전자상거래활성화를 위한 암호화 정책 동향 분석

*김현태, *나인호, **이경근

*군산대학교 정보통신공학과, **호원대학교 전자계산학과

An Analysis of Encryption Policies for Enhancement of Electronic Commerce

*Hyun-tae KIm, *In-ho Ra, Kyung-keun Lee

*Dept of Telecommunication Eng., Kunsan National University

**Dept of Computer Science., Howeon University

E-mail : ihra@ks.kunsan.ac.kr

요 약

인터넷과 같은 개방된 네트워크에서 전자상거래를 활성화하기 위해서는 시스템 및 네트워크상에서 거래 정보에 대한 신뢰성과 안정성이 확보되어야 한다. 암호화 기술은 전자상거래 시스템에서의 정보 보호를 위해 활발히 연구되고 있는 부분으로서 OECD를 중심으로 표준화된 암호화 기술 개발이 이루어지고 있으며 국내외적으로 EC 활성화를 위한 법·제도적 장치의 보완이 진행중에 있다. 본 연구에서는 국제기구 및 주요국가의 암호화 정책을 분석하여 우리나라에 적합한 암호화 정책 방향을 제시하고 전자상거래에서 상거래 정보의 신뢰성을 확보할 수 있는 방안 및 대응책에 대해 기술하였다. 또한 전자상거래에서 암호화를 이용한 응용 기술과 정부부처, 각 협력업체들의 정책동향 및 국내 기업의 전자상거래를 위한 암호기술개발 동향을 분석하였다.

I 서 론

정보통신기술의 발전으로 인하여 지역적으로 사용하던 네트워크 환경이 인터넷과 같은 개방형 구조를 갖는 대규모 네트워크 환경으로 변해가고 있다. 이와 더불어 선진국을 중심으로 전자상거래 등과 같이 개방된 네트워크 환경의 장점을 살린 국제적 서비스 시스템을 구축하려는 노력이 적극적으로 추진됨에 따라 단순한 통신 수단의 인터넷 환경이 이제는 경제구조의 변화에 중추적인 역할을 담당하게 되었다. 이러한 개방된 네트워크 환경에서는 무엇보다도 정보통신 시스템의 안전성 및 신뢰성이 확보되야 한다. 이를 위해 많은 수단과 방법이 연구되고 있으나 그 중에서도 암호화 기술이 가장 적합한 방법으로 받아들여지고 있다.

이전까지 암호기술을 단지 국가 안보나 외교 차원의 전략적인 기술로만 취급되어 국가의 이익을 보호하기 위해서 주로 사용되어 왔다. 그러나 전자상거래등 다양한 서비스의 발전으로 민간분야에서 정보보호가 점차 중요해짐에 따라 암호기술을 국가 기밀 유지 목적 이외에도 민간부분에서 사용할 수 있도록 법·제도적인 장치를 보완하고 있다.

본 논문에서는 주요 선진 국가 및 국제기구에서 정보보호을 위한 암호화 정책 추진 현황을 살펴보고 전자상거래에서 정보보호를 위한 암호 정책 및 기술 동향을 분석하여 국내의 전자상거래를 증진시킬 수 있는 암호화 정책의 방향을 살펴보고 앞으로 우리가 해결해야 할 과제를 기술하였다. 본 논문의 구성은 다음과 같다. II장에서는 주요 선진국 및 국제기구에서 추진하고 잇는 암호화 정책의 개발동향에 대해 기술하고 III장에서는 전자상거래 활성화를 위한 고려 사항에 대해 기술한다. IV과 V에서는 각각 국내 암호화 동향과 향후 대책 방안 및 결론에 대해 기술한다.

II 국외 암호화 정책 동향

최근 정보보안에 대한 중요성이 국내·외적으로 정부나 업계에서 중요한 문제로 부각되고 있다. 1997년 3월 OECD 이사회에서는 OECD 과학기술산업국(DSTI)의 정보·컴퓨터·통신정책위원회(ICCP)에서 상정한 '암호정책 지침'을 통과시켰다. 이런 지침에 대한 작업은 ICCP에서 관장하고 있으며 이 회의에서는 미국, 프랑스, 일본 등 OECD 20여개 회원국의 국가대표와 기업산업자문위원회 BIAC(Business and Industry Advisory Committee) 및 국제상공회의소인 ICC (Integrational Chamber of Commerce) 등의 대표 및 전문가들이 모여 정보보호에 관련된 8가지 기본원칙에 대하여 사안 별로 합의를 도출하였다.

OECD 이사회에서 도출된 '암호정책 권고'의 기본적인 구조는 목적, 범위, 용어정의, 통합(Intergration) 및 기본원칙(Principles) 등 5개의 부분으로 구성되어 있으며 암호정책 권고의 핵심이 되는 8가지 기본원칙은 암호기법의 신뢰성, 자유로운 암호기법의 선택, 시장원리에 의한 암호기

법의 개발, 암호기법의 표준, 사생활과 개인정보의 보호, 합법적인 암호정보의 액세스, 암호서비스 제공자와 암호키 사용자의 책임, 암호이용의 활성화를 위한 국제협력 방안을 제시하였다[1].

