KAIS 97 추계학술대회

SET 표준과 우리 나라 인증기관의 구성 방안

주재훈
동국대학교 상경대학 경상학부

요약

본 연구에서는 인증기관의 필요성과 기능, 인증기관이 갖추어야 할 요건, 미국을 비롯한 인터넷 상거래가 활성화되어 가는 몇몇 나라에서의 인증기관에 대한 사례, 신용카드를 지불수단으로 사용하여 안전한 전자상거래를 지원하는 SET(Secure Electronic Transaction) 표준에서의 인증기관의 구성 예에 대하여 분석해 보기로 한다. 또한 본 연구에서는 이들 사례를 토대로 신뢰할 수 있는 웹공간을 구성하기 우리 나라에서의 인증기관 구성 방안에 대하여 고찰하고자 한다.

1. 서론

오늘날 인터넷은 광고 및 마케팅 매체이자 분배채널이 되기도 한다. 이에 더하여 인터넷은 전자시장(electronic market)이기도 하다(Bakos, 1991; Klein, 1996; Malone, 1987, Zabih, 1996; Hoffman, D. L. and T. P. Novak, 1996, AberdeenGroup, 1997). 인터넷이라는 전자시장에서 판매자와 소비자는 전자적으로 일면식도 없이 상거래를 하게 된다. 많은 기업에서는 인트라넷(intranet)을 구축하여 기업 내 부문간의 의사소통 및 협동업무를 지원하고, 엑스트라넷(extranet)을 통해 고객 및 공급자와 의사소통 및 협동업무를 지원하기도 한다.

인터넷이라는 전자시장에서 안전하고 건전한 상거래가 이루지기 위해서는 메시지 기밀성, 인증성, 메시지 무결성, 거래사실 부인방지 등의 기본적인 보안 서비스가 제공되어야 한다. 인터넷을 신뢰할 수 있는 전자시장으로 발전시키기 위해 공개키 암호방식이 적용되고 있다(RSA Data Security, 1995). 메시지 암호화를 통해 기밀성이 유지되고, 전자서명(digital signature)을 통해 인증성·무결성·부인방지 서비스가 가능하다. 그러나 전자서명만으로 인터넷에서 거래 상대를 완전히 신뢰하기가 어렵다. 왜냐하면 전자서명으로는 공개키를 신뢰할 수 있다는 가정하에서 거래 상대를 인증할 수 있기 때문이다. 따라서 신뢰할 수 있는 인터넷 웹공간을 구성하기 위해서는 신뢰할 수 있는 제3자로서의 인증기관(Certification Authority: CA)이 필요하다(Froomkin, 1996; Burr, 1996; Burr, etc., 1997)).

본 연구에서는 인증기관의 필요성과 기능, 인증기관이 갖추어야 할 요건, 미국을 비롯한 인터넷 상거래가 활성화되어 가는 몇몇 나라에서의 인증기관에 대한 사례, 신용카드를 지불수단으로 사용하여 안전한 전자상거래를 지원하는 SET(Secure Electronic Transaction) 표준에서의 인증기관의 구성 예에 대하여 분석해 보기로 한다. 또한 본 연구에서는 이들 사례를 토대로 신뢰할 수 있는 웹공간을 구성하기 우리 나라에서의 인증기관 구성 방안에 대하여 고찰하고자 한다.

2. 인증기관과 전자인증서

1) 공개키의 인증 문제

대면관계도 없이 불특정 다수를 대상으로 하는 가상공간에서 거래에 따른 부정 활동을 방지하기 위해서 전자서명이 이용되고 있다. 수기서명에 비해 전자서명을 위조하기란 어렵

지만, 전자서명만으로 상대를 완전히 믿을 수는 없다. 전자서명은 "갑"이라는 이름을 가진 사람이 전자문서를 작성했다는 사실을 확인할 수 있도록 해준다. 그러나 전자서명은 "갑"이라는 사람이 실제로 존재하는 사람인지, 갑이 실제로 존재하긴 하지만 "병"이 "갑"인 것처럼 가장하여 등록을 하고 "갑"을 사칭하고 있는지에 대한 사실을 입증해 주지는 못한다. 특히, 전자상거래에서는 불특정다수가 서로 일면식도 없는 상황에서 컴퓨터 네트워크를 통해 거래를 하게 된다. 따라서 어떤 사람이 실제로 존재하는 사람이 아니거나 타인의 명의를 처음부터 도용하는 사람일 가능성은 현실의 대면관계에 기반을 둔 거래에서보다 훨씬 높고, 많은 문제가 발생할 수 있다.

전자서명을 이용하는 시스템에서는 공개키가 다른 사람을 사칭하지 않은 실제 전자서명을 한 당사자의 것이라는 전제하에서 상대를 인증해 줄 뿐이다. 공개키 암호방식을 이용한 전자서명에서는 송신자가 자신의 비밀키로 메시지에 서명하고 수신자에게 송신자의 공개키를 분배한다. 수신자는 자신의 비밀키로 메시지를 해독하고 송신자의 공개키로 전자서명을 확인한다. 수신자는 비밀키를 알고 있는 자신만이 메시지를 해독할 수 있다고 믿고 있다. 그러나 수신자는 송신자의 공개키를 믿을 수 있는지, 수신자 자신의 정확한 공개키가 배포되었는지를 확인할 수 없다. 만약 "병"이 "갑"을 사칭하여 어떤 쇼핑몰 또는 결제시스템을 이용하는 경우, 즉 "병"이 "갑"의 이름으로 등록한 경우라면, "병"은 "갑"의 이름, "병"의 전자우편 주소, "병"의 공개키로 거래하므로 "병"과 거래하는 당사자는 상대가 "갑"인지 "병"인지를 알 수 없게 된다.

공개키 암호 방식을 사용한 전자서명에서는 위의 경우와 같이 등록시 공개키를 사칭하는 문제 외에도 공개키를 분배할 때 다음과 같은 문제점이 발생할 수 있다:

① "갑"이 "을"에게 공개키와 함께 전자서명을 한 전자 문서를 보내는 경우: "병"이 전자문서를 가로채어 문서를 변조하여 "병"의 미빌키로 서명을 하고 "병"의 공개키를 "갑"의 이름으로 사칭하여 "을"에게 보낸다. "을"은 "병"의 공개키가 "갑"의 것으로 인식한다.

② 전화번호부와 같은 온라인 디렉토리에 공개키 목록을 저장해 두고 누구나 디렉토리에서 공개키를 확인할 수 있도록 하는 경우에는 ①의 문제점을 해결할 수 있다. 그러나 "을"이 온라인 디렉토리에서 "갑"의 공개키를 가져올 때, "병"이 이를 가로채어 "갑"의 공개키 대신 "병"의 공개키를 보낸 경우, "을"은 "병"의 공개키를 "갑"의 공개키로 오인하게 된다.

