전자서명 인증관련 주요 정책방향

신용섭 · 정보통신부 정보보호과장

Ⅰ. 전자서명과 인증

1. 정보화 진전과 전자문서 이용증가

정보통신기술의 급속한 발달과 정보통신망 확산으로 종이문서가 전자문서로 급격히 대체되고 있으며, 행정민원 신청, 공문서 결재 및 교환, 기업간 거래 및 정보교환, 전자상거래, 전자자금이체 등 전자문서를 이용하는 전자적 행위가 증가일로에 있다.

이러한 전자문서 이용으로 기업이나 정부의 생산성이 향상되고 국민 개인의 생활편익이 증진되게 되었다.

2. 전자문서를 이용한 전자거래의 문제점

그러나 전자문서를 이용한 전자거래는 비접촉, 비대면으로 이루어지기 때문에 거래당사자간에 상대방의 신원과 거래의사의 진정성 여부를 확인하기 어렵고, 타인으로 위장하여 전자문서 등을 부정하게 사용할 위험이 있다. 또한 전자문서는 유통되는 과정에서 위·변조가 용이하고, 문서작성 사실을 입증하기 곤란할 뿐만 아니라, 전송내용의 비밀유지가 곤란하다는 문제점이 있다.

3. 종이문서와 전자문서의 특성비교

종이문서와 전자문서의 특성을 비교하면 다음과 같다.

구분	종이문서	전자문서
기록매체	종이	전자기록 매체
전달방법	우편, 인편	네트워크를 통한 전송
안전·신뢰성	위·변조가 비교적 어려움 종이의 물리적 특성으로 위·변조 식별 가능	위·변조가 용이함 전자기록 매체의 물리적 특성으로 위·변조 식별 불가능
진정성 증명	수기서명, 날인	전자서명

4. 해결방안

이 같이 전자문서 및 전자거래가 가지는 문제점을 해소하기 위하여는 다음과 같은 방안이 있다. 거래 상대방의 신원을 확인하고 전자문서의 위·변조 및 부인을 방지하기 위하여 전자서명기술을 활용하며, 신뢰할 수 있는 제3자(인증기관)가 거래당사자의 전자서명을 인증해주

는 전자서명 인증제도를 도입하는 것이 그것이다. 또한 전송내용의 비밀을 유지하기 위하여 암호를 사용하는 방안이 있다.

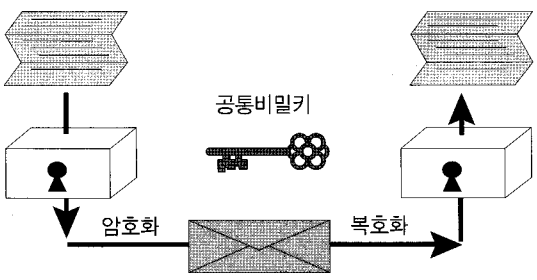
5. 전자서명 기술

전자서명이란 전자문서를 작성한 자의 신원과 전자문서의 변경여부를 확인할 수 있도록 비대칭 암호화방식을 이용하여 전자서명생성키로 생성한 정보로서 그 전자문서에 고유한 것을 말한다(법 제2조).

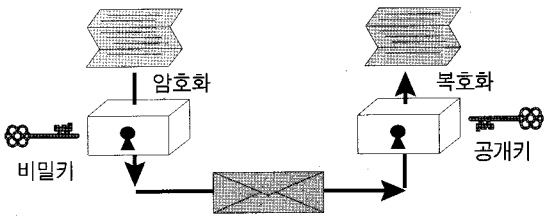
전자서명이 갖추어야 하는 요건은 다음과 같다. 첫째, 서명자의 인식이 가능하여야 한다. 둘째, 문서내용의 변경여부를 확인할 수 있어야 한다. 셋째, 동일한 전자서명의 재사용이 불가능하여야 한다. 넷째, 문서작성 사실에 대한 부인을 방지할 수 있어야 한다.

