通信情報保護學會誌
第7卷 第3號, 1997. 9

전자상거래 관련 기술

Technologies for Electronic Commerce

강 명 호*, 송 주 석*

요 약

본 논문에서는 현재 비약적으로 발전하고 있는 전자상거래를 분류하고 이와 관련된 기술을 통신망 기술, 암호 기술, 그리고 인증 기술로 나누어 정리하였다. 특히 최근 그 시장이 확대되고 있는 통신망을 통한 신용카드 거래 시스템과 전자화폐 시스템의 동향과 대표적인 프로토콜을 서술하였다.

1. 서론

월드와이드웹(World Wide Web : 이하 웹이라고 표기)의 등장과 더불어 인터네트 사용자가 폭발적으로 증가 하고 있으며 인터네트를 통한 사이버스페이스에서의 상거래 서비스가 시작되고 있다. 이제는 단순히 인터넷을 이용하여 전자우편이나 뉴스그룹을 통한 정보 공유 차원을 넘어서, 통신망을 통한 모든 종류의 거래에 적극 활용할 수 있는 방안이 연구되고 있는데, 이를 가리키는 용어가 전자상거래이다.

전자상거래는 원래 미국 국방예산의 운영 및 유지 시 소요되는 비용을 절감하기 위하여 정부 조달 시스템의 효율적인 운영을 위하여 구상된 CALS 및 EDI로부터 발전한 개념으로서, 단순한 개인적인 상품 매매의 관점을 벗어나 정부 및 기업의 모든 거래에 필요한 전자적 수단을 통칭한다. 하지만 최근 들어 인터넷이 확산되면서 각종 상품의 매매가 통신망을 통하여 이루어지면서, 전자상거래의 개념이 통신망을 통한 신용카드 거래 및 전자화폐를 이용한 거래 행위를 가리키게 되었다.

따라서 전자상거래는 보는 관점에 따라 개념을 달리하는데, 광의의 전자상거래 개념은 CALS로 지칭되는 기업과 기업간, 기업과 정부간의 정보 인프라를 의미하고 협의의 전자상거래 개념은 전자상점, 사이버쇼핑몰 등과 같은 상품 거래 시스템을 의미한다. CALS는 개별적인 기업들이 하나의 단체와 같이 통합된 정보체계 하에서 생산, 구매, 재무, 수송, 행정 및 서비스 등의 모든 업무 처리를 자동화하기 위한 표준화된 프레임워크를 말하며, 이를 통하여 기업 운영 방식을 재창조하고 비용 절감 등을 통해 기업의 이윤을 극대화 시키는 것을 목적으로 한다. 반면 협의의 전자상거래는 개

. 연세대학교

인 사용자의 상품 구매시 보다 편리한 환경 제공과, 서비스의 제공자인 상점의 효율적인 운영을 위하여 안전한 상거래 프레임워크를 제공하는데 그 목적을 둔다.

이미 미국을 비롯한 선진 각국에서는 이를 위한 다양한 기술 개발이 활발하게 이루어지고 있다. 최근들어 국내에서도 전자상거래와 관련된 정부 차원의 대규모 과제가 진행되면서 대학, 연구소, 그리고 기업체에서도 활발히 연구되고 있으며, 통신 관련 기업들은 전자상거래를 위한 컨소시엄을 구성하여 국내 실정에 맞는 전자상거래 환경 구축을 진행하고 있다.

본 논문에서는 협의의 전자상거래 개념을 중심으로 전자상거래 프로토콜을 살펴보고, 전자상거래 시스템 구축시 필요한 기반 기술을 고찰하도록 한다.

2. 전자 화폐 시스템

인류가 사용하고 있는 화폐는 조개 껍질, 금속 화폐를 거쳐 현재는 종이로 된 지폐 시대와 신용카드 시대가 공존하고 있다. 그러나 정보화의 높은 물결로 전자 화폐가 서서히 새로운 통화수단으로 등장하고 있다 전자 화폐는 현금을 대신하는 결재수단으로 전자 현금, 전자 지갑, 사이버 화폐, 디지털 현금, 스마트 화폐, 가상 현실 화폐 등 많은 관심만큼이나 다양하게 불리고 있다.

전자 화폐가 출현하게 된 것은 지폐가 중심이 되어온 기존 화폐가 갖고 있는 여러 가지 문제점에 기인한다. 그 중 하나로 기존 화폐는 통화발행이 인가된 기관 외에는 화폐 제작을 할 수 없고 물리적인 안전 대책에만 화폐 제도의 안전성이나 신용 의존하고 있다는 점이다. 미국을 비롯한 선진 각국에서는 전자화폐를 위한 기술 개발이 활발히 이루어지고 있으며, 인터네트를 통한 전자 상거래에 본격적으로 활용되기 시작하고 있다. 그러나 아직 여러 가지 미흡한 문제점들이 많이 지적되고 있다.

2.1 전자 화폐의 등장 배경

컴퓨터 및 정보통신기술의 비약적인 발달로 금융업무의 전자화가 세계각국에서 일반적인 현상으로 자리잡아가고 있으며 이는 전자 자금 이체 시스템(EFTS : Electronic Fund Transfer System)의 확대 뿐만 아니라 지급결재수단의 전자화를 의미한다.

- ◆ 경제규모의 확대에 따른 결재량의 증대 및 정보통신기술의 급격한 발달에 따라 지급결재수단은 종전의 현금, 수표, 어음 중심의 결재 수단에서 카드 및 전자자금 이체 등의 결재 수단으로 전환되고 있는 추세이다.
- ◆ 특히, 선불(Prepaid), 직불(Debit), 신용(Credit) 카드 등 카드매체를 이용한 지급 결재 수단의 도입 필요성 증대에 따라 등장한 IC카드가 조만간 자기띠(MS : Magnetic Stripe) 카드를 대체할 것으로 전망된다.
- ◆ 전자 화폐는 현재의 물리적인 화폐와 기능이 유사하고, 화폐의 사용시 화폐 발급기관의 주전산기와 연결없이 오프라인(off-line)으로 사용되어 사용할 수 있다.
- ◆ 전화 망이나 인터네트와 같은 개방된 통신망에서의 신용카드를 이용한 거래가 증가하면서 이를 위한 안전한 트랜잭션의 처리가 필요하게 되었다.
- ◆ 광범위한 분야의 일상적 거래가 오프라인 상태에서 전자적으로 암호화되어 신속, 안전하게 처리될 수 있다.

현재의 소비자들은 5가지의 주요한 지급수단 즉, 현금, 수표, 신용카드, 선불 또는 직불카

드, 지로(자동계좌이체제도 : ACH debit)등을 사용하여 물품 또는 서비스를 구매하고 있다. 그러나, 종전의 현금, 어음, 수표중심에서 각종 카드 결재 수단을 매개로한 결재 수단의 거래 비중이 급속이 높아지고 있다. 94년중 신용카드 발급매수는 2천 5백만매, 가맹점은 190만개로서 총 사용금액은 39조원이고 현금서비스를 제외한 무현금 결재 금액은 18조원에 달한다. 94년 9월 부터 판매된 범용선불카드는 94년중 11억원의 판매 실적을 보이고 있다. 또한 정보통신기술의 급격한 발달에 따라 현금의 수수없이 통신회선을 통한 은행 계좌간 전자자금이체 등이 활발해 짐에 따라 기존의 화폐가 뚜렷이 전자화되고 있는 등 거래수단으로서 화폐에 대한 기존 개념이 변하고 있다. 94년중 전자방식 결재동향을 보면 결재건수는 436백만 건으로, 93년 대비 45% 증가하여 거래비중이 27%이고, 결재금액은 238조원으로 93년 대비 115% 증가하여 금액비중이 3.9%를 차지하고 있어 전자방식 결재는 주로 소액거래에 이용되고 있음을 알 수 있다.

