(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)

(11) 공개번호 10-2006-0020305
(43) 공개일자 2006년03월06일

(21) 출원번호 10-2004-0069122
(22) 출원일자 2004년08월31일

(71) 출원인 인천대학교 산학협력단
인천 남구 도화동 177번지 인천대학교내

(72) 발명자 신승호
서울특별시 서대문구 남가좌동 173-18
박상민
서울특별시 강남구 대치동 900-39

(74) 대리인 조용식

심사청구 : 없음

(54) 모바일 통합안전 인증 프로토콜을 이용한 인증방법

요약

본 발명은 모바일 통합안전인증 프로토콜을 이용한 인증방법을 이용한 인증방법을 개시한다.

본 발명에 따른 모바일 통합안전인증 프로토콜을 이용한 인증방법은, 모바일 3-D Secure 프로토콜을 이용한 인증방법에 있어서, 카드 사용자가 카드 발급사에 통합안전인증을 사용하기 위하여 팬(PAN), 팸(PAM), 카드 비밀번호, 카드 만기일, 사용자 이름, 질문(비밀번호 분실시 사용자 확인을 위한 질문), 답변(사용자 확인을 위한 질문의 답변)으로 된 사용자 정보를 제공하여 사용자 등록을 요청하는 단계; 카드 발급사 또는 카드 사용자로부터 제공받은 정보를 기초로 타원곡선암호를 이용한 공개키, 비밀키 생성 및 인증서를 발급하는 단계; 카드 사용자로부터 입력된 신용정보를 해쉬(HASH)함수를 이용하여 팬(PAN) 분리 저장하고 카드 사용자와 인증서버에 각각 인증서를 제공하는 단계를 포함하여 이루어진다.

상기와 같이 구성되는 모바일 통합안전인증 프로토콜을 이용한 인증방법은, 3-D Secure 사용자 등록과정에서 타원곡선암호(ECC) 알고리즘을 사용하여 데이터 전송 보안을 강화하였고, 인증서 발급을 사용하여 무선 구간에서 사용자 인증절차를 간편하고 효율적으로 작동될 수 있도록 하였으며, 타원곡선암호와 HASH함수를 이용하여 인증서버로부터의 신용정보 유출에 대비할 수 있는 PAN 분리저장 방식을 제공하여 인증신뢰도를 대폭적으로 높일 수 있는 유용한 효과를 제공한다.

대표도

도 3

색인어

공개키 기반구조, 전자서명, 암호화, 인증서버, 카드

명세서

도면의 간단한 설명

도 1은 종래 기술에 따른 모바일 3-D Secure의 구조를 나타낸 도면이다.

도 2는 종래 기술에 따른 이동통신 기기를 이용한 모바일 3-D Secure의 인증처리 과정을 설명하기 위한 도면,

도 3은 본 발명에서 3-D Secure 사용자 등록화면의 일예를 나타낸 도면,

도 4는 본 발명에서 PAN 분리저장을 설명하기 위한 모식도,

<도면의 주요 부분에 대한 부호의 설명>

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 모바일 통합안전인증 프로토콜을 이용한 인증방법에 관한 것으로서, 보다 상세하게는 모바일 환경에서 타원곡선암호와 해쉬함수를 사용하여 데이터 전송보안을 수행하면서 타원곡선암호와 해쉬함수를 이용하여 시용정보 유출을 차단하고 간소한 인증절차를 제공하는 모바일 통합안전인증 프로토콜을 이용한 인증방법에 관한 것이다.

컴퓨터와 인터넷 사용자의 폭발적인 증가는 신용카드 사용자들과 인터넷 쇼핑몰을 운영하는 사람들에게 편리한 전자상거래 환경을 제공해주었다. 전자상거래의 거래 규모는 해마다 지속적인 성장을 이루어 왔으며, 현재 도입 단계에 있는 이동통신 단말기를 이용한 새로운 모바일 쇼핑 환경의 등장으로 인해, 향후 놀랄만한 전자상거래의 변화와 성장을 이룰 것으로 예상하고 있다. 하지만 그러한 성장의 이면에는 신용카드의 도용 및 부정사용, 해킹에 의한 신용정보 누출 등의 위험이 끊임없이 도사리고 있다.