6. 암호기술

암호 알고리즘은 사용하는 키의 수 혹은 키의 관리방법에 따라 이를 대칭키 시스템과 비대칭키 시스템으로 구분한다. 대칭키 시스템은 관용키 시스템 혹은 비밀키 시스템이라고도 하며, 암호화와 복호화 할 때 동일한 키를 사용한다. 비대칭키 시스템은 공개키 시스템이라고도 하며, 암호화에 사용하는 키와 복호화에 사용하는 키가 서로 다르다. 전자의 대표적인 예로 DES, SKIPJACK, IDEA 등이 있으며, 후자의 예로 RSA, ElGamal 등이 있다.



(그림 1) 대칭형 암호시스템



(그림 2) 비대칭형 암호시스템

7. 전자서명 생성 및 검증

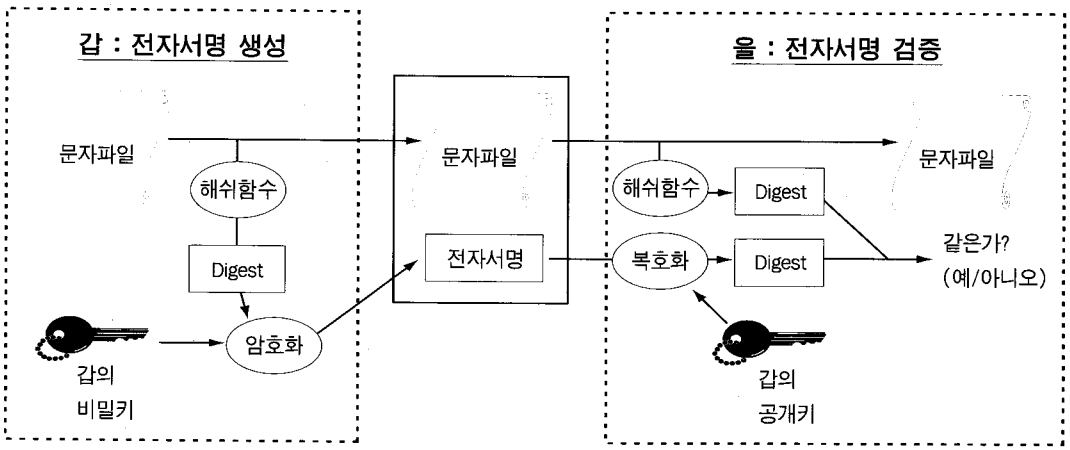
가. 전자서명의 생성

전자서명을 사용하기 위해 첫 번째 단계로 사용자는 공개키와 비밀키 쌍을 생성하여야 한다. 키의 생성은 자신이 가입한 인증기관에서 사용하는 공개키 알고리즘 중의 하나에 따르거나, 특정한 알고리즘에 따라서 사용자가 직접 생성한다. 두 번째의 단계는 사용자가 보낼 전자문서의 메시지 요약(message digest)을 생성하는 단계이다. 세 번째 단계는 메시지 요약을 송신자의 전자서명생성키로 서명하여 전자서명을 생성하는 단계이다. 네 번째 단계는 생성된 전자서명을 원래의 메시지에 더하여 수신자에게 전송하는 단계이다.

나. 전자서명의 검증

첫 번째 단계로 전자서명된 메시지(메시지와 그의 전자서명값)를 수신자가 받으면, 수신자의 컴퓨터에서 송신자의 전자서명검증키를 이용하여 송신자의 메시지 요약을 복원한다. 만일 메시지 요약이 복원되지 않으면 송신자의 전자서명검증키가 진정한 것이 아니므로 송신자의 신원확인에 실패한 것이 되고, 전자서명의 복호화(확인)가 가능하면, 송신자가 일치함을 확인(송신자의 신원확인)한다. 다음으로 수신된 메시지의 메시지 요약을 만들어 이미 복원한 메시지 요약과 비교하여, 양자가 일치하면, 메시지가 바뀌지 않았음을 확인(메시지의 무결성 확

인)한다(그림 3).