공개키 사칭에 따른 문제점을 해결하고, 신뢰할 수 있는 웹공동체를 구성하기 위한 두 가지 접근법이 제시되고 있다.

그 첫째는 구매자와 판매자 외의 신뢰할 수 있는 인증기관에서 발급하는 전자인증서(electronic certificate)를 이용하는 방법이다. 인증기관에서 구매자와 판매자 등의 사용자 신원을 파악하여 전자신분증에 해당하는 전자인증서를 발행하고 관리한다. 인증기관에서 발급하는 전자인증서에는 사용자 이름을 비롯하여 사용자의 공개키와 신원에 대한 사항이 들어 있다. 인증기관에서는 전자인증서를 제시하는 사람이 실제 공개키의 소유자라는 것을 보증해 준다. 따라서 구매자와 판매자가 인증기관에서 발급한 전자인증서를 믿을 수 있다면, 거래시 제시하는 전자인증서를 통해 상호 신원을 파악할 수 있다.

전자상거래를 위한 전자인증 서비스를 제공하는 대표적인 조직으로는 베리사인(VeriSign)사를 들 수 있다(VeriSign, 1997). 이 회사는 1995년 RSA 데이터시큐리티사의 자회사로 설립되었다.

두 번째 접근방법은 별개의 인증기관 없이 웹사용자간에 공개키를 인증할 수 있도록 하는 것이다. 여기서는 웹사용자들이 알고 있고 신뢰할 수 있는 사람들의 공개키를 인증해주므로써 어떤 공개키가 특정인을 사칭하는 사람이 아닌 정당한 사람의 공개키라고 다른 사람들이 믿을 수 있게 한다. 예를 들어 "갑"이 알지 못하는 "병"을 신뢰하게 되는 경우를 살펴보자. "을"은 "병"을 알고 그를 신뢰하므로 "병"의 공개키를 인증하는 전자서명을 한다. "갑"은 "병"을 알지 못하지만 "병"의 공개키에 "을"의 전자서명이 첨부되어 있으므로 "병"의 공개키를 믿을 수 있다. 이와 같이 다양한 사용자들간에 인증사슬이 구성될 수 있다. 예를

들어, "갑"은 "을"을 알지 못하지만 "갑"의 친구인 "병"이 "정"의 공개키에 서명을 했고, "정"이 "을"의 공개키에 서명을 했다. 이 경우에는 "갑"의 친구인 "병"이 "을"의 공개키를 인증하는 경우보다 못하지만 "갑"은 "을"의 공개키를 어느 정도 믿을 수 있다. 인증 체인의 길이가 길수록 공개키에 대한 신뢰도는 떨어지게 된다. 그러나 인증경로가 어느 정도 긴 경우에도 서로 다른 몇 개의 공개키 목록으로부터 여러 사람들의 서명을 확인하게 되면 신뢰도는 증가하게 된다. 이러한 형태로 웹사용자들이 상호 공개키를 인증하여 제공하므로써 신뢰할 수 있는 웹공동체를 구성하게 된다. 이와 같이 웹공동체를 구성하여 공개키를 인증하는 대표적인 예로는 PGP(Pretty Good Privacy)가 있다(따로, 1996).

PGP는 비밀키 암호방식과 공개키 암호방식 둘다를 이용한 복합 암호프로그램으로 전자우편의 보안도구로 사용되고 있다. PGP에서는 독립된 인증기관도 없이 사용자들이 상호 공개키를 인증해 주는 방법을 이용하고 있다. PGP에서 공개키를 인증하는 방식으로는 공개키마다 고유하게 부여되는 일종의 전자지문인 핑거프린트(fingerprint)를 이용하는 방법과 키서명을 이용하는 방법이 있다.

"갑"이 "을"을 알고 있는 경우, "갑"이 수신한 "을"의 공개키가 실제로 "을"의 것인지를 확인하기 위해 "갑"은 "을"에게 전화로 확인할 수 있다. PGP에서 키 식별자(key identifier)로 상대를 확인한다고 하자. "을"을 사칭하는 "병"의 키식별자와 "을"의 키식별자가 같은 경우, "갑"은 이를 구별할 수 없다. "갑"은 PGP에서 키식별자를 입력하여 산출한 핑거프린트와 전화로 확인한 핑거프린트가 일치하는 경우, "을"의 공개키를 믿을 수 있다.

PGP에서는 불특정 다수간에 공개키를 인증하는 방법으로 키서명방식을 사용하고 있다. "갑"과 "을"이 친구이거나 서로 잘 아는 경우에는 상호 공개키에 서명을 하여 이를 키서버의 데이터베이스에 등록하거나 다른 사람에게 전송하거나 자신의 파일에 저장해 둘 수 있다. "을"을 잘 알지 못하는 "병"은 공개키 서버를 검색하여 "을"의 공개키를 검색하여 "병"이 잘 알고 신뢰할 수 있는 "갑"이 "을"의 공개키에 서명을 했으므로 "을"의 공개키를 인증할 수 있다.

어떤 키가 계속 쓰이다 보면 사용자들이 그 키에 자신의 서명을 붙이게 된다. 서명을 붙이는 사용자가 자신의 이름을 걸고 그 키의 진위를 증명해 줄 수 있어야 한다. 왜냐하면 "갑"이 "을"의 공개키에 서명을 붙여 놓게 되면 "갑"을 믿는 사람들이 "을"의 공개키를 믿고 사용할 수 있기 때문이다. 따라서 PGP에서는 사용자 개개인이 얼마나 정확하게 공개키를 확인하여 서명을 하느냐에 따라 공개키에 대한 신뢰도가 좌우되므로 사용자 개개인의 역할이 대단히 중요하다. 또한 PGP에서는 어떤 공개키에 서명한 사람의 신뢰도에 따라 그 사람이 서명한 공개키를 어느 정도 믿을 것인가를 사용자 스스로의 판단에 맡기고 있다. 왜냐하면 공개키 서버에서는 CA와는 달리 그 데이터베이스에 저장된 키가 정확한 것인지를 조사하지 않기 때문이다. 또한 PGP에서의 공개키 인증은 단지 사용자 이름과 그의 공개키와의 관계만을 확인할 수 있도록 해주는 신분확인 증명서 역할만을 한다.

2) 인증기관의 역할

가상공간에서 신뢰할 수 있는 제3자로서의 인증기관은 다음의 주요 기능을 수행한다:

- 등록업무: 온라인 또는 실제 확인 과정을 거쳐 인증서 신청자의 신원에 관한 정보를 등록하는 업무
- 인증서 발행·폐기·갱신·대체 업무: 등록 정보를 기초로 인증서를 발행하고, 인증서 사용을 중지하고, 사용되지 않고 있던 인증서를 새로이 사용할 수 있게 하고, 유효기간이 지나지 않은 인증서를 폐기하고, 새로운 인증서를 발행하는 업무 등.
- 인증서폐기목록 관리: 인증서폐기목록(Certificate Revocation List: CRL)이란 유효기간이 지나지 않았지만 폐기된 인증서 목록이다. 인증서 소유자가 발행기관의 등록을 취소하거나 비밀키가 손상된 경우에는 인증서를 폐기해야 한다.
- 인증서 분배 및 디렉토리 서비스: 인증서와 CRL과 같은 정보를 저장하고 있는 데이터베이스 서비스. 인증서 사용자들은 CA가 관

리하는 디렉토리(또는 리파지토리)에 접근하여 폐기된 인증서 및 등록된 인증서를 검색해 볼 수 있다.

