전자서명법 , 전자금융거래법 개정안

- 인증제도 및 보안기술 규제의 선진화 , 글로벌화 전략 -

2013.5.23

김기창 (고려대학교 법학전문대학원 교수)

1. '정부 주도' 보안의 문제점 1 – 공인인증서

1-1. '권한구분' 개념이 없던 시절에 개발된 낡은 기술

- 현행 공인인증서 기술은 윈도우 운영체제가 일반유저/관리자 권한 구분을 하지 아니하던 미개한 시절(윈도우 2000 이전)의 보안 상황을 전제로 설계됨. 유저 인증서(공인인증서)를 운영체제의 시스템 파일 폴더에 저장하는 문제
- 윈도우 비스타부터는 심지어 ActiveX 도 non-admin 권한(제한된 권한)으로 설치, 실행할 수 있도록 개선되었으나, 국내 보안인력은 이런 사실을 이해 못하고 여전히 관리자 권한을 전제로 공인인증서 기술을 구현하고 있는 후진적 상황

1-2. Keystore, Keychain, Keyring, Credentials Storage 개념에 대한 몰이해

- "NPKI 폴더"에 유저인증서와 유저개인키를 저장하는 공인인증서 기술은 개인인증서 사용을 위하여 애초에 주요 OS 에 구현되어 있는 Keystore, Keychain, Keyring, Credentials Storage 라는 기술의 존재 자체를 몰랐거나, 이들의 기능이나 존재 이유를 제대로 이해하지 못한 시점에 개발된 후진적 기술이었음. 아이폰 도입 후에 비로소 (아이폰에 한하여) Keychain 사용.
- NPKI 폴더에 저장된 유저개인키는 무단 복제가 무한정 가능함. 그러나 이 사실을 모르는 컴맹 이용자를 상대로 하여 "암호 입력"이나 16 자리 또는 8 자리 숫자의 "인증 코드 입력"을 요구함으로써, 이 취약점을 기만적으로 가려 덮으려 함.

1-3. 플러그인에 의존하는 해법

- 유저 행태를 '위험하도록' 유도: "설치하시겠습니까?" "예"

- 추가적 '보안플러그인' 설치를 거듭 강요함으로써, 유저 행태를 더욱 위험하게 유도
- 하지만, 추가적 보안플러그인은 실제로는 실효성이 없음:
    - '심리적 안심'을 주려는 보안 쇼(security theatre)에 불과함.
    - '파일+고정 암호'의 유출을 보안플러그인 '설치'로 막을 수는 없음

1-4. '서버' 인증 개념 부존재

- 공인인증서는 "HTTP 접속+플러그인" 형태로 구현되는 것. 따라서 유저가 플러그인을 내려받을 때(서버 identity 확인이 가장 필요한 순간)에는 어떠한 서버 인증 수단도 없음.
- 공인인증서 기술은 오로지 '유저' 인증 용도로 개발된 것이라는 근본적 한계가 있음.
- KISA 와 국내 공인인증기관들은 아직도 '서버'인증서를 제대로 만들지 못함. 오페라 웹브라우저로 국내 공인인증기관이 발급한 서버인증서를 장착한 웹서버에 접속을 시도하면, 접속 오류 발생. ex. https://www.kisa.or.kr (7 년이 지난 오늘도 해결 못하고 있음)
- 공인인증기술과는 달리, 웹브라우저에 기본 탑재된 "유저인증 HTTPS 프로토콜 접속" 기술은 서버인증과 유저인증을 '동시에' 수행함. 예제, https://openweb.or.kr/cert/auth

1-5. 루트인증기관에 대한 독립적 , 전문적 , 정기적 검증(실사) 결여

- 공인인증체계의 논리적, 제도적 정점에 위치한 루트인증기관(KISA)는 누구로부터도 검증 받지 아니함.
- 루트인증기관의 신뢰성 확보가 전세계적으로 어떻게 이루어지는지 이해하지 못한 시점에 도입된 인증체제가 바로 한국의 공인인증체계 임.
- 국제적으로 고립된 인증체계
- 국가간 "상호 인정 협정"을 거론하는 법 제 27 조의 2 는 전세계적으로 구축된 루트인증기관의 신뢰성 확보 메카니즘(제 3 자 검증)에 대한 몰이해를 노출할 뿐.
    - 루트인증기관이 한국처럼 제 3 자에 의하여 검증받지 아니하는 경우, 그를 정점으로 구축된 인증체계를 믿을 이유는 없음.
    - 실제로 지금까지 한국은 어떤 나라와도 상호 인정 협정을 체결하는데 성공한 바 없음.