(그림 3) 전자서명 생성 · 검증과정

8. 전자서명 인증개요

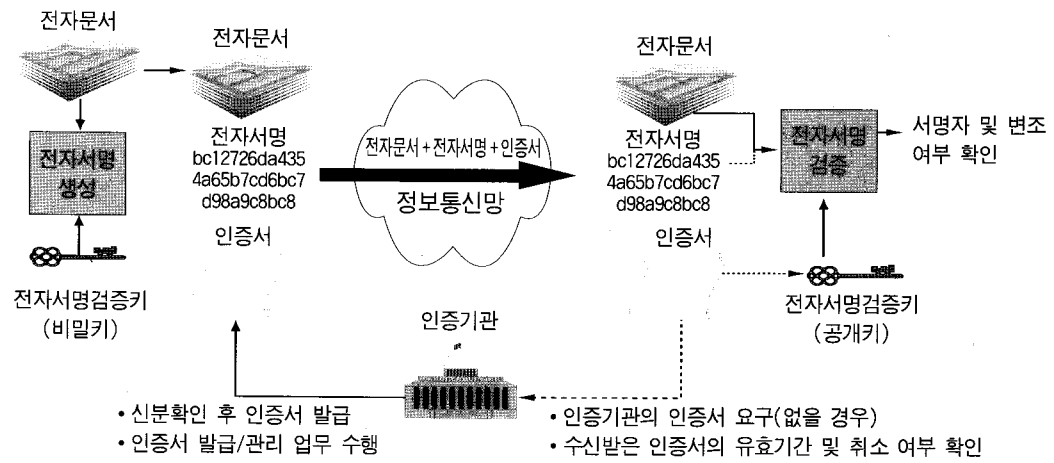
「전자서명 인증」이란 전자서명검증키가 자연인 또는 법인이 소유하는 전자서명생성키에 합치한다는 사실을 공신력 및 전문성을 갖춘 인증기관이 확인 · 증명하는 행위를 말한다. 인증기관은 이를 위하여 서명자, 전자서명검증키 등의 정보가 포함된 전자적 인증서를 발급한다.

9. 인증기관의 필요성 및 업무

불특정 다수인의 전자서명키 인증을 효율적으로 수행하고, 전자서명키 인증의 공신력을 제고하여 전자문서 이용관련 분쟁을 최소화하기 위하여는 인증기관의 존재가 필수적이다.

인증기관은 인증서 발급 · 정지 · 폐지, 인증관련 기록보관 등의 인증업무와 시점확인(Time Stamp), 내용증명 등의 부수업무를 수행한다.

10. 인증서를 이용한 전자서명 체계도(그림 4)



(그림 4) 인증서를 이용한 전자서명 체계도

Ⅱ. 전자서명법 제정

1. 외국의 전자서명법 입법동향

미국에서 Utah주('95) 등 41개 주, 독일('97), 이탈리아('98), 말레이시아('97), 싱가폴('98)이 전자서명법을 제정, 시행하고 있다. 또한 덴마크, 영국, 핀란드, 일본 등도 법 제정을 추진중이다.

한편 각국의 전자서명법제가 상이함으로 인하여 전자서명이 국제적으로 통용하는 데 장애가 되므로 이를 제거하기 위하여 UNCITRAL을 중심으로 전자서명통일규칙(Uniform Rules on Electronic Signatures)을 작성하고 있으며, EU 차원에서도 전자서명 입법지침의 제정을 추진중이다.

2. 국내 전자서명법제 추진경과

정보통신망을 통하여 처리되는 전자문서의 안전·신뢰성을 확보함으로써 전자상거래 활성화, 전자정부 구현 및 전자화폐 이용 등 정보화를 촉진하고 국민생활의 편익을 증진하기 위하여 '97. 10월 전자상거래 활성화 대책에서 정보통신부 주관으로 전자서명법의 제정을 추진하는 내용의 기본정책 방향이 결정되었다.

전자서명법안의 준비를 담당한 정보통신부는 '98. 2월부터 5월까지 학계, 연구기관 및 산업계 전문가 10여명으로 전자서명법 제정을 위한 연구작업반을 구성하여 수차례의 회의를 거쳐 전자서명법 시안을 마련하였다. '98. 4월부터 5월까지 관계기관 의견수렴 및 전자공청회를 실시하였으며, '98. 6월 18일 '전자서명법 제정을 위한 토론회'를 개최하여 각계 각층의 의견을 폭넓게 수렴하였다.

