通信情報保護學會誌
第9券 第3號, 1999. 09

금융분야의 인증시스템 구축 및 서비스 계획

김 상래*

요 약

정보통신 기술의 발달로 사회의 모든 분야에서 인터넷의 활용이 급속히 확산되어 전자 결제, 전자상거래, 인터넷뱅킹 등의 편리한 서비스가 제공되고 있다. 그러나 인터넷을 이용한 여러 종류의 거래는 거래 당사자간 비접촉·비대면을 특징으로한다. 이러한 특징이 편리함을 제공하는 반면 거래당사간의 상호신뢰에 있어서 취약하다는 문제점을 가진다. 이 문제점을 해결하기 위해 정부는 전자거래기본법, 전자서명법 등 법적·제도적 장치를 마련하여 "공인인증" 제도를 도입하였으며 이에 부응하여 금융결제원은 금융분야 공인인증기관으로 인증서비스를 제공하기 위해 준비중이다.

본고에서는 금융결제원의 인증서비스의 추진원칙,인증서비스 제공을 위한 시스템 구축, 인증서를 이용한 서비스에 대한 부분으로 나누어 서술한다. 인증서비스의 추진원칙은 1999년 내에 공인인증기관 지정획득을 하고 IETF의 PKIX 표준안, RSA의 PKCS 표준안, OpenGroup의 CDSA 표준안을 충실히 따르는 인증시스템을 일괄 개발한다. 인증서비스 제공을 위한 시스템 구축은 최상위 인증기관인 전자서명인증관리센타에서 제시한 기본원칙을 충실히 따르며 금융분야 인증서비스를 위해 알맞게 변경하여 구축한다. 금융결제원이 발행한 인증서는 인터넷 뱅킹과 전자상거래등에 이용된다.

Ⅰ. 서 론

정보통신 기술의 발달로 인하여 정부기관, 기업체, 연구소 등 사회의 모든 분야가 컴퓨터 네트워크로 연결되고 이것의 활용 또한 급격하게 확대되고 있다. 예를 들면 인터넷을 통해서 은행에 직접나가지 않고도 계좌이체나 대출신청 같은 은행 업무를 할 수 있다든가, 매장에 나가는 번거로움 없이 물건을 구매할 수 있는 등의 다양한 서비스가 개발되고 있다.

그러나 인터넷을 이용한 거래는 기존의 거래와는 달리 거래 당사자간 비접촉·비대면의 특징을 바탕으로 하고 있으며 이러한 특징이 편리성이라는 장점을 제공하는 반면에 상호신뢰에 대한 보장이 기존 제도에 비해서 취약할 수 밖에 없는 단점을 가지고 있다.

이러한 장애 요인으로 인터넷을 이용한 은행과 공공기관 등의 업무 활성화와 실용화는 한계에 부닥칠 수 밖에 없다. 이에 정부에서는 전자거래 활성화의 주된 장애 요소를 제거하고 이의 보급을 촉진하기 위하여 거래 당사자와 거래자체의 신뢰성과 안정성을 보장하기 위한 전자서명법과 전자거래기본법등 법적·제도적 장치를 마련하였다.

이에 부응하여 금융결제원은 한국정보보호센터를 중심으로 한 국가 공인인증체계에서 금융분야 공인인증기관으로서 만반의 준비를 다하고 있다.

본고에서는 금융결제원의 인증서비스 추진원칙과 인증서비스를 제공하기 위한 시스템 구축 및 인증서를 이용한 서비스에 대하여 알아본다.

Ⅱ. 추진 원칙

금융결제원의 금융분야 인증서비스 추진 원칙은 다음과 같다.

* 금융결제원 전자금융연구소 소장

첫째, 국가 정보보호정책 및 추진체계를 준수하고 금융전산망 보안시스템 개발체계에 따른 보안 수준을 유지함은 물론 정부의 정책 취지를 적극적으로 뒷받침할 수 있도록 1999년 내에 공인인증기관 지정을 획득하고 인증업무를 실시할 수 있도록 한다.

둘째, 인증시스템 구축은 공인인증기관 지정요건 및 기준에서 요구하는 신뢰성·보안성·효율성 등을 확보할 수 있도록 금융전산망 보안시스템 개발체계에 따라 개발함은 물론 금융기관의 개발 및 비용 부담을 최소화할 수 있도록 인증시스템 뿐만 아니라 등록관리시스템과 사용자 소프트웨어까지 일괄적으로 개발하며 국제 거래도 수용할 수 있도록 호환성과 확장성을 확보한다.

