OECD 암호정책을 수용한 CALS/EC 보안 기술 체계

임신영, 유창열, 송유진*, 함호상

시스템공학연구소, 동국대학교*

CALS/EC Security Framework considering OECD Cryptography Guidelines

Shin-Young Lim, Chang-Yeol Yoo, You-Jin Song*, Ho-Sang Ham

Systems Engineering Research Institute

Dongguk University*

Abstract

정보화 사회에서 개인의 프라이버시와 국가 차원의 보안의 균형있는 발전은 매우 중요한 과제이며, 1997년 3월 국제 경제개발 협력기구(OECD)는 암호기능을 적용하기 위한 정책인 'OECD 암호정책'을 수립하였으며, 이 지침의 특기할 점은 암호화된 데이터를 국가 등의 제 3자가 강제적으로 해독하는 것을 인정하였다는 것이다. 이러한 OECD 암호정책은 공공의 안전성 확보에 필요한 조치임과 동시에 개인 프라이버시 침해의 위험을 내포한 암호정책으로 세계를 상대로한 CALS/EC 산업에 이러한 기술이 표준화되어 적용될 가능성이 높기 때문에 향후 국내외 CALS/EC 보안 서비스 제공시 중요한 지침이 될것이다. 본 논문에서는 CALS/EC 보안 서비스를 실현하기 위하여 연구 개발해야 할 보안 기술 중 암호문의 강제 해독 기술 및 인증 기술을 포함한 보안 프레임워크를 제안한다.

1. 서론

최근 CALS/EC(Commerce At Light Speed/Electronic Commerce) 기술 및 서비스가 국가 경쟁력과의 직접적인 관련성을 인식하면서 CALS/EC 관련 기술 개발 및 시범사업 사례가 증가하고 있다. 이와 같이 CALS/EC와 관련된 정보의 중요성이 증가됨에 따라 암호기술을 기반으로하는 정책 수립등이 중요한 부분으로 등장하고 있다.

여기서 전자 상거래는 일반적으로 기업간의 상품 수주, 발주 및 결제가 포함된 일반 소비자를 위한 쇼핑을 전산망과 컴퓨터 시스템을 이용하여 거래하는 것으로 정의된다. 인터넷에 의한 통신판매의 지불 수단으로 신용카드를 사용하는 전자 지불 프로토콜은 표준 프로토콜로 제안되어 있으며 국내에도 비자와 마스터카드 회사에서 제안한 SET(Secure Electronic Transaction)을 기준으로 실험적인 전자 상거래가 시도되고 있다. 또한 CALS의 의미는 제품의 설계, 개발, 제조, 운용 및 보수라는 제품의 라이프사이클을 통하여 발생되는 정보를 통합된 데이터베이스로 일원적으로

관리하고 이를 발주자, 수주자, 개발자 등이 공유함으로써 각종 작업을 지원하는 하부 구조로써 정보의 공유와 흐름을 최적화하여 품질 향상, 비용 절감, 상품화까지의 시간 단축과 상품 가격의 경쟁력 획득의 실현을 목표로 한다. CALS/EC를 이와같이 활용하면 모든 사용자 계층(구매자, 판매자, 금융기관)은 기존의 상거래 방식에 비하여 월등한 경쟁력을 보장한다.

CALS/EC가 주축이되는 정보화 사회로 이전되는 과정에서 개인의 프라이버시와 국가 보안의 균형있는 발전은 매우 중요한 과제이며, 1997년 3월 국제 경제개발 협력기구(OECD)는 암호기능을 적용하기 위한 정책인 'OECD 암호정책'을 수립하였으며, 이 지침의 특기할 점은 암호화된 데이터를 국가 등의 제 3자가 강제적으로 해독하는 것을 인정하였다는 것이다. 이러한 OECD 암호정책은 공공의 안전성 확보에 필요한 조치임과 동시에 개인 프라이버시 침해의 위험을 내포한 암호정책으로 세계를 상대로한 CALS/EC 산업에 이러한 기술이 표준화되어 적용될 가능성이 높기 때문에 향후 국내의 CALS/EC 보안 서비스 제공시 중요한 지침이 될것이다.

OECD는 경제의 안정적인 성장과 무역확대를 목적으로 1961년 9월에 발족한 국제 기구로 현재 가맹국은 26개국이다. OECD는 기구의 설립 목적에 대한 각종 지침을 작성하는 역할을 하며, 기본적으로 가맹국은 합의된 지침 또는 권고안에 기초하여 각국의 방침을 결정하게 된다. 특히, OECD도 CALS/EC 기술이 무역확대를 촉진케하는 기술로 간주하고 있으며, 21세기 초반에는 시공을 초월하여 전세계 국민을 대상으로 국경없는 무역을 추진하게 될 기술 인프라 역할을 할 이 기술의 암호정책을 OECD에서 제안하였다는 것은 향후 CALS/EC 분야의 암호 기술이 CALS/EC 기술의 실현에 있어 핵심적인 역할을 할것으로 예상할 수 있다. 이와 같이 OECD가 암호학 및 암호 응용 실무 분야의 새로운 영역인 'CALS/EC 보안 응용 분야'에 관심을 갖고 암호정책을 도출하게 된 배경에는 전세계를 대상으로 국경없는 무역을 추구하는 강대국의 영향이 작용하였다고 볼 수 있다.

본 논문은 CALS/EC기술에 대한 국내 움직임에 대하여 관련 기술의 소개 및 기술 적용 방안에 대하여 OECD에서 제안한 암호정책을 고려한 CALS/EC 보안 서비스를 실현하기 위하여 연구 개발해야 할 보안 기술 프레임워크를 제안한다. 이 프레임워크는 OECD 암호정책의 내용인 암호문의 강제 해독 기술 및 인증 기술을 포함하고 있다.

본 논문의 구성은 2장에서는 OECD에서 제안한 암호정책의 주요 사항과 OECD의 암호정책과 관련한 암호 기술 분야를 다루었다. 3장에서는 OECD의 암호 정책을 고려한 CALS/EC 보안 기술 프레임워크의 제안과 향후 기술 연구개발의 방향에 대하여 제안하였다.

2. OECD 암호정책과 관련 기술

2.1. 개요

CALS/EC에서는 전산망 및 컴퓨터 시스템에 존재하는 데이터의 보호와 이용자 신분 확인을 위한 암호 응용 기술이 필수 불가결하다. 또한 각종 전표와 의료진료 카드, 개인 신상 정보 등이 전자화됨에 따라 암호 응용 기술의 중요성이 증대되고 있다. 한편 암호 기술이 범죄에 사용되면 조사에 필요한 정보가 암호화로 인하여 은폐될 염려가 있으며, 이런 상황에서는 안전한 사회생활이 위협받게 된다. 이와 같이 암호 기술에는 데이터의 안전성 보증과 범죄 수사 등 만일의 경우에 강제적으로 암호화된 개인 정보를 해독할 수 없으면 곤란한 서로 모순된 요구가 있다.

이러한 상반된 문제를 동시에 해결하기 위해 OECD는 암호기능을 적용하기 위한 정책으로 'OECD 암호 정책'을 작성하여 1997년 3월말에 공개하였으며, 이 정책은 향후 국가의 정보처리 정책은 물론, 정보처리 관련 기술개발 및 일반인의 사회생활에도 막대한 영향을 미칠것으로 예상된다. 특히, 문제가 되는 부분은 국가의 안전확보를 목적으로 암호화된 데이터를 국가 등이 강제적으로 해독하는 것을 인정한 점이다. 이 때문에 프라이버시가 침해되는 것은 아닌가라는 우려가 있다.