각계의 의견을 수렴하여 정리한 전자서명법안은 '98. 7월 입법예고를 거쳐 '98. 11월 국회에 제출되었다. 이 법안은 소관 상임위원회와 법제사법위원회의 심의를 거쳐 '98. 12월 24일 국회 본회의를 통과하였으며, 이듬해인 '99. 2월 5일 법률 제5792호로 공포되었다. 전자서명법은 '99. 7월 1일 시행된다.

정부는 현재 전자서명법의 원활한 시행을 위하여 시행령과 시행규칙을 제정하는 작업을 진행중이다. 이를 위하여 관련 분야 전문가 20여명으로 전자서명법 하위법령 제정작업반을 구성하여 운영하고 있다.

3. 전자서명법의 주요내용

○ 전자거래의 활성화를 위하여 공인인증기관이 인증한 전자서명에 대하여 법적 효력 부여(법 제3조)
- 공인인증기관이 인증한 전자서명은 법령이 정하는 서명 또는 기명날인으로 간주
- 공인인증기관의 인증을 받은 전자서명으로 서명한 전자문서의 경우 당해 전자서명이 당해 전자문서의 명의자의 서명 또는 기명날인이고, 당해 전자문서가 전자서명된 후 그 내용이 변경되지 아니하였다고 추정

○ 정보통신부 장관이 공인인증기관을 지정
- 전자서명 인증업무에 대한 공신력을 제고하기 위하여 정부가 지정하는 공인인증기관 제도를 도입하고
- 기술적·재정적 능력 등 일정요건을 갖춘 국가기관, 지방자치단체 또는 법인을 공인인증기관으로 정보통신부장관이 지정할 수 있도록 하며 인증기관의 임·직원에 대한 결격사유 등을 규정함(법 제4조, 제5조)
- 전자서명법은 공인인증기관의 지정절차에 관하여 직접 규정하지 아니하고, 시행령(대통령령)에서 지정절차, 기타 필요한 사항을 세부적으로 규정하도록 위임(법 제4조)

○ 인증업무의 지속성 및 적정성 보장을 위한 공인인증기관 관리제도
- 인증업무수행에 필요한 인증실무준칙의

신고, 인증기관의 업무 휴·폐지 등 인증기관 운영에 관한 사항을 규정함(법 제6조 내지 제10조)
- 공인인증기관의 적정한 업무수행을 보장하기 위하여 지정취소, 업무조사 등에 관한 사항을 규정함(안 제12조, 제14조)

○ 인증업무의 신뢰성 확보를 위한 인증서 발급
- 인증업무에 대한 신뢰성 확보를 위하여 인증서에 포함할 사항을 명확히 하고 인증서의 발급·효력정지·폐지 등에 관한 사항을 규정함(법 제15조 내지 제18조)

인증업무 수행관련 개인정보 보호
인증업무에 필요한 개인정보의 수집 및 사용의 제한, 누설금지 등 개인정보 보호에 관한 사항을 규정하고 이를 위반한 자를 처벌함(법 제24조, 제32조 내지 제34조)

국가간 인증서에 대한 상호인정
전자거래의 범세계적 활성화를 위하여 외국의 인증기관이 발행한 인증서 등을 국제협정에 의하여 상호인증할 수 있도록 규정함(법 제27조)

○ 인증기관의 책임과 의무 등
- 인증서 변조방지대책 강구, 안전·신뢰성 있는 인증관리체계 운영, 전자서명키의 안전한 관리, 인증관련 기록의 안전한 관리 등 의무를 규정함(법 제19조, 제21조 및 제22조)
- 인증기관이 법적의무 불이행 등으로 인하여 이용자에게 손해를 주었을 때에는 배상하도록 함(법 제26조)

○ 전자서명 및 전자문서 보호
- 전자서명 및 전자문서의 안전·신뢰성 확보를 위하여 타인의 명의를 도용하여 허위로 인증서를 발급받는 행위, 타인의 전자서명키 도용행위 등을 금지하고 이를 위반한 자를 처벌함(법 제23조, 제31조 및 제32조)