셋째, 금융기관 고유영역인 고객 신용관리 기능에 기반한 관련 업무를 금융기관이 스스로 수행할 수 있도록 금융기관과의 역할을 적절하게 분담하고 이를 활용한 금융기관의 다양하고 새로운 전자금융서비스 및 상품 발굴을 적극적으로 지원한다.

넷째, 전자금융거래 내용의 무결성, 거래당사자의 신원확인, 거래 사실의 부인봉쇄 등을 제공하는 전자서명용 인증서 뿐만 아니라 거래내용의 기밀성도 보장할 수 있는 암호용 인증서를 병행 발급하여 완벽한 전자금융 정보보호 서비스를 제공할 수 있도록 금융분야의 공개키 기반구조를 구축한다.

Ⅲ. 시스템 구축 및 서비스 계획

1. 시스템별 세부 구축 계획

1.1. 기본원칙

금융결제원의 금융분야 인증서비스 시스템 구축 기본 원칙은 다음과 같다.

첫째, 엄격한 다단계 역할 기반 접근 통제를 하여 인증서비스 시스템을 보호한다.

둘째, 네트워크 침입차단 및 침입탐지 체계를 구축하여 인증 서비스 시스템을 운영하는 네트워크를 보호한다.

셋째, 키 생성 및 인증서 생성·관리시스템 등 중요 시스템은 오프라인 또는 편도 라인으로 구축한다.

넷째, 키 생성 시스템, 인증서 생성·관리시스템, 디렉토리 시스템, 시점확인 시스템으로 구성되는 핵심 인증시스템을 이중화하여 운영한다.

1.2 시스템 및 네트워크 구성도

인증기관의 시스템은 키생성 시스템, 인증서 생성·관리 시스템, 디렉토리 시스템, 시점 확인 시스템, 웹시스템, 등록관리시스템으로 구성된다. 그림 1은 인증기관의 전체적인 시스템과 네트워크 구성도를 나타낸다.

그림 1에서 보듯이 인증기관은 공인인증기관에 위치한 시스템과 금융기관에 위치한 등록관리 시스템으로 나눌수 있으며 공인인증기관에 위치한 시스템과 금융기관에 위치한 시스템 사이의 네트워크 보안을 위해 현재의 금융 공동망을 이용한다. 공인인증기관에 위치한 시스템 사이의 네트워크는 시스템 구축 기본원칙에 따라 키생성 시스템은 오프라인으로 하며 인증서 생성·관리 시스템과 디렉토리 시스템 및 시점확인시스템 사이는 편도라인을 이용하여 네트워크를 보호한다.

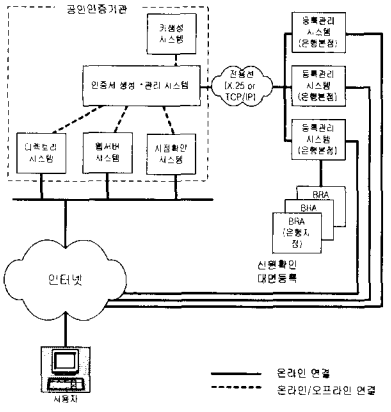

그림 1. 인증기관의 시스템과 네트워크 구성도

1.3 적용 표준

금융결제원의 금융분야 인증서비스 제공을 위해 적용하는 표준은 IETF의 PKIX(public key infrastructure (X.509))[1][2][3][4], RSA의 PKCS(public key cryptography stradard)[5][6][7], OpenGroup의 CDSA(common data security architecture)를 따른다.

IETF의 PKIX는 PKI에 대한 구조, 인증서에 대한 프로파일, 인증서를 처리하는데 사용되는 프로토콜 등을 대상으로 표준화한 문서이며 RSA의 PKCS는 여러 분야에서 공개키를 사용할 수 있도록

RSA사를 중심으로 만든 표준안이다. 또한 CDSA는 Intel, RSA, IBM 등의 업체가 중심이 되어 1998년 초에 표준으로 확정하였으며 다양한 환경과 요구 사항을 수용하기위한 알고리즘의 다이나믹한 링크 기능이 주요한 특징을 가진다.

이러한 표준들을 금융분야 인증서 서비스에 적용한 분야는 표 1과 같다.