아시아 태평양 지역 인터넷 상거래상의 부도거래 액수는 연간 2천만 달러에 이르며, 2004년에는 부도거래 금액이 연간 3억 달러로 늘어나고, 그에 따른 신용카드 회원사의 처리비용도 연간 1억 달러로 증가할 것으로 예상되고 있다.

전자상거래에서 발생하는 이러한 부정적인 소식들은 인터넷에서 신용카드 사용자들에게 자신의 신용카드 정보와 신용정보가 유출될 수 있다는 불안감을 안겨주었다. 그러한 상황은 모바일 인터넷에서 더욱 심각한 문제로 받아들여지고 있다. 만일, 적절한 보안대책이 없는 상황에서 인터넷 전자상거래 시장이 현재의 비율로 지속적인 성장을 하게 된다면, 사회적으로 큰 혼란을 초래할 수도 있게 된다.

이러한 문제를 해결하기 위하여 1999년 비자(VISA)는 마스터카드, 아이비엠, 마이크로소프트 등과 공동으로 지불결재 프로토콜인 SET를 개발하였으나 설치비용과 시간이 많이 걸리는 등의 여러 가지 문제점이 드러나, 2000년 말에 3D Secure와 모바일 3-D Secure가 제안되었다.

3D Secure의 개발로 보안 시스템 시장은 비자의 3D Secure와 마스터카드의 SPA, 그리고 SET로 대별되었으나, 세계 카드 시장의 60% 이상을 차지하고 있는 비자가 3D Secure를 선택함으로써 표준화로 채택될 가능성이 매우 높아지게 되었다.

도 1은 종래 기술에 따른 모바일 3-D Secure의 구조를 나타낸 도면이다.

(1) 발급사 도메인(Issuer domain)

발급사는 신용카드를 발급하는 곳으로 3-D Secure 서비스 등록 및 인증을 관리한다. 카드 소지자가 인터넷에서 지불결재시, 사용자 인증을 받으려면 3-D Secure 서비스 신청을 하여야만 한다.

(2) 매입사 도메인(Acquirer domain)

매입사는 상점으로부터 신용카드 전표를 매입하는 곳으로서 국내의 경우 발급사와 매입사는 같은 의미를 갖는다.

(3) 상호 운영 도메인(Interoperability domain)

발급사 도메인과 매입사 도메인이 인증 및 지불 메시지를 운용하는 비자 네트워크 영역에 해당한다.

이와 같은 구조를 갖는 모바일 3-D Secure의 인증처리 과정은 다음과 같다.

3-D Secure는 SSL 기반의 인증 지불 프로토콜로서 인터넷 쇼핑몰에서 지불결재 진행 시 발급사로부터 사용자 인증을 먼저 받도록 하는 과정에 해당한다. 신용카드 사용자를 인증하는 방식은 비밀번호 방식외에도 다양한 방식을 활용할 수 있으나 초기 이동통신 기기를 이용한 지불 인증 방법으로는 비밀번호 방식이 널리 사용되고 있다.

이동통신 기기를 이용한 모바일 3-D Secure의 인증처리 과정은 도 2와 같다.

(1) 사용자가 쇼핑몰에서 구매물품을 장바구니에 담고 결재를 진행한다.

(2) MPI는 PAN(비자암호)과 채널정보와 사용자 기기 정보를 비자 디렉토리로 전송한다.

(3) PAN이 유효한 번호라면 비자디렉토리는 인증 가능 여부를 ACS(Access Control System)에 전송한다.

(4) ACS는 PAN이 3-D Secure에 등록되었는지 그리고 신용카드 사용자의 기기와 채널 정보하에서 인증이 가능한지의 여부를 비자디렉토리로 회신한다.