이러한 암호정책은 정보 시스템 기반 구축과 개방된 네트워크와 같은 인터넷의 등장과 멀티미디어 기술의 발전으로 가상의 세계에서 상거래를 올바르게 형성할 수 있게 경제구조가 변모되어야 한다는데 초점을 두고 있다. 변화되는 경제구조 속에서 개인의 비밀 보호나 소비자의 신뢰성 확보를 위해서는 국가 차원에서의 정보보호를 위한 법·제도적인 규제의 정비와 기술개발이 국내에서도 활발히 추진되어야 할 것이다.

2.1 미국

미국은 정보보호 분야에 선두주자로서 1960년대부터 정보보호 관련 기술에 대한 연구 개발을 시작하였다. 1984년 이전까지는 주로 국방부에서 국가 비밀에 관련된 사항은 관장하였고 국가 비밀이 아닌 사항은 모두 상무부에서 관장하여 왔다. 국가 보안의 경우 국방부와 중앙정보부가 보안 정책을 개발하는 임무를 수행하고, NSA는 표준화, 연구개발, 평가 및 기술 자문 등의 임무를 수행하였다. 또한 1990년에 DES 암호 알고리즘의 안전성 문제가 대두됨에 따라 미국의 클린턴 행정부는 1993년에 Clipper Project 정책을 발표하였고 64비트 Skipjack 블록 알고리즘을 개발하여 현재 ISO/IEC JC1/SC27의 국제 표준 알고리즘 등록 절차(ISO/IEC9979)에 의해 현재 이름만 등록되어 있는 상태이다.

Skipjack 알고리즘을 반도체로 하드웨어화 한 것을 Clipper Chip이라고 하며, 미국의 디지털 서명 표준인 DSS(Digital Signature Standard)를 포함한 Capstone Chip라는 반도체 칩을 발표하였다[2].

1996년 6월 연방의회의 요구로 준비된 "정보사회를 보호하기 위한 암호의 역할"이라는 NRCI의 연구 보고서는 정부가 광범위한 암호의 상업적 사용을 증진해야 함을 표명하고 있다. 또한 이 보고서는 수출규제가 점진적으로 완화되어야 하지만 없어서는 안되며, 위탁된 암호의 채택은 자발적이어야 한다고 조언하고 있다.

1996년 5월 관리예산청에서는 "Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure"라는 보고서를 통해 키(key) 위탁을 통합한 키 관리기반의 필요성을 거론하였으며, 암호를 자유롭게 선택하고 키 관리기반를 활성화하기 위한 자발적인 참여의 필요성을 거론하였다.

이와 같은 정책을 기반으로 1997년 7월 1일 '범세계적 전자상거래 기본계획'에서 전자상거래 5가지 원칙과 재정적 이슈, 법적 이슈, 시장접근 이슈에 대한 9개 사안에 대한 미국의 입장을 발표하였다. 이 기본계획에 의하면 전자상거래는 민간주도형이며, 정부의 개입은 일관된 법제 환경을 구축하는 등 필요 최소한의 경우로 제한되어야 하고 범세계적 전자상거래 활성화를 위해 전세계가 공동의 노력을 기울여야 한다는 내용을 발표한 바 있다.

2.2 일본

일본은 통상성과 우정성이 각기 다른 정책을 펴고 있는데 우정성은 암호정책을 개발하거 이것은 통상성에 의해 실현되고 있다. 최근에는 사법성과 경시청에서도 이 분야에 관여하고 있다. 또한, 통상성은 1997년 5월 "Towards the Age of the Digital Economy - For Rapid Progress in the Japanese Economy and World Ecoonmic Growth in the 21st Centry"라는 보고서를 발간하여 전자상거래에서 암호의 중요성을 역설하고, 암호기술개발과 연구프로젝트가 증진되어야 한다고 주장하였다.

특히, 최근 2년 동안 일본에서는 전자상거래에 대한 많은 관심을 보이고 있으며, 전자상거래를 국제적인 정보기술(IT)에 관한 중심 주제로 전환하였고 전자상거래실증추진협의회(ECOM)에서 이 분야의 국제 회의에 적극 참여하고 있을 뿐만아니라 정부차원에서도 전자상거래 실현을 위한 연구를 진행하고 있다[3]. 특히, 통상성에서는 95년초 「전자상거래환경정비연구회」를 발족하여 제도적 장치에 대한 다양한 연구를 수행하고 있으며, 우정성은 96년 말 「네트워크를 통한 인증업무에 관한 조사연구회」를 결성하여 「인증기관에 관한 가이드라인」을 발표하였다. 게다가 우정성은 「고도정보사회를 실현하기 위한 환경정비에 관한 법률 사이버법(가칭)」을 제언하기도 했다. 이와 더불어, 대장성는 「전자화폐법(가칭)」을 검토하고 법무성은 전자거래제도를 연구하여 2001년 실용화시킬 계획을 가지고 있다.