미국 정부 등이 암호키 길이가 40비트 이내의 암호 장비만을 수출 허가하는 것은 근본적으로 자국의 안전을 보장 하기 위해서이다. 암호 기술을 악용하면 '국가 전복을 위한 테러활동 계획'과 같은 정보를 완전하게 숨길 수 있기 때문이다. 이 때문에 구미 여러 국가는 암호장치를 무기와 동등하게 취급하여 사용제한과 수출규제의 대상으로 삼아 왔다. 이와 같이 암호 기술은 획득이 용이한 도구라 해도 사용제한과 수출규제 때문에 충분한 안전성을 보장 또는 입증할 수 없는 상황하에서는 국제적인 CALS/EC 정보망의 구축은 곤란하다. 또한 미국의 경우, 자국의 암호 기술을 민수용으로 전환하여 정보화 시대인 21세기 동안 이 분야의 핵심 기술로 세계 시장을 점유하기 위한 전략으로 고급 암호 기술을 조건부로 외국에 수출하는 길을 열기 위한 자구책으로 '법에 근거한 암호키의 입수'를 근거로 암호화된 데이터의 해독 기능을 추가한 고급 암호 기술을 해외에 수출할 수 있도록 제도화 하였다.

위의 두가지 문제 즉, 국가 보안과 고급 암호 기술 사장의 장악 문제를 해결하기 위해 미국 정부는 법적인 절차에 입각해서 암호화된 데이터를 해독 즉, '법 강화를 위한 강제 암호키 및 데이타 입수(Law Enforcement)'의 기능을 갖춘 암호 기술의 적용을 권하고 있다. 이 기능은 1994년 2월에 미국 정부 표준이 되었으나, 이 기능이 악용되면 개인의 프라이버시가 침해될 위험이 있기 때문에 발표 당초부터 그 기술의 적용에 관해서 많은 우려와 반대가 있었다. 이와 같은 상황에 입각해서 OECD는 국제 규모의 CALS/EC 전산망 시스템에서 안전하게 정보를 교환할 수 있는 암호 기술을 적용하기 위한 암호 정책을 제안하는 작업을 하게되었다.

OECD가 제안한 암호정책에 대한 각국의 각계반응은 다음과 같이 요약된다.

▷ 국제 비즈니스를 실현하는 데에 국제적인 가이드라인을 작성한 것의 의의는 크다.

▷ 국제무역을 원활하게 실현하는 데에 암호의 수출규제 문제의 해결은 중요한 과제이다. 동시에 시장의 요구에 기초해서 기술개발과 표준화가 추진되는 일도 중요하다.

▷ '법에 근거한 암호키의 입수'에 대해서는 그 절차와 책임을 명확히 해 두는 것이 국제무역을 원활이 추진하는 데에 중요하다.

▷ '법에 근거한 암호키의 입수' 대상이 되는 암호키는 은닉목적의 키에 한정하는 것을 강조해야 한다. 식별과 보전만을 위한 키가 법적인 해독의 대상이 되는 사례가 있으면 이용자는 안심하고 상거래를 할 수 없다.

▷ 국제표준은 중요하다. 현재 국제표준은 업계주도, 합의존중, 시장원리, 국제적 조직에 따라 작성되고 있으며, 호환성, 유통성, 적용성을 확보하는 것을 목적으로 하고 있다. 표준에 근거하고 있는 것을 확인하기 위해서 'OECD 암호정책'의 기준을 작성 및 평가하고자 하는 취지를 선언하고 있으나 이번의 'OECD 암호정책'은 이 상황을 충분히 반영하지는 않았다. 즉, 표준은 시장의 요구에 기초해야 하며 이것을 명문화하는 것이 타당하지만 이번 암호정책에는 반영되지 않았으며, 또한 평가는 중요하지만, 표준과는 별도의 문제임을 인식해야 하며, 평가기준도 업계주도로 시장요구에 근거해서 작성되어야 한다. 업계주도 및 시장요구에 근거한 표준화가 명확히 되지 않으면 국가수준의 표준이 난립하고 국제무역의 큰 장벽이 된다. 국제표준에 준거하고 있는 제품 및 서비스라면 국제규모로 이용할 수 있으므로 이용자에게 안도감을 준다.

▷ 프라이버시에 대해서는 이미 80년대에 OECD에서 가이드라인을 제정하고 합의하였다. 암호정책에서 그 이상의 것을 언급해서는 안된다.

▷ 국제무역을 촉진한다는 관점에서 구체적인 정책이 정해지는 것을 기대한다.

▷ 시장의 요구에 근거한 기술개발, 표준화, 적용이 중요하다. 또한 표준화에 대해서는 합의에 기초해서 비영리인 동시에 국제적인 업계주도의 표준기관을 설치하여 그 기관이 표준을 제정하는 중요성을 강조해야 한다.

▷ 암호기능을 이용할 때 이용자의 자유로운 선택권을 해쳐서는 안된다.

2.2. 주요 정책 내용

인터넷을 이용한 비즈니스가 확대되면 유통정보의 지적 재산권과 프라이버시 보호에 관한 법률과 규칙을 국제적으로 통일하는 것이 필요하게 되었으며, 특히 보안과 프라이버시에 관한 대책과 기술 수준에 대하여 각국의 의식이나 지표가 다르면 국제적인 CALS/EC를 이용한 산업 활성화를 저해하는 요소가 된다. CALS/EC를 사용하는 일반 소비자를 포함한 이용자가 안전하다고 확신할 수 있는 보안 대책과 프라이버시 보호 대책이 실시되지 않는 한, 광범위한 CALS/EC 서비스가 불가능하다. 결과적으로 이러한 문제의 해결책이 암호 기술이라는 인식하에 OECD는 1995년 12월

이에 관한 첫 회의를 개최하게 되었으며, 회의명은 '암호 방침에 관한 OECD 전문가 회의'로 여기서는 본 회의에 대한 국제적인 협조가 필요하다는 점, 그리고 프라이버시 보호와 공공의 안전을 위한 '법에 입각한 입수'의 균형에 관해서 통일된 해결책이 필요하다는 점을 확인하였다. 즉, 프라이버시 확보와 공공 안전의 균형을 어떻게 유지하는 점이 'OECD 암호 정책' 작성의 가장 중요한 과제였다. 암호 기술을 적용하기 위한 정책의 최초 원안은 국제 상공회의소와 OECD의 민간 자문 위원회인 BIAC(Business and Industry Advisory Committee to the OECD)가 작성하였으며 이 원안에는 다음과 같은 9 원칙이 포함되었으며, 이를 기준으로 OECD의 암호 정책이 제안되었다.

- 자유선택
- 시장주도
- 암호방식에 관한 표준
- 정부의 책임과 규칙
- 키 관리
- 책무에 관한 사항
- 정부에 의한 해독
- 국제협력
- 가이드라인의 채택

OECD의 암호정책 최종안은 1997년 3월 27일 OECD 위원회에서 승인되었고, 최종안은 8원칙으로 구성되었다. 향후 각국 정부는 이 암호정책에 따라서 자국의 CALS/EC보안 정책을 결정하고 실시해야 할 것이며, 이러한 정책 결정에 따라 암호 응용 기술이 연구개발될 것으로 예상한다.

'OECD 암호정책'의 주요 목적을 다음과 같이 요약한다.

▷ 유효한 암호기능의 도입으로 국제무역의 추진을 도모한다.

▷ CALS/EC 전산망등의 정보망상에서 유통되는 데이터 안전과 프라이버시 정보의 보호를 위해 암호 기술의 이용을 추진한다.