(5) 비자디렉토리는 ACS의 응답을 MPI에 전달한다.

(6) MPI는 ACS를 경유하여 사용자의 이동통신 단말기에 요약된 지불 인증 요청서(CPRQ)를 보낸다.

(7) ACS는 지불인증 요청서를 받는다.

(8) ACS는 PAN과 PAM을 통하여 사용자를 확인하고 지불인증 확인서(CPRS)를 작성한다.

(9) ACS는 MPI를 통하여 사용자의 기기에 지불인증 확인서를 보내고, 지불인증 요청서에 관한 모든 데이터를 인증서버로 보낸다.

(10) MPI는 지불인증 확인서를 받고 서명을 확인 한 다음 나머지 입력과정을 실행한다.

(11) 상점은 매입사로부터 매매 승인을 받고 구매절차를 완료한다.

* PAN (Personal Assurance Number)

* PAM (Personal Assurance Message)

* MPI(Merchant Plug-in: 3-D Secure를 사용하는 상점서버에 설치되는 프로그램)

그러나 상기와 같은 종래 기술에 따른 모바일 3-D Secure는 다양한 인증방법을 포함하는 것에 의해 결과적으로 전송 프로토콜을 점점 더 복잡하게 만드는 원인을 제공하며, 이러한 이유로 인증과정 및 지불결재에 필요한 절차가 복잡해져 사용자의 편리성이 저하될 뿐만 아니라 이동통신 단말기의 사용 효율성이 악화되는 문제점을 초래한다.

발명이 이루고자 하는 기술적 과제

본 발명은 상기한 문제점을 해결하기 위하여 창출된 것으로서, 본 발명의 목적은 3-D Secure 사용자 등록과정에서 타원곡선암호 알고리즘을 사용하여 데이터 전송보안을 강화할 수 있도록 하면서 타원곡선암호와 HASH함수를 이용하여 인증서버로부터의 신용정보 유출을 차단할 수 있도록 한 모바일 통합안전인증 프로토콜을 이용한 인증방법을 제공하는데 있다.

본 발명의 다른 목적은 인증서 발급을 사용하여 무선 구간에서 사용자 인증 절차가 간편하고 효율적으로 수행될 수 있도록 한 모바일 통합안전인증 프로토콜을 이용한 인증방법을 제공하는데 있다.

발명의 구성 및 작용

상기의 목적을 실현하기 위한 본 발명에 따른 모바일 통합안전인증 프로토콜을 이용한 인증방법은, 모바일 3-D Secure 프로토콜을 이용한 인증방법에 있어서,

카드 사용자가 카드 발급사에 통합안전인증을 사용하기 위하여 팬(PAN), 팸(PAM), 카드 비밀번호, 카드 만기일, 사용자 이름, 질문(비밀번호 분실시 사용자 확인을 위한 질문), 답변(사용자 확인을 위한 질문의 답변)으로 된 사용자 정보를 제공하여 사용자 등록을 요청하는 단계;

카드 발급사 또는 카드 사용자로부터 제공받은 정보를 기초로 타원곡선암호를 이용한 공개키, 비밀키 생성 및 인증서를 발급하는 단계;

카드 사용자로부터 입력된 신용정보를 해쉬(HASH)함수를 이용하여 팬(PAN) 분리 저장하고 카드 사용자와 인증서버에 각각 인증서를 제공하는 단계를 포함하는 것을 그 특징으로 한다.

본 발명의 특징 및 이점들은 첨부도면에 의거한 다음의 상세한 설명으로 더욱 명백해질 것이다. 이에 앞서 본 명세서 및 청구범위에 사용된 용어나 단어는 발명자가 그 자신의 발명을 가장 최선의 방법으로 설명하기 위해 용어의 개념을 적절하게 정의할 수 있다는 원칙에 입각하여 본 발명의 기술적 사상에 부합되는 의미와 개념으로 해석되어야만 한다.

이하 본 발명에 따른 모바일 통합안전인증 프로토콜을 이용한 인증방법의 바람직한 실시예를 첨부된 도면을 참조하여 상세히 설명하면 다음과 같다.