- 인증 제도의 근본 기초인 '신뢰성 확보 메커니즘' 자체에 대한 무지를 노출할 뿐.

- '권위주의'에 입각한 공인인증제도: 아무도 검증 안하는 KISA 를 정점으로 구축된 공인인증 체제를 무작정 믿으라고 국민에게 강요하는 정부의 요구는 상식을 벗어난 것.

2. ' 정부 주도' 보안의 문제점 2 – 규정 보안

끊임없이 변하는 기술적 디테일을 '행정 규칙'의 형태로 '정부'가 제정, 운용하는 것이 과연 적절한지?

2-1. 금융위원회 고시

- 전자금융감독규정 제 3 장은 매우 상세한 보안 기술적 디테일을 규정화 하고 있음(ex. 손전등 비치 의무 등).

2-2. '행정안전부' 고시 (아직 미래부로 변경되지도 않음)

- 공인인증기관의 시설 및 장비등에 관한 규정은 "RSA 또는 KCDSA 1024 비트 이상의 전자서명키 생성 기능" 등 낡은 기준을 그대로 방치
- 공인인증기관의 보호조치에 관한 규정은 "시스템에 대한 논리적인 접근통제를 설정할 것" 등 공무원이 검사할 역량도 없는 내용

3. ' 정부 주도' 보안의 문제점 3 – 점검 부실, 부재

- 기술적 디테일을 담은 '규정'이 과연 실제로 준수되는지 여부를 누가 검사/검증/실사 하는지?
- '규정상'으로는 전자금융감독규정의 준수 여부는 금감원이 검사.
  - "보안성 심의"는 일회성 검사. 하지만 실제로 금감원 직원이 검사를 수행할 전문성이 있는지?
  - 감독규정의 나머지 부분은 과연 언제, 얼마나 자주 금감원이 검사하는지? (대형 사고 발생하면 '특별 검사'를 실시, 하지만 과연 실효성 있는지?)
- 공인인증기관에 대한 정기 점검은 KISA 가 수행.
- 그러나, KISA 에 대한 검증은 누가 하나? Nobody.
  - 미래부 직원이 과연 KISA 를 검증할 역량이 있는지?
- 검증수행기관을 미래부나 금융위가 평가하고 판단하여 '지정'할 역량이 있나?

4. ‘관치 보안’, ‘규정 보안’의 참담한 결과

- “북한이 그랬어요 ㅠㅠ ...”
- 악성코드 배포 웹서버 ‘비율’ 세계 최고
- 개인 PC 감염 비율 세계 정상급
- 면피용 보안:
  - “우리는 규정이 하라는 것은 모두 했다. 따라서 면책되어야 한다”는 주장 제기 가능성만을 제공할 뿐.
  - ‘최소’ 요건을 행정 규정화하고 위반시 제재 규정을 둘 경우: 규정된 이상은 하지 아니하는 결과로 되어 원래 의도와는 달리 ‘최소’ 규정이 사실상 ‘최대’ 조치 내용으로 둔갑.
  - 규정을 충족하였다고 주장하며 ‘면책’될 가능성이 생기기 때문에, ‘자발적’으로 보안에 투자할 인센티브는 감소. 이 문제를 극복해 보겠다고 ‘억지 투자를 강요’하는 규정을 또다시 도입(전자금융감독규정 제 8 조, 인력, 조직 및 예산에 관한 규정; 위헌 소지 있음)
- 이러한 악순환은 결국 소비자 피해로 귀결

