 공인인증서 보급율은 0.7%에 불과함.

공인인증서는 이미 대규모로 유출되고 있음.

- 2007 년에 5000 장 이상 유출됨 http://www.boannews.com/know_how/view.asp?page=40&gpage=31&idx=1539&numm=1211&search=title&find=&kind=03&order=ref
- 2013 년에도 700 여장 유출됨 http://www.nocutnews.co.kr/show.asp?idx=2401707
- 드러나지 않은 유출 규모는 알 수 없음.
- 공인인증서 탈취용 악성코드는 널리 퍼져 있고, 이용자에게 '주의'를 당부하는 것으로는 역부족임. http://www.ddaily.co.kr/news/news_view.php?uid=103122

그림 왼쪽은 정상적인 공인인증서 이용 프로그램이고 오른쪽은 공인인증서와 비밀번호를 탈취하는데 사용되는 악성코드임. 웬만해서는 식별 불가.

2. 금융소비자의 피해

정부가 특정 '보안' 기술을 강제하거나 후원(endorse)할 경우,

- 해당 기술의 '안전성'에 대하여 과장된 인식이 자리하게 되고
- 법관 마저도 공인인증기술이 마치 대단히 안전한 기술이라고 오해하게 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
- 정부가 특정 보안 기술에 대하여 '안전하다'는 공식 입장을 취할 경우, 그 기술을 사실상 판

촉(promote)하거나 후원(endorse)하는 셈이 되는데, 정부의 이런 행위는 무모할 뿐 아니라, 억울한 피해자를 양산하게 될 위험이 있음.

3. 정부 정책 및 규제의 기술 중립성

공인인증서 사용 강제는 전자금융거래법 제 6 조에 위반될 소지가 있음

- 전자금융거래법 제 6 조 제 1 항은 "금융기관 또는 전자금융업자는 전자금융거래를 위하여 접근매체를 선정하여 사용"하도록 하고 있는바, 공인인증서를 사용하도록 강요하는 금융위원회의 행위는 금융기관 등이 접근매체를 '선정'하지 못하게 하는 것이므로 모법 조항의 취지에도 어긋나고 있음.

금융위원회의 공인인증서 사용 강제 조치는 한국정부의 국제법적 의무에도 위반됨

- 한국정부는 2009 년 3 월 15 일에 바젤위원회(BCBS) 회원국이 되었으므로, 동 위원회가 채택하는 은행감독 원칙을 준수할 국제법적 의무를 지고 있음.
- 바젤위원회는 "어떤 인증 기법을 사용할 것인지는 … 은행경영진의 평가에 기초하여 은행이 결정하여야 한다"는 원칙을 채택하고 있음(Risk Management Principles for Electronic Banking, Principle 4). 전자금융거래법 제 6 조 제 1 항도 같은 취지임.
- 공인인증서의 사용을 강제하는 금융위원회의 규제는 이 원칙에 위반됨

국내법과 동등한 효력이 있는 한미 FTA 에도 어긋남

- 한미 FTA 제 15.4 조 (전자인증 및 전자서명) 제 1 항 '가'호는 "전자거래의 당사자가 그 거래를 위하여 적절한 인증 방법을 상호 결정하는 것을 금지하는 법령"을 한국이나 미국이 채택하거나 유지할 수 없도록 규정하고 있음.
- 현행 전자금융거래법 제 21 조 제 3 항에 기하여 공인인증서 사용을 강제하는 한국 정부(금융위원회)의 조치는 인증방법을 거래당사자가 적절히 선택하여 결정하도록 해야 한다는 이 조항에 어긋남.
- 한미 FTA 제 15.4 조 제 2 항은 "정당한 정부 목적에 기여"하고, 그 목적 달성과 "실질적으로 연관"된 경우에 한하여 정부가 당사자의 인증방법 선택권을 제한할 수 있도록 규정하고 있음. 그러나,
    - 공인인증서 사용을 강제하는 조치는 공인인증 관련 업체들에게 부당한 사업적 특혜를 부여할 뿐, 정당한 정부 목적에 기여하는 것이 아님.
    - 거래의 '안전'은 모든 정부가 추구하는 정당한 목적이지만, 이미 15 년이나 지난 낙후된 보안기술의 하나에 불과한 '공인인증서'만이 '안전'을 제공하는 기술 수단이라는 주장은

근거가 없음.

- 국가의 모든 전자금융거래가 하나의 인증기술에만 의존하는 상황은 오히려 안전을 해하는 것이므로, 현행 공인인증서 강제 조치를 폐기하는 것이 오히려 정당한 정부 목적에 기여하는 것임.

4. 경쟁을 통한 보안 기술의 발전, 혁신 필요

- 공인인증서 사용 강제로 인해 국내 보안 기술 시장에는 의미있는 경쟁이 지난 13 년간 존재하지 않았음
- 공인인증 관련 업체들의 과점 상태로 인하여 보안 기술 시장이 위축
- 인증 및 보안 기술의 자유로운 선택이 보장될 경우, 더욱 선진적인 인증기술이 국내시장에 도입될 수 있고, 앞으로도 더욱 빠른 속도로 보안 기술이 개선 발전될 것임
- 취약한 보안 기술은 이를 채택하는 금융기관에게 직접적이고 즉각적인 손해를 발생시키는 것이므로, 업계는 더욱 안전한 보안 기술을 스스로 선택할 강력한 동기(incentive)가 이미 존재함.
- 사고거래의 책임을 금융기관에게 부담시키는 현행 전자금융거래법 제 9 조가 제대로 적용되어, 사고의 책임을 개인 고객에게 떠넘기지 않도록 금융감독기구가 올바르게 감독하고, 법원이 특정 인증/보안 기술을 명백한 기술적 근거 없이 신뢰하지 않도록 하는 것이 보안 기술 발전의 관건임.

첨부 문서:

1. 미국 국립표준기술 연구소(NIST), 전자인증 가이드라인(Electronic Authentication Guideline) (2006), 제 39 면
2. 바젤위원회(BCBS), 전자금융 위험관리 원칙(Risk Management Principles for Electronic Banking) 중, 제 4 원칙
3. 한미 FTA 제 15.4 조 (전자인증 및 전자서명)
4. 2007 년 7 월 10 일자 보안뉴스 보도(공인인증서 5000 여장 유출)
5. 2013 년 2 월 11 일자 CBS 노컷뉴스 보도(이번엔 금융권 공인인증서 대량 해킹 '비상')

6. 2013 년 4 월 7 일자 디지털데일리 보도 (공인인증서 탈취 악성코드 발견, 주의요망)
7. 2013 년 4 월 2 일 자 연합뉴스 보도 <전화사기 피해자 잇단 패소…'본인인증'이 발목>
8. 서울중앙지방법원 2013.2.15 선고 2012 가단 5088900 판결 판결문
9. “공인인증서 FAQ” (오픈넷) http://opennet.or.kr/1789