인증기관과는 달리 등록업무를 수행하는 등록기관(Registration Authority: RA)이 있다. 등록기관에서는 전자서명 및 인증서 발행 기술이 부족하여 등록신청을 받아 등록정보 데이타베이스만 관리하고 인증기관에 인증서 발행업무를 의뢰한다. 인증기관에서는 등록기관에서 제공받은 인증서의 자료를 사용하여 인증기관의 비밀키로 전자서명을 한 인증서를 발행한다.

위의 기능을 수행하는 인증기관에서는 다음과 같은 능력을 갖출 필요가 있다:

- 기술: 암호 기술과 전자서명 등의 보안 기술, 등록정보를 관리할 수 있는 데이터베이스 기술 등
- 설비: 자동 백업 및 회복 기능이 있는 안전한 설비, 고객지원 서비스 능력 등을 갖추고 전세계 사용자들에게 인증서비스를 제공할 수 있는 기반체계, 즉 공개키인프라(Public Key Infrastructure: PKI)를 갖추어야 한다.
- 실무: 인터넷에서 공신력있는 제3자로서 역할을 수행할 수 있는 능력, 법적 구속력이 있는 실무준칙서(Certification Practice Statement: CPS)의 운영 능력. 인증실무준칙서란 인증기관에서 인증서를 발행하는데 이용하는 실무지침서로서, 여기에는 CA의 운영 규칙과 정책, 인증서를 발행하는데 요구되는 조건과 제약, 인증서 발행정책 등의 세부 사항이 명시되어 있다.

3) 전자인증서의 종류

전자인증서(electronic certificate)란 전자서명을 한 본인이 주장하는 자신의 속성에 대한 사실여부를 거래 상대가 확인할 수 있도록 제3자가 전자적으로 발급하는 증명서이다. 달리 표현하자면, 이는 공개키의 소유자라고 주장하는 사람이 실제 그 키의 소유자인지를 제3자가 확인해 주는 인증서이다.

인증서 양식은 CCITT의 ITU 권고 X·509가 많이 사용되고 있다. 이 양식에는 인증서 소유자 ID나 공개키와 함께 인증기관의 전자서명이 들어 있다. 전자서명은 인증기관이 발송한 공개키로 대표되는 증명서의 내용이 수정되지 않았다는 것을 증명하기 위한 것이다.

[표 1] 인증기관의 전자인증서에 포함된 정보 (X·509)

• 버전번호 • 일련번호 • 인증서 유효기간 • 사용자 ID • 사용자 이름 • 사용자 공개키와 관련정보(알고리듬, 파라미터) • 전자서명 관련정보(알고리듬, 파라미터) • 인증기관명
• 인증기관의 전자서명

인증기관에서 발행하는 인증서에는 소유자의 공개키와 이름을 연결하여 신원을 확인해 주는 것에서 이름과 공개키 뿐만 아니라 주소, 나이, 특정 제품의 구매 권한을 입증해 주고 전자 타임스탬핑 서비스를 제공하는 것에 이르기까지 다양한 종류가 있다(Froomkin, 1996). 또한 인증기관에서는 등록시 등록자 본인에 대한 사항을 얼마나 엄밀하게 확인하는가에 따라 서로 다른 종류의 인증서를 발행한다. 예를 들면, 베리사인사에서는 전자인증서를 발급하기에 앞서 신청자의 신원을 얼마나 정확하고 상세하게 파악하는가에 따라 서로 다른 4종류의 전자인증서를 발행하고 있다.

단순 인증서(identifying certificate)에서는 등록자의 이름과 공개키를 연결하여 공개키를 통해 본인을 확인할 수 있도록 해준다. "갑"이 인증기관으로부터 단순 인증서를 발행받았다고 하자. "갑"은 기밀을 요하는 메시지를 "을"에게 보낸다. "을"은 "갑"의 인증서를 발행한 인증기관을 신뢰하고 있다. 전자인증서에는 "갑"이라는 사람의 공개키가 진실로 "갑"의 것이라는 것을 입증하는 인증기관의 전자서명이

들어 있다. "갑'이라고 주장하는 사람으로부터 전자서명이 들어 있는 메시지를 받은 "을"은 "갑"이 제시하는 전자인증서를 확인하고 메시지의 전자서명이 "갑"을 사칭하는 타인이 아닌 "갑" 본인이 한 것이라고 믿을 수 있다.

단순히 공개키만을 입증하는 인증서로는 거래자가 다음과 같은 상황에서 거래 상대를 신뢰할 수 없다. 성인인 소비자만이 구입할 수 있는 제품을 어떤 구매자가 구입하고자 하는 경우 판매자는 단지 공개키의 진실성만 믿고 그 구매자를 신뢰할 수 없고, 그가 성인이라는 것을 입증하는 전자인증서를 필요로 하게 된다. 미연방정부에서는 사전허가 없이 미국에서 고급의 암호 알고리듬을 수출할 수 없도록 규정하고 있다. 미국 시민이나 미국에 거주하는 외국인은 인증서를 통해 암호 알고리듬을 입수할 수 있는 권한이 있다는 것을 입증할 수 있어야 한다.

승인 인증서(authorizing certificate)에서는 등록자의 이름과 공개키 뿐만아니라 등록자의 주소, 등록자의 나이, 등록자가 어떤 단체의 회원인가에 대한 내용도 입증해 준다. 인터넷 비즈니스 교과목을 수강하는 학생들을 대상으로 교수가 퀴즈 문제를 교환한다고 하자. 학생들은 이 교과목을 수강한다는 것을 입증할 수 있어야 문제를 받아볼 수 있다. 수강학생들은 승인 인증서를 제시함으로써 본인을 인증할 수 있다. 그 외도 위에서 설명한 바와 같이, 성인만을 대상으로 상품을 판매하는 경우나 암호알고리듬의 배포 등에서 승인 인증서가 이용될 수 있다.

단순 인증서나 승인 인증서 외에도 특정 거래 사실을 입증하는 거래 인증서(transactional certificate)와 특정 시점에 전자문서를 작성했다는 것을 입증해 주는 위조 불가능한 전자 타임스탬프(digital time stamp)가 첨부된 인증서 등이 있다.