5. 보안 기술 발전 , 보안감사 서비스 산업 토대 마련 필요

<u>5-1. 금융보안 및 인증업무수행 ‘기준’을 마련하고 관리할 역량</u>

- 민간 업계/전문기술 단체가 자율적으로 제정하고, 관리(업데이트)하는 금융보안 및 인증 업무수행 기준이 생겨나도록 권장, 지원할 필요 있음.
- 국제적으로 인정받는 다음 기준들은 모두 ‘전문기술 단체’가 자체적으로 마련하고 관리하는 것임. 어느 나라의 행정 조직도 여기에 개입하지는 않음:
  - PCI DSS (Payment Card Industry Data Security Standards) (금융보안 기준)
  - WebTrust Program for Certification Authorities (인증업무수행 기준)
  - Public key infrastructure for financial services — Practices and policy framework (인증업부수행에 관한 ISO 기준)
  - Electronic Signatures and Infrastructures (ESI) Policy requirements for certification

authorities (ETSI) 유럽연합통신표준 기구가 제정한 인증업무수행 기준

- 한국의 전문기술 단체도 이제는 그 역량을 개발, 향상할 시점에 도달했다고 봄. 국제적으로 인정받는 이러한 기준을 연구, 참고하여 우리도 이들에 버금가는 기준을 마련하고 자체적으로 관리할 역량을 길러나가야 할 것임.
- 전문적 기술 기준을 '정부'나 '행정 규정'에 일임하는 태도를 계속한다면, 국내의 전문기술 집단은 영원히 후진성을 면할 수 없고, 세계 수준의 기술 역량을 기를 기회는 박탈될 것임.

5-2. 민간 전문 업체가 수행하는 보안 감사 서비스 시장 활성화 필요

- 위에 소개한 '기준'을 제정하고 관리하는 '전문기술 단체'들은, 금융회사나 인증기관이 그 기준을 과연 준수하는지를 점검할 전문 점검(보안 감사) 업체에 대한 품질 관리도 자율적으로 수행하고 있음.
  - Licensed WebTrust Practitioners : International
  - SysTrust Seal
  - WebTrust Seal
  - PCI Qualified Security Assessors (QSAs)
- 국내의 '전문기술 단체'들도 이제는 이처럼 '보안 감사 업체의 품질 관리'를 수행할 수 있는 역량을 자체적으로 기르도록 노력해 나가야 할 때가 되었다고 봄.
- 보안 점검(금융보안 기준이나 인증업무수행기준을 금융회사나 인증업체가 과연 준수하는지 여부에 대한 점검)을 정부, 행정 부서가 하겠다고 나설 경우,
  - 민간의 전문 보안감사 서비스 업체가 등장할 수가 없고, 활발히 영업할 수도 없고,
  - 민간 보안감사 업체의 품질 관리를 국내의 '전문기술 단체'들이 할 역량을 기를 기회도 원천 박탈됨.
- 현재의 공인인증체제와 전자금융감독체제는 금융보안이나 인증서비스 보안 점검을 KISA/금감원/미래부가 '독점'하겠다는 것이지만, 다음과 같은 심각한 문제가 있음
  - KISA 자체는 아무도 검증 안함
  - 금감원/미래부는 보안 점검을 수행할 역량 자체가 없음.

6. 한국의 공인인증제도에 대한 국제적 평판

- “I am well aware of the South Korea screw up. We use it as an example of how not to do it.” - Mr Andy Smith (BCS The Chartered Institute for IT) 2013.4.23.
- Mr Andy Smith 는 영국 정부의 국무회의(Cabinet Office)가 채택한 아래 백서의 집필자임
  - PKI Implementation Strategy, v. 1.0 (2013.2.28)
  - Public Key Infrastructure, v. 1.0 (2011.7.28)

7. 전자금융거래법 개정안

- 제 21 조 제 3 항을 다음과 같이 개정:

  금융위원회는 전 항의 기준을 정함에 있어서 보안기술과 인증기술의 공정한 경쟁을 저해하거나, 특정기술 또는 서비스의 사용을 강제하여서는 아니된다 .
- 이를 계기로, 전자금융감독규정의 전면 재검토 역시 필요함:
  - 감독규정은 근본 원칙만을 제정 (BCBS 전자금융위험관리 원칙 참조)
  - 상세한 보안 감사 기준은 업계 / 전문기술 단체가 제정하고, 상시 관리(업데이트)하는 것이 옳음.
  - 보안 점검은 전문 보안 감사 업체(security auditor)가 정기적으로 실시하고, 보안 감사 보고서를 공개.
  - 보안 감사 업체는 자신의 전문성을 소명하고 금융위에 등록하고 영업
  - 금융회사는 자신이 어느 업체로부터 보안 감사를 받는지를 공지하고, 보안 감사 보고서도 투명하게 공개하여야 함.