화폐의 제작, 관리, 파기에 막대한 예산과 인력 소요로 특히 소액관리에 따른 관리가 심각하며, 우리나라의 10원짜리 동전 생산에 드는 비용이 27원 정도로 소요되고 있다. 금융 EDI인 SWIFT(Society for Worldwide Interbank Financial Telecommunication)와 사이버 쇼핑 등 컴퓨터 통신망을 통한 금융거래가 활발해 지고 있다.

이러한 출현 배경으로 등장한 각종 전자 화폐는 각국의 지대한 관심으로 개발과 보급이 시작되고 있다. 사이버캐쉬, 퍼스트 버추얼, 오픈 마켓, 디지캐쉬 등의 전자화폐 관련회사들이 인터네트의 급속한 보급과 멀티미디어 산업과 맞물려 전자 화폐의 사용을 이미 시작하고 있다. 스마트 카드를 바탕으로한 유럽의 전자 화폐 개발 프로젝트인 CAFE(Conditional Access For Europe), 영국의 National Westminst 은행, British Telecommunication사의 연합 벤처기업이 개발하여 실험 운용중인 몬덱스 전자 화폐 시스템은 세계의 주목을 받고 있으며, 일본의 대장성과 NTT 그리고 민간 기업도 연합하여 전자 화폐의 개발을 서두르고 있다.

2.2 전자 화폐 시스템의 종류

현재 전 세계적으로 10여종 이상의 전자 화폐가 시험 운영 중이며 네트워크 상에서의 상거래가 활발해지면서 그 종류도 다양화될 전망이다. 이와 같은 전자 화폐는 기술개발 측면에서 가치저장형(SVC)을 비롯해 지불지시형(신용카드나 직불카드), 네트워크형 등 세가지 종류로 분류할 수 있다. 먼저 간단히 요약하면 다음과 같다.

◆ 가치저장형 전자 화폐
- 각국에서 스마트 카드 기술 개발 및 활용중
- 본격적인 화폐인 영국의 몬덱스 카드는 소규모로 시범 사용중
- 미국의 VISA 캐쉬 및 마스터 캐쉬 개발중

◆ 지불지시형 전자 화폐
- 미국 사이버캐쉬사의 사이버캐쉬 활용중
- 미국 퍼스트버추얼홀딩스사의 퍼스트 버추얼 활용중
- VISA 및 Mastercard사 제휴하에 SET 프로토콜 개발

◆ 네트워크형 전자 화폐
- 네덜란드 디지캐쉬사의 e-캐쉬 활용중
- 본격적인 디지털 전자 화폐 기능 제공

(1) 가치저장형 전자 화폐

스마트 카드와 같은 저장 가능한 매체를 이용하여 화폐 가치를 IC에 저장한 후 필요할 때 꺼내서 사용하는 형태의 화폐이다. 스마트 카드를 이용하기 전에 화폐 가치를 저장하기 위해서 은행창구나 ATM, 공중전화 등의 단말기기를 이용할 수 있도록 개발되고 있다. 실제로 상품 구매시 가치저장형 화폐를 사용할 경우에는 상점에 설치되어있는 지불용 단말기들을 이용하게 된다.

이와 같은 SVC(Stored Value Card)형 전자 화폐는 영국의 몬덱스카드를 비롯해서 VISA 캐쉬, Master 캐쉬 등이 있으며 실용화를 위해 특정 지역을 대상으로 실험되고 있다.

(2) 지불지시형 전자 화폐

지불 브로커 시스템이라고도 불리는 지불지시형 전자 화폐는 미국의 VISA사와 Mastercard사가 개발한 SET 프로토콜(Secure Electronic Transaction Protocol)과 미국 사이버캐쉬(CyberCash)사가 개발한 전자지불시스템인 '사이버캐쉬'로 대표되며, 그 밖에도 많은 시스템들이 개발되고 있다. 이와 같은 시스템에서는 PC 환경에서 구동되는 전용 소프트웨어를 통해서 신용 카드의 번호를 입력하고, 이 값을 암호화하여 지불지시형 전자 화폐 서비스 제공회사의 중개로 네트워크 상에서 결재되도록 한다.

이와 같은 지불지시형은 기존의 지불 메커니즘을 이용하기 때문에 쉽게 적용할 수 있다는 장점이 있는 반면, 신용카드 등의 지불 비용(조회 비용, 수수료)이 추가되기 때문에 이용료가 비싸진다는 단점이 있다. 현재 시험적으로 서비스되고 있는 대부분의 전자 지불 시스템이 바로 이러한 지불지시형 시스템의 형태를 갖으며 대표적인 예가 사이버캐시, 퍼스트 버추얼, SET 등이다.

이와 같이 지불지시형 전자 화폐의 종류는 매우 다양하므로, 거래 정보의 보안 유지, 효율적인 비용 문제 해결, 온라인 거래 등을 만족시키기 위해서는 개방형 단일 명세, 즉 표준안의 개발이 필요하다. 이러한 취지에서 1997년 5월에 세계 최대의 신용 카드 회사인 VISA사와 Mastercard사가 제휴하여 SET 프로토콜을 개발하여 프로토콜 버젼 1.0을 공개하였다. 이 프로토콜은 개방형 네트워크를 통하여 안전한 카드 결재를 할 수 있는 표준적인 방법을 제공한다. SET 프로토콜은 신용카드 거래 시스템의 표준화를 지향하고 있으며, 이를 위한 기능과 방법을 자세하게 명세하고 있다. 응용 소프트웨어는 정의된 명세를 근간으로 개발하도록 권장하고 있다.

(3) 네트워크형 전자 화폐

네트워크형 전자 화폐는 진정한 전자 화폐의 의미를 지니는 것으로서, 실생활의 화폐 대신에 화폐의 특성을 가지도록 구성된 전자적 데이터를 사용한다. 즉, 통신망을 통하여 은행으로부터 화폐 가치를 인출한 후, 암호학적 기술을 이용하여 하드디스크와 같은 사용자의 영구기억매체에 동일 가치의 화폐 데이터를 생성시킨다. 이 데이터는 오프라인성, 재사용 방지, 익명성 등 실제 화폐가 가져야 할 특성들을 만족시켜야 하며, 통신망 상에서 일반 화폐와 동일하게 취급된다.

현재 네트워크형 전자 화폐를 인터네트상에서 상용으로 서비스하고 있는 대표적인 회사는 네덜란드의 디지캐쉬(Digicash)사이다. 디지캐쉬사는 E-cash라는 전자 화폐를 개발하였으며 E-cash의 이용자는 은행에 미리 계좌를 개설해 입금을 해놓고 네트워크를 통해 화폐 데이터를 전송, 물건을 구입한다. E-cash를 받은 상점은 은행에 화폐 데이터를 전송, 확인절

차를 거친 후 자신의 계좌로 해당 금액을 입금받는다. 디지캐쉬사는 미국의 마크트웨인 은행과 EUNet(핀란드), Deutsche Bank(독일) 등과 연합으로 전자 화폐를 발행해서 서비스하고 있다.