○ 전자서명인증관리센터의 설립·운영
- 전자서명의 안전한 이용환경 조성과 인증기관의 효율적인 관리를 위하여 한국정보보호센터로 하여금 인증기관의 전자서명키에 대한 인증업무 등을 수행하는 인증관리센터를 운영(법 제25조)

4. 전자서명법 시행령·시행규칙의 주요내용

가. 서 언

○ 전자서명법 시행령 및 시행규칙에서는 전자서명법의 시행에 필요한 다음의 세부 사항을 규정
- 공인인증기관 지정요건
- 공인인증기관 지정절차
- 기타 공인인증기관 관리에 관한 세부사항

나. 공인인증기관의 지정요건

○ 전자서명법 시행령(안)과 시행규칙(안)은 전자서명법 시행('99. 7. 1)을 위하여 공인인증기관 지정요건, 지정절차 등 법 시행에 필요한 세부사항을 규정
- 시행령(안)은 공인인증기관 지정요건, 공인인증기관 지정절차에 대하여 규정하고 있으며, 시행규칙(안)은 공인인증기관 세부 지정요건 및 관리에 관한 사항을 규정

○ 신뢰할 수 있는 제3자

○ 시행령(안)에서는 공인인증기관의 지정요건으로 인증기관의 독립성을 보장하기 위

하여 '중립적이고 신뢰할 수 있는 제3자'로 규정

- '신뢰할 수 있는 제3자'란 전자서명 인증을 이용하는 전자거래의 일방 당사자가 아닌 제3자로서 당해거래에 있어서 재정적 이해관계가 없는 자를 말함

○ 재정능력

- 시행령(안)은 또한 공인인증기관의 재정적 요건으로 '자본금 또는 기본재산 100억 이상'으로 규정

○ 기술능력, 보호설비, 인력 및 관리능력

- 시행령(안)은 기술적 능력, 보호설비, 공인인증기관 운영에 필요한 인력 및 관리적 능력을 갖출 것을 규정하고 있으며, 이와 관련하여 시행규칙(안)에서 각 사항에 대하여 다음과 같이 구체적으로 규정

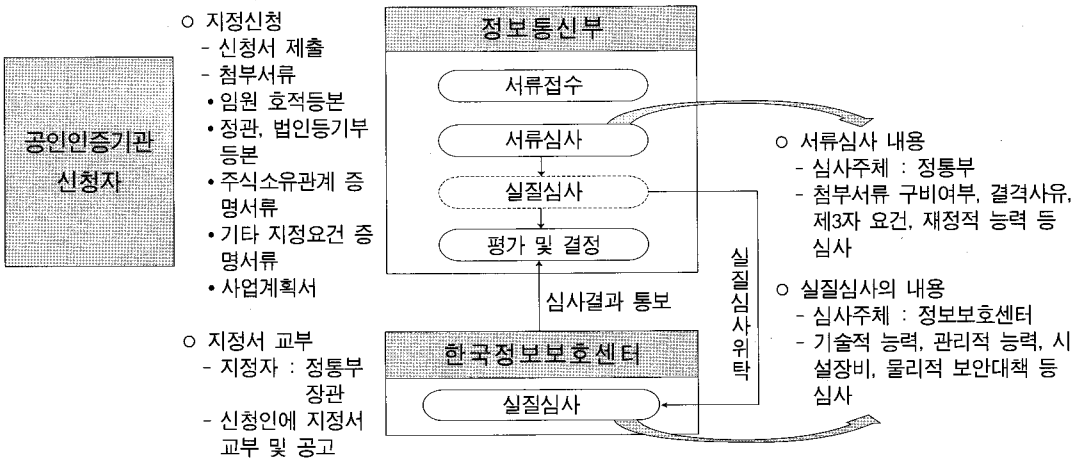
- 기술적 능력
  - 가입자 신원확인 및 등록, 전자서명키 관리, 인증서 관리, 시점확인 등 전자서명 인증업무를 안전하고 신뢰성있게 수행할 수 있는 기술적 능력을 갖추어야 함