8. 전자서명법 개정법률안

- “공인” 제도 폐지
- ‘일방적’ 전자서명 강요 중단 : 합의에 기한 전자서명 사용 (한미 FTA 참조)
- 전자서명의 ‘추정력’ 규정 삭제(법관의 자유심증 존중)
- 루트인증기관에 대한 제 3 자 검증 제도 도입(인증서비스에 대한 Governance, safety assurance

의 문제).

- 미래부는 인증업무수행기준의 핵심 원칙과 최소한의 가치만을 제정 , 공지
  - 구체적인 인증업무수행기준 자체는 업계/전문기술 단체가 독자적, 자율적으로 작성하고, 상시 관리(업데이트)
  - 국제적으로 인정받는 인증업무수행기준은 이를 국내에서도 존중하고 반영해야 함.
- 인증업무수행기준 준수 여부는 전문 보안감사 업체가 상시적(정기적)으로 점검(실사)
  - 전문 보안감사(인증업무 감사) 업체는 자신의 전문성을 소명하고 미래부에 등록하고 영업
  - 보안감사 업체들의 품질 관리는 업계/전문기술 단체가 자율적인 License, 감사서비스 품질 관리 제도를 운영함으로써 확보
  - 국제적으로 인정받는 보안감사 업체의 전문성과 신뢰성은 국내에서도 이를 존중

9. 행정권력의 사전 통제 v 업계의 자율 규제 + 사법부에 의한 사후 통제

- 정부의 사전 지정, 사전 인가의 폐해
  - 예들 들어, “정보보호 사전점검에 관한 고시”(방통위 고시)를 보면, ‘사전점검 수행기관’(보안감사 서비스 업체)를 정부(방통위)가 지정하도록 규정하고 있으나(제 6 조), 이러한 제도는 보안감사 서비스 시장에 대한 ‘진입장벽’으로 작용할 뿐 아니라, 방통위 직원이 전문 보안감사 업체의 역량과 전문성을 실제로 ‘평가’할 역량은 없음.
  - 정부는 보안감사 업체의 품질관리를 수행하는데 필요한 전문성이 없음.
  - 그럼에도 정부가 보안감사 업체를 ‘지정’하려 할 경우, 민간/업계의 역량, 기술, 전문성 발달의 기초가 아예 박탈됨.
- 민간 자율, 진입 장벽 제거, 자유 경쟁 확보 필요
  - 업계/전문기술 집단의 ‘평판’에 기초한 사전적 품질 관리가 이루어질 것
  - 수검 기관 / 금융회사의 “self interest”가 작동함을 이해할 필요 있음: ‘무료’ 검사가 아니라, 비싼 돈을 지불하고 “유료 검증”을 받는 금융회사 등이, 허술한 검증 서비스를 일부러 묵인할 이유는 없음.

- “충분한”, “적절한”, “합리적인” 등에 대한 판단은 (사후적) 재판 절차를 통하여 판정.

10. 전자금융 사고거래에 대한 책임 (개인고객의 경우)

- 한국 : 금융회사가 배상 (전자금융거래법 제 9 조)
  - 개인고객의 고의, 중과실을 금융회사가 입증하면 고객 부담
- 미국 : 금융회사가 배상 (EFTA; 15 U.S.C. § 1693g(a))
  - 접근매체 유출 / 분실을 고객이 “알고나서 이틀 내에 신고하면” 그 사이에 아무리 많이 사고거래가 이루어졌더라도 50 달러만 고객부담
  - ‘신용카드 번호’를 공격자가 알아내서 거래한 경우, 고객이 해당 거래사실을 통보 받은 날 (거래명세서를 배달받은 날)로부터 60 일 내에 이의 제기하면, 고객 부담은 0.
  - 문제의 거래내역을 통지받고 60 일이 지나도록 고객이 문제 제기를 안하면, 고객 부담액 증가.
- 영국: 금융회사가 배상 (Financial Conduct Authority 규정)
  - Your bank may only refuse a refund for an unauthorised transaction if it can prove you are at fault because you acted fraudulently, or because you deliberately, or with gross negligence, failed to protect the details of your card, PIN or password in a way that allowed the transaction.