한편 인터넷상의 전자 상거래는 주로 소액중심이고 특히 1달러 이하의 지불이 필요한 상거래가 있는데 현재의 지불브로커 시스템이나 전자 화폐 시스템의 지불 비용이 비싸 이를 서비스할 수 없는 형편이다. 따라서 소액 거래를 위한 소액전자 지불 프로토콜이 요구되는데, 현재 개발된 소액전자 지불 시스템으로는 Milicent (DEC사), MPTP(Micro Payment Transfer Protocol, W3C사), PayWord와 MicroMint (Rivest, Shamir) 등이 있다.

2.3 전자 신용카드 거래 시스템

신용 카드 거래 시스템이란 기존의 신용 카드를 이용하여 인터네트를 통한 전자 상거래의 대금 지불 문제를 해결하도록 하는 것으로서, 사용자에게 안전성과 편리성을 제공할 수 있어야 한다. 신용 카드는 이미 전 세계적으로 신용 판매 혹은 통신 판매를 위한 수단으로 이용되고 있으며, 따라서 많은 사용자들을 확보하고 있다. 또한 소지하기에 부담스러운 일반 화폐의 단점을 극복하는 금융 서비스의 중요한 매체로서 인식되고 있다. 한편, 인터네트 사용 인구의 폭발적인 증가로 인한 하나의 결과로서, 전자 상거래가 금융 서비스 산업에 지대한 영향을 미칠 것이라는 사실은 매우 당연하다.

이와 같이 시장의 요구를 만족하기 위한 보안, 효율적인 비용, 온라인 거래를 달성하기 위해서는 개방형 단일 명세, 즉 표준안의 개발이 필요하다. 이러한 취지에서 신용 카드 회사인 VISA와 Mastercard가 제휴하여 SET 프로토콜을 정의하고 있으며 이것은 개방형 네트워크를 통하여 안전한 카드 결재를 할 수 있는 방법을 제공한다. 이 프로토콜에서는 표준화를 지향하는 기능과 방법을 자세하게 명세하고 있으며, 소프트웨어는 정의된 명세를 근간으로 개발하도록 권장하고 있다.

(1) 전자 신용카드 거래 시스템 요구 사항

전자 신용 카드 시스템을 위해서는 다음과 같은 요구 사항이 만족되어야 한다.

① 비밀성

지불 정보에 대한 비밀성이 제공되어야 한다. 지불 정보에는 사용자 번호, 사용자 계정 정보, 거래 금액, 거래 내용 등이 포함된다. 또한 주문 정보에 대해서도 비밀성을 보장할 수 있어야 한다. 비밀성은 메시지 암호화를 통해서 이루어진다.

② 인증

카드 소지자 및 상점에 대한 안전한 인증이 이루어져야 한다. 이것은 결국 서로간의 상호 인증이 안전하게 이루어져야 함을 의미한다. 인증은 디지틀 서명 및 당사자의 인증서를 통해서 이루어진다.

- 카드 소지자의 인증 : 상점이 임의의 카드 소지자가 제시한 지불 카드 계정의 합법적인 사용자인지를 인증할 수 있어야 한다.
- 상점의 인증 : 카드 소지자가 임의의 상점이 제시한 종류의 지불 카드 거래를 받아들일 수 있는지를 금융 기관과의 관계를 통해서 인증할 수 있어야 한다.

③ 무결성

주문 정보 및 지불 정보에 대한 무결성이 제공되어야 한다. 즉, 전송되는 모든 정

보의 무결성이 보장되어야 한다. 무결성은 디지틀 서명을 통해서 이루어진다.

④ 암호화 알고리즘 및 프로토콜

위와 같이 지불과 관련된 세가지 주요 서비스를 제공하기 위한 암호화 관련 알고리즘과 프로토콜이 정의되어야 한다.

⑤ 상호 운용성

다양한 판매자들에 의해 개발된 응용 프로그램간의 상호 작용 문제가 해결되어야 하며 서로 상호 운용될 수 있어야 한다. 또한 하부적인 면에서 네트워크 제공자와의 상호 운용성도 고려되어야 한다. 상호 운용성은 특정한 프로토콜과 메시지 포맷을 통해서 이루어진다.

⑥ 채용성(acceptability)

하나의 카드 회사가 아닌 다양한 카드 회사, 은행 및 상점에게 쉽게 채용될 수 있도록 마련된 표준을 근간으로 한 구현이 필요하다.

⑦ 호환성

인터네트 상에서 사용되는 다양한 컴퓨터 플랫폼에서 호환성을 가지며 또한 이식성 및 확장성을 가질 수 있도록 표준화된 소프트웨어 개발이 필요하다.

(2) 전자 신용카드거래 프로토콜

본 절에서는 대표적인 전자 신용카드거래 프로토콜인 SET에 대하여 설명한다. SET은 안전한 전자 트랜잭션 프로토콜의 명세로서 VISA사와 Mastercard사가 공동으로 제안하고, GTE, IBM, Microsoft, Netscape, SAIC, Terisa 그리고 Verisign사가 지원하기로 한 전자 신용카드 거래 프로토콜이다.

SET의 목적은 통신망 상에서 안전한 신용카드 거래를 위하여 정보의 전달의 비밀성, 지불 데이타의 무결성, 그리고 상인과 고객간의 상호 인증을 제공하는 일관된 환경을 마련하는데에 있다.

SET의 명세는 1997년 5월에 버전 1.0이 발표되었으며, 1997년 중반부터 SET 프로토콜을 따르는 응용 프로그램이 개발되고 있다.

① SET의 범위

SET에서는 보다 원활한 전자 신용카드 거래를 위하여 각 거래 참가자들 간의 기본적인 메시지 프로토콜들을 정의하며, 이에 따르는 구매 메시지 형식, 인증 메시지 형식, 그리고 입금 메시지 형식을 제공한다. 또한 이를 위한 암호화 알고리즘인 RSA와 DES의 사용 방법을 정의하고 있으며, 특히 개인의 인증을 위한 인증서의 사용 형식과 메시지 형식을 정의한다.

각 신용카드 회사 및 전자 상거래를 위한 응용 소프트웨어 제작사들은 이와 같은 프로토콜 명세에 따라 자유롭게 자신의 목적에 맞는 용도로 SET을 수용할 수 있으며, 이에 따르는 허가권(licence)는 요구하지 않는다.

SET이 전자 신용카드 거래 프로토콜의 명세로서 범주에 넣지 않고 있는 부분은 다음과 같으며, 이 부분은 서비스 제공 업체 또는 소프트웨어 제작 업체의 목적에 맞게 구성하여 자신의 수요를 창출할 수 있는 부분으로 활용할 수 있다.

- 상품 쇼핑, 주문 및 배달을 위한 메시지
- 은행 또는 신용카드사의 고객과 상인에 대한 인증서 발행
- 각 상점의 상품 판매 화면과 상품의 주문 내용 입력 형식
- 신용 지불 카드의 범위를 벗어난 형태의 지불 방식

- 바이러스, 트로이 목마, 그리고 해커로부터의 고객, 상점 그리고 지불 게이트웨이 시스템의 데이터에 대한 보안

② SET의 기본적인 프로토콜

SET 프로토콜은 앞에서 언급한 것처럼 전자 신용카드 거래를 위한 가장 기본적인 프로토콜의 명세만을 제공하며, 보다 자세한 프로토콜의 개발과 보안과 관련 없는 시스템 구성요소에 대하여는 시스템 개발자와 서비스 제공자의 자율에 맡기고 있다.