표1. 분야별 적용 표준

분야	적용 표준
◦ 전자서명 알고리즘	- KCDSA - RSA(PKCS #1)
◦ 인증서 규격	- X.509v3 ※확장필드 · authority key identifier · subject key identifier · key usage · private key usage period · certificate policies · subject alternative name · issuer alternative name · Name constraints · Policy constraints
◦ 인증서 폐지목록 규격	- X.509v2
◦ 인증서 효력정지 목록 규격	- X.509v2 활용
◦ 인증서신청 요구 규격	- PKCS #10
◦ 디렉토리 규격	- LDAP 디렉토리
◦ 인증기관과 사용자 프로그램 사이의 통신	- RFC 2510
◦ 사용자 프로그램	- CDSA
◦ 해쉬 알고리즘	- SHA-1(PKCS #1) - HAS-160

1.3 시스템별 세부 구축 계획

1) 키 생성 시스템

전자서명용 인증서와 암호용 인증서를 발행하기 위한 키를 생성하는 시스템이다. 키 생성 시스템에서는 공개키와 개인키 생성시 문제가 발행할 것을 대비하여 키의 백업과 복구 기능을 지원한다. 키 복구시 몇 사람이 모여야만 키를 복구할 수 있는 비밀분산 기능을 지원한다. 이 시스템의 주요 기능은 아래와 같다.

- 인증기관 공개키/개인키 쌍 생성 및 백업/복구 기능
- 스마트 카드 관리
- 비밀 분산(secret sharing) 기능
- 운영 내역 기록 관리 기능

2) 인증서 생성·관리 시스템

인증서 생성·관리 시스템은 인증시스템의 핵심 구성요소로 인증서 발급, 갱신, 정지, 폐지, 폐지목록 게시 등의 인증서에 관한 처리를 담당한다. 이 시스템에서는 가입자 키쌍을 생성하는 이유는 키 생성 시스템이 오프라인이므로 효율적인 인증서 생성을 위해 가입자 키 쌍을 생성한다. 이 시스템의 주요 기능은 아래와 같다.

- 인증서 생성 발급/취소/정지/폐지 게시 기능
- 가입자 키쌍 생성/갱신 기능
- 가입자 키관리용 키쌍 생성 및 복구 기능
- 폐지/정지 목록 생성 및 게시 기능
- 상호인증 및 게시 기능
- 사용자 엔트리 생성 기능

3) 시점확인 시스템

GPS로부터 표준 시간을 수신하여 시점 확인을 요구하는 사용자의 요청에 따라 시점확인 서비스를 제공한다. 이 시스템의 주요 기능은 아래와 같다.

- 인증서 생성 시점 확인 기능
- 전자문서 제출 시점 확인 기능

4)디렉토리 시스템

디렉토리 시스템은 글러벌한 디렉토리 서비스 모델인 LDAP(Lightweight Directory Access Protocol 기반으로 한다. 이러한 LDAP를 이용하여 가입자에게 인증서 및 인증서 유효 검증을 위한 상태 정보 등을 실시간으로 검색할 수 있도록 한다. 이 시스템의 중요한 기능은 아래와 같다.

- 인증서 저장 및 검색 기능
- 폐지/정지 목록 저장 및 검색 기능

5) 웹 시스템

인증서 사용자에게 필요한 여러 정보를 제공하며 주요 기능은 아래와 같다.

· 인증기관 홈페이지 운영 기능
· 사용자 S/W 배포 기능

6) 등록관리 시스템

등록관리 시스템은 인증서를 발행하는 인증기관과 인증서를 발급받는 사용자 사이의 중간 매개체 기능을 수행하며 가입자의 인증서 발급신청 접수 및 신원확인, 인증서 신청/정지 및 폐지 등의 승인 및 거부 권한을 가진다. 이 시스템의 주요 기능은 아래와 같다.

· 가입자 등록 요청/폐지 수신 기능
· 가입자 등록 정보 기록/관리 기능
· 인증서 발급 요청 기능
· 가입자 속성정보 조회 및 속성변경 요청 기능

7) 사용자 소프트웨어

사용자 소프트웨어는 인증기관에 발급된 인증서를 사용하여 메시지를 암호화하고 전자서명을 다룰수 있도록한 사용자 모듈이다. 이 소프트웨어의 주요 기능은 아래와 같다.