- 공인인증기관 운영에 필요한 인력
  - 공인인증기관의 24시간 운영체계 구축 및 기술개발 등을 위하여 인증관리체계 운영인력, 기술개발인력, 행정지원인력 및 보안경비인력을 두어야 함
  - 임원(1인 이상), 인증관리체계 운영인력(15인 이상), 기술개발인력(3인 이상), 행정지원인력(2인 이상) 및 보안경비인력

- 인증관리체계에 대한 보호설비
  - 인증업무를 안정적·지속적으로 수행하기 위하여 출입통제 시스템, 침입탐지 및 경보장치, 감시통제 장치 등 인증관리체계에 대한 물리적 보안설비를 갖추어야 함
  - 전자서명인증 설비(Dual system), 인증관리체계에 대한 보호설비, 무정전전원공급장치, 냉각기, 화재진압·경보장치 및 물리적으로 분리된 이중 저장수단(Data backup)

- 관리적 능력
  - 인증업무 수행의 안전한 관리를 위하여 인증업무 관련 중요자료의 문서화, 보안감사 및 보안교육 등을 실시할 수 있는 수단을 갖추어야 함
  - 인증업무관련 중요자료의 문서화, 보안교육, 인증업무 수행실태에 대한 보안감사

다. 공인인증기관의 지정절차(그림 5)



(그림 5) 공인인증기관 지정절차도

○ 공인인증기관 지정에 있어서 행정절차의 투명성 및 예측가능성을 제고하기 위하여 시행령(안) 및 시행규칙(안)에서 공인인증기관 지정절차를 명확히 함

○ 공인인증기관으로 지정받고자 하는 자는 첨부서류를 구비하여 정보통신부장관에게 지정신청

○ 공인인증기관 지정신청자의 기술적 능력, 보호설비, 관리적 능력 등에 대한 실질심사를 거쳐 지정요건을 충족한 경우 지정서를 교부함

Ⅲ. 공인인증기관 정책방향

1. 외국 인증기관 현황

외국 인증기관으로는 미국의 Verisign, Cybertrust, 캐나다의 Keywitness Canada, 독일의 Deutsche Telecom 등이 대표적이며, 1~2개 주도 인증기관이 각국의 인증시장 전체를 장악하고 있다. 각국 인증기관은 인증서비스 이용자그룹과 전략적 제휴관계를 유지하고 있다. 미국은 시장주도, 유럽은 국가주도의 인증정책을 유지하고 있다.

2. 우리나라 인증기관 현황

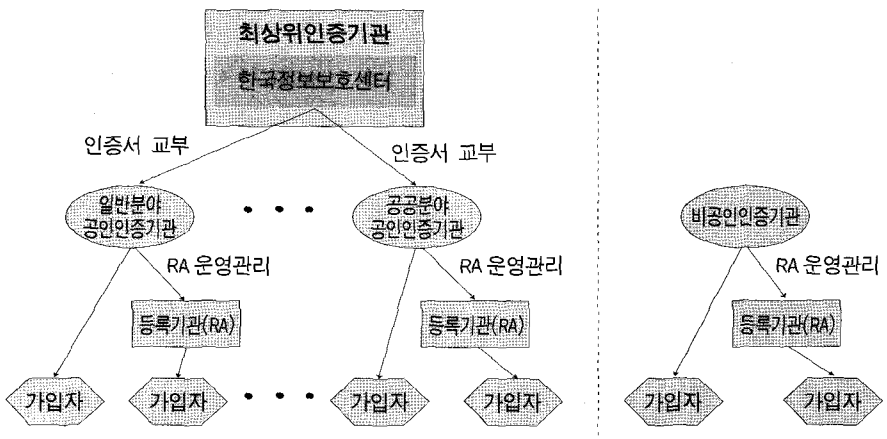
대부분의 전자상거래업체가 외국 인증기관을 이용하고 있으며, 일부 대기업에서는 사내 인증서비스를 제공 또는 준비중이다. 또한 정보보호 업계에서 전자서명 인증기술을 개발중에 있다.