2.3 국제기구

■ 경제개발협력기구(OECD)

OECD는 '97년 11월 투르크 회의에서 전자상거래에 관련된 논의를 OECD 전체 차원으로 확대하여 전자상거래의 장애요인 철폐를 위한 논의를 주도하였으며, '98년 10월 캐나다 오타와 각료회의에서는 범세계적인 전자상거래 활성화를 위한 일반적 합의와 주요 지침의 채택 및 실행계획을 구체화시킨 것으로 알려져 있다. 특히 개인정보 및 사생활 보호, 조세에 관한 원칙, 소비자의 권리 및 의무, 전자인증을 통한 전자상거래 촉진 등에 대한 정책적 가이드라인 제정에 대해 논의하였다.

■ 유럽연합(EU)

1997년 10월 유럽위원회는 기밀성과 인증, 무

결성 모두에 대해 기술한 "Ensuring Security and Trust in Electronic Communication Towards a European Framework for Digital Signatures and Encryption"보고서의 발간하였다. 이 보고서에서는 키 복구나 키 위탁이 각국에서 암호규제의 일환으로 적용될 수 있다고 밝히고 있으며, 이는 암호키에 대한 합법적 접근권이 각국의 환경에 따라 결정되어야 한다는 것을 시사하고 있다. 또한 암호기술이 중요 정보의 불법적 사용을 완전히 차단하지는 못하지만, 외부의 침입으로부터 데이터와 통신상의 비밀을 효과적으로 방어하기 위한 방법으로 사용될 수 있음을 강조하였다. 그 외에도 EU 회원국이 암호기술의 사용에 따른 규제와 법집행기관의 역할에 대하여 유럽연합의 자유유통조항(Free Circulation Provisions)과 데이터보호 지침을 준수하도록 권고하고 있다.

■ 아시아 · 태평양 경제협력체(APEC)

APEC은 미국의 전자상거래 관련 정책 발표 이후 전자상거래를 전체 APEC 차원에서 논의하기 시작하였으며, '97년 11월 APEC 정상회의 선언문에 전자상거래에 관한 내용을 포함하였다. 또한 1998년 6월 정보통신장관회의 및 통상장관회의에서 전자상거래 작업계획 수립에 대한 기여 방안을 논의하여, '98년 11월 쿠알라룸푸 정상회의에서 그 성과를 보고하도록 합의한 바 있다.

아 · 태지역의 전자문서교환표준개발에 주력해 온 아시아 DEIFACT 이사회(ASEB)가 최근 이란 테헤란 국제회의 센터에서 한국을 비롯해 일본, 싱가포르, 대만, 말레이시아 등 9개국이 참가한 가운데 개최되었으며 EC에 대응할 만한 기구로 개편하기로 결정하고 초대 의장국에 한국을 선정하였다. 99년 9월에 1차 총회를 의장국인 한국의 서울에서 개최기로 하였다.

■ G7

'94년 7월 나폴리 G7 정상회담과 '95년 2월 브뤼셀 G7 정보통신장관회의에서 11개 G7 정보화 시범사업 프로젝트를 확정하였다. 이 중에서 '범세계적 중소기업 시장조성'이라는 프로젝트는 주로 중소기업의 전자상거래 활동을 지원하는 프로젝트로서, 경제활동의 기초이며 혁신과 고용창출의 핵심인 중소기업이 필요한 정보의 접근과 독자적인 범세계적 무역에 적극적으로 참여할 수 있는 환경을 조성하기 위한 것이었다.

■ 유엔국제상거래법위원회(UNCITRAL)

UNCITRAL는 범세계적 상거래의 법제 환경을 조성하기 위해 '96년 5월 '전자상거래 모델법'을 제정하였다. 이 모델법은 각국의 국내법을 제정, 개정할 때 모델법을 반영할 것을 요청하는 권고사항적 성격을 가지고 있다. 현재는 전자상거래 분야중에서 전자서명과 인증기관에 대한 논의에 초점을 두고 있다. 또한, 향후 작업과제로서 공개키 암호화 방법에 대한 기술적 대안 문제, 전자계약 문제, 인터넷상의 재판권 문제 적용법 문제 및 분쟁해결 문제 등을 제시하고 있다.

III 전자상거래 활성화를 위한 고려사항

범세계적인 정보통신 기반을 이용하여 전자상거래를 활성화하기 위해서는 정보보안에 대한 소비자 신뢰 및 안정성 확보 문제가 우선적으로 선결되어야 하고, 이를 바탕으로 전자상거래를 부흥시켜야 할 것이다. GII에서는 기본적으로 EC를 위한 선결과제로 다음과 같은 4가지 사항이 해결해야 한다고 주장하고 있다.

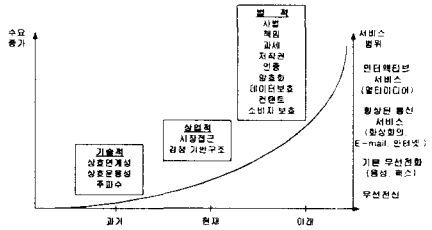

그림 1. The Need for strengthened international coordination

- 안전하고 신뢰할 수 있는 통신망
- 개방형 정보시스템들을 보호하기 위한 효과적인 수단
- 전자정보의 기밀성과 인증체제의 효과적 수단
- 정보시스템과 전자자료의 보호를 위한 전문가

특히, OECD는 위에서 언급된 4가지 사항들에 대해 인증기능을 공신력 있게 믿을수 있도록 제3자(Trusted Third Party)의 역할을 수행하는 인증기관(Certification Authority)과 국제적인 상거래 시대를 대비한 국제적인 인증기관 및 제도의 필요성을 역설하였다.