SET 프로토콜 명세에 정의되어있는 기본적인 프로토콜은 다음과 같다.

- 고객 등록(cardholder registration)
- 상점 등록(merchant registration)
- 구매 요구(purchase request)
- 지불 허가(payment authorization)
- 지불 capture(payment capture)

◆ 고객 등록 프로토콜

전자 신용카드 거래를 원하는 사람이 처음 가입하는 절차이다. 즉, 신용카드사의 인증을 담당하는 인증 허가 기관(CA : Certification Authority)을 통하여 고객의 등록과 인증서의 처리가 이루어지는 절차이다. 이때 생성된 고객의 인증서는 SET 트랜잭션 내에서 고객의 신용카드의 역할을 한다.

◆ 상점 등록 프로토콜

신용카드의 사용자와 마찬가지로 상점 역시 인증 허가 기관에 등록하여 자신의 인증서를 만들어야만 한다. 이 절차를 명시해 놓은 것이 상점 등록 프로토콜이며 그 절차는 다음 그림과 같이 이루어진다. 상점의 인증서는 그 상점이 가입한 신용카드 브랜드를 나타낸다.

◆ 구매 요구 프로토콜

구매 요구 프로토콜은 모두 5단계로 이루어지며, 서로간의 인증을 위하여 인증서를 전달하는 작업으로 시작한다. 이 프로토콜은 고객이 상품을 구입하기 위하여 상점에게 원하는 상품을 주문하여 구매 계약이 끝나는 시점까지를 명시하고 있다. 구매 요구 프로토콜이 종료된 후, 상점에서는 물리적인 또는 전자적인 상품의 배달도 함께 이루어져야 한다.

◆ 지불 허가 프로토콜

지불 허가란 상점이 지불 게이트웨이를 통하여 자신에게 물품을 구입하고자 하는 고객의 신용카드의 사용을 허가받는 절차를 의미한다. 이 프로토콜은 신속히 이루어져야 하므로 모두 3단계로 이루어진다.

◆ 지불 capture 프로토콜

지불 capture 프로토콜은 고객으로부터 상품 구매 계약을 성립시킨 이후에 상점의 구좌에 그에 상응하는 금액을 입금시키도록 요구하는 절차이다.

상점은 먼저 capture 요청서를 작성하여 서명한 후 대칭키를 발생시켜 암호화하여 고객으로부터 받은 capture 토큰과 함께 지불 게이트웨이로 전달한다. 지불 게이트웨이는 상점의 capture 요청서와 고객의 capture 토큰을 비교하여 맞으면 금융기관 네트워크를 통하여 고객의 은행에 capture 요구를 보낸다. 지불 게이트웨이는 capture 응답서를 작성하여 상점에게 서명하여 보내고 상점은 이를 확인한다.

2.4 네트워크형 전자 화폐 시스템

(1) 전자 화폐를 위한 요구 사항

전자 화폐가 기존의 화폐 시스템을 대체하기 위해서는 실생활의 화폐가 가지고 있는 다음과 같은 조건을 만족해야만 한다. 특히 디지털 데이터로 표현되는 전자 화폐는 대량 위조가 쉬우며, 중앙에서 통제하기 용이하고, 일반 통신망 응용이 가지고 있는 보안의 허점을 그대로 지니고 있기 때문에 악용될 우려가 있다.

① 비의존성(Independence)

물리적인 조건에 의존하지 않아야 한다. 그래야만 네트워크를 통해서 전송될 수 있다.

② 안전성(Security)

전자 화폐를 재사용하거나 위조하는 것이 방지되야 한다. 일반 지폐에 있서는 위조가 있으나 전자 화폐에서는 이중 사용(Double spending) 이 있다. 지폐에서의 위조는 은행 또는 정당한 발행 기관의 허가없이 돈을 만들거나 기존의 돈으로부터 새로운 돈을 만드는 행위를 말하지만 전자 화폐는 전자 정보로 이루어져 쉽게 복사가 가능하다. 1회 사용후 다시 다른 곳에 동일한 전자 화폐를 사용할 수 있다. 지폐에 대한 위조를 방지하기 위해서는 복사하기가 어려운 특수 잉크, 특수 도안 등이 사용되어 위조 지폐의 발행을 어렵게 하지만 전자 화폐에 대한 이중 사용 방지는 사용된 전자 화폐의 정보로부터 컴퓨터가 동일한 전자 화폐를 조사하여 이중 사용자의 계좌 번호와 사용자의 신분을 알아내는 방식을 주로 취하고 있다. 온라인인 경우 이중 사용의 방지가 용이하나 오프 라인인 경우 전자 화폐 사용전 거래 중지가 곤란하기에 추후 부정 사용자 방지 대책을 세워야 한다.

③ 익명성(Anonymity-Privacy/Untraceability)

사용자에 대한 정보나 사용 내역 등은 보호되어야 한다. 즉, 사용자와 상점간의 거래 내역, 관계 등은 다른 사람에 의해서 추적될 수 없어야 한다. 사용된 돈으로부터 그 돈의 사용자를 추적불가능하고 또 똑같은 계좌에서 두번의 거래가 이루어져도 그 두 거래가 똑같은 계좌에서 이루어졌다는 사실을 알길이 없도록(Unlinkable) 설계되야 한다. 이러한 보호는 돈세탁이나 탈세, 통화 통제 불가능 등의 부정적인 면이나 전자 화폐 시스템의 효율을 떨어뜨릴 수 있기에 완전한 익명성의 구현은 신중히 고려되야 한다.

④ 오프라인(Off-line) 거래

사용자가 전자 화폐를 상점에 지불했을 때 사용자와 상점간의 거래 과정은 오프라인 방식으로 이루어져야 한다. 즉, 상점은 사용자와의 거래시에 메인 호스트에 연결해야만 할 필요가 없어야 한다. On-line 금융 체계는 안전에 관한 대부분의 문제는 해결되지만 운영경비가 많이 들고 효율적이지 못하다. 온라인은 고객 관리 및 전자 화폐 관련 정보를 수록한 거대한 데이터 베이스를 유지하여 매 지불단계시 마다 허가를 해주는 중앙 허가 기관 즉 은행과 직접 모든 참가자가 접촉하는 것을 말한다. 다시 말해 지불단계와 결재 단계가 거의 동시에 행하여지는 것을 말하며 이중 사용을 지불단계에서 사전에 방지할 수가 있으나 많은 통신량이 한곳으로 집중화되는 문제점과 거래에 따른 통신 비용이 증가하게 되는 문제점이 생기게 된다 .

오프라인은 지불단계와 결재 단계가 동시에 이루어지지 않는 형태이며 일정 시간 경과후 수신된 전자 화폐를 일괄 처리해 은행에 결재 요구하는 것으로 모든 단계가 완료된 후에 이중사용이 이루어지고 난 후 은

행에서 이중 사용자에 대한 신분 검출이 가능한 문제점이 생기게 된다. 이중 사용한 후 도피할 수 있는 문제점이 생기나 통신량의 집중화 방지와 거래에 따른 통신 비용은 적게 든다.