▷ 암호 기술의 이용이 공공의 안전과 국가 안전을 위협하는 일이 없도록 한다.

▷ 국제적으로 상호 운용을 가능하게 하는 암호 정책과 법제한의 필요성을 널리 이해시킨다.

▷ 각국이 암호 기술에 관한 방침을 결정할 때에 참고가 되는 원칙을 제시한다.

▷ 국내 및 국제적인 암호에 관한 활동에 있어서 정부와 산업계가 협력한다.

OECD가 암호 정책을 수립하는 과정에서 제안 배경과 현실 환경에 대한 정부의 역할, 정부의 산업계에 대한 책임, 공공의 안전, 또는 공공의 안전에 대한 정부의 책임과 권한등, 암호 기술과는 직접 관계가 없는 사항까지 검토되었다. 이와 같이 다각도로 검토된 후 도출된 'OECD 암호정책'의 8 원칙 및 각 원칙에 대한 배경과 관련 사항을 <표 1>에 요약한다.

2.3. OECD 암호정책 관련 기술

2.3.1. 전자 지불 시스템을 위한 인증 기술

CALS/EC등 금융 정보를 취급해야 하는 전자 지불 시스템(Electronic Payment System)은 지불 정보 등에 대한 보안 기술이 필수적이다. 인터넷상에서의 현실적인 지불 수단으로 전자 화폐와 기존 신용 카드 시스템의 활용을 들 수 있으며, 이를 정보화하기 위해서는 암호 기술이 필수불가결하다. 전자 화폐는 전자적인 정보형태로 사용하는 디지털 정보로 현재 현금 정보를 기입한 IC 카드를 상점에서 실제 화폐대신 이용하는 방식(오프라인 방식)과 인터넷의 가상점포에서 전자적인 정보를 이용해서 대금은 구매시 은행을 경유하여 지불하는 방식(온라인 방식)이 있다. 이러한 서비스의 구현에 따른 프라이버시 보호와 비밀 데이터의 은닉과 보전에도 암호 기술이 필수적으로 적용되고 있다.

일반적으로 공개키 암호방식에서는 공개키의 정당성을 보증하기 위해 공개키 그 자체를 인증할 필요가 있다. 이러한 인증을 전담하는 기관이 인증기관(Certificate Authority)이다. 인증 기관에서 공개키 증명서를 발행하여 사용하는 인증 절차를 <그림 1>에서 설명한다. 이 절차에서 증명서가 위조되거나 내용이 부당하게 수정되는 일이 없도록 암호 기술을 이용한다. 이 절차를 세부적으로 설명하면 ① 먼저 이용자 A는 자신의 서명과 공개키를 인증기관인 CA에 신고하고 공개키의 증명서 발행을 신청한다. ② 인증기관 CA는 서명 등으로 이용자 A를 확인할 수 있으면 이용자 A에게 공개키의 증명서를 발행한다. ③ 이용자 A는 자신의 공개키를 사용하는 이용자 B에게 증명서를 보낸다. 이용자 B는 증명서가 인증기관 CA에서 발행된 것임을 확인하고 나서 이용자 A의 공개키를 사용한다.

2.3.2. 키 복구 기술

OECD 암호 정책의 원칙 중 키 복구 기술은 법 강화를 위한 강제 암호키 및 데이타 입수를 가능하게 하는 방법에 대하여 <그림 2>와 같이 두 가지 방식을 검토하고 있다.

방식 A는 데이터의 암호화에 사용하는 비밀키를 신뢰할 수 있는 기관에 등록하여 보관해 두고 방식 B는 데이터의 암호화에 사용한 암호키를 데이터에 첨부한다.

각 방식을 단계별로 검토하면 다음과 같다.

방식 A에서는 ① 먼저 이용자가 비밀키를 신뢰할 수 있는 키 관리기관에 등록한다. ② 이 비밀키를 사용해서 데이터를 암호화한다.. ③ 암호화한 데이터를 통신회로상에 송신한다. 만일의 경우는 정부를 포함한 제3자인 개인 또는 기관이 키 관리기관에서 비밀키를 입수해서 암호화된 데이터를 해독(복호화)할 수 있다. 방식 A에서는 이용자는 자신의 비밀키를 사전에 신뢰할 수 있는 기관에 등록해 둔다. 데이터를 암호화하는 방법은 이전과 변함이 없다. 법 강화를 위한 강제 암호키 및 데이타 입수가 필요할 때에 해독을 요구하는 기관(예를 들면 범죄조사기관)은 키관리기관으로부터 비밀키를 입수할 수 있다.

방식 B에서는 ① 키 관리기관의 공개키가 포함된 암호기능을 이용한다. ② 먼저 이용자의 비밀키를 사용해서 데이터를 암호화한다. ③ 키관리기관의 공개키가 편입된 암호기능을 사용해서 이용자의 비밀키를 암호화한다. ④ 이 데이터를 이용자의 비밀키로 암호화한 데이터와 함께 통신회로상에 송신한다. 만일의 경우는 키관리 기관의 비밀키를 사용해서 집어넣은 정보를 복호화함으로써 이용자의 비밀키를 입수할 수 있다. 이 비밀키를 사용하면 암호화된 데이터를 해독할 수 있다. 방식 B에서는 키관리기관의 공개키를 사용해서 이용자의 비밀키를 암호화한다. 이 데이터를 이용자의 비밀키로 암호화한 데이터의 헤더부분에 부가한다. 법 강화를 위한 강제 암호키 및 데이타 입수가 필요할 때 해독을 요구하는 기관은 키관리기관의 비밀키로 헤더부분의 정보를 복호화함으로써 데이터의 암호화에 사용한 비밀키를 입수할 수 있다.

3. CALS/EC 보안 프레임워크

현재 국내에서 CALS/EC 보안 기술을 도출하고자 하는 움직임이 매우 활발하지만 OECD의 암호정책을 적극적으로 수용한 보안 프레임워크에 대한 결과는 도출되고 있지않다. 또한 이 프레임워크가 최적 상태로 구현되기 위한 관련 보안 기술에 근거하여 CALS/EC의 보안 특성이 종합적으로 고려되어야 한다. 이러한 관점에서 본 장은 OECD 암호정책을 고려한 보안 기술을 핵심으로 하는 CALS/EC 프레임워크를 제안한다.

CALS/EC 보안 프레임워크를 제안하기 위하여 고려해야 할 보안 관련 분야는 다음과 같다.

* 사이버공간에서 상호 신분을 확인하는 인증 및 공증 기술
* 사이버공간에서 거래 내역에 대한 공증 사무소 역할을 수행할 수 있는 시스템 기술
* 개인의 공개키 및 비밀키 분실에 따른 키 관리 및 복구 기술
* 각종 보안 기술들을 통합적으로 관리할 수 있는 즉, CALS/EC 보안 서비스 실시간 관리 기술

본 논문에서 제안하는 CALS/EC 보안 기술은 이와 같은 고려사항을 수용하여 프레임워크를 구성할 때 관련 기술 요소와 전체 구성도간의 관련성을 검토 정립한다. 이러한 프레임워크를 정립하기 위한 기술 요구사항의 체계는 다음과 같이 공통보안 기반 소프트웨어, 공동작업 서비스 보안 소프트웨어, 이질망간 연동 및 관리 소프트웨어, 보안 표준, 평가 및 감리 소프트웨어 등으로 분류된다.