3.1 전자상거래의 특징 및 보안 침해

전자상거래에서는 다음과 같은 환경과 특성으로 인하여 정보보호 방안이 필수적으로 제시되야 한다.

- 컴퓨터 네트워크: EC는 비대면 상거래이기 때문에 네크워크 상에서 시스템과 네트워크에 대한 정보의 기밀성(Confidentiality)을 유지할 필요가 있다.
- 디지털: 모든 거래정보가 디지털 형태이므로 동일한 복제가 가능하며 위조가 용이하다. 그

리고 디지털 자료를 거래에 대한 증거로서 사용하기 위한 보조적인 보안 요소들이 필요하다.

- 익명성: 현재 인터넷과 같은 컴퓨터 네트워크는 신분을 확인할 수 있는 기반구조가 없다. 따라서 안전한 전자상거래를 위해서는 거래 당사자의 신분을 인증할 수 있는 기반구조가 필요하다.
- 범세계적: 상거래를 하는 당사자끼리 지역적인 제약을 받지 않는다는 특징을 제공하지만 지역적으로 블록화된 세계경제구조를 넘어서 거래가 이루어지기 때문에 환율, 배달, 지불방식, 거래물품의 품질, 환불, 소비자보호, 문화적 차이 등에 있어서 해결해야 할 과제가 많다.

이와 같은 특성과 개방된 네트워크로 인하여 전자상거래에서는 여러 가지의 위험요소를 갖는다. 일반적으로 전자상거래에서 예상되는 보안 침해 형태는 3가지로 나눌 수 있다.

- 시스템 공격: 네크워크에 연결된 컴퓨터는 외부인으로부터 침입하여 부당하게 컴퓨터시스템을 사용하거나, 정보를 유출하거나, 정보를 파괴할 위험이 있다.
- 데이터 공격: EC에서 데이터 공격을 시스템내에 저장된 데이터를 공격하는 형태와 네트워크상에 흘러 다니는 데이터에 대한 공격 형태로 나눌 수 있다.
- Business 공격: 전자상거래의 특징으로 인해서 발생할 수 있는 제3의 공격으로써 이를 통칭해서 비즈니스공격이라고 한다. 전통적인 상거래에서 발생하는 불법행위가 전자상거래에서도 일어날 수 있다.

이러한 공격은 시스템 자체적으로는 보안을 유지하고 사용자에게 신뢰성 및 안전성을 제공하기에는 역부족이므로 공격을 당했을 경우에 법·제도적인 장치, 법적인 보장, 보험 등의 전자적인 시스템 외의 보완이 보장되어야만 한다.

3.2 정보보호에 대한 기술적인 측면

앞에서 언급한 정보에 대한 침해를 극복하기 위하여 전자상거래 시스템에서 제공해야 할 보안성 기능들은 아래와 같으며, 이것들는 필수적으로 보장받을 수 있어야 한다.

- 기밀성(Confidentiality)
- 인증(Authentication)
- 무결성(Integrity)
- 부인방지(Non-repudiation)

정보보호 기술 분야는 컴퓨터 시스템 보호, 통신 보호, 네크워크 보호 등을 나눌 수 있으며 이것들에 대한 최근 기법들을 살펴봄으로써 위의 4가지 기능을 구현하는데 필요한 이론적인 기반을 제공할 수 있다[4]. 이러한 특성들을 만족시키기 위해 그동안 여러 가지 암호 기술들이 연구 개발되어 왔으며, 지금까지 널리 알려진 암호기술은 크게 다음과 같이 나눌 수 있다[5].

- 비밀키 암호기법(Secret-Key Algorithm): 안전한 통신을 하고자 하는 두 사람이 서로 똑같은 비밀키를 소유하여 메시지의 송신자가 비밀키를 이용하여 암호화한 것을 수신자가 받아서 비밀키를 이용하여 복호화 하는 방식을 말한다. 이러한 기법은 "Stream Cipher"과 "Block Cipher"의 두가지 종류가 있다. 전자는 비트열로 입력되는 데이터를 비트단위로 암호화하는 기법으로써 RC4, SEAL등이 있고, 후자는 비트열로 입력되는 데이터를 일정한 길이의 비트열(보통 64비트)로 잘라서 그것을 단위로 암호화하는 기법으로써 DES, IDEA, RC2, FEAL 등이 있다.

- 공개키 암호기법(Public-Key Algorithm): 메시지를 암호화할 때와 복호화할 때 사용하는 키가 다르. 이러한 서로 다른 두 개의 키 중에서 하나를 비밀키라고 하며 나머지 하나를 공개키라고 한다. 이 두 종류의 키 중에서 어느 것도 암호화와 복호화가 가능하고 단지 수학적인 계산이나 유추에 의해서 하나의 키로부터 나머지 하나의 키를 알아낼 수 없도록 만들어져야 한다. 그 예로 RSA, Diff-Hellman알고리즘 등이 있다.