도 3은 본 발명에서 3-D Secure 사용자 등록화면의 일예를 나타낸 도면이고, 도 4는 본 발명에서 PAN 분리저장을 설명하기 위한 모식도이다.

이에 나타내 보인 바와 같이, 본 발명의 모바일 통합안전인증 프로토콜을 이용한 인증방법은 카드 사용자와 카드 발급사 그리고 인증기관의 인증서버의 상호간의 데이터 송수신에 의해 이루어진다.

이때, 상기 사용자는 모바일 기기(이동통신 단말기, 통신킷이 탑재된 PDA 등)를 소지하고 있으며, 이 모바일 기기를 이용하여 카드 발급사에 3-D Secure를 사용하기 위해 사용자 등록을 요청하면, 상기 카드 발급사는 해당정보를 기초로 인증서를 생성하여 발급하고, 이 인증서는 인증서버로 제공된다.

즉, 본 발명의 모바일 통합안전인증 프로토콜을 이용한 인증방법은 카드 사용자가 카드 발급사에 통합안전인증을 사용하기 위하여 팬(PAN), 팸(PAM), 카드 비밀번호, 카드 만기일, 사용자 이름, 질문(비밀번호 분실시 사용자 확인을 위한 질문), 답변(사용자 확인을 위한 질문의 답변)으로 된 사용자 정보를 제공하여 사용자 등록을 요청하는 단계와,

상기 단계에 이어서 카드 발급사 또는 카드 사용자로부터 제공받은 정보를 기초로 타원곡선암호를 이용한 공개키, 비밀키 생성 및 인증서를 발급하는 단계와, 그리고 카드 사용자로부터 입력된 신용정보를 해쉬(HASH)함수를 이용하여 팬(PAN) 분리 저장하고 카드 사용자와 인증서버에 각각 인증서를 제공하는 단계로 수행된다.

이하, 본 발명의 인증방법을 상세하게 설명하면 다음과 같다.

(1) 타원곡선암호(ECC : Eliptic Curve Cryptography) 기반의 사용자 등록

인터넷 쇼핑몰에서 "비자안전지불서비스"라는 항목으로 제공되는 3-D Secure를 사용하기 위해서 카드 사용자는 우선, 카드 발급사에 3-D Secure 사용자 등록신청을 한다.

여기서, 3-D Secure의 등록 요구사항은 팬(PAN), 팸(PAM), 카드 비밀번호, 카드 만기일, 사용자 이름, 질문(비밀 번호 분실시 사용자 확인을 위한 질문), 답변(사용자 확인을 위한 질문의 답변), 카드 발급사에서 지정한 항목 등이 해당한다. 모바일 3-D Secure 등록은 유선과 무선, 양쪽 모두에서 등록이 가능하며, 유선 데이터 전송시 적용되는 보안 프로그램이 사용된다.

도 3은 구현화면을 나타낸 것으로 사용언어는 Java(J2SDK 1.4.0)가 사용되었고, 등록서버는 Windows 2000 Server와 익스플로러를 사용하였으며, "타원곡선암호로 안전하게 등록하기" 버튼 클릭 시 타원곡선암호(ECC) 공개키에 의해 암호화되어 전송된다.

(2) 타원곡선암호(ECC) 기반의 인증서 발급

인증서를 발급하는 방법은 이동통신 단말기 사용자가 직접 인증서를 발급하는 방법과 인증기관으로부터 인증서를 발급받는 2가지 방법이 있다.

인증서를 효율적으로 사용하는 방법은 무선 지불결재를 원하는 사용자에게 철저한 신원확인 후 신뢰할 수 있는 제3의 인증서버로부터 인증서를 제공한 다음 지불결재시 카드 사용자의 단말기에 저장되어 있는 인증서와 전자결재를 활용하는 것이다.

(3) 타원곡선암호(ECC) 기반의 신용정보 관리

도 4는 본 발명에서 PAN 분리저장을 설명하기 위한 모식도이다.