3.1. CALS/EC 공통 보안 기반 소프트웨어

CALS/EC에서 사용할 보안 기술로 전자 신분증 즉, 공개키 기반 암호화를 사용하기 위하여 공개키 인증서를 지원할 수 있는 암호 기술외의 복합적인 기술의 개발이 최우선되어야 할 것이다. 공개키 인증 기술을 기반으로 CALS/EC에서 제공할 다양한 지불 수단 즉, 기존 신용카드와에 직불 카드, 선불 카드의 카드계 지불 처리 방식과 은행 계좌 이체 그리고 국내에서는 시험적인

단계에 진입하지만 외국에서는 이미 상용화 단계에 접어든 전자 화폐 및 전자 수표 지불 방식의 수용을 위한 통합 지불 기술이 그 다음으로 제공되어야 할 것으로 보인다. 또한 거래의 공정성과 거래 성사 결과에 대한 상호 부인을 방지하기 위한 '공정 거래 위원회' 및 '공증사무소'에 대한 기능도 요구될것으로 예측되며 이러한 기능을 수행하는 현행 체계(즉, 물리적인 공증 사무소)에서 전산망을 통하여 사이버공간에서 효과적으로 제공하기 위한 기술적인 기반으로 공개키 인증기술, 여러 사람의 증명을 위한 다중 서명 기술 및 공개키와 비밀키의 안전을 위한 키 위탁 기술이 요구된다. CALS/EC 사용자들이 사용하는 사용환경 즉, 플랫폼은 현재 예상하는 바로는 인터넷 웹 서비스를 이용할 것으로 보인다. CALS의 경우, 해상도가 높은 설계도면을 취급하는 경우, 특수한 기능이 인터넷 웹 브라우저에 제공되도록 관련 기술이 제공되어야 할것으로 보이며 이러한 인터넷 웹의 안전한 사용을 위한 보안 기술이 위의 기술과 병행된 연구가 예상된다. 한편 전자 상거래의 경우, 사용자의 편이를 위하여 이동 전화, PCS, 인터넷 전화등을 사용하여 전자 상거래 서비스를 제공할 경우의 보안 기술도 향후 고려할 부분으로 보인다. 또한 암호화 기반 기술 즉, 공개키 및 비밀키 암호화를 위한 암호 알고리듬의 국산화와 함께 이를 암호화 라이브러리로 구축하여 사용가능 하도록 라이브러리 및 개발자를 위한 소프트웨어가 필요할 것으로 보인다. 다음은 이러한 기술 분야의 체계를 요약한 내용이다.

- ▶ 전자 신분증 인증기관(Certification Authority(CA))을 위한 서명 및 인증 소프트웨어
- ▶ 거래 내역의 공증을 처리하는 거래정보 공증 및 키 위탁 소프트웨어
- ▶ 전산망을 통한 다양한 지불 처리를 수용할 수 있는 통합 지불 프로토콜 소프트웨어
- ▶ 암호화 라이브러리 및 개발자 인터페이스 소프트웨어
- ▶ 인터넷 웹 서버 및 브라우저 보안 소프트웨어

3.2. 공동작업 서비스 보안 소프트웨어

CALS/EC 환경의 판매자 입장에서 사용하는 서비스의 예로 자동차 회사와 협력사들의 단위 전산망(회사별 내부 전산망)들이 공동 전산망 즉, 인터넷으로 연결되어 자동차 생산에 대한 공동작업(기술 협의 회의, 도면 설계, 자동 수치 제어기기 제어 등)을 수행할 경우, 관련 특정 서비스를 제공하는 공동작업 공간에서 이를 수행하게 되며 이러한 환경을 통하여 작업한 결과 정보 및 작업 내역 정보에 대하여 인가되지 않은 외부의 접근과 주요 정보의 위변조 및 유출을 방지하기 위한 기술이 필요하다. 또한 내부에서 공동작업 과정에 대한 내역을 향후 상호 부인을 방지하기 위한 기술적인 방안도 요구될 것으로 보인다. 다음의 요약은 이러한 기술적 요구사항을 기술 체계 형식으로 정리한 사항이다.

- ▶ 공동작업 서비스 사용자별 공동작업 내역 공증 소프트웨어
- ▶ 사용자별 공동작업 공간 접근 제어 소프트웨어
- ▶ 다중 공동작업을 지원하는 분산서버 시스템 보안 소프트웨어

3.3. 이질망(Heterogeneous(Multi-Domain Security) Network)간 연동 및 관리 소프트웨어

CALS/EC가 구현되어 실제 사용될 환경은 각 기관 및 회사에서 관리 운영하는 전산망이 다양한 보안 정책 즉, 기관의 고유한 정보 및 시스템 보호 관리 체계가 상이한 상태로 인터넷에 상호 연동되어 관련 서비스 및 정보를 교환할 것으로 보이며 이러한 환경을 안전하게 연동하고 관리하기 위한 기술이 요구될 것 으로 보인다. 특히, 전산망 보안 이전에 전산망 관리의 기술이 안정화되어 전산망을 통한 CALS/EC의 제반 서비스가 안정적으로 사용가능 하도록 CALS/EC에 특화된 기술 연구개발이 요구되며, 이를 바탕으로 전산망 보안 관리가 전산망 관리의 통합적인 관리 구조 내부에서 관리될 수 있다면 기관 및 CALS/EC 단위 서비스를 관리하는 측면에서 매우 경제적이며 또한 효과적인 방안이라고 할 수 있다. 또한 CALS/EC는 국내의 범주가 아닌 국제적인 범주의 서비스를 제공할 수 있으며 이를 위한 각 국가간 국제거래를 처리할 수 있는 관문 역할을 망관리 체계에서 1차적으로 수용하여 보안 공격에 대한 예비(방지) 및 탐지(추적) 기술이 적용되어야 할 것으로 보이며, 국제거래의 공증 역할도 요구될 것으로 보인다. 다음은 위의 기술적인 요구사항에 대한 기술 체계를 요약한 사항이다.

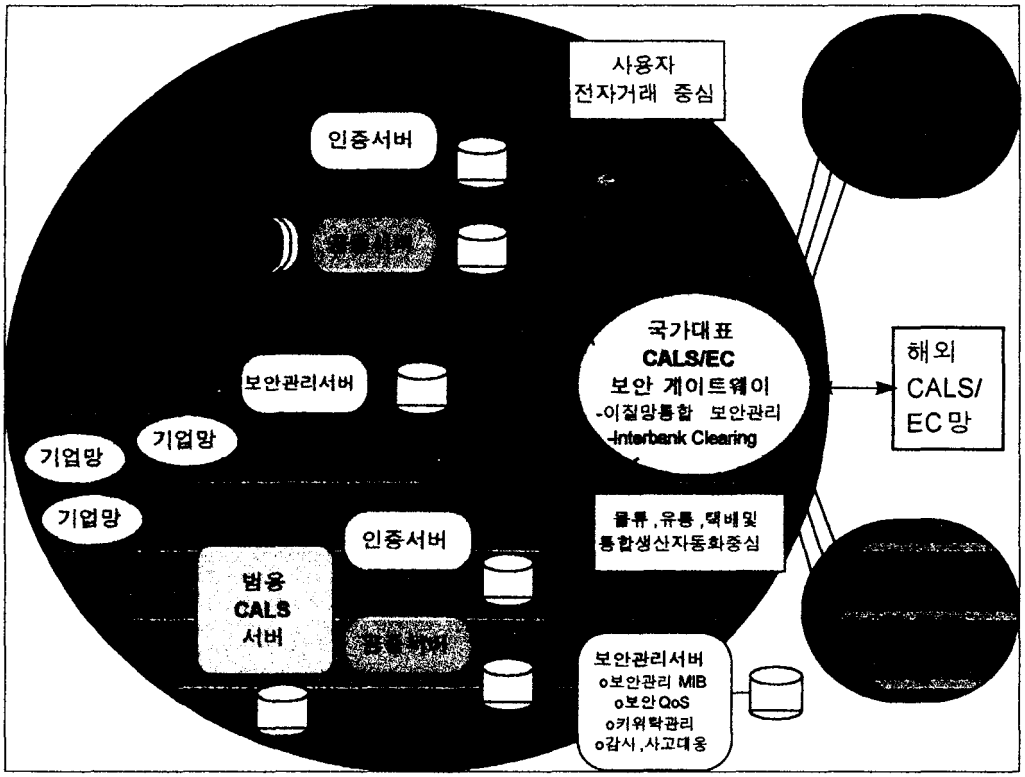
- ▶ 이질망간 보안 관리 정보 베이스 및 보안 QoS 관리 소프트웨어
- ▶ 국제거래(Interbank Clearing 포함) 보안 및 공증 소프트웨어
- ▶ CALS/EC 단위 서비스별 통합 보안 관리 소프트웨어