3.3 전자상거래 응용기술

3.3.1 디지털서명(Digital Signature)

기존의 종이 문서에 서명이나 도장을 찍어 인증을 보장하는 것과 전자문서에서도 문서내용에 대한 인증 방식이 필요하다. 이러한 서명 방식들 중에서 암호학적 기법을 응용하여 만든 방식을 디지털 서명이라고 한다. 즉, 문서 작성자를 규정하고, 문서에 표시된 내용이 본인에 의해 바르게 표시되었다는 것을 추인하는 서명과 동일한 기능을 가지는 일종의 전자적인 암호 처리 등의 절차를 말한다. 디지털 서명은 일반적인 서명은 다음과 같은 특징을 보장할 수 있어야 한다.

- 위조 불가성(Unforgability)
- 부인봉쇄(Non-Repudiation)
- 재사용 불가성(Non-reusability)
- 문서의 변경 불가성(Message integrity)

디지털 서명은 서명과정과 서명확인 과정에 참여하는 사람들이 누구인가에 따라서 크게 직접서명 방식과 간접서명 방식으로 나누어진다. 전자는 메시지의 송신자가 서명을 하고 수신자가 서명확인을 직접하는 방식이고 후자는 메시지의 송신자

가 서명을 하고 그 메시지와 서명을 중재자에게 보내면 중재자는 서명을 확인한 후 그 결과를 수신자에게 보낸다. 또한, 일반적으로 이용하고 있는 암호기법의 종류에 따라서 비밀키 암호기법에 기반을 둔 방식과 공개키 암호기법에 기반을 둔 방식의 두 가지로 나누어진다.

3.3.2 전자지불시스템

전자 상거래를 구성하기 위해서는 안전하게 전자 지불을 할 수 있도록 전자지불 인프라구조를 제공해야 한다. 현재, 인터넷상의 전자상거래를 제공하는 시스템에서의 지불환경은 첫째, WWW 폼-입력 기반 시스템(WWW Form-CGI System)이 있고 둘째, 가입자 기반 시스템(Subscibe Base System)과 셋째, 인터넷상의 전자지불 시스템을 이용해 지불을 처리하는 방식이 있다. 우선적으로 첫 번째와 두 번째는 사용자 ID와 패스워드를 기본적으로 요구하기 때문에 네트워크상에서 안정을 보장받을 수 없다. 물론, SSL 보안 프로토콜을 이용해 채널 보안을 얻을 수 있으나 사용자들의 거래에 대한 부인봉쇄, 상거래 서버의 사기 등에 대한 안전장치가 결여되어 있다.

이와 같이 인터넷과 같은 환경에서 암호기술을 응용한 보안 시스템으로써 전자지불 시스템을 선택하고 있다. 일반적으로 다음과 같은 3가지의 모델이 있다[6].

- 지불 브로커 시스템(Payment Broker System): 독립적인 지불방식은 아니지만, 전자상거래 환경에서 신용카드번호나 은행계좌번호를 안전하게 주고받을 수 있도록 중계해주는 시스템이다. 즉 금융환경을 필요로 하지 않기 때문에 지불정보를 전달하는 트랜잭션만 안전하고 편리하게 처리해주는 메카니즘을 만들면 비교적 쉽게 구현가능하다.
- 전자 화폐 시스템(Electronic Cash System): 자신만의 신용을 기반으로 화폐와 같은 부채나 가치를 발행하는 형태로써 외부 지불방식의 직접적인 도움이 필요 없어 시스템 흐림이 간단하다. 하지만, 화폐 발행의 법적인 효력, 기존의 금융기관과의 역할의 중복성 등의 제도적인 문제점이 있다(디지케쉬의 ECach, 이니텍의 이니텍페이).
- 소액전자지불시스템(Micropayment System): 전자화폐 시스템의 한 형태로 소액지불을 전문적으로 처리하기 위한 전자지불 시스템이다. 특히, 인터넷상의 전자상거래 방식 가운데 온라인 출판(Online publishing), 온라인 정보검색, 온라인 DB서비스 등에 주로 소액지불이 이루어 진다. (MPTP, 밀린센트(Millicent), 마이크로민트(MicroMint) 등이 있다)

표 1. 전자지불 프로토콜 분류

분류	회사/프로토콜	특징
신용카드 응용	FV(First Virture 사)	암호화 사용 안함, 메일 기반
	CyberCash(CyberCash사)	
	SmartWallet(V-One사)	
	CFWallet(Check Free사)	
	iKP(IBM)	프로토콜 스펙만 있음
	Secure Courier(Netscape)	프로토콜 스펙만 있음, SSL
	SET(VISA, MasterCard)	신용카드 기반
네트워크 신용 응용	NetCheque(California대학)	
	NetBillCarnegie(Mellon 대학)	
	전자현금 Ecach(DigiCash사)	
	NetCash(California대학)	
	CAFE(13개 유럽연합)	IC 카드기반
	Mondex(영국)	IC 카드기반
e은행	SFNB	95년 10월

표 1은 알려진 저자 지불 프로토콜을 전지 지불 방식에 따라 회사별, 특징별로 분류한 것이다[7].