온라인은 고액거래로 높은 안전성을 요구하면서 운용비에 대한 부담이 크게 중요하지 않는 현금시장에 적합하고 오프 라인은 많은 양의 소액 거래가 이루어지는 곳으로 부정 가능 금액이 소규모이고 운용비 부담이 문제가 되는 곳에서 필요하다.

⑤ 양도성(Transferability)

전자 화폐는 일반 현금처럼 다른 사람에게 쉽게 양도될 수 있어야 한다.

⑥ 분할성(Dividability)

일반 현금이 다른 작은 단위로 나뉘어지는 것과 같이 전자 화폐도 쉽게 나누어질 수 있어야 한다.

⑦ 수용성(Acceptability)

여러 은행의 화폐 사용이 가능해야 한다. 즉, 타 은행과의 상호 작용 및 통화 조절이 가능해야 하고 이것이 자동적으로 처리되어야 한다. 대부분의 시스템은 단일 은행을 대상으로 하고 있지만 이상적인 것은 다중 은행의 존재가 가능해야 하는 것이다.

⑧ 확장성(Scalability)

전체 시스템 성능에 큰 손실이 없이 사용자나 화폐를 추가할 수 있어야 한다. 중앙 서버의 간섭이 최소화되고 이중 사용 발견 등에 필요한 데이터베이스의 크기를 최소화해야 한다.

(2) 네트워크형 전자 화폐 프로토콜

전자 화폐 프로토콜은 앞에서 살펴본 전자 화폐의 요구조건인 비의존성, 안전성, 익명성, 오프라인 거래, 양도성 등을 만족하도록 설계되어야 한다.

전자 화폐에서 사용되는 프로토콜은 크게 인출 프로토콜, 지불 프로토콜, 입금 프로토콜로 나눌 수 있다. 가장 대표적인 전자 화폐를 위한 프로토콜은 Chaum이 제안한 CFN 방식[11]의 전자 화폐이며 'Cut and Choose' 방식을 이용하였다. 그가 제안한 중복사용 검출을 위한 프로토콜은 확률적으로 동작하므로 실제로 사용하기에는 문제가 있다. Brands는 'Challenge and Response' 방식을 이용하여 새로운 프로토콜을 제안했는데, 이는 전자 화폐의 중복 사용 시 반드시 중복 사용 여부를 확인 할 수 있고, 이산 대수 문제의 확장인 표현 문제(representation problem)에 안전성을 근거하고 있다. Brands[10]의 프로토콜은 특수한 블라인드 서명기법과 비밀 분산 방안을 사용하여 화폐 발행 프로토콜과 지불 프로토콜을 간소화 하였다.

다음은 전자 화폐 시스템의 개념적인 프로토콜과 Brands가 제안한 전자 화폐의 프로토콜을 설명한 것이다.

① 전자 화폐 시스템을 위한 개념적인 프로토콜

- 인출 프로토콜

  사용자 : 난수 r 생성

  사용자 : 난수 r을 감추고 은행에 서명 받을 전자 화폐를 제출

  은 행 : 금액을 인출시킨 후 감춰진 난수 r에 서명하고 돌려줌

- 지불 프로토콜

  사용자 : 돌려받은 전자 화폐를 상점에 제출

상 점 : 은행의 서명을 확인한 후 물건을 건네줌

- 입금 프로토콜

상 점 : 사용자로부터 받은 전자 화폐를 은행에 제시

은 행 : 상점의 계좌에 입금함

- 난수를 감추기 위한 방법

난수 r, a

은행의 공개키 e

은행의 비밀키 d

사용자 : $Z = rea \bmod N$

은 행 : $Z^d = rad \bmod N$

사용자 : $Z^d/r = ad \bmod N$

이 값을 화폐로 사용함.

② Brands 방식의 전자 화폐 프로토콜

- 인출 프로토콜

사용자 : 다음을 만족하는 x_1, x_2, y_1, y2를 임의로 선택

$a = x_1 + x_2 \bmod P\text{-}1$

$a+U = y_1 + y_2 \bmod P\text{-}1$

$G = H(g_1^{x1}g_2^{y1}, g_1^{x2}g_2^{y2})$ 계산 (H는 안전한 일방향 해쉬함수)

$I_A = f(U)$ 계산

은행에 $Z = r^e \times G \bmod N$ 제출

은행에게 영지식증명을 이용하여 (IA, Z)가 위의 모든 식을 만족함을 증명

은 행 : $Z^d = r \times G^d \bmod N$을 계산하여 사용자에게 돌려줌

사용자 : $Z^d / r = G^d$를 계산하여 다음의 화폐를 얻음

$(G, G^d, g_1^{x1}g_2^{y1}, g_1^{x2}g_2^{y2})$

- 지불 프로토콜

사용자 : 상점에 전자 화폐 제시

상 점 : G와 $H(g_1^{x1}g_2^{y1}, g_1^{x2}g_2^{y2})$가 같은지 검사

$(G^d)^e$와 G가 같은지 검사

상 점 : 난수 a 발생시킨 후 사용자에게 전송

사용자 : 다음과 같이 v, w를 계산하여 상점에 전송

$v = x_1 + ax_2 \bmod P\text{-}1$

$w = y_1 + ay_2 \bmod P\text{-}1$

상 점 : $g_1^v g_2^w = g_1^{x1}g_2^{y1}(g_1^{x2}g_2^{y2})a \bmod P\text{-}1$이면 사용자에게 물건 제공

- 입금 프로토콜

상 점 : 은행에 C, a, v, w 제시

은 행 : 상점의 계좌에 적정 금액 입금

- 중복 사용 검사

다음의 식을 이용하여 x_1, x_2, y_1, y_2 값 알아냄

$$v_1 = x_1 + a_1x_2$$

$$v_2 = x_1 + a_2x_2$$

$$w_1 = y_1 + a_1y_2$$

$$w_2 = y_1 + a_2y_2$$

x_1, x_2, y_1, y_2값을 이용하여 첫번째 식으로부터 a와 a+U값을 얻은 후 사용자 아이디인 U 검출.

3. 전자상거래 관련 기술

지금까지 살펴본 전자 화폐 시스템 및 전자 신용카드 거래 시스템은 실생활의 상거래 시스템보다 나은 편리성 및 안전성을 확보하기 위하여, 네트워크 기술, 암호 기술, 그리고 인증 기술을 필요로 한다.

3.1 네트워크 기술

(1) 월드와이드웹 보안

통신망을 이용한 전자상거래는 대부분 웹을

기반으로 이루어진다. 웹은 하이퍼텍스트를 기반으로 뛰어난 사용자 인터페이스를 제공하기 때문에 널리 산재한 인터넷의 자원(resource)들을 효율적으로 검색할 수 있도록 해주고, 상업 도메인에서는 웹이 제공하는 멀티미디어 기능을 활용하여 자사의 상품을 효과적으로 표현하여 사용자에게 실생활의 쇼핑몰과 유사한 효과를 제공한다.

이와 같은 웹을 전자상거래에 활용하기 위해서는 상거래시 전송되는 민감한 정보에 대한 안전성을 확보해야만 한다.