기존의 인증서버는 3-D Secure 등록시 카드 사용자로부터 입력된 신용정보를 모두 ACS에 저장하도록 되어 있었으나, HASH함수를 이용한 팬(PAN) 분리저장 방식을 사용하면, 카드 사용자의 신용정보를 관리하는 인증서버에 신용정보가 유출되더라도 부정카드 사용을 방지할 수 있다.

3-D Secure의 핵심은 팬(PAN)을 이용하여 지불결재 이전에 카드 사용자의 본인 여부를 확인하는 인증절차를 거친다는 것이다. 즉, PAN은 지불결재를 진행할 수 있는 가장 주요한 열쇠가 되므로 반드시 보호되어야 한다.

1) 사용자 등록과정

본 발명에서 제안하는 ACS의 PAN 분리 저장방식은 다음과 같다.

(1) PAN, INFO(PAM, 카드비밀번호,사용자 이름, 카드 유효기간)의 신용정보를 입력받은 인증서버는 신용 정보 파일을 HASH 알고리즘을 이용하여 일정길이의 출력값으로 만든다음 인증서버로부터 PAN을 완전히 삭제한다.

(2) INFO와 HASH출력값만을 ACS에 저장한다.

2) 지불결재 과정

(1) 쇼핑몰에서 원하는 물품을 선택한 후 결재를 진행한다. 이때 신용카드번호와 비밀번호를 입력하여 전송한다.

(2) 카드 사용자는 인증서와 PAN을 요구하는 메시지를 받는다.

(3) 카드 사용자는 PAN을 입력하여 응답 메시지를 보낸다.

(4) 인증서버는 카드 사용자로부터 제공받은 PAN과 인증서버에서 보관하고 있던 정보를 합하여 HASH알고리즘으로 출력값을 얻은 다음 보관중이던 HASH 출력값과 비교하는 인증 절차를 수행한다.

(5) 인증 확인에 이상이 없는 경우 지불결재를 진행한다.

(6) 지불결재가 완료된 경우 인증서버는 카드 사용자로부터 입력받은 PAN을 다시 삭제한다.

상기와 같이 수행되는 모바일 통합안전인증 프로토콜을 이용한 인증방법은 타원곡선암호(ECC) 기반의 전자지불 프로토콜은 우선 및 무선 인터넷에서 지불결재를 하는 사용자들에게 편리하고 안전한 지불환경을 제공하고, 특히 무선 환경에서 타원곡선암호(ECC)은 이동 단말기의 자원을 최소로 하므로 지불결재의 가장 중요한 부분인 보안성과 편리성을 높일 수 있게 된다.

한편, 본 발명은 기재된 실시예에 한정하는 것이 아니고, 본 발명의 사상 및 범위를 벗어나지 않고 다양하게 수정 및 변형을 할 수 있음은 이 기술 분야에서 통상의 지식을 가진 자에게는 자명하다. 따라서, 그러한 변형예 또는 수정예들은 본 발명의 특허청구범위에 속한다 해야 할 것이다.

발명의 효과

상기와 같이 구성되고 작용되는 모바일 통합안전인증 프로토콜을 이용한 인증방법은, 3-D Secure 사용자 등록과정에서 타원곡선암호(ECC) 알고리즘을 사용하여 데이터 전송 보안을 강화하였고, 인증서 발급을 사용하여 무선 구간에서 사용자 인증절차를 간편하고 효율적으로 작동될 수 있도록 하였으며, 타원곡선암호와 HASH함수를 이용하여 인증서버로부터의 신용정보 유출에 대비할 수 있는 PAN 분리저장 방식을 제공하여 인증신뢰도를 대폭적으로 높일 수 있는 유용한 효과를 제공한다.

(57) 청구의 범위

청구항 1.