3.3.3 공개키 기반 구조 (PKI: Public Key Infrastructure)

전자상거래의 안전성과 신뢰성을 기술적이나 법·제도적인 모든 면을 고려하여 확보하기 위해서 전자인증제도가 요구되며, 이것은 전자서명기술의 안전한 운영을 의미한다. 전자서명기술에 사용되는 공개키 알고리즘은 비밀키의 기밀성과 공개키의 무결성을 보장하여야 하며 이를 해결하고자 하는 것이 바로 공개키 기반구조이다. 즉, 공개키 기반구조 구축은 전자인증제도를 실체화한 것이다.

PKI로 제공할 수 있는 서비스를 통해 프라이버시, 접근제어, 무결성, 인증, 부인봉쇄를 보장할 수 있다. PKI 모델에서는 정책 승인기관, 정책인증기관, 인증기관이 계층적으로 구성되어 있다. 또한 인증기관과 사용자 사이에서 인증서를 신청받아서 인증기관에 인증서 요청을 수행하는 등록기관이 있고 인증서, 사용자 관련 정보, 상호인증서 쌍 및 인증서 취소록 등을 저장 검색하는 장소로 디렉토리를 가지고 있으며 이는 X.500 디렉토리 서비스를 제공하고 있다. 마지막으로 사용자 또는 시스템 자체를 의미하는 인증을 요구하는 고객으로 구성되어 있다.

3.4 암호화정책의 법·제도적인 측면

개방된 네트워크 환경에 적합하도록 인증기관은 소비자에게 안전성과 신뢰성을 제공하여 믿을 수 있도록 해야 하고 전자상거래를 원활하게 이용할 수 있도록 제도적인 규제를 마련해야한다. 그러므로 인증기관이 인증해준 정보가 사용자에 의해서 신뢰받을 수 있도록 운용정책을 수립해야 한다. 인증기관에 대한 신뢰 방법은 2가지로 확립

할 수 있다. 첫째, 정부가 인증기관을 허가하거나 스스로 인증기관으로서의 역할을 수행하는 것이다. 둘째, 믿을 수 있는 민간기관이 인증기관의 역할을 하는 것이다. 인증기관의 역할이나 영역의 확장으로 인증기관 역시 인증을 요구할 경우가 있는데 이것은 인증기관들의 조직이나 국제적인 인증메카니즘에서 특히 요구되는 상호 인증시스템 측면에서 논의할 필요가 있다. 현재 OECD는 국제간 상호인증의 필요성은 인정하나 뚜렷한 논의 주제나 문서화된 기본원칙이 아직 작성되지 않은 상태이다.

따라서, 인증기관의 신뢰성은 법적인 측면과 기술, 상업적인 측면을 모두 고려한 국제적인 검증된 기준으로 평가하여야 한다고 여겨지고 있다. 그리고 인증기관은 이러한 기준에 의거하여 능력있는 전문가 집단에 의해 공인되어야 한다고 판단되고 있다. 이러한 관점에서 전자상거래 활성화와 민간 분야에서의 전자서명 기술의 사용을 촉진하기 위해 OECD의 각 회원국 정부는 다음과 같은 기본원칙 하에 전자상거래 활성화를 위한 환경구축에 전념하고 있다.

- 정부가 민간서비스의 정책과 관련된 전자환경에서의 요구되는 기술과 응용프로그램 개발촉진
- 문서 기반의 정책을 개정하여 전자문서의 법적인 효율성을 보장하는 법·제도의 입법화
- 법·제도의 방향은 전자서명기술에서 특정 기술이나 미디어의 편애 방지와 UNCITRAL의 전자상거래 모델법과의 상호 호환성을 보장
- 국내 인증 발행 장소와 무관하게 외국의 인증기관이 발행한 인증서에 사용된 전자서명의 법적 효율성의 확보를 위한 UNCITRAL과의 지속적인 협조
- 국가간 혹은 지역간의 상호인증제도의 구축을 위한 UNCITRAL과의 지속적인 협조
- OECD가 개발한 전자상거래의 기반구조안에서 인증기관에 대한 승인 및 지속적인 감사를 위한 국제적인 검증된 기준개발촉진.

이와 같은 기준에 의거하여 인증기관에 대한 검증 및 승인을 국제적으로 인정할 수 있는 호환성 있는 절차를 구축할 수 있다.

3.5 EC 활성화를 위한 기본 정책 이슈

전자상거래 당사자들은 인증기관에 의해 인증된 정보가 정보의 변형이나 인증기관의 실수나 고장 등으로 인한 책임분담에 관한 계약서나 법·제도에 대해 세부적인 논의를 요구해야 하고 인증 메카니즘과 인증기관 관련 정책 수립과정에서 프라이버시나 개인정보보호에 관한 논의와 보호 메카니즘에 관해 많은 관심을 기울여야 한다. 이러한 차원에서 앞서 언급한 문제점의 해결방법으로 가장 신뢰받고 있는 암호기술 및 정책에 대한 토의가 OECD 회원국 사이에 활발하게 논의되고 있다. 암호기술 및 정책에 있어서 가장 밀접하게 관련되어 있는 인증 키 복구 정책과 관련하여 '97년 10월에 개최된 GII상에서의 보안, 프라이버시 및 지적재산권에 관한 전문가 회의에서 OECD 대부분 회원국들의 의견은 다음과 같다.