· 전자서명키 생성 기능
· 전자서명 생성 및 검증 기능
· 공개키/대칭키 암복호 기능
· 전자서명생성키의 안전한 보관
· 인증서 발급, 갱신, 정지, 폐지 요청기능
· 인증서 인수 기능
· 인증서 검증 기능
· 시점 확인 관련기능
· 폐지/정지목록 다운로드 기능
· 스마트카드 관리

2. 인증 업무

금융결제원의 금융분야 인증서비스 인증 업무는 인증서를 발급하는 인증기관, 인증서를 발급 받는 사용자 프로그램, 가입자 등록을 대행하는 등록기관 사이에서 이루어지며 주 업무는 인증서 발급, 인증서 갱신, 인증서 폐지로 나눌 수 있다.

2.1 인증서 발급

인증서 발급은 지역적으로 분산된 등록기관에 가입자가 방문하여 인증서 발급을 신청하면서 사용자 소프트웨어를 교부 받는다.

인증서 발급 신청시 등록기관은 국가·지방자치단체가 발급한 증명서(대면 확인시 대조 가능한 것) 혹은 법인의 대리인과 같이 자격·신분의 확인이 가능한 증명서를 이용하여 신원확인을 한며 사용자 소프트웨어를 교부한다.

인증서 발급절차에 따라 신원확인을 통과한 가입는 신청 등록시 교부 받은 사용자 소프트웨어를 이용하여 전자서명키를 생성한 후 인증기관의 웹사이트에 접속한다. 이 때 사용자 소프트웨어는 사용자 확인용 키, 전자서명검증키 및 전자서명한 인증서 발급신청를 전송하며 이 정보를 이용하여 인증기관은 전자서명키 합치여부를 확인한 후 유효한 경우 인증서를 발급한다. 발급한 인증서는 법 제15조 제2항의 규정에 의하여 가입자의 이름, 가입자의 전자서명검증키, 가입자와 금융결제원이 이용하는 전자서명 방식, 인증서의 일련번호, 인증서의 유효기간, 인증기관의 명칭, 인증서의 이용범위 또는 용도를 제한하는 경우에 이에 관한 사항, 가입자가 제3자에 대한 대리권 등을 갖는 경우 이에 관한 사항이 포함된다.

위에서 설명한 인증서 발급의 절차의 예는 그림 2와 같다.

① 가입자는 가까운 금융기관을 방문하여 인증서 발급신청을 한다.
② 금융기관 지점에서는 신청자의 신분과 개인정보를 확인한다.
③ 신원확인 후 적합할 경우 본점으로 등록 요청을 한다.
④ 본점은 인증기관에게 사용자 등록 요청을 한다.
⑤ 인증기관은 요청된 사용자를 등록한다.
⑥ 인증기관의 접속인증코드를 금융기관 본점을 거쳐 지점으로 전송하며 금융기관 지점은 신청자에게 등록완료통지와 함께 인증기관이 발행한 접속인증코드를 전달한다.
⑦ 가입자는 자신이 사용할 전자서명키를 직접 생성한다.
⑧ 인증기관이 발행한 접속인증코드를 사용하여 인증기관에 접속한다.
⑨ 자신이 생성한 전자서명검증키와 관련 개인정보를 사용하여 인증기관에게 인증서 발급 요청

을 한다. 인증기관은 인증서 발급요청자의 키 암호용 키쌍을 생성하고 전자서명용 키의 인증서와 키 암호용 키의 인증서를 발급한다.

⑩ 발급된 인증서를 디렉토리에 게재한다.