모바일 통합안전인증 프로토콜을 이용한 인증방법에 있어서,

카드 사용자가 카드 발급사에 통합안전인증을 사용하기 위하여 팬(PAN), 팸(PAM), 카드 비밀번호, 카드 만기일, 사용자 이름, 질문(비밀번호 분실시 사용자 확인을 위한 질문), 답변(사용자 확인을 위한 질문의 답변)으로 된 사용자 정보를 제공하여 사용자 등록을 요청하는 단계;

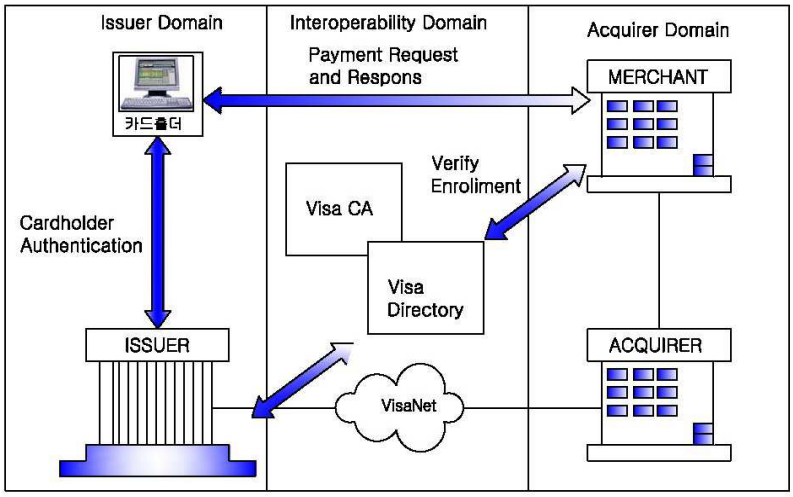
카드 발급사 또는 카드 사용자로부터 제공받은 정보를 기초로 타원곡선암호를 이용한 공개키, 비밀키 생성 및 인증서를 발급하는 단계;

카드 사용자로부터 입력된 신용정보를 해쉬(HASH)함수를 이용하여 팬(PAN) 분리 저장하고 카드 사용자와 인증서버에 각각 인증서를 제공하는 단계;

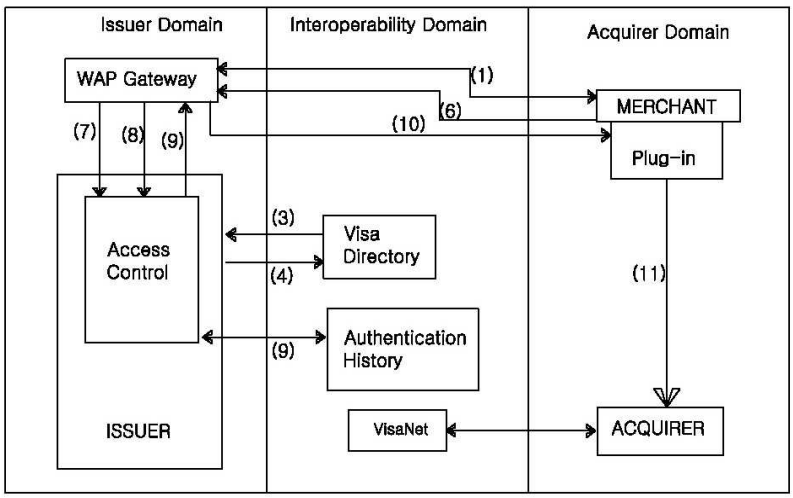
를 포함하는 것을 특징으로 하는 모바일 통합안전인증 프로토콜을 이용한 인증방법.