3.4. CALS/EC 보안 표준, 평가 및 감리 소프트웨어

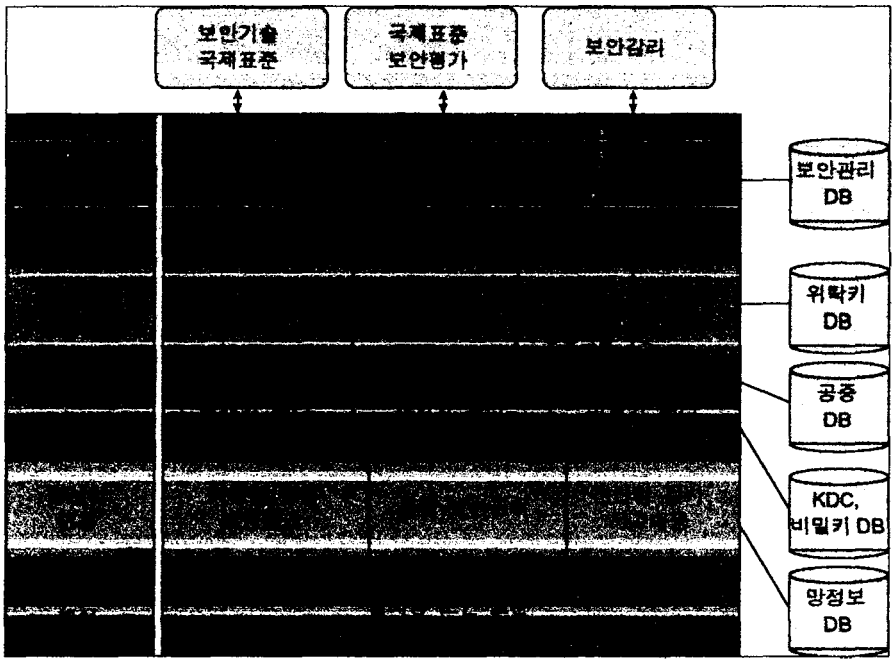
CALS/EC의 서비스가 국제적으로 안전하게 사용되기 위하여는 보안 및 관련 기술의 표준화가 또한 요구될 것으로 보이며 또한 구축된 보안 기술에 대한 감리 체계도 표준화된 절차와 감리 기준이 국제 표준으로 정착되어야할 것으로 보인다. 이러한 기술 표준이 정착되면 이를 전산화하는 기술의 연구개발이 요구될 것으로 예상된다.

- ▶ 개발 대상 CALS/EC 보안 기술의 국제 표준(ISO IEC JTC1 SC27 등) 연구
- ▶ CALS/EC 국제 표준 보안 평가 소프트웨어
- ▶ CALS/EC 보안 감리 기법 및 소프트웨어
- ▶ 법 제도권의 CALS/EC 보안 기술 수용을 위한 단계적 법제 방법론 연구

위의 각 기술체계를 총체적인 모습으로 표현한 CALS/EC 보안 소프트웨어의 통합 모형은 <그림 3>과 같으며, CALS/EC 보안 기술과 기존 CALS/EC 서비스 및 기술과의 계층적 관계도는 <그림 4>와 같이 표현할 수 있다. 앞서 전개한 기술 요소와 이를 통합한 전체 구도에 대한 이해를 돕기 위하여 <그림 3>과 기술 요소간의 연관성을 <표 2>와 같이 정리하였다.