규제 당국의 올바른 자세는, “금융회사들, 당신들이 알아서 보안기술을 선택하라. 단, 사고가 나면 철저히 물어줘야 한다”는 것임.

규제 당국이 금융회사에게 특정 보안기술(공인인증서)을 사용하도록 강제할거면, 사고거래 책임도 그 기술 사용을 강요한 금융위/금감원 해당 공무원이 지는 것이 옳을 것임. 배상책임도 지지않을 규제 당국이 금융회사의 인증/보안 기술 선택에 개입해서 이래라 저래라 강요하는 것은 무책임하고, 위법한 것임(특정 업계와의 결탁 의혹을 사게 됨).

전자금융감독규정 제 3 장 (현행 감독규정 제 7 조-제 41 조)의 개정 방향 [예시]

[금융위원회 고시]

제 3 장 전자금융거래의 안전성 확보 및 이용자 보호

제 1 절 규제자의 임무

제 7 조(금융소비자 보호) 금융위원회와 금융감독원은 전자금융 서비스가 기술 발전을 반영한 합리적 방법으로 안전하게 제공되고, 전자금융거래와 관련된 분쟁이 신속하고 정당하게 해결되도록 하여 금융소비자가 적절히 보호되는데 필요한 감독을 수행한다.

제 8 조(금융회사 등의 책임성 확보) 금융위원회와 금융감독원은 금융회사 등이 우월적 지위를 남용하거나 법령이 정한 책임을 부당하게 소비자 또는 다른 사업자에게 전가하거나 회피하지 않도록 하는데 필요한 감독을 수행한다.

제 9 조(기술 및 서비스의 자유로운 경쟁과 발전) 금융위원회와 금융감독원은 전자금융거래 서비스 제공에 사용되는 거래기술, 보안기술 및 보안감사 서비스가 활발하고 공정하게 경쟁하고 발전할 수 있는 시장 환경이 손상되지 않도록 감독을 수행한다.

제 10 조(규제의 투명성 및 형평성) 금융위원회와 금융감독원은 전자금융거래 서비스와 관련된 정보가 적절한 수준에서 투명하게 공개되고 규제의 형평성이 유지되도록 한다.

제 2 절 금융회사 최고 경영진의 책임

제 11 조(관리 감독 체계의 확립) 금융회사 등의 이사진과 최고 경영진은 전자금융 사업에 관한 위험을 관리하고 책임소재를 분명히 하는데 필요한 관리 감독 체계를 자체적으로 확립하여야 한다.

제 12 조(일괄 위임의 금지) 금융회사 등의 이사진과 최고 경영진은 자신의 전자금융 사업에 적용되는 보안 통제 절차의 핵심적 사항을 직접 검토하고 승인한다.

제 13 조(외주 계약 관계 등의 점검과 관리) 금융회사 등의 이사진과 최고 경영진은 자신의 전자금융 사업이 외주 계약 관계 등 제 3 자에게 의존하는 부분에 대하여 적절히 점검하고 관리하는데 필요한 상시적 체계를 수립한다.

제 14 조(직원의 훈련 및 교육) 금융회사 등의 이사진과 최고 경영진은 전자금융 사업에 수반되는 위험을 관리하는데 필요한 인력을 충분히 확보하고 그들에 대한 상시적이고 정기적인 훈련 및 교육 프로그램을 마련한다.

제 3 절 보안 통제 조치

제 15 조(적절한 인증기술의 채택) 금융회사 등은 거래의 성격과 해당 거래에 수반하는 위험의 수준을 고려하여 업계의 기술 수준을 반영한 합리적인 당사자 인증 기술을 채택하여야 한다.