■ 암호기술은 인증기능의 구현과 밀접한 관계에 있음을 인정
- 공개키 암호 기술을 기반으로 한 전자서명을 정보의 신뢰성 확보 방안으로 인식
- 비밀성을 위한 암호키와 데이터 무결성 위한 암호키과 구분이 어려움을 인식
- 키생성, 키분배 등과 같은 키관리 서비스는 공개키를 인증하여 주는 인증기관의 범주에 속하지만 인증서와 관련된 키관리, 키복구, 암호정책에 관한 정책 수립이 어려움을 인식

■ 각국의 정부가 고려하고 있는 키복구 및 키위탁시스템의 필요성을 인정
- 데이터를 암호화한 개인 키를 읽거나 파기된 경우 위탁된 키를 사용하여 데이터 복구 가능
- 법집행기관으로 하여금 특정한 이유로 인하여 개인키에 대한 접근성 허용 여부
- 전자서명 개인키를 소유자 외에 접근할 수 있다는 것은 개인의 정보보호에 위배됨

IV. 국내 암호화 동향

4.1 암호정책 관련 국가기관

정부차원에서 전자상거래기본법, 전자서명법 등을 입법 예고하고 민간 전자상거래 활성화를 위해 필수적으로 수반되는 규제 분야가 바로 암호화 정책의 정립이다. 우리나라는 정보보호 관련 제반사항을 안기부에서 통제하고 있는데, 이것은 공공분야에 대해 폭 넓은 규정을 적용함으로써 정보보호산업 육성에 걸림돌로 작용하고 있다. 특히, 금융망에 대한 암호규제사 문제시 되고 있다. 따라서 안기부는 보안지침을 현실에 맞게 개선해야 하고 보안규제 대상 기관 및 정보를 국방, 외교, 통일 등 핵심 기밀 분야로 축소 조정하고 암호알고리즘의 규제도 이 분야로 한정시켜야 할 것이다. 또한, 국가 안보 분야와 기타 분야로 이원화하여 안보와 직결된 부분만을 안기부가 직접 관할해야 전사상거래를 부흥시킬 수 있을 것이다.

민간분야를 기술적·제도적으로 지원하기 위해서 1996년 3월에 새롭게 발족한 한국정보보호센터는 체계적이고 안정적으로 보안 관련 활동을 수행하고 있는데, 이곳에서는 외국의 정보 보호센터에 관한 정보 수집, 정보 보호를 위한 정책 및 제도의 조사 및 연구, 정보화 역기능 분석 및 대책 연구, 보안 관련 사고의 조사 및 대책 연구, 정보 보호에 관련된 표준이나 기준의 연구, 정보보호 시스템의 시험 및 평가, 정보 보호를 위한 홍보 활동, 정보 보호에 관한 자문 역할 등을 수행하고 있다.

1998년 2월 산업자원부는 각 16개 관련 부처별 대책을 종합하여 "인터넷의 전자상거래 종합대책"이라는 보고서를 통해 정부차원의 공식적인 입장을 대내외적으로 최초로 밝힘으로서 전자상거래 활성화에 대한 정부의 의지를 확고히 한 바 있다. 산업자원부는 1996년 인터넷에 쇼핑몰((인터파크, 롯데인터넷 백화점)이 개설된 후부터를 국내에서 본격적인 전자상거래가 시작된 시기로 보고 산업자원부가 주관부처가 되어 "산업정보화 사업"의 일환으로 전자상거래 정책을 총괄하고 있다. 개별 사안별로는 안기부는 국가 기밀에 관련된 정책을 추진하고, 재경부는 금융권에서의 전자자금 이체법을 추진하고 있으며, 정통부와 문화관관부에서는 정보보호산업을 전략적으로 육성하기 위한 정보보호산업발전대책 등을 준비하고 있다[8].

4.2 국내 업계 동향

최근 IBM회장은 "한국의 전자상거래 규모가 98년 2억 4천만 달러에서 오는 2001년에는 50억 달러까지 늘어날 것"이라고 예상한 바 있다. 인터넷을 통한 전자상거래는 우리 삶의 방식을 개혁할 또 하나의 정보 산업혁명이 될 것이다. 현재 국내 기업들은 국가 및 기업의 경쟁력을 강화하기 위한 하나의 부분으로서 전자상거래에 막대한 투자를 하고 있다[9]. LG 경제연구서에 의하면 우리나라 전자상거래의 시장규모를 96년에 14억원 정도로 보고 있으며 올해는 94억원 정도가 될 것으로 예상하고 있다. 앞으로 2002년에는 2천1백억원대의 시장을 형성할 것으로 내다보고 있다.

이와 같은 거대한 범세계적인 시장을 위해서는 전자상거래에 필요한 여러 가지 기반 기술들이 확보되어야 하는데 이 중에서 암호기술은 중요한 위치를 차지하고 있다. 전자상거래 보안 기술에 대한 가시적인 국내 움직임은 1995년 후반기부터 본격적으로 시작되었다고 볼 수 있다.