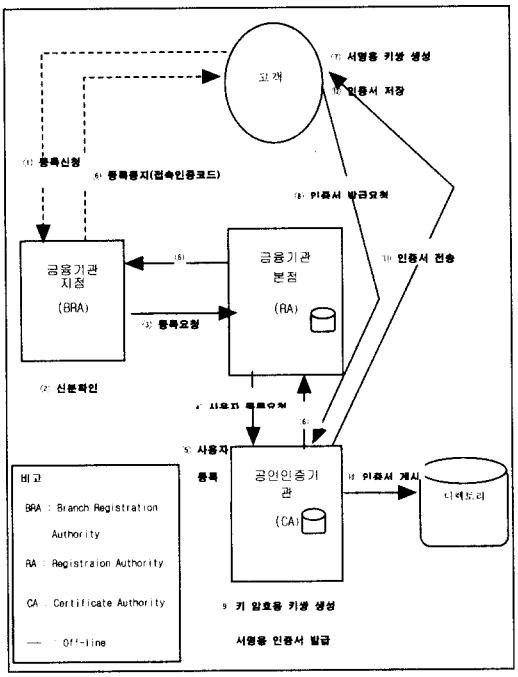

그림 2. 인증서 발급절차

2.2 인증서 갱신

인증서 갱신은 가입자가 인증서내의 정보가 변경된 경우 인증서 갱신발급을 요청하여 인증서를 갱신한다. 이 때 신원확인 절차는 신규발급과 동일한 절차로 신원확인을 하며 인증서가 유효기간중이며 인증서에 포함된 동일한 전자서명검증키를 인증기관에 제출해야 한다. 인증서 갱신 절차의 예는 그림 3과 같다.

① 가입자는 가까운 금융기관을 방문하여 인증서 갱신신청을 한다.

② 금융기관에서는 신청자의 신분과 개인정보를 확인한다.

③ 신분확인 후 적합할 경우 금융기관은 인증기관으로 인증서 갱신 요청을 한다.

④ 인증기관은 금융기관의 요청에 따라 인증서를 갱신한다.

⑤ 변경된 인증서를 게시한다.

⑥ 가입자에게 전송한다.

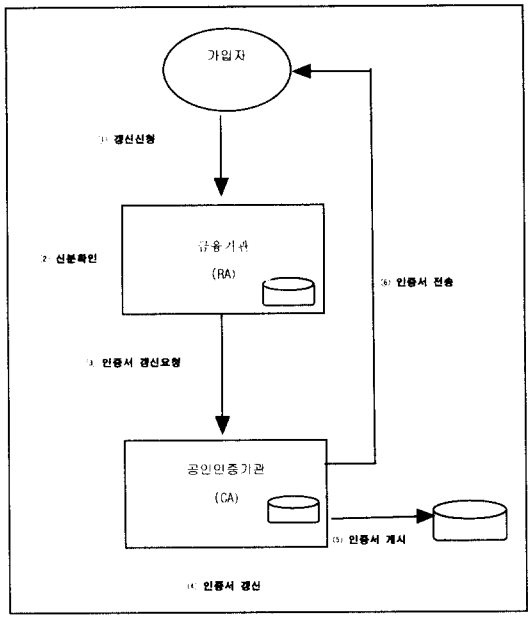

그림 3. 인증서 취소 절차

2.3 인증서 폐지

인증기관이 발급한 인증서는 다음 사유가 발생한 경우 이를 폐지한다.

- 가입자 또는 그 대리인이 인증서 폐지를 신청한 경우
- 가입자가 사기나 위조, 기타 부정한 방법으로 인증서를 발급받은 사실을 인지한 경우
- 가입자의 사망·실종신고 또는 해산사실을 인지한 경우
- 가입자의 전자서명생성키가 분실·훼손 또는 도난·유출된 사실을 인지한 경우

위에 언급한 사항에 해당되면 가입자 혹은 그 대리자는 금융기관을 방문하여 인증서 폐지 신청을 한다. 이 때 신원확인 절차는 신규발급과 동일한 절차로 신원확인을 하며 인증기관은 인증서 폐지 목록을 갱신하고 인증기관관리체계에 의하여 누구든지 그 사실을 항상 확인할 수 있도록 한다. 인증서 폐지 절차의 예는 그림 4와 같다.

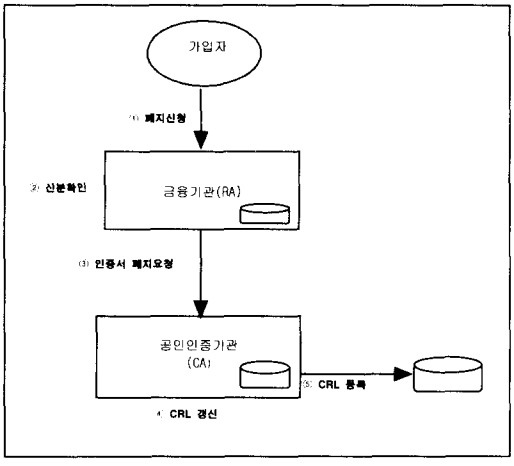

그림 4. 인증서 폐지 절차

① 가입자는 금융기관을 방문하여 인증서 폐지신청을 한다.
② 금융기관에서는 신청자의 신분과 개인정보를 확인한다.
③ 신분확인 후 적합할 경우 금융기관의 RA는 인증기관으로 인증서 폐지 요청을 한다.
④ 인증기관은 금융기관의 요청에 따라 인증서를 폐지한후 폐지목록을 갱신한다.
⑤ 갱신된 폐지목록을 게시한다.