① 웹의 보안상의 문제점

- 웹 구조상의 문제점

  웹은 기본적으로 암호화 기능을 포함하고 있지 않으며, 프로토콜의 구조상 메세지를 암호화하기 어렵다. 특히 응용 계층에서 구현되어있는 웹은 기본적으로 IP spoofing에 대한 대책이 없으며 사용자 인증을 위한 패스워드마저도 단순한 스크램블 기법만으로 전달하도록 한다. 웹은 구조상으로 볼 때 정보 암호화, 접근 제어, 디지틀 서명 기법을 제공하고 있지 않으며, 인증 기법만이 제공되나 그 기능이 매우 미약하다. 따라서 웹을 그대로 이용할 경우 중요한 문서의 유통 및 전자 상거래에는 부적합하다.

- 웹 브라우저의 문제점

  웹 브라우저는 인터네트상에서 가장 크고 정교한 프로그램이라고 할 수 있으며, 하이퍼 텍스트를 근간으로 구성되어 매우 복잡한 구조를 갖는다. 특히 브라우저는 HTTP 프로토콜뿐만이 아닌 다양한 프로토콜 및 형식을 지원하도록 하는 다기능 프로그램이다. 따라서 복잡한 프로그래밍에서 야기되는 보안 홀(Security Hole)이 있을 수 있으며, 이것은 침입자에게 악용될 여지가 많다. 특히 최근에는 브라우저가 다른 외부 응용 프로그램과 연결되어 실행되므로 여기서 비롯되는 많은 문제들은 정보의 보안에 있어서 심각한 위험을 가져온다. 일종의 플러그-인 기법이나 MIME helper 기능을 통하여 제공되는 외부 응용 프로그램과의 연결은 다양한 형식의 정보를 처리할 수 있다는 장점을 제공하는 반면, 침입자에 의해서 악용될 우려가 있는 것이다.

② 현재 개발된 웹 보안 기술

웹 보안 기술은 웹 서버들이 기본적으로 제공하는 보안 기능 외에, 보안 메카니즘이 제공되는 계층에 따라 응용 계층에서의 보안과 네트워크 계층에서의 보안으로 나뉜다.

- 기본적인 웹 보안 기능
  - 기본인증(Basic Authentication)

    사용자 인증이라고도 불리우는 이 메카니즘은 HTTP의 한 부분으로서 초기부터 제공되었으며, 사용자에게 익숙한 사용자/패스워드 형태로 비교적 약한 인증 기능을 제공한다. 기본인증은 단순한 반면 관리가 어렵고 패스워드가 평문형태로 전달되므로 불안전하다.
  - IP 필터링(filtering)

    대부분의 웹 서버에서 제공되며, 기본인증과 혼용될 수 있다. 관리가 쉬운 반면, IP spoofing에 대한 대책이 없다.
- 응용 계층에서의 웹 보안
  - NCSA Mosaic/httpd의 PGP/PEM 인증 및 암호화

    NCSA의 XMosaic과 httpd에 메세지 암호화와 서명을 처리하는 외부 프로그램을 실행할 수 있도록 기능이 추가한 예이다. 즉, PGP(Pretty Good Privacy)나 PEM(Privacy Enhanced

Mail) 같은 독립적인 암호화 응용 프로그램과 연결하여 인증 및 암호화를 제공한다.

- EIT의 Secure-HTTP

EIT(Enterprise Integration Technologies)에서 개발된 S-HTTP는 기존 HTTP 프로토콜에 보안 기능을 추가한 확장 버전이다. S-HTTP는 DES, RC2, RC4, IDEA 등의 관용 암호화 방식과 RSA, DSS 등의 공개키 암호화 방식, 그리고 MD2, MD5, SHS 등의 해쉬 알고리즘과 같은 다양한 암호화 알고리즘을 지원하며 앞서 설명한 바 있는 NCSA의 방법과 유사하다.

- Message Digest Authentication

메시지 다이제스트 인증은 기본 인증을 간단히 대치하기 위한 것으로 패스워드가 평문의 형태로 전달되지 않도록 성능을 개선하였다. 즉, 일방향 해쉬 함수를 이용하여 패스워드를 암호화하여 보내도록 한다.

- Kerberized Mosaic/httpd

커베로스(Kerberos)는 이미 네트워크 보안을 위해서 다양하게 적용되고 있는 프로그램이다. 특히 안전한 제3자의 개념을 이용하여 비교적 안전한 보안 시스템을 구축하도록 하고 있다. 그러나 넓은 범위를 갖는 영역에서 적용하기 어렵다는 단점이 있다. 이 커베로스의 티켓 개념을 웹에 응용하도록 하는 예가 있다.

• 네트워크 계층에서의 웹 보안

- Netscape's Secure Socket Layer(SSL)

웹의 보안을 개선하기 위해서 가장 최근에 시도되고 있는 방법이 바로 네트스케이프사의 SSL이며 이것은 인터네트 전반에 걸쳐 다양한 응용에서도 시도되고 있다. 주 아이디어는 웹 프로그램이 상주하는 응용 계층에서 메세지를 암호화하여 불안전한 채널로 전송하는 대신에, 응용 계층은 안전한 채널을 설정하도록 하는 특수한 소켓 루틴만을 이용하고 어떠한 데이터라도 안전한 채널을 통해서 전송하도록 하는 데에 있다.

(2) JAVA 보안 기술

사용자에게 정적인 환경을 제공해주는 HTML을 보강하고자 Sun Microsystems에서 발표한 JAVA는 바이트코드(byte code)라는 형태로 응용프로그램을 전송하여 보다 동적인 웹 사용자 환경을 제공해 주는 기술이다. JAVA는 현재 개발자들을 위하여 JDK(JAVA Development Kit)라고 불리는 개발자 라이브러리를 제공하고 있으며 1997년 4월에 발표된 JDK 1.1.1은 JAVA Security API와 JAVA Commerce API를 포함하고 있다.

① JAVA Security API

JAVA Security API는 JDK 1.1에 포함된 core API의 하나로서, 기본적인 암호화 기능, JAVA와 관련된 시스템 보안, 그리고 분산 컴퓨팅 환경에서의 보안 기능 등을 제공한다. 특히 JAVA Security API에는 차후 개발될 새로운 암호화 알고리즘을 수용할 수 있도록 유연한 프레임워크를 가지고 있다.

JAVA Security API가 제공하는 주요 기능은 다음과 같이 요약할 수 있다.

• 디지털 서명

DSA 등의 디지털 서명 알고리즘을 제공하며, 서명을 위한 공개키 및 비밀키 생성, 임의의 디지털 데이타의 서명 및 검증 기능을 제공한다.

• 메시지 다이제스트

MD5, SHA-1 등과 같은 암호학적으로

안전한 메시지 다이제스트 알고리즘을 제공하여 데이터에 대한 디지털 핑거 프린트를 생성한다.

- 키관리
  개인 또는 그룹의 키들 생성하여 인증서를 생성, 관리한다. JDK에서 관리하는 인증서 시스템은 X.509 버전 3의 일부를 수용한다.
- 접근 제어 리스트
  통신망 상의 자원에 대한 사용자의 접근을 제어하며, 프로그래머에게 고차원적인 시각(high-level overview)을 제공한다.

② JAVA Commerce API

JECF(JAVA Electronic Commerce Framework)라고 불리며, 인터넷 상에서 보다 안전한 상거래를 지원하기 위하여 개발되었다. JECF는 JAVA Security API를 이용하여 구축되며 JAVA 애플릿(applet)을 통하여 상품 및 거래정보 content를 안전하고 효율적으로 전송하는 것을 목적으로 한다.