제 16 조(분쟁 예방 및 대처) 금융회사 등은 거래 내용을 고객이 분명히 이해할 수 있도록 유저 인터페이스를 설계하고, 거래의 주체와 거래의 내역을 신뢰성 있는 방법으로 확인하고, 거래 데이터가 변조되지 않도록 하며, 변조 여부를 판별하는데 필요한 합리적 조치를 채택함으로써 전자금융거래와 관련된 분쟁을 예방하고, 분쟁에 대처하여야 한다.

제 17 조(업무 권한의 분할) 금융회사 등은 전자금융거래 시스템, 데이타베이스, 프로그램의 운용에 있어서 각 직원의 임무가 적절히 분리, 분할되도록 하는데 필요한 조치를 취함으로써 자신의 전자금융 업무가 직원들 간에 상호 검증될 수 있도록 해야 한다.

제 18 조(접근, 출입 권한의 통제) 금융회사 등은 전자금융거래 시스템, 데이타베이스, 프로그램에 대한 접근 권한 및 출입 권한 통제가 적절히 이루어지도록 함으로써 각 직원이 자기 권한을 스스로 변경할 수 없도록 하며, 업무권한의 분리, 분할을 통한 상호 검증 체계가 우회되지 않도록 해야 한다.

제 19 조(거래 기록 등의 보호) 금융회사 등은 전자금융거래 내역, 거래 기록 등의 정보가 변경되지 않고 보존될 수 있도록 하는데 필요한 조치를 마련하여야 한다.

제 20 조(검사 이력 및 증거 확보) 금융회사 등은 고객의 모든 전자금융거래에 대하여 감사/검사 이력(audit trails)이 남도록 하고, 법원에 제출될 수 있는 증거자료를 평소에 확보하고, 증거자료가 사후에 변조되지 않도록 하는데 필요한 적절한 조치들을 상시로 취해야 한다.

제 21 조(고객의 비밀 보호) 금융회사 등은 전자금융거래 내역의 비밀성을 유지하는데 필요한 적절한 조치를 마련하여야 한다.

제 4 절 법적 책임 및 평판에 관한 사항

제 22 조(고객에게 제공되어야 할 정보) 금융회사 등은 고객이 거래할지 여부를 제대로 판단하는데 필요한 정보(명칭, 규제상황 등)를 적절히 제공하여야 한다.

제 23 조(개인정보보호) 금융회사 등은 고객의 개인정보를 법령에 따라 준수하여야 한다.

제 24 조(사업지속에 필요한 대비책) 금융회사 등은 전자금융 서비스가 상시 제공될 수 있도록 사업규모, 사업지속 및 비상 대책에 관한 사전 기획 절차를 마련하여야 한다.

제 25 조(재난 회복 및 사고 대응책) 금융회사 등은 전자금융 서비스에 대한 내부자의 공격이나 외부자의 공격 등 불의의 사태를 관리하고 피해를 최소화 하는데 필요한 사고 대응책을 적절히 개발하여 시행한다.

제 26 조(사고 보고 및 분쟁절차 모니터링) 금융감독원은 전자금융 사고거래의 내용과 규모를 정확히 파악하고, 공평하고 신속한 분쟁해결을 위하여 다음 조치를 취한다:

1. 전자금융 서비스와 관련된 소비자의 불만, 이의, 환불신청 등을 통합적으로 접수할 수 있는 페이지(금융소비자 보호페이지)를 금융감독원이 관리하고, 각 금융회사는 이 페이지의 링크를 자신의 홈페이지에 게시한다.
2. 금융감독원은 금융소비자 보호페이지를 통하여 접수된 소비자의 불만, 이의, 환불신청을 해당 금융회사 등에 이첩하고, 분쟁해결 과정을 모니터링 한다.
3. 금융감독원은 각 금융회사 별 사고거래의 내용과 규모를 신뢰성 있는 방법으로 파악하여 보안기술의 연구 개발 및 서비스 품질 향상에 필요한 한도에서 적절한 수준과 방법으로 공표한다.