<그림 3> CALS/EC 보안 기술 프레임워크 모델



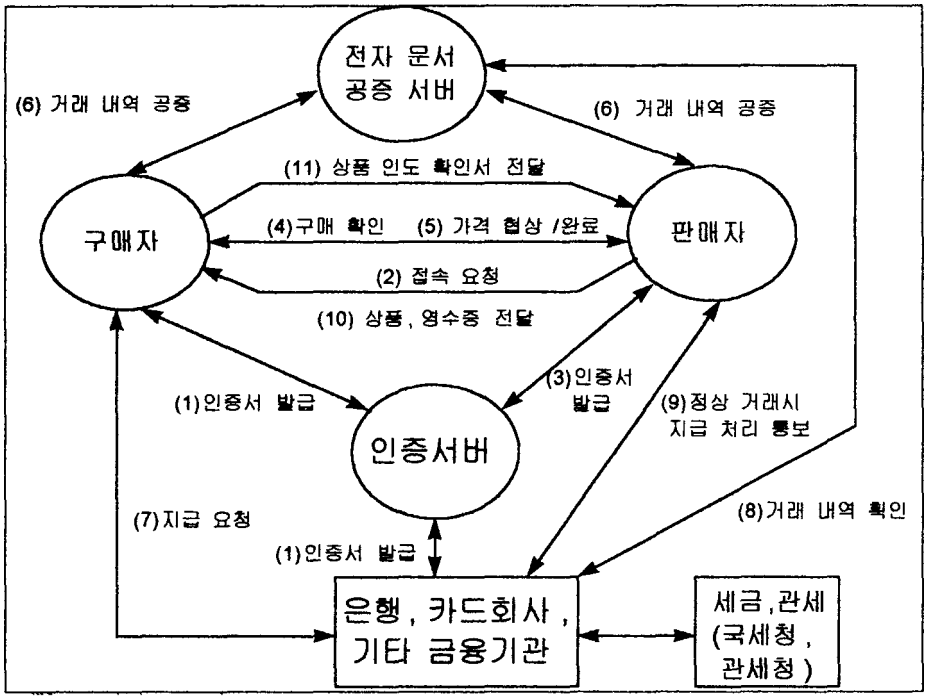
<그림 4> CALS/EC 서비스/기능과 보안 기술과의 계층적 개념

<표 2> CALS/EC 보안 기술 요소와 프레임워크 모델간의 연관표

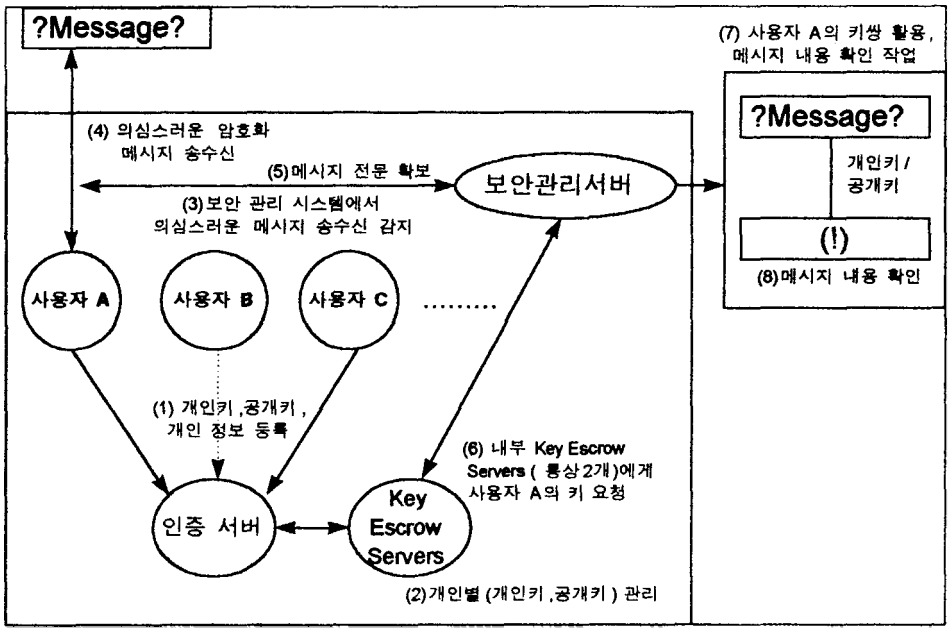
분 야	세부 기술 요소	<그림 3>의 관련 부분
CALS/EC 공통 보안 기반 소프트웨어	전자 신분증 인증기관(CA)를 위한 서명 및 인증 소프트웨어	인증 서버
	거래 내역의 공증을 처리하는 거래정보 공증 및 키 위탁 소프트웨어	공증 서버
	전산망을 통한 다양한 지불 처리를 수용할 수 있는 통합 지불 프로토콜 소프트웨어	EC 망 내부
	암호화 라이브러리 및 개발자 인터페이스 소프트웨어	인증 서버, 공증 서버, 범용 CALS 서버, 보안 관리 서버, 국가 대표 CALS/EC보안 게이트웨이에 적용
	인터넷 웹 서버 및 브라우저 보안 소프트웨어	사용자(구매자, 판매자, 기업망 사용자) 및 사용자 인터페이스 부분
공동작업 서비스 보안 소프트웨어	공동작업 서비스 사용자별 공동작업 내역 공증 소프트웨어	범용 CALS 서버
	사용자별 공동작업 접근 제어 소프트웨어	기업망과 범용 CALS 서버
	다중 공동작업을 지원하는 분산 서버 시스템 보안 소프트웨어	범용 CALS 서버 및 보안 관리 서버
이질망간 연동 및 관리 소프트웨어	이질망간 보안 관리 정보 베이스 및 보안 QoS 관리 소프트웨어	보안 관리 서버
	국제 거래(Interbank Clearing 포함) 보안 및 공증 소프트웨어	EC망 내부의 지불 서버, 국가 대표 CALS/EC 보안 게이트웨이 시스템
	CALS/EC 단위 서비스별 통합 보안 관리 소프트웨어	보안 관리 서버
CALS/EC 보안 표준, 평가 및 감리 소프트웨어	개발 대상 CALS/EC 보안 기술의 국제 표준 연구	국가 대표 CALS/EC 보안 게이트웨이 시스템, 해외 CALS/EC 망
	CALS/EC 국제 표준 보안 평가 소프트웨어	전체 환경에 해당
	CALS/EC 보안 감리 기법 및 소프트웨어	전체 환경에 해당
	법 제도권의 CALS/EC 보안 기술 수용을 위한 단계적 법제 방법론 연구	전체 환경에 해당

특히 주목할 부분은 기존 금융 서비스의 모든 부분을 수용하기 위하여 보험망, 금융망 및 증권망을 연결하여 CALS/EC 사용자가 보험 및 금융 서비스 그리고 증권의 매매를 국제적으로 할 수 있는 정보화 기반 서비스 체계를 CALS/EC 범주에 포함시킨 점이다. 향후 CALS/EC 정보화 서비스가 국제적으로 연동될 경우, 이와 같은 글로벌 체제로 서비스가 제공될 것으로 예측된다.

그리고 인증 및 공증 기능이 포함된 단순한 형태의 전자 지불 정보 흐름도는 <그림 5>와 같으며, 기관/기업 내부망에서의 키 복구(또는 키 위탁) 모델은 <그림 6>과 같다.



<그림 5> 단순 전자 지불 정보 흐름도



<그림 6> 기관/기업 내부망 키 복구 모델

4. 결론

OECD 암호 정책 중 암호화된 데이터를 국가 등의 제 3자가 강제적으로 해독하는 기술이 CALS/EC 산업에 표준화되어 적용될 가능성이 높기 때문에 향후 국내의 CALS/EC 보안 서비스 제공시 중요한 지침이 될 것이다. 본 논문에서는 키 복구 기술, 인증 기술 등을 고려한 OECD 암호 정책에 대하여 검토하였다. 또한 CALS/EC 보안 서비스를 실현하기 위하여 연구 개발해야 할 보안 기술 중 암호문의 강제 해독 기술 및 인증 기술을 포함한 보안 기술 프레임워크를 제안하였다.

특히, OECD 암호 정책에 대한 각국의 각계 반응을 고려할 때 국내의 대응 방안이 다각도로 이루어져야 할것으로 보이며 이를 위한 법제도 측면과 기술의 연구개발 측면외에 실수요자의 요구사항이 반영되어 '20세기 산업 사회'에서 '21세기 정보화 사회'를 위한 현실적이며 의미있는 변화가 시급히 요망된다. 이러한 가운데 본 논문에서 제안한 보안 기술 프레임워크가 향후 CALS/EC 보안 기술을 적용한 분야에 다소 지침이 될 수 있기를 기대한다.

참고문헌

[1] Architecture for Public-Key Infrastructure(draft-ietf-pkix-apki-00.txt), 1996. 11.

[2] Cryptography in Public Internetworks with Sun Screen, 1995.

[3] Federal Public Key Infrastructure Technical Specification Part A : Requirements, NIST, 1996.1.31, http://csrc.ncsl.nist.gov/pki/require5.ps

[4] Federal Public Key Infrastructure Technical Specification Part B : Technical Security Policy, NIST, 1996.1.24, http://csrc.ncsl.nist.gov/pki/tspolicy.ps

[5] Federal Public Key Infrastructure Technical Specification Part C : Concept of Operations, NIST, 1996.2.12, http://csrc.ncsl.nist.gov/pki/conops.ps

[6] Federal Public Key Infrastructure Technical Specification Part D : Interoperability Profile, NIST, 1995.9.27, http://csrc.ncsl.nist.gov/pki/cross.ps

[7] GOC Public Key Infrastructure, http://www.cse.dnd.ca/cse/english/gov.htm

[8] ICE-TEL, Architecture and General Specifications of the Public Key Infrastructure, 1996.9, http://www.darmstadt.ut.de/ice-tel/deliverables/download/D1-Architecture.rtf

[9] Internet Public Key Infrastructure Part I : X.509 Certificate and CRL Profile (draft-ietf-ipki-part1-03.txt), 1997. 6.

[10] Internet Public Key Infrastructure Part II : Operational Protocols (draft-ietf-ipki2opp-00.txt), 1997. 3.

[11] Internet Public Key Infrastructure Part III : Certificate Management Protocols (draft-ietf-ipki2cmp-01.txt), 1996. 12.

[12] Internet Public Key Infrastructure Part IV : Certificate Policy and Certification Practices Framework (draft-ietf-ipki-part4-00.txt), 1997. 3. 25.

[13] Nikei Computer, Japan 1997. 5. 26 pp.275-288.