3. 인증서 활용 계획

인증서비스를 이용한 금융권의 활용예로 인터넷 뱅킹에 이용하는 경우와 전자상거래에 이용하는 경우를 들수 있다. 이에 관하여 간략한 예를 들어 설명한다.

3.1 인터넷 뱅킹

고객이 직접 은행창구를 방문하지 않고 영업시간의 제한없이 인터넷을 통한 잔액 및 거래내역조회, 당/타행계좌이체 등 다양한 금융서비스를 이용할 수 있는 서비스를 인터넷 뱅킹이라고 한다. 인터넷 뱅킹을 통하여 고객은 은행에 오가는 시간과 노력을 절감할 수 있고 24시간 내내 어디서나 금융서비스를 받을 수 있는 장점을 가진다. 그러나 인증서에 기반하지 않는 인터넷 뱅킹은 사용자 ID와 암호를 기반으로 하므로 타인이 사용자 ID와 암호를 도청할 수 있는 문제점이 있다. 인증서를 사용하게 되면 인터넷 뱅킹 이용자의 신원확인과 거래내역의 무결성을 확인 할 수 있으므로 안전한 인터넷 뱅킹 서비스를 이용할 수 있다. 인증서 기반의 계좌이체 서비스에 관한 예는 그림 5와 같다.

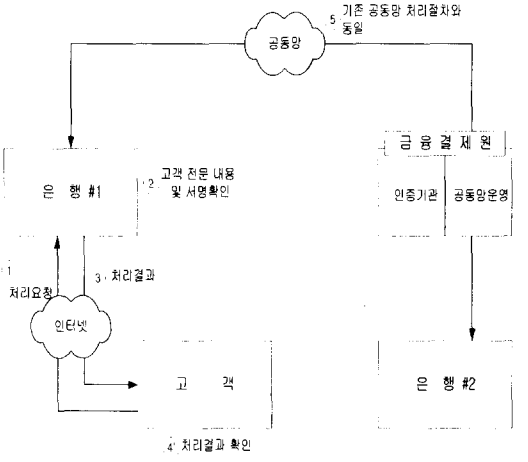

그림 5. 인터넷 뱅킹 이용예

① 고객은 인터넷 뱅킹 사이트에 접속하여 비밀키(#1)를 생성한 후 계좌번호, 비밀번호 등 계좌이체 요청 내용을 전자서명하여 암호화하고 은행#1 인증서 내의 공개키로 비밀키(#1)을 암호화하여 자신의 인증서와 함께 은행으로 전송한다.
② 은행은 자신의 개인키로 복호화 한 비밀키(#1)를 이용하여 고객의 전문을 복호화 하고 고객 인증서내의 고객 공개키를 이용하여 고객서명을 확인한다.
③ 은행은 고객에게 처리결과를 전자서명하여 전송한다.
④ 고객은 은행 인증서를 이용하여 처리결과에 대한 은행의 서명을 확인한다.
⑤ 기존 금융공동망 처리절차에 따라 계좌이체를 처리한다.

2.2 전자상거래에 이용

전자 상거래는 넓은 의미로는 기업이나 소비자가 컴퓨터 통신망상에서 행하는 광고, 발주, 상품과 서비스의 구매 등 모든 경제 활동을 뜻하나 일반적으로 인터넷을 통해 소비자와 기업이 상품과 서비스를 사고 파는 행위를 나타낸다.

고객은 쇼핑몰에 접속하여 쇼핑몰에서 보내온 인

증서를 받아서 SSL 채널을 생성후 신용카드 번호와 유효기간을 쇼핑몰에 넘겨준다. 신용카드 번호와 유효기간을 넘겨받은 쇼핑몰은 카드사 및 VAN사 등의 지급결제기관을 통하여 대금결제를 한다. 이 방법은 고객의 카드번호와 유효기간의 유출 위험을 가지고 있고, 또한 쇼핑몰이 고객의 금융정보를 볼 수 있는 문제점을 가진다. 이 문제점은 고객과 쇼핑몰 및 지급결제기관에서 인증서를 사용하여 안전한 보안 채널을 생성함으로써 해결할 수 있다. 인증서 기반의 전자상거래 방식의 예는 그림 6과 같다.