JECF를 이용한 전자상거래에서는 다음과 같은 개체들이 보다 용이하게 상거래 환경을 구축하도록 도와준다.

- JAVA Wallet
  JECF를 이용한 상거래 환경에서 클라이언트 측의 트랜잭션을 담당하는 소프트웨어이다. 사용자에게 그래픽 사용자 환경을 제공해주고 Wallet 데이터베이스를 이용하여 상거래 트랜잭션을 처리한다.
- JAVA Cassettes
  상점에서 처리 가능한 전자상거래 프로토콜을 제공하는 패키지로서, 상거래를 제공하는 상점에 의하여 분배된다. Cassette는 JAVA Commerce Toolkit을 사용하여 생성시키며, 상점과 클라이언트들에게 초기에 분배된다. SET 프로토콜을 비롯한 신용카드를 이용한 전자상거래 프로토콜뿐만 아니라 전자 화폐를 이용한 프로토콜을 수용할 수 있다.
- JAVA Shopping Cart
  JECF를 이용한 전자상거래에 참여하는 사용자가 상품에 대한 지불 이전에, 원하는 상품에 대한 정보를 전달하기 위한 애플릿이다.

3.2 암호 기술

본 절에서는 전자 화폐 시스템에서 요구되는 주요 암호화 관련 알고리즘을 간략히 설명하도록 한다. 요구되는 알고리즘으로는 메시지의 무결성을 보장하기 위한 해쉬 알고리즘과, 메시지의 비밀성을 보장해 주기 위한 대칭키 및 공개키 암호화 알고리즘이 있다.

(1) 해쉬 알고리즘

메시지의 무결성을 제공하기 위해서, 원래의 메시지를 입력값으로 하여 일방향으로 작은 값을 만드는 알고리즘이다. 이 값은 collision-freeness 및 일방향의 성질을 가질 수 있어야 한다.

MD5 메시지 다이제스트 알고리즘과 SHA(Secure Hash Algorithm)는 현재 가장 널리 사용되고 있는 해쉬 알고리즘이다. 대표적인 전자신용카드 거래 시스템인 SET 프로토콜에서는 일방향 해쉬 알고리즘으로서 SHA를 사용한다.

SHA는 NIST(National Institute of Standards and Technology)에서 개발하였고, 1993년 FIPS PUB 180(Federal Information Processin Standard)로 공포되었다. 설계는 MD5의 전신인 MD4 알고리즘에 기반을 두고, 설계는 MD4와 유사하게 모델화하였다. SHA

는 SET 프로토콜 및 JAVA Security API에서 기본 해쉬 알고리즘으로 사용된다.

다음 표는 대표적인 해쉬 알고리즘인 MD5와 SHA를 비교한 표이다.

표 1 SHA와 MD5의 비교

	MD5	SHA
다이제스트 길이	128 비트	160비트
처리의 기본 단위	512 비트	512 비트
단계 수	64(16번의 4라운드)	80
최대 메시지 크기	INF	264 비트
기약 논리 함수	4	3
덧셈 상수	64	4

(2) 대칭키 암호화 알고리즘

비밀키 암호화 방식 혹은 관용 암호화 방식으로 알려져 있으며, 암호키와 복호키가 같은 암호화 알고리즘이다. 따라서 전송자와 수신자는 같은 키를 공유할 수 있어야 한다. 이것을 키 분배 혹은 키 교환이라고 한다.

현대 블록 알고리즘으로 가장 널리 알려져 있는 대칭키 알고리즘은 DES이며 SET 프로토콜을 비롯한 전자상거래 프로토콜에서는 기본적인 대칭키 알고리즘으로 DES를 사용한다. DES는 64비트의 키를 입력받아 64비트 블록을 16 라운드에 거쳐서 암호화를 수행한다.

(3) 공개키 암호화 알고리즘

비대칭 암호화 방식으로 알려져 있으며, 암호키와 복호키가 하나의 쌍을 이루는 암호화 알고리즘이다. 따라서 암호화와 복호화에 다른 키가 사용되게 되며, 암호화를 위한 공개키에는 비밀성이 보장될 필요가 없다. 그러나 복호화를 위한 비밀키에 대해서는 반드시 비밀성이 보장되어야 한다.

공개키 암호화 알고리즘 중 산업계의 표준으로 사용되고 있는 RSA는 1978년 Rivest, Shamir, Adleman이 제안한 암호 시스템이다. 이 알고리즘은 매우 큰 정수의 소인수 분해가 어렵다는 가정하에서 설계된 것이다.

공개키 암호화 알고리즘을 사용하여 구축된 전자상거래 프로토콜은 일반적으로 RSA사에서 제안한 공개키 표준안(PKCS)을 따른다. 특히 PKCS #7에는 암호화된 데이터(encrypted data), 서명된 데이터(signed data), 다이제스트 데이터(digested data), 봉인된 데이터(enveloped data) 등이 정의되어있으며, 데이터들은 알고리즘 식별자(algorithm identifier)가 가리키는 암호화 방식으로 처리된다.

(4) 디지틀 서명 알고리즘

메시지의 무결성과 인증을 제공하기 위해서 공개키 암호화 알고리즘을 이용하여 서명하도록 하는 알고리즘이다. 메시지 다이제스트(해쉬 함수 처리)를 통해서 만들어진 메시지에 대한 작은 값을, 감추어진 비밀키를 사용해서 암호화하며 이것이 서명에 해당된다. 그러면

다른 사용자가 공개키를 이용해서 복호화할 수 있으며 마찬가지로 메지지의 해쉬값을 서로 비교하여 서명을 확인하도록 한다.

(5) 이중 서명 알고리즘

이중 서명 알고리즘은 전자 신용카드 거래 시스템인 SET 프로토콜에서 사용되는 알고리즘으로서 고객의 사생활 침해을 방지하기 위하여 도입된 것이다. 이것은 두 개의 메시지를 한번의 서명 처리 수행을 통해서 함께 서명하도록 하는 알고리즘이다. 두 개의 메시지의 해쉬값을 각각 구한 후, 두 해쉬값에 대한 해쉬값을 다시 구한다. 이 값을 기존의 서명 알고리즘으로 서명한다. 이 방식은 카드 소지자가 상점에게만 주문 메시지를 전달하고 상점을 통하여 금융 기관에게만 지불 명령을 전달하려고 할 경우 이용된다. 지불 명령에는 카드 사용자의 계정 정보가 포함되어 있다.

3.3 인증 기술

통신망을 통한 전자상거래의 모든 주체는 트랜잭션 이전에 상호간의 인증 작업을 거쳐야 한다. ITU-T 권고안 X.509는 개방시스템에서의 인증 프레임워크를 기술하고 있는데, 인증을 크게 단순인증과 강한 인증으로 구분 제시하고, 공개키 기반 프로토콜에서 주로 사용되는 인증서를 기술하고 있다. 본 절에서는 인증서에 대하여 설명하도록 한다.

(1) 인증서의 정의

인증서란 사용자(인증서의 소유자)의 믿을 만한 공개키를 의미하는 것으로서 믿을 수 있는 공인 기관에서 사용자의 인증서를 보장해 준다. 인증서에는 단순히 공개키 정보만 존재하는 것이 아니라 인증서의 소유자를 인증하는데 필요한 기타 정보들이 인증서를 발급한 인증 기관의 서명키로 서명되어 있다. 이러한 인증서는 다음과 같은 특징을 가진다.