4) 신뢰사슬

"갑"은 "을"이 보낸 전자서명이 첨부된 비밀문서와 함께 "정"이라는 인증기관에서 "을"에게 발행한 전자인증서를 받았다고 하자. "갑"은 "을"의 전자인증서에 있는 공개키로 "을"의 전자서명을 확인할 수 있다. 그러나 "갑"이 "정"이라는 인증기관을 믿을 수 없거나 "정"의 공개키가 정당한 것인지를 확인할 필요가 있는 경우에는 인증기관의 공개키를 인증해 주는 인증기관이 요구된다.

B가 A를 인증해 주고, C가 B를 인증해 주고, 다시 D가 C를 인증해 주고, 최종적으로 R이 D를 인증해 준다고 하자. R의 공개키가 모두에게 알려져 있고 믿을 수 있는 것이라면, A의 전자인증서를 받은 공개키 암호방식의 어떤 사용자는 인증기관 B를 통해 A의 공개키를 인증하고, C를 통해 B를 인증하는 형식으로 하여 최종적으로 루트 인증기관인 R을 통해 D를 인증함으로써 A를 인증하게 된다. 이러한 신뢰관계의 사슬구조를 신뢰사슬(trust chain)이라 한다.

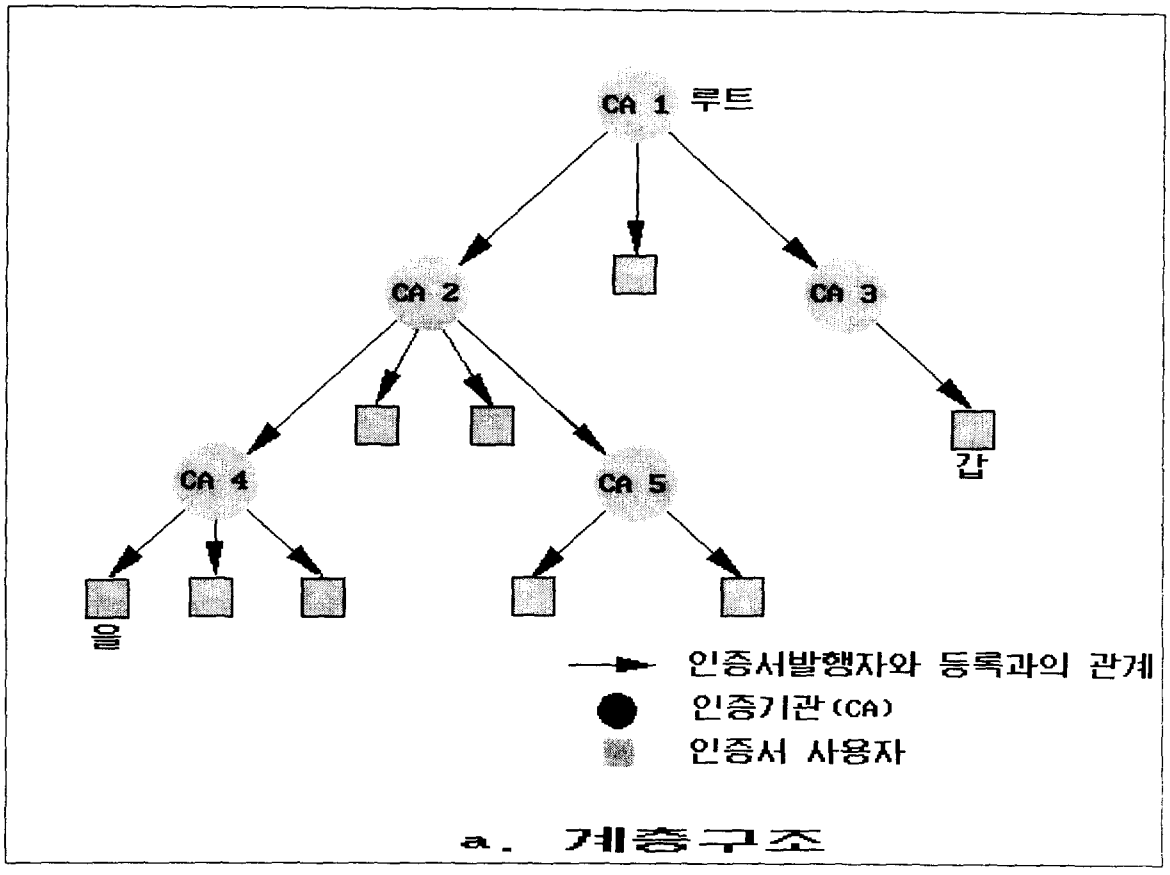
이러한 신뢰사슬을 구성하는 방식 또는 토포로지(topology)에는 계층구조와 네트워크 구조 방식이 있다.

[그림 1]에서와 같이 계층구조를 갖는 신뢰사슬의 최상위 계층에는 하위 CA에 인증서를 발행하는 루트(root) CA가 있고, 하위 CA는 계층구조상 그의 하위에 있는 CA 또는 사용자들에게 인증서를 발행한다.

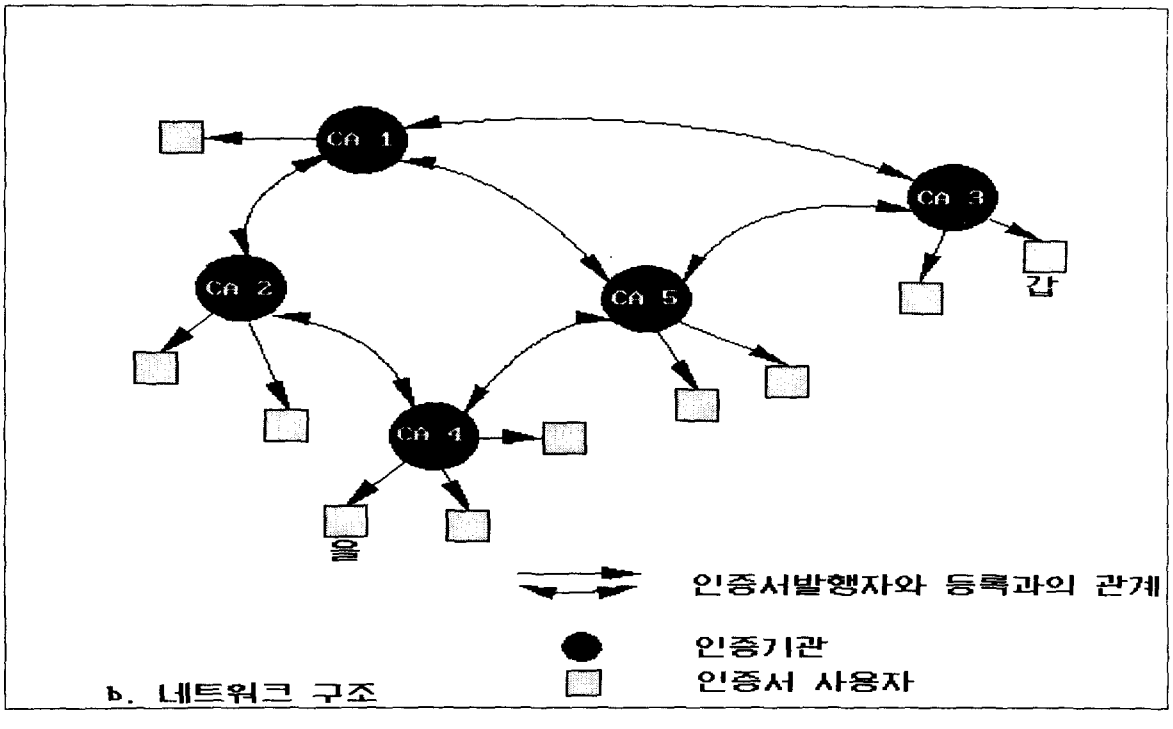
루트 CA의 공개키는 모든 사용자들에게 공개된다. 어떤 사용자의 인증서는 루트 CA에 이르기까지 신뢰사슬의 인증경로를 거슬려 올라가는 검색과정을 통해 검증된다. [그림 1]에서 "을"의 인증서를 받은 "갑"이 "을"의 인증서를 검증하는 과정을 살펴보자. 먼저 "갑"은 "을"의 인증서를 검증하기 위해 "을"의 인증서를 발행한 CA4의 인증서를 검증해야 한다. 그런 다음, CA4의 인증서를 검증하기 위해서는 CA2의 인증서를 검증해야 한다. 최종적으로 이미 알고 있는 루트 CA(CA1)의 인증서를 통해 CA2의 인증서를 검증한다.