[14] Robin Whittle, Public Key Authentication Framework: Tutorial, 1996.6, http://www.ozemail.com.au/~firstpr/crypto/pkaftute.htm

[15] Standards Australia, Strategies for the implementation of a Public Key Authentication Framework(PKAF) in Australia, SAA MP75-1996

[16] The OECD Guidelines on Cyrptography Policy, OECD 1997. (http://www.oecd.org/dsti/iccp/cryptome.html)

[17] Schenier, B., E-Mail Security, John Wiley & Sons Inc., 1995.

[18] The Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Teansborder Flows of Personal Data, OECD, Sep. 1980.

[19] The Recommendation of the Council concerning Guidelines for the Security of Information Systems, OECD, Nov. 1992.

[20] The 1994 Mitre PKI Study Final Report, NIST, http://csrc.ncsl.nist.gov/pki/mitre.ps

[21] Utah Digital Signature Act, 1996, http://www.gvnfo.state.ut.us/ccjj/digsig/dsut-act.htm

[22] VeriSign Web Home Page : www.verisign.com

[23] 미국 전자서명법 관련 종합사이트, http://www.abanet.org/scitech/isc/matrix10.html

[24] 박성준, 제 2회 정보호호 심포지움 발표 자료집, 1997.

[25] 심영철, 제 1회 한국 전산망 보안기술(NETSEC-KR'95) 워크숍 발표자료집, 1995. 5.

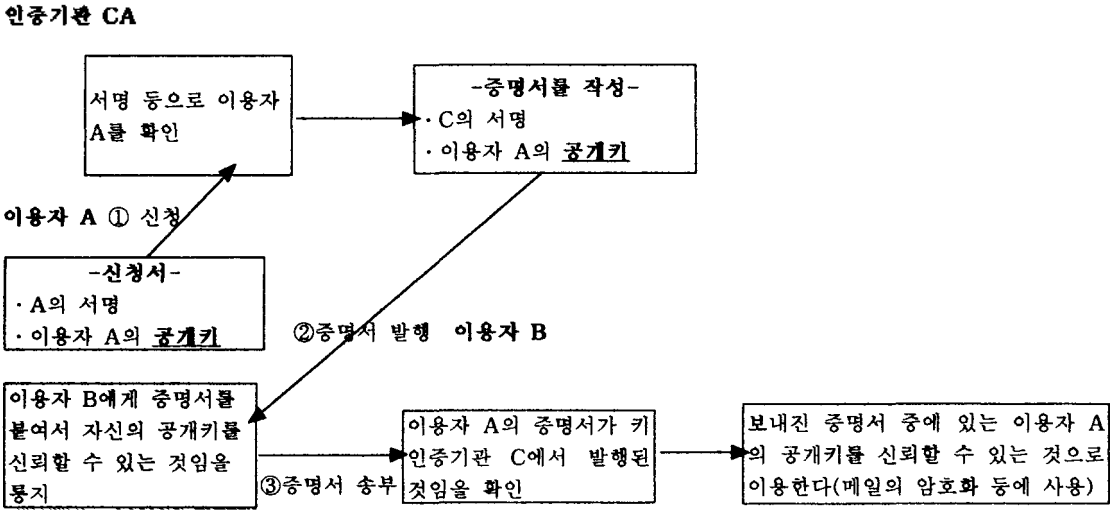
[26] 임신영 외, 전자거래 사용자 보안 서비스 요구 사항 분석 및 설계, 1997년 한국정보처리학회 춘계 학술발표논문집 제 4권 제 1호, 1997. 4.

[27] 최용락 외, 통신망정보보호, 1996.2.

<표 1> OECD 암호 정책 8대 원칙

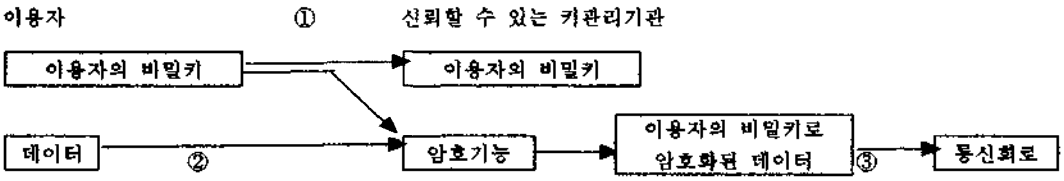
원칙	요구 사항	원칙의 배경 및 의미
1.암호기술의 신뢰성	암호기술은 이용자가 정보시스템과 통신 시스템에 적용할 때에 온닉성을 확보할 수 있도록 신뢰성이 높은 것이어야 한다.	· 사용자의 요구에 근거하여 개발된 기술을 제공하여 정보시스템과 통신시스템의 신뢰성을 확보해야 한다. 정부가 제정하는 규칙, 허가제도 및 암호기술의 이용 역시 신뢰성 확보에 기여한다. 또한 암호기술에 대해서 시장에서 인지된 기준에 의한 평가도 신뢰성 확보에 기여한다. · 신뢰성을 확보하기 위해 암호키의 관리 시스템에 대해서 어떤 법률을 적용하는가를 사용자와 암호키 관리기관이 교환하는 계약서에 규정해야 한다.
2. 암호기술의 자유선택	사용자는 적용되는 법률을 기준으로, 이용하는 암호기술을 자유로이 선택할 수 있어야 한다.	· 사용자는 정보시스템과 통신시스템의 보안성을 확보하고, 데이터의 온닉과 보전을 보증하기 위해 요건에 맞는 암호기능을 이용할 수 있어야 한다. 데이터를 관리, 이용, 보관하고 있는 개인과 조직은 그 데이터에 대한 온닉과 보전의 책임이 있으며, 그 책임을 다하기 위한 최적의 암호기술을 이용할 수 있어야 한다. 데이터의 보안성에 대한 다른 요구에 대응하기 위해서 다른 종류의 암호기술이 요구된다. 사용자는 적용되는 법률을 기준으로 데이터에 대한 최적의 보안성 레벨을 자유로이 결정하고, 이를 위해서 최적의 암호기술을 자유로이 선택하고 도입할 수 있어야 한다. 암호기술에는 암호키 관리시스템도 포함된다. · 개인정보와 전자 상거래에 관한 정보등 사회에 영향을 끼치는 정보보호에 관해서 충분한 보안성을 확보하기 위해 정부는 암호기술에 관한 정책을 책정할 수 있다. · 암호기술에 관한 정부의 관리는 정부가 그 책임을 수행하는데에 필요한 최소한의 것이어야 한다. 이러한 정부의 관리는 사용자가 암호기술을 자유로이 선택할 수 있는 권리를 침해해서는 안된다. 이 원칙은 사용자의 자유로운 선택을 제한하는 것과 같은 규칙을 정부가 제정하지 않도록 권장하고 있다.
3. 시장요구에 근거한 암호기술의 개발	암호기술의 개발은 개개의 사용자와 산업계, 정부의 요청에 답하는 것이어야 한다.	· 암호기술의 개발과 제공은 자유경쟁시장의 원칙에 의해 결정되어야 한다. 이로써 기술변화에 대응하고 사용자의 요청에 답할 수 있어 실제의 정보시스템과 통신시스템의 위험에 대항할 수 있게 된다. 암호기술에 관한 국제적인 기술표준과 기준, 프로토콜 개발도 시장의 요구에 근거해야 한다. 정부는 암호기술의 개발을 위해 산업계와 연구기관의 활동에 대해 지원 협력해야 한다.
4. 암호기술의 표준	암호기술에 관한 기술표준, 기준, 프로토콜은 국가 및 국제적 레벨에서 개발 및 그 적용을 추진해야 한다.	· 시장의 요구에 근거해서 국제적으로 인지된 표준화 기관과 정부, 산업계와 그외 관련 전문가는 상호운용성이 있는 기술표준, 기준, 프로토콜 개발과 그 운용을 추진하기 위해 필요한 정보를 공유하고 서로 협력해야 한다. 또한 암호기능에 관한 국가표준이 존재하는 경우에는 그 표준은 국제적인 상호운용성과 편리성을 확보할 수 있도록 국제표준에 모순돼서는 안된다. 기술표준에 대한 적합성 시험과 평가를 위한 방법은 그 결과가 널리 인정될 수 있는 것이어야 한다.