제 5 절 보안감사 서비스

제 27 조(정기적, 전문적, 독립적 보안감사) ① 금융회사 등은 다음 중 하나의 보안점검 기준에 따른 보안감사를 수행할 전문성과 독립성이 있는 보안감사 업체와 계약을 체결하고 보안감사를 년 1 회 이상 받아야 한다.

1. PCI DSS 등 국제적으로 인정받는 금융거래 보안 기준
2. 금융감독원이 공표하는 별지의 보안 기준(금융감독원 데이터 보안 기준; Korea Financial Supervisory Service Data Security Standards)(이하, FSS DSS 라 함)

② 금융감독원은 FSS DSS 의 지속적인 업데이트 및 국제화 작업, FSS DSS 기준에 따른 보안감사 서비스 제공자의 자격 요건 및 품질 관리에 필요한 업무를 지원한다.

제 28 조(신규 솔루션에 대한 제 3 자 검증) ① 금융회사 등이 전자금융 거래 솔루션을 신규로 채용할 경우에는 독립적이고 전문적인 보안감사 업체의 검증을 받고, 그 검증 보고서를 해당 서비스 개시 후 6 개월 이내에 금융감독원에 제출하여야 한다.
② 전항의 검증 보고서는 해당 금융회사의 웹사이트에도 공지하여야 한다.

인증업무수행 기준 등에 관한 고시 [예시]

[미래창조과학부 고시]

제 1 조(인증업무수행기준) 전자서명법 제 4 조 제 1 항 및 제 2 항에 따른 인증업무수행기준은 다음 각 호의 하나로 한다.

1. WebTrust "Principles and Criteria for Certification Authorities 2.0"
2. WebTrust "Principles and Criteria for Certification Authorities - Extended Validation Audit Criteria 1.4"
3. ISO 21188:2006 Public key infrastructure for financial services -- Practices and policy framework
4. ETSI TS 101 456 V1.4.3
5. ETSI TS 102 042 V2.3.1
6. 미래창조과학부 장관은 위 기준들과 대등하다고 인정하는 기준을 추가할 수 있다

제 2 조 (점검업무 수행자의 전문성, 독립성) ① 전자서명법 제 4 조 제 1 항의 인증기관은 인증업무수행기준 준수 여부를 다음 요건 중 하나를 충족하는 제 3 자로부터 연 1 회 이상 점검받아야 한다.

1. 제 1 조의 각 인증업무수행기준을 제정, 관리하는 주체로부터 해당 기준 준수 여부를 검사할 전문성과 독립성이 있음을 인정받은 자
2. 제 1 조의 인증업무수행기준 준수 여부를 검사할 전문성과 독립성이 있다는 사실을 소명하고 미래창조과학부 장관에게 신고한 자.

② 제 1 항 제 2 호의 점검업무 수행자의 전문성은 다음 요건을 기준으로 판단한다.

1. 공개키기반구조 및 관련 기술 기준 등 인증업무의 기술적 내용에 대한 지식이 있는지 여부
2. 보안 감사, 보안 평가, 위험 분석 등의 작업을 수행한 경험이 있는지 여부
3. 정직성과 객관성을 유지할 수 있는지 여부

③ 제 1 항 제 2 호의 점검업무 수행자의 독립성은 다음 요건을 기준으로 판단한다.

1. 해당 점검업무의 정당한 대가 외에 인증기관으로부터 급여, 자문료 기타 명목 여하를 막론한 금전을 지급받는지 여부
2. 만일 전항의 금전을 지급받을 경우, 그 성격과 액수가 공시되는지 여부
3. 법령이나 자신이 소속된 직업 단체의 자치 규약에 따라, 정직하고 객관적인 평가를 하여야 할 의무를 부담하는 자인지 여부

제 3 조 (개인정보보호법 준수) 전자서명법 제 4 조의 1 항에 따른 인증기관은 개인정보보호법 준수 여부에 대한 변호사의 검토 의견을 자신의 웹사이트에 공지하여야 하며, 이 검토 의견은 연 1 회 이상 갱신되어야 한다.

제 4 조 (배상책임 재원의 확보) 전자서명법 제 4 조 제 1 항에 따른 인증기관의 자산액이 10 억원 미만일 경우, 최소 10 억원 이상의 배상책임 보험을 가입하여야 한다.