인터넷에서의 신용카드를 이용한 안전한 거래를 지원하는 표준인 SET에서는 계층구조의 신뢰사슬을 이용하고 있다.

신뢰사슬은 독립된 인증기관들이 상호 서로를 인증해 주는 신뢰관계의 네트워크 구조일 수도 있다. 인증서 사용자는 이를 발행한 인증기관의 공개키를 알고 있고, 그 인증기관을 신뢰하고 있다. 인증서 사용자는 다른 사용자 인증서를 발행한 인증기관에서 그가 신뢰하는 인증기관에 이르는 인증경로를 검색하여



[그림 1] 계층구조



[그림 2] 네트워크 구조

다른 사용자 인증서를 검증한다. 예를 들어, [그림 2]에서 "갑"이 "을"의 인증서를 검증한다고 하자. "갑"은 그의 인증서를 발행한 CA3의 공개키를 알고 있고, "을"은 그의 인증서를 발행한 CA4의 공개키를 알고 있다. "을"에서 "갑"에 이르는 여러 인증경로가 있지만 대개 "갑"은 최단경로를 통해 "을"의 인증서를 검증한다.

① "갑"은 "을"의 인증서에 있는 CA4의 공개키를 이용하여 CA4를 통해 "을"의 인증서를 검증한다.
② CA5를 통해 CA4를 검증한다.
③ 최종적으로 "갑"이 신뢰하고 그 공개키를 알고 있는 CA3를 통해 CA5의 인증서를 검증한다.

미연방 정부의 공개키 인프라를 구축하고 있는 NIST에서는 네트워크 구조의 신뢰사슬을 이용하고 있다(Burr, 1996).

3. 사례분석: 베리사인의 디지털 ID

베리사인(Verisign)사는 1995년 RSA 데이터시큐리티(RSA Data Security)사의 설립되었다. 1997년 6월 현재, 이 인증기관에서는 마이크로소프트사의 인터넷 익스플로러와 넷스케이프사의 네비게이터 사용자를 대상으로 750,000개 이상의 디지털 ID(Digital ID)를 발행한 것으로 보고되고 있다.

1) 디지털 ID란?

디지털 ID란 베리사인사에서 제공하는 전자인증서의 브랜드명이다. 베리사인사에서는 여러 종류의 디지털 ID를 발행하고 있다. 디지털 ID의 종류에 따라 사용자를 인증하는 수준이 다르다. 예를 들면, 지역 할인매장을 이용하기 위해서는 회원권이 필요하지만, 여권을 발급받기 위해서는 주민등록증과 같은 신원을 매우 세밀하게 파악할 수 있는 정보가 필요하다. 베리사인사에서는 클래스 1, 클래스 2, 클래스 3, 프라이비트 레이블(private label)이라는 4종류의 디지털 ID를 발행하고 있다.

베리사인사에서 발행하는 전자인증서 클래스 1은 신청자 이름과 전자우편 주소만을

[표 2] 디지털 ID의 종류와 특징

디지털 ID의 종류	유사한 신분증	사용자 정보	일반적 사용범위	예
클래스 1	회원권	· 이름 또는 별명 · 전자우편 주소 · 개인 정보	· 웹사이트 접근제어 · 안전한 전자우편	· 온라인 출판물 읽기 · 비밀 전자우편 송신
클래스 2	운전면허증	· 실명 · 전자우편 주소 · 우편주소	· 웹사이트 접근제어 · 안전한 전자우편 · 상거래	· 사무 기기의 온라인 구매
클래스 3	여권	· 실명 · 전자우편 주소 · 우편주소 · 공증인이 확인한 신원	· 접근제어 · 안전한 전자우편 · 고액거래 · 법적인 거래	· 건설 계약에의 서명
비밀신용카드 레이블	신용카드	· 개별적 요구사항에 따라 다름	· 은행과 같은 기밀을 요하는 사이트에의 접근	· 은행의 개인계좌에의 접근

증명하고, 전자우편으로 이를 확인하여 발행된다. 클래스 2는 이름과 전자우편 외에도 개인 신상에 관한 추가 정보를 증명하고, 상용 데이터베이스나 기타 확인절차를 걸치게 된다. 클래스 3은 공증인 또는 베리사인이 승인한 지역 등록기관의 확인을 거친 후 제시된 문서를 기초로 발행된다. 가장 엄격한 인증서인 글래스 4는 등록시 본인확인과정을 거쳐 등록 정보를 철저히 조사한 후 발행된다.

[표 2]에서는 디지털 ID별 특징을 요약하고 있다.

2) 디지털 ID의 이점

웹사이트의 방문자를 파악하는 방식으로 쿠키(cookies)와 비밀번호 방식이 이용되어 왔다. 그러나 디지털 ID를 사용하는 경우, 웹사이트에서 기대할 수 있는 이점은 다음과 같다.

• 사용자 편리성

웹사이트 방문자는 로그인 방식으로 디지털 ID를 사용할 수 있어 웹사이트 방문시마다 사용자 이름과 비밀번호를 입력하지 않아도 된다. 웹관리자는 디지털 ID의 정보를 기초로 방문 고객의 선호도에 맞게 정보를 입수할 수 있다.