원 칙	요구 사항	원칙의 배경 및 의미
5. 프라이버시와 개인정보의 확보	통신비밀과 개인정보의 보호를 포함한 프라이버시에 관한 개인의 기본적 권리는 국가 암호방침의 책정과 암호기술의 도입과 운용에 있어서 충분히 존중되어야 한다.	· 암호기술은 데이터와 통신 온닉 및 이용자 보호 등 프라이버시 보호를 위해 유익한 수단이다. 나아가 암호기술의 이용으로 안전성과 익명성을 보장하는 지불과 상대방과의 비밀통신과 대화가 가능하고 개인 데이터 수집을 최소한으로 할 수 있다. 동시에 통신할 때의 데이터 보전을 확보함으로써 프라이버시 보호에도 도움이 된다. 개인 데이터의 수집과 개인식별을 위한 시스템 구축의 실시에 있어서는 내용의 충분한 설명과 프라이버시 보호가 실시되어야 한다. · 「프라이버시 보호」 및 「개인 데이터의 역외 유출」에 관한 OECD 정책은 개인정보의 수집과 관리에 관한 기준이 된다. 암호기술의 도입에 관한 법률은 이 내용을 충분히 반영해야 한다.
6. 법에 근거한 입수	국가는 암호정책에 의해 암호화된 데이터의 보통문장 또는 복호화를 위한 암호 키를 법에 근거해서 입수할 수 있다. 이 정책의 실시에 있어서는 OECD암호 정책이외의 원칙을 충분히 배려해야 한다.	· 「법에 근거한 입수」를 가능하게 하는 암호기술에 관한 정책을 고려할 때에 정부는 공공의 안전과 법의 집행, 국가의 안전과 그 암호기술의 부정 사용에 따른 위험과 암호기술의 신규개발에 의한 추가경비, 기술부족에 따른 손해 등을 충분히 고려해야 한다. 이 원칙은 정부에 「법에 근거한 입수」를 위한 규칙제정을 강요하거나 또한 금지하는 것도 아니다. · 암호화된 데이터의 평문 또는 복호화를 위한 암호키의 입수는 법적인 절차에 근거해서 실시된다. 입수를 요구하는 개인 또는 조직은 평문을 소유할 법적인 권한을 가지고 있어야 한다. 또한 법에 근거해서 입수한 데이터는 법으로 허가된 목적 이외에 사용해서는 안된다. 이 「법에 근거한 입수」에 관한 기록 정보를 수집하여, 국가의 법률에 근거해서 감사 또는 검사가 실시되어야 한다. 이 「법에 근거한 입수」를 위한 조건은 명기되고 공개되어 암호기술의 사용자와 제공자 및 암호키의 관리자가 쉽게 이해할 수 있도록 해 두어야 한다. · 암호키 관리시스템은 사용자와 「법에 근거한 입수」를 집행하는 기관의 이해의 균형을 조정하는 역할을 다할 수 있다. 이 암호키 관리시스템은 암호키를 분실했을 때 데이터 복구에도 이용할 수 있다. 데이터의 은닉에 이용되는 암호키와 기타 목적에만 이용되는 암호키에서는 「법에 근거한 입수」 절차는 다른 것이어야 한다. 데이터의 인증과 보전을 위해서만 이용되는 암호키는 그 법적인 소유자인 개인과 조직의 동의없이 이용돼서는 안된다.
7. 책무	암호 서비스를 제공하거나, 암호 키를 보관 또는 이용하는 개인 또는 조직에 관한 계약서가 작성되거나 규칙이 제정되는 경우는 그 책무에 대해 계약서 또는 규칙에 명기해야 한다.	· 암호 서비스를 제공하든지, 암호키를 보유 또는 입수하는 개인 또는 조직의 책무는 관계자가 서로 교환하는 계약서 또는 적당한 국가의 규칙과 국제적인 동의서에 명시해야 한다. 해당 조직에는 정부관련기관도 포함된다. 사용자가 자신의 암호키를 부정하게 사용한 경우의 책무도 명확히 해야 한다. 키 관리자는 「법에 근거한 입수」에 따라서 암호키 또는 암호 데이터의 평문을 제공할 때에는 어떠한 책무도 지지 않는다. 「법에 근거한 입수」에 따라서 암호키 또는 암호 데이터의 평문을 입수한 기관은 그 부정 이용에 관해서 책임을 져야 한다.
8. 국제협력	정부는 암호정책을 수행하기 위해 국제협력을 해야 한다. 이외 가시적인 수행을 위하여 정부는 무역을 저해하는 암호정책을 제정해서는 안된다. 그러한 암호정책이 존재하는 경우에는 제지해야 한다.	· 암호의 국제적인 이용과 국제적인 정보망의 촉진을 위해서 각국의 암호정책은 국제적으로 협조할 수 있는 것으로 해야 한다. 이를 위해 본 암호정책을 이용해야 한다. · 암호키 관리시스템을 개발할 경우에는 암호의 국제적인 이용이 가능하게 하는 것으로 해야 한다. · 국가간 「법에 근거한 입수」는 관계국간의 협력과 합의에 의해 실시되어야 한다. · 정부는 암호 정책에 근거해서 암호 데이터의 자유로운 통신을 방해해서는 안된다. · 국제무역의 촉진을 위해서 정부는 국제 상거래를 저해하는 암호 정책을 채택해서는 안된다. 또한 정부는 암호기술의 국제적인 이용을 부당하게 방해해서는 안된다. · 암호의 국제적인 이용과 국제적인 정보망의 촉진을 위해 각국의 암호 정책은 국제적으로 협조할 수 있는 것으로 해야 한다. 이를 위해 본 암호정책을 이용해야 한다.

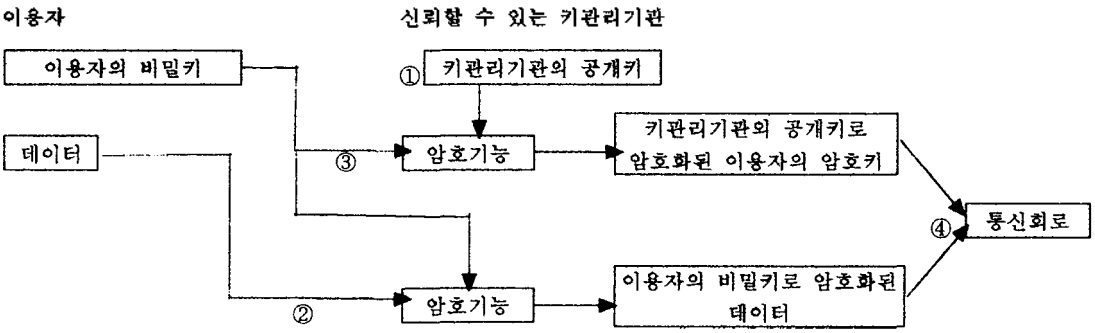


<그림 1> CA에 의한 공개키 인증 절차

<방식 A>



<방식 B>



<그림 2> 「법 강화를 위한 강제 암호키 및 데이터 입수」를 위한 암호화 절차