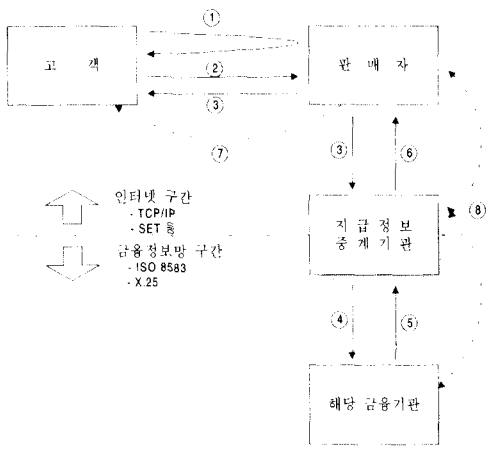

그림 6. 전자상거래 이용예

① 고객은 인터넷상의 판매자에 접속하여 쇼핑한 후 해당 판매자의 정당성을 확인시켜주는 판매자 및 지급정보중계기관(Payment Gateway, 이하 'PG')의 인증서 수신한다.

② 고객은 판매자와 PG 인증서를 확인하여 정당한 경우 상품주문 및 결제정보와 자신의 인증서를 송부함으로써 구매요청을 한다).

③ 판매자는 고객인증서를 확인하여 정당한 경우 고객이 암호화한 결제정보를 이용하여 해당 PG에게 승인요청하고 동시에 고객에게 구매응답전문을 송신한다.

④ PG는 고객과 판매자의 인증서를 확인하여 정당한 경우 결제정보를 해당 금융기관이 이용가능한 공동망 FORMAT으로 변환하여 승인요청을 한다.

⑤ 해당 금융기관은 고객의 신용한도를 고려하여 승인여부를 전송한다.

⑥ PG는 해당전문을 인터넷 FORMAT으로 변환하여 판매자에게 전송한다.

⑦ 판매자는 PG의 응답전문에 의거하여 해당고객에 영수증 및 물품을 인도한다.

⑧ PG는 판매자와 고객은행간의 정상처리분에 대한 결제요청 처리를 실시한다.

Ⅳ. 결론

앞으로 전자상거래의 발전은 크게 두가지 요인에 의해서 그 성패가 결정될 것이다. 첫째는 핵심인프라인 국가 공개키기반구조의 성공적 구축이 전제되어야 할 것이고, 둘째로는 이러한 기반 위에서 실용적으로 활용될 수 있는 새로운 비즈니스의 창출이 반드시 필요하다.

이러한 이유로 금융결제원은 인터넷 기반의 새로운 전자금융서비스의 발굴에도 만전을 기함으로써 국내 금융기관의 경쟁력 제고와 국가 정보화 기반 구축에 실질적으로 이바지할 것이다.

참 고 문 헌

[1] R. Housley, W. Ford and D. Solo, RFC 2459 : Internet X. 509 Public Key Infrastructure Certificate and CRL Profile, *IETF X.509 PKI (PKIX) Working Group.*, January, 1999

[2] C. Adams, S. Farrell, RFC 2510 : Internet X. 509 Public Key Infrastructure Certificate Management Protocols, *IETF X.509 PKI (PKIX) Working Group.*, March, 1999

[3] M. Myers, C. Adams, D. Solo, D. Kemp, RFC 2511 : Internet X.509 Certificate Request Message Format, *IETF X.509 PKI (PKIX) Working Group.*, March, 1999

[4] S. Boeyen, T. Howes, P. Richard, D. Kemp, RFC 2559 : Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2, *IETF X.509 PKI (PKIX) Working Group.*, April, 1999

[5] RSA Laboratories, PKCS #1 : RSA Encryption Standard, November 1993.

[6] RSA Laboratories, PKCS #5 :

password-Based Encryption Standard , March 1999.
[7] RSA Laboratories, PKCS #10 : Certification Request Syntax Standard, November 1993.

著者紹介

김 상 래

1978년 2월 : 고려대학교 물리학과 졸업
1992년 2월 : 건국대학교 산업대학원 졸업
1998년 8월~현재 : 금융결제원 전자금융연구소 소장

<관심분야> 정보보호, 전자금융, S/W공학