• 보안의 개선

디지털 ID는 사용자 신원을 인증하는 수단이다. 비밀번호를 이용하는 방식과는 달리 비밀번호를 공유할 필요가 없다. 권한이 없는 타인이 디지털 ID를 가로채어 사용할 가능성은 희박하다. 베리사인사에서는 디지털 ID의 절도, 사칭, 파괴에 따른 경제적 손실을 보상하는 계획안(Netsure SM protection plan)도 실행하고 있다.

• 유지 및 고객 지원 비용의 절감

디지털 ID로 사용자 신원을 파악하는 경우, 웹서버에서는 비밀번호 데이타베이스를 유지할 필요가 없고, 사용자의 비밀번호 문의에 대한 지원서비스도 감소된다.

• 마아케팅 능력의 개선

웹사이트에 접근하는 방문객을 파악함으로써, 웹사이트 관리자는 고객의 웹사용 패턴과 프로필 정보를 입수할 수 있다. 누가 웹사이트를 처음 방문하여 다시 방문했으며, 누가 한 번 방문 후 다시 방문하지 않았는지에 관한 정보를 기초로 웹사이트 유인전략과 판매전략을 개발할 수 있다.

• 안전한 전자우편

사용자는 디지털 ID로 보안이 유지되는 전자우편을 송수신할 수 있다. 웹클라이언트 소프트웨어인 마이크로소프트사의 인터넷 익스플로러 4.0과 넷스케이프사의 커뮤니케이터 웹 클라이언트 소프트웨어의 사용자들은 정보검색 및 보안이 유지되는 전자우편용으로 디지털 ID를 사용할 수 있다.

• 기타

디지털 ID가 웹사이트 관리자에게 제공할 수 있는 기타 잠재적 이점으로는 일단계 등록 과정, 민감한 또는 가치있는 정보에의 접근제어, 웹사이트 정보내용 및 특정 방문객에 맞는 광고 등이다.

3) CA 제품

Entrust(www.etrust.com): Entrust Technologies, Inc.

- FIPS 표준과 호환
- 윈도우즈 3.1/95/NT, Macintosh, HP-UP, Solaris, SunOS clients 지원
- 특정 암호기술과 서명기술과 독립성
- 다양한 하드웨어 토컨을 지원
- API 응용개발 가능
- 서버는 AIX 윈도우즈 95/NT 코드에서 작동되지 않음

Cybertrust(GTE, Inc): www.cybertrust.com

- 다수 플랫폼 클라이언트
- X.509 versions 1 & 3
- PCMCIA 토큰 지원

- RSA, DSA, MD5, SHA-1 알고리듬을 사용
- 다수 접근 제어
- 웹과 전자우편 인터페이스
- SSL, S/MIME, SET 지원
- 서버는 Solaris만 지원

SecretAgent, BusinessSafe, & CDK(AT&T): www.att.com/secure_software/

- FIPS 표준과 호환
- 윈도우즈 3.1, 멕켄토시, 유닉스 시스템 지원
- X.500/X.509 인증서 지원
- 전자우편 패키지와 통합
- BusinessSafe은 현재 판매되지 않음

Caviar(ISODE Consortium) www.isode.com
- RSA, DSA 등의 알고리듬
- 하드웨어 토컨 지원 하지 않음
- X기반 관리자 인터페이스
- 유닉스 기반 응용 지원
- 클라이언트 지원 않음
- X.500

Intelligent Security Agent(Zoomit International, Inc) www.zoomit.com
- Entrust와 전자우편 클라이언트와 통합
- Banyan VINES와 Novell Netware systems만 지원

Verisign CA(Verisign, Inc.) www.verisign.com

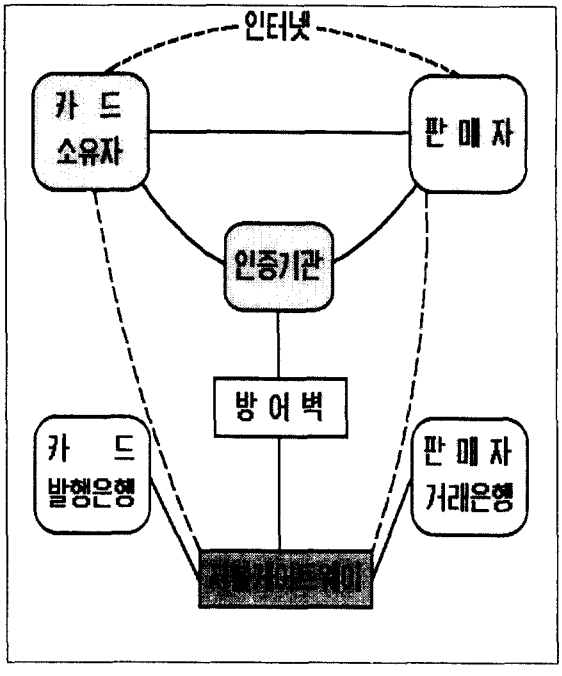
ArmorMail(LJL Entrises, Inc.) www.ljl.com
- Microsoft Mail, Lotus cc:Mail 내에서 Entrust 지원
- 서명 능력
- 윈도우즈, 맥킨토시, 유닉스 플랫폼 상의 여러 전자우편 클라이언트 지원

4. SET 표준과 인증기관

SET(Secure Electronic Transaction)이란 비자와 마스터 카드에서 인터넷과 같은 개방 네트워크에서 안전한 은행카드 거래를 이원하도록 공동 개발한 전자지불 프로토콜이다. 이 표준은 어떤 은행카드에 의한 지불 서비스에도 이용될 수 있다. 이 표준을 개발하는 데는 비자와 마스터 카드 외에도 GTE, IBM, Microsoft, Netscape, SAIC, Terisa, VeriSign 등이 참여하고 있다.

1) SET의 특징

SET 거래에의 참가자들은 [그림 3]과 같다.



[그림 3] SET에의 참가자들

SET에서는 비밀키 암호방식과 공개키 암호방식을 둘다 이용하는 복합 암호방식으로 메시지 기밀성을 유지하고 있다. 또한 SET에서는 전자서명과 전자인증서를 통해 거래 상대를 인증하고 있다.

- 암호화과정
- 이중서명(dual signature)

SET에서는 이중서명이라는 새로운 방식의 전자서명을 적용하고 있다. 다음의 시나리오를 생각해 보자:

시나리오: "홍길동"은 판매자인 "갑상사"에

게는 구매 오퍼 메시지를 전송하고, 은행에는 "갑상사"에서 구매 오퍼를 수락하는 경우에 한하여 대금지불을 승인해 줄 것을 명시한 지불지시 메시지를 전송하고자 한다. 그러나 "홍길동"은 은행에서 구매조건을 모르게 하고 싶어하며, 판매자인 "갑상사"에게는 은행계좌정보를 알지 못하도록 하기를 바란다. 더구나 "홍길동"은 "갑상사"가 구매 오퍼를 수락하는 경우에만 자금이체가 되도록 오퍼와 자금이체를 연계할 수 있기를 바란다. 그는 이중서명이라는 단 한번의 서명작업, 즉 은행과 판매자에게 송신되는 두 메시지 모두에 전자서명을 함으로써 이 문제를 해결할 수 있다.