1996년에 금융계 최초로 동남은행에서 하나로 전자지갑카드를 시험 운용하였으며, 1996년 11월에는 관련 전문 업체인 동성 정보통신이 웹서버와 IC카드 인터페이스 기술을 보유하고 있다고 발표된 바 있다. 1996년 10월에는 데이콤 연구소에서 SoftCach 전자지불시스템을 개발하였다. SoftCach 전자지불시스템은 지불 브로커형 전자지불시스템으로서 대금결재방식으로 신용카드를 통한 결재와 은행계좌이체를 통한 대금결재가 모두 가능하도록 인터넷 WWW기반의 전자지불을 구현한 시스템이다.

또한, EC의 응용기술로서 전자문서교환(EDI) 활성화를 위한 기술적 난제 중 하나인 인터넷상의 보안 시스템을 국내 기술로 개발한 한국통신은 순수 자체 기술로 EDI 보안 시스템을 업계 최초로 개발해 미국방부 인증을 획득하여 앞으로 국가망용으로 사용할 것이라고 보도된 바 있다. 커머스넷 코리아에서는 전자화폐 기반의 전자상거래서비스가 국내 최초로 개발하여 시범서비스를 하고 있다.

KAIST는 세계 최초로 IC카드를 이용한 SET프로토콜 기반 전자상거래 쇼핑몰 시스템을 국내 연구진을 통해 세계에서 처음으로 개발했하였. 개발된 쇼핑몰은 독립적인 쇼핑몰들간 상품 비교는 물론이고 원스톱쇼핑(One-Stop Shopping)이 가능할 뿐 아니라 개인용 전자지갑으로 대금지불이 가능한 malltomall 구조로 설계되었으며, 비자와 마스터카드가 공동으로 제안한 SET 프로토콜기반의 지불시스템을 구현한 「메타랜드 쇼핑몰 시스템」의 개발을 의미한다.

V. 결론

우리나랑가 OECD에 정식으로 가입함으로써, 회원국 상호간의 암호정책 이행에 필요한 제반 준비가 시급히 요청되고 있다. 따라서 이에 대한 법·제도적인 측면에서의 대응방안으로서 암호사용의 규제완화, 정보보안산업의 육성, 비밀정보 액세스를 위한 법제화, 암호관리체계의 분리, 관련 기관의 유기적인협력 체제 구축 등의 방안을 조속히 마련하여야 할 것이다.

전자상거래가 과연 활성화될 것인가에 대한 부정적 견해도 있지만 전자상거래가 세상을 혁신할 것이라는 확신은 누구도 부인할 수 없을 것이다. 따라서 국제 시장에서 살아 남기 위해서는 경제흐름을 어떻게 읽고 준비하느냐에 달려 있다고 볼 수 있다. 다가오는 21세기의 범 세계적인 전자상거래 구조에 대해 민첩하게 대응하기 위해서는 다음과 같은 대비책을 준비해야 할 것이다.

- 보안 관련 업체 전문성 부여
- 민·관 공동 프로젝트 보안 시스템 개발 유도
- 보안 관련의 정부 부처별 정책 수립 및 국가적 차원의 표준화 사업주도
- 하드웨어 토큰 기술의 확보
- 국가 차원의 지속적인 보안 제품의 개발 지원
- 보안제품 도입시 개인정보와 공공이익 간의 긴장관계를 고려한 합리적 추진 정책

이와 같은 제한된 조치를 기반으로 키에스크로우 정책의 도입도 고려할 만하다. 이를 통해 사용자 부주의로 인한 암호키의 망실로부터 개인정보 보호를 위한 키 복구 시스템의 도입도 자연스럽게 이뤄질 수 있을 것이다.

그러나, 암호화기술은 단순히 암호화 알고리즘의 문제에서 끝나지 않고, 암호화 알고리즘의 컴퓨터 프로그램으로의 표현 문제, 암호화 프로토콜 문제 등 실제암호화 시스템을 개발하는데 있어서 풀어야할 많은 문제들이 있다. 특히 최근 들어 한국형 암호화 프로토콜인 K-SET이 문제시 되고 잇는데 암호프로토콜을 어떻게 정의하느냐에 따라 개발 방향에 많은 영향을 줄 것으로 예상된다.

참고 문헌

[1] OECD, "Guidelines for Cryptography Policy", http://www.oecd.org/dsti.iicp/crypto.html_e.html

[2] 박태완, "보안제품에 대한 동향", 한국정보과학회지 제14권 3호, pp 33-37, 1996.

[3] ECOM, "Electronic Commerce in japan",http://www.ecom.or.jp/eng/ec_japan/ohp3.htm

[4] 이임영, 박춘식,"암호기법", 한국정보과학회지 제 15권 제4호, pp 14-20, 1994.

[5] Taher Elgamal, Credit Card Payment Application over The Internet, http://home.netscape.com/newsref/std/credit.html, July 14, 1995

[6] VISA, Master Card, SET(Secure Ellectronic Transaction) http://www.visa.com, http://www.mc.com/.

[7] 권도균, "WWW보안과 전자화폐",http://ku-mkang.tins.co.kr/doc/ec4.html

[8] 산업자원부, "인터넷 전자상거래 종합대책", 1998.

[9] 임신영, 권도균, "전자상거래", 정보과학회지 제 15권 제 4호, pp 45-51, 1997.