- ◆ 인증서를 발급한 인증 기관의 공개키에 접근이 가능한 모든 사용자들은 인증된 사용자(인증서의 소유자)의 공개키를 인증서로부터 얻을 수 있다.
- ◆ 인증서를 발급한 기관을 제외한 어떠한 곳도 인증서를 수정할 수 없다.

ITU-T에서는 디렉토리 서비스를 정의한 X.500 계열의 일부로 X.509 인증서 메커니즘을 인증 서비스를 위해 권고하고 있다. 디렉토리란 사용자 정보 데이터베이스를 유지 및 관리하는 분산된 서버 혹은 서버들의 집합이라고 할 수 있으며 X.509는 X.500 디렉토리에 기반을 두고 인증 서비스를 수행하는 프레임워크를 정의한 것이다. 이때 디렉토리는 공개키 인증서가 존재하는 저장소로서의 기능을 한다.

Version
Serial Number
Algorithm
Parameters
Issuer
Not before
Not after
Algorithm
Parameter
Key
Signature

그림 1 X.509 인증서의 구성

X.509의 핵심은 각 사용자들에 관련된 공개키 인증서에 관한 것으로 인증서는 신뢰할 수 있는 인증기관에 의해 생성되어 인증기관 혹은 사용자에 의해 X.500에 기반한 디렉토리에 저장된다. 다음은 인증서의 일반적인 형식이다.

그림 1에서 보이는 기본적인 인증서의 구성요소들을 설명하면 다음과 같다.

- Version : 인증서 형식의 버젼. 기본값은 1988년의 버젼 1
- Serial Number : certificate를 발급한 인증기관 (CA)에 대해서 유일하게 할당된다
- Algorithm Identifier : certificate를 sign한 알고리즘, 관련 파라메터
- Issuer : 인증서를 발급하고 서명한 인증기관
- Period of validity : not before, not after
- Subject : 사용자 주체
- Public-key information : 주체의 공개키, 키가 사용되는 암호 알고리즘의 식별자이다.
- Signature : certificate의 나머지 필드들에 대한 해쉬값. 인증기관의 공개키로 암호화 한다.

(2) 인증서의 확인 및 사용

인증서는 위조될 수 없기 때문에 인증서가 저장되는 디렉토리에 대한 특별한 보호 장치가 필요하지 않다. 만약 모든 사용자가 동일한 인증기관에 가입되어 있다면 하나의 공통적으로 신뢰 가능한 인증기관이 존재한다는 의미가 된다. 하지만 다양한 사용자 계층이 존재하는 현실에서는 모든 사용자가 동일한 인증기관에 가입되는 것은 현실적이지 못하다.

인증기관의 서명이 들어있는 인증서를 검증하기 위해서 각 사용자는 반드시 인증기관의 공개키를 보유하고 있어야 한다. 이때 공개키는 절대적으로 안전한 방법으로 각 사용자에게 제공되어야 한다.

만약 A는 인증기관 X1으로부터 그리고 B는 인증기관 X2로부터 각각 인증서를 발급 받았다고 가정하고, A가 X2의 공개키를 알지 못한다면 X2에 의해서 발급된 B의 인증서는 사용할 수 없게 된다. 즉 A는 B의 인증서를 읽을 수는 있지만 A는 B의 인증서를 검증하지는 못한다. 하지만 만약 두 인증기관이 서로의 공개키를 안전하게 교환 하였다면 다음과 같은 시나리오로 A는 B의 공개키를 얻을 수 있다.

◆ A는 X1에 의해 서명된 X2의 인증서를 얻는다. A는 X1의 공개키를 알고 있기 때문에 X1이 서명한 인증서로부터 X2의 공개키를 검증할 수 있다.

◆ A는 X2의 공개키를 이용하여 X2가 서명한 B의 인증서를 얻을 수 있다.

4. 결 론

본 논문에서는 최근 활발히 연구되고 있는 전자상거래 기술들과 이를 뒷받침하고 있는 기반 기술들을 살펴보았다. 특히 전자상거래 분야 중 협의의 개념인 전자 신용카드 거래 프로토콜과 전자 화폐 프로토콜을 고찰하고, 이러한 시스템의 구축에 필요한 웹 보안 기술, JAVA 보안 기술, 암호 기술, 그리고 인증서로 대표되는 인증 기술을 자세히 고찰하였다.

앞으로 우리나라가 세계시장에서 국제 경쟁력을 확보하기 위해서는 전자상거래의 기반 기술인 암호기술 및 인증기술을 확보하고, 전 분야에서 전자상거래를 빠른 시일내에 도입, 이를 확산시키기 위한 범 국가적인 대책 마련이 시급하다고 하겠다.

참 고 문 헌

[1] M. A. Sirbu, "Credits and debits on the internet," IEEE Spectrum, Feb. 1997

[2] Scott Hamilton, "E-Commerce for the 21st Century," IEEE Computer, Vol.30, No.5, May 1997

[3] 임춘성, "전자상거래 개관," 월간자동인식기술, Vol.2, No.9, 1997.9

[4] VISA International, "The Keys to Safe Shopping," http://www.visa.com/cgi-bin/vee/sf/set/setsafe.html, May 1997

[5] "Secure Electronic Transaction - Book 1 : Business Description," Ver. 1.0, VISA International, May 1997

[6] "Secure Electronic Transaction - Book 2 : Programmer's Guide," Ver. 1.0, VISA International, May 1997

[7] Sun Microsystems Inc., "Java Electronic Commerce Framework Architectural Overview," http://java.sun.com/ products/commerce/jecf_arch.htm, Dec. 1996

[8] Arthur Coleman, "Java Commerce : A Business Perspective," JavaSoft, http://java.sun.com/products/commerce /jecf_arch.htm, Dec. 1996

[9] T. Okamoto, K. Ohta, "Universal Electronic Cash," Advances in Cryptology, Proceedings of Crypto 91, 1991

[10] S. Brands, "Untraceable Off-Line Cash in Wallet with Observers," Advances in Cryptology, Proceedings of Crypto 93, 1993

[11] D. Chaum, A. Fiat, M. Naor, "Untraceable Electronic Cash," Advances in Cryptology, Proceedings of Crypto 88, 1988

[12] William Stallings, "Network and Internet Security," Prentice Hall, 1995

[13] Adam Cain, "Introduction to Web Security," NCSA, 1995

[14] A. Schiffman, "The Secure Hypertext Transfer Protocol," Internet Draft, 1994

□ 著者紹介

강 명 호

1992년 2월 연세대학교 컴퓨터과학과 이학학사
1995년 2월 연세대학교 컴퓨터과학과 이학석사
1995년 3월 ~ 현재 연세대학교 컴퓨터과학과 박사과정 재학중

※ 주관심 분야 : 컴퓨터 통신망 보안, 암호학, PCS, 지능망 시스템, EDI 시스템

송 주 석

1976년 2월 서울대학교 전기공학과 학사
1979년 2월 한국과학원 전기 및 전자공학과 졸업 석사
1988년 8월 Univ. of. California at Berkeley 전산과학과 석사
1979년 2월 ~ 1982년 한국전자통신연구원 전임연구원
1988년 9월 ~ 1989년 2월 Naval Postgraduate School Information System Department 조교수
1989년 3월 ~ 현재 연세대학교 컴퓨터과학과 교수