송신자는 수신가 A와 수신자 B에게 보낼 서로 다른 두 메시지 각각의 다이제스트를 산출하여, 이 두 다이제스트를 함께 연결한 결과의 메시지 다이제스트를 산출한다. 그 후 송신자는 비밀 서명키로 이 다이제스트에서 서명을 한다. 송신자는 수신자가 이중서명을 확인할 수 있도록 다른 사람에게 보낼 메시지의 다이제스트도 함께 송신한다. 예를 들면, 송신자는 수신자 A에게 보낼 메시지는 물론이고 수신자 B에게 보낼 메시지의 다이제스트도 함께 수신자 A에게 보낸다. 수신자 A는 수신 메시지의 다이제스트를 산출하고 수신한 다른 메시지의 다이제스트와 연결하고, 그 결과의 메시지 다이제스트 계산하여 메시지의 신빙성을 점검한다. 이 새로이 산출한 다이제스트가 전자서명을 복구한 결과의 다이제스트가 일치하는 경우, 수신자 A는 메시지를 신뢰할 수 있다. 즉, 새로이 산출된 다이제스트가 이중서명의 다이제스트와 일치하는 경우, 수신자는 메시지 무결성을 입증할 수 있다.

- 상호운영성
- SET에서 지원하는 5개의 주요 거래과정

2) 전자인증서 및 신뢰사슬

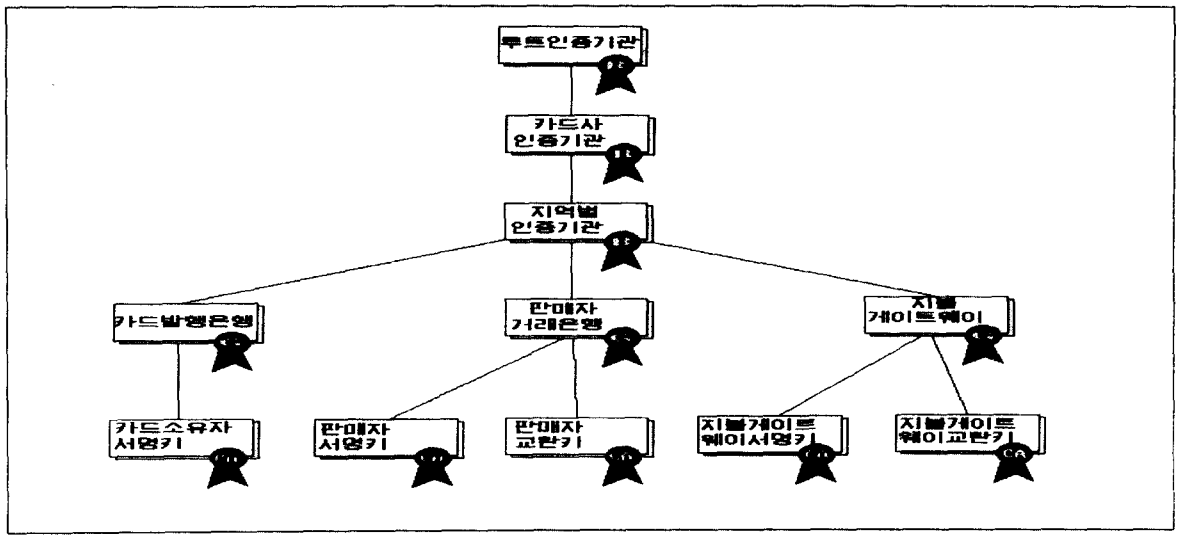
SET 표준에서는 다음과 같은 인증서가 이용된다.

- 카드 소유자 인증서
- 판매자 인증서
- 지불 게이트웨이 인증서
- 매입사 인증서
- 발행사 인증서

SET의 각 인증서는 신뢰사슬, 즉 신뢰계층구조(hierarchy of trust)를 통해 확인된다. 각 인증서는 그 발행기관의 인증서와 연결되어 있다. [그림 4]와 같이 신뢰 트리를 따라 잘 알려진 신뢰할 수 있는 인증기관까지 거슬러 올라가므로써 인증서의 유효성이 검증된다.

[표 3] 키의 종류와 기능

암호방식	키의 종류	키의 기능	분배방법
비밀키 암호방식	대칭키(비밀키)	메시지 암호화	송신자는 수신자의 공개키(교환키)로 대칭키를 전자봉투(digital envelope)에 밀봉하여(암호화하여) 수신자에게 전송한다.
공개키 암호방식	교환키쌍(공개키와 비밀키)	대칭키를 암호화하여 전자봉투를 산출하거나, 전자봉투에 들어 있는 대칭키를 꺼집어내는데 사용됨	공개키는 전자인증서에 첨부되어 배분된다.
	서명키쌍(공개키와 비밀키)	전자서명을 하거나 전자서명을 확인하는데 사용됨	공개키는 전자인증서에 첨부되어 배분된다.



[그림 4] SET 표준에서의 신뢰사슬

예를 들면, 카드소유자의 인증서는 발행금융기관의 인증서와 연결되어 있고, 발행금융기관의 인증서는 카드사의 인증서를 통해 루트 인증기관까지 연결되어 있다. 모든 SET 소프트웨어에는 루트 인증기관의 공개 서명키가 들어있고, 이 루트 공개 서명키는 각 인증서를 확인하는데 사용된다.

5. 결론: 우리 나라 인증기관의 구성

인증기관은 무엇보다도 다음과 같은 조건을 구비해야 한다. 첫째, 공개키 인프라(PKI)를 갖추어야 한다. 인증기관은 전자서명과 전자인증서 발행 및 관리는 물론이고, 인증실무준칙서를 작성하여 실행할 수 있어야 한다. 둘째, 인증기관은 신뢰할 수 있는 기관이어여야 한다.

인증서비스를 제공할 것으로 보이는 국내의 기관은 다음과 같다.

CommerceNet Korea
(http://cnkorea.dacom.co.kr/)

- 1996년 11월 설립, 1997년 4월 법인등록
- 신용카드사, 금융기관, 유통업체, 컴퓨터 및 통신부문 H/W 제조업체, S/W 업체, 인터넷 서비스업체, 웹기반 SI 업체 등으로 구성된 컨소시엄
- 특별회원(대홍기획, 데이콤, 삼성전자, LG소프트, 조흥은행, 한국아이비엠, 한국오라클)과 일반회원(ICEC, 다우기술, 다음커뮤니케이션, LG 전자 등 11업체)

소프트포럼(http://www.spftforum.co.kr)

- 미래산업(주) 보안기술 분야 전문연구소
- 1997년 8월, 국내 최초로 인증기관을 설립, 시범서비스 개시
- PGP-Net과 연동해 키(key)서버 운영

장미디어 인터렉티브(http://www.jmi.co.kr)

- 공증사무소(http://CA.jmi.co.kr)

기타 공개키 인프라를 기반으로 인증기관으로서 기능을 수행할 수 있는 기관은 다음과 같다.