국내 인증시장은 규모가 작아 초기에 적자를 볼 것으로 예상되며, 따라서 공인인증기관의 중립성 확보 및 분야별 공인인증기관을 집중 육성하는 것이 필요하다.

3. 공인인증기관의 중요성

공인인증기관은 전자상거래, 전자정부 구현, 전자화폐 이용 등 정보화 촉진을 위하여 핵심적인 역할을 수행하게 된다. 또한 전자서명 인증을 위하여 전자거래와 관련한 중요 개인정보를 용이하게 수집할 수 있는 위치에 있게 되며, 암호기술 등 정보보호 기술의 축적이 가능하게 된다. 따라서 전자서명 인증은 향후 고도성장이 예견되는 분야라 할 수 있다.

4. 전자서명 인증체계와 구성요소(그림 6)



(그림 6) 전자서명 인증체계

○ 최상위인증기관(Root CA)
- 공인인증기관에 대한 인증서 발급 및 공인인증기관 관리
- 한국정보보호센터가 최상위인증기관 역할 수행(법 제25조)

○ 공인인증기관
- 가입자에 대한 인증서 발급 등 인증업무 수행
- 정보통신부장관이 지정(법 제4조)

○ 등록기관(RA)
- 가입자의 신원확인 및 등록업무 수행(시행령 제3조)

※ 지정받지 아니한 비공인인증기관도 있음

5. 외국의 공인인증기관 허가요건

전자서명법을 입법한 국가의 대부분이 공인인증기관의 안전·신뢰성 확보를 위하여 엄격한 허가요건을 두고 있다. 특히 독일의 경우 147개의 요구조건을 두고 있다.

외국 입법례에서 공인인증기관의 허가와 관련하여 일반적으로 요구하는 조건은 다음과 같다.

- 인증기관 운영의 독립성
- 손해배상 등을 위한 재정적 능력
- 2인 이상의 관리자에 의한 시스템 운영
- 핵심인증시스템의 이원화
- 불법침입, 화재, 홍수, 지진 등에 대비한 물리적 보안설비

6. 우리나라 정책방향

정부는 공인인증기관의 난립을 방지하고 이를 집중 육성하기 위하여 공인인증기관 지정요건을 강화하는 한편, 분야별 컨소시엄 형태로 공인인증기관을 지정할 계획이다. 그러나 공인인증기관의 인증업무 활성화를 위하여 비공인인증업무의 수행에 대하여는 이를 규제하지 않을 방침이다. 정부의 최종목표는 민간 전자상거래 부문과 전자정부 기타 공공부문을 통합하는 공개키기반구조를 구축하는 것이다.

7. 컨소시엄 추진현황

현재 공인인증기관 설립은 크게 공공분야와 민간분야로 나누어 추진되고 있다. 민간분야에서는 금융 및 증권 부문에서 금융결제원과 한국증권전산(주)가 각각 공인인증기관 설립을 추진중이며, 그밖의 부문에서 1개의 컨소시엄 형태의 공인인증기관 설립이 추진되고 있다. 이 컨소시엄에는 현재 30여개 업체가 참여의사를 표명하였다. 주식회사 형태를 취하게 될 이 공인인증기관의 설립은 모집설립의 방법을 취하게 되며, 발기인조합 결성후 주주의 공개모집이 있을 예정이다. 현재 컨소시엄 설립을 위한 전담반이 설치되어 운영중이다.

한편 공공분야에서 인증업무를 수행할 공인인증기관의 설립은 관련기관과 협의중에 있다.

IV. 새로운 천년을 여는 정보화의 선구자

전자서명법은 국가전체의 공개키기반구조 구축을 위한 기본적 사항을 정한 법이다. 전자서명법에 의한 공개키기반구조 구축은 정보화촉진의 핵심과제이다. 공개키기반구조가 구축되면 사회 전반의 생산력이 크게 향상되고 국민의 편익도 증진할 것이다. 전자서명 인증제도는 새로운 천년을 여는 정보화의 선구자라고 할 수 있다.