도면

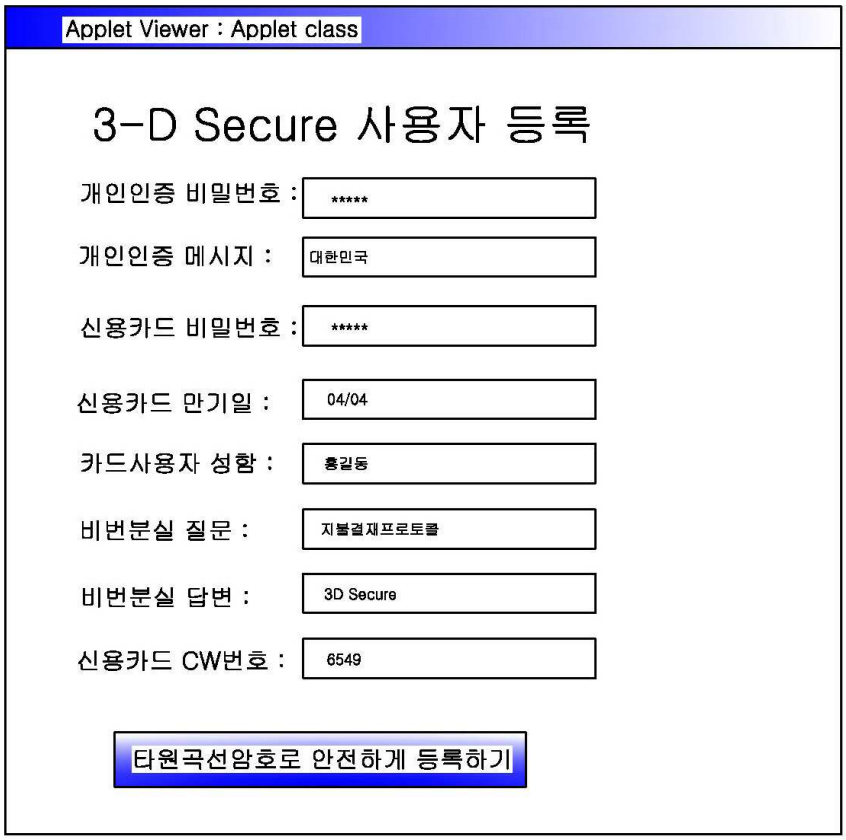
도면1


Issuer Domain
Interoperability Domain
Acquirer Domain
Payment Request
and Respons
MERCHANT
카드홀더
Verify
Enroliment
Visa CA
Cardholder
Authentication
Visa
Directory
ISSUER
ACQUIRER
VisaNet

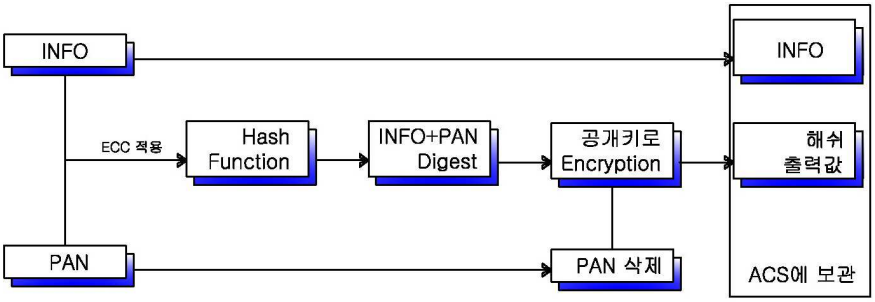
도면2


Issuer Domain
Interoperability Domain
Acquirer Domain
WAP Gateway
(1)
(6)
(10)
MERCHANT
Plug-in
(7)
(8)
(9)
(3)
Visa
Directory
(4)
Access
Control
(11)
(9)
Authentication
History
ISSUER
VisaNet
ACQUIRER

도면3


Applet Viewer : Applet class
3-D Secure 사용자 등록
개인인증 비밀번호 :
*****
개인인증 메시지 :
대한민국
신용카드 비밀번호 :
*****
신용카드 만기일 :
04/04
카드사용자 성함 :
홍길동
비번분실 질문 :
지불결재프로토콜
비번분실 답변 :
3D Secure
신용카드 CW번호 :
6549
타원곡선암호로 안전하게 등록하기

도면4


INFO
INFO
ECC 적용
Hash Function
INFO+PAN Digest
공개키로 Encryption
해쉬 출력값
PAN
PAN 삭제
ACS에 보관