- 한국통신
- 데이콤
- 메타랜드 등 웹기반 기술개발 업체

신뢰할 수 있는 기관으로서 등록기관 또는 인증기관으로서 역할을 수행할 수 있는 기관은 다음과 같다.

- 지역상공회의소

- 체신부
- 경제정의실천시민연합

인증기관은 웹을 통한 전자상거래에서 신뢰를 형성하는 중요한 역할을 수행한다. 따라서 인증기관에 대한 책임과 의무를 법으로 규정하여 규제할 필요가 있다. 한편, 인터넷 상거래가 초기단계에 있는 우리 나라에서 인증기관에 대한 법적 규제가 엄격할수록 인증기관으로 기능을 수행하고자 하는 기관이 나타나지 않게 될 것이다. 기본적으로 인증서비스를 제공하고자 하는 기관들은 자율적 시장원리 맡길 수밖에 없다. 따라서 신뢰할 수 있는 전자상거래가 활성화되도록 하기 위해서는 인증기관의 법적 책임과 의무에 대한 법적 규제와 인증기관에 대한 인센티브간의 균형점을 찾을 필요가 있다.

국내의 경우에는 전자상거래를 촉진하는 차원에서 공개키 인프라를 갖추는데 투자를 해야 하며, 신뢰사슬의 루트 인증기관은 정부기관이나 공공 단체가 그 역할을 맡고, 이하 인증기관에 대해서는 민간 부문에서 인증기관 역할 수행할 수 있도록 하는 정책이 필요하다.

참고문헌

1. 주재훈, 『인터넷 비즈니스: 혁신과 전자상거래』, 비봉출판사, 1997.

2. Abelson, H., etc., "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption, http://www.crypto.com/key_study/report.shtm, 1997.

3. AberdeenGroup, "BroadVision Dynamic Web Applications Enhance Employees, Clinch Customers, and Pamper Parters, http://www.broadvision.com/press_tour/Aberdeen/welcome.html, 1997.

4. Bakos, J. Y. (1991), "A Strategic Analysis of Electronic Marketplaces," *MIS Quarterly*, Vol. 15, No. 3, 295-310.

5. Belsign, Belsign Certification Practice Statement, ftp://www.belsign.be/repository/cps.html, 1996.

6. Burr, W. E., "Public Key Infrastracture(PKI) Technical Specifications(Version 2.3): Part C - Concept of Operations", Draft TWG-96-100, 1996.

7. Burr, W. E., D. Dodson, N. Nazario, and W. T. Polk, "Minimum Interoperability Specification for PKI Components, Version 1," NIST, http://csrc.nist.gov/pki, 1997.

8. Chaum, D. (1992) "Security without Identification: Transaction Systems to Make Big Brother Obsolete," *Communications of ACM*, Vol. 28, No. 10, 1030-1044.

9. Diffie, W. and M. Hellman (1976), "New Directions in Cryptography," *IEEE Transactions on Information Theory*, Vol. 22, No. 6, 644-654.

10. Froomkin, A. M. (1996a), "It Came From Planet Clipper: The Battle Over Cryptographic Key 'Escrow'," http://www.law.miami.edu/~froomkin/articles/

11. Froomkin, A. M. (1996b), "The Essential Role of Trusted Third Parties in Electronic Commerce," http://www.law.miami.edu/~froomkin/articles/

12. Garfinkel, S. (1994), *PGP: Pretty Good Privacy*, O'Reilly Associates.

13. Goodhue, D. L., M. D. Wybo, and L. J. Kirsch (1992), "The Impact of Data Integration on the Costs and Benefits of Information Systems," *MIS Quarterly*, Vol. 16, No. 3.

14. Hoffman, D. and T. P. Novak, "A New Marketing Paradigm for Electronic Commerce," http://www2000.ogsm.vanderbilt.edu/novak/new.marketing.paradigm.html, 1996.

15. Klein, S. (1996), "The Strategic Potential of Electronic Commerce-An Introduction for Beginners," http://www-iwi.unisg.ch/iwi4/cc/genpubs/ecintro.html

16. Malone, T. W. (1987), "Modeling

Coordination in Organizations and Markets," *Management Science*, Vol. 33, 1317-1332.
17. Malone, T. W., J. Yates, and R.J. Benjamin, "Electronic Markets and Electronic Hierarchies," *Communications of ACM*, Vol. 30, 484-497.
18. Novak, T. P. and D. L. Hoffman, "New Metrics for Media: Toward the Development of Web Measurement Standards," Project 2000 White Paper, 1996. http://www2000.ogsm.vanderbilt.edu/
19. Phelan, S. E., "Internet Marketing: Is the Emphasis Misplaced?," Annual Meeting of the Austrlian & New Zealand Academy of Management, December 1996.
20. RSA Data Security, Inc. (1995a), " RSA's Frequently Asked Questions About Today's Crytography," http://www.rsa.com/
21. RSA Data Security, Inc. (1995b), " RSA's Frequently Asked Questions About Today's Crytography: Capstone, Clipper, and DSS," http://www.rsa.com/
22. RSA Data Security, Inc. (1995c), " RSA's Frequently Asked Questions About Today's Crytography: DES," http://www.rsa.com/
23. RSA Data Security, Inc. (1995d), " RSA's Frequently Asked Questions About Today's Crytography: Factoring and Discrete Log," http://www.rsa.com/
24. RSA Data Security, Inc. (1995e), " RSA's Frequently Asked Questions About Today's Crytography: General," http://www.rsa.com/
25. RSA Data Security, Inc. (1995f), " RSA's Frequently Asked Questions About Today's Crytography: Key Management," http://www.rsa.com/
26. RSA Data Security, Inc. (1995g), " RSA's Frequently Asked Questions About Today's Crytography: Miscellaneous," http://www.rsa.com/
27. RSA Data Security, Inc. (1995h), " RSA's Frequently Asked Questions About Today's 89. Crytography: NIST and NSA," http://www.rsa.com/
28. Schneier, B. (1994), *Applied Cryptography: Protocol, Algorithms, and Cource Code in C*, New York: John Wiley & Sons.
29. Tygar, J. D. (1996) "Atomicity in Electronic Commerce," *ACM/IEEE 21st Conference on Principles of Distributed Computation.*
30. VISA (1996), "SET Specifications," http://www.visa.com/cgi-bin/sf/set/intro.html
31. VeriSign, "About VeriSign, Inc," http://www.verisign.com/
32. Zabih, R. (1996), "Creating an Efficient Market on the World-Wide Web," http://www.priceweb.com/curr/essay.html.