(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0108599
(43) 공개일자 2012년10월05일

(51) 국제특허분류(Int. Cl.)
G06Q 20/40 (2012.01)
(21) 출원번호 10-2011-0026682
(22) 출원일자 2011년03월25일
심사청구일자 없음

(71) 출원인
주식회사 스마트솔루션
경기도 성남시 수정구 복정로 76, 동서울대학 창업보육센터 5402호 (복정동)
(72) 발명자
서정훈
경기도 용인시 기흥구 마북로154번길 16, 교동마을정광아파트 105동 604호 (마북동)

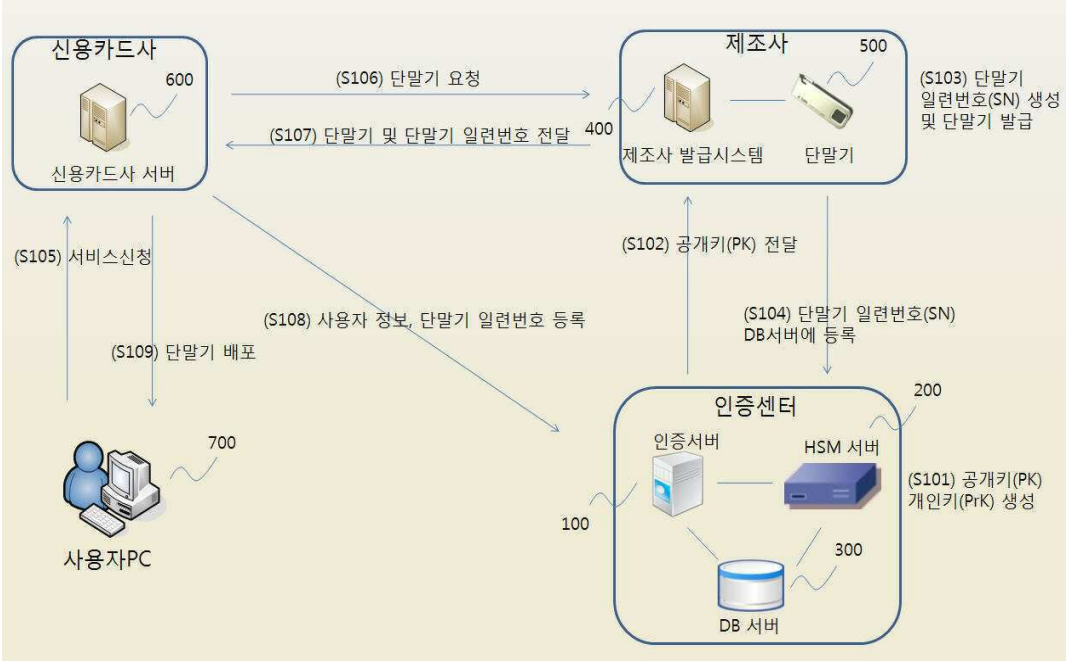
전체 청구항 수 : 총 1 항

(54) 발명의 명칭 **온라인 신용카드 결제 단말기를 활용한 신용카드 결제 서비스**

(57) 요 약

본 발명은 온라인 신용카드 결제 단말기를 활용한 신용카드 결제 서비스에 관한 것이다. 구체적으로 신용카드결제가 되기 위해서 등록된 단말기와 신용카드를 소지하고 단말기 비밀번호와 신용카드 비밀번호를 알고 있어야 한다. 단말기와 인증서버는 단말기 발급시 생성된 공개키와 개인키를 이용해 상호인증을 하고 상호인증이 완료되면 암호통신을 위해 세션키를 공유하게 되며 세션키를 이용하여 암호채널을 형성하고 신용카드 결제에 필요한 정보(신용카드 번호, 신용카드 비밀번호, 사용자명 등)을 암호통신 한다. 이로인해 PC 또는 네트웍상의 악성코드 또는 악의적목적을 가진 해커에 의해 정보가 유출되지 않고 안전하게 신용카드 거래를 할 수 있다.

대 표 도



특허청구의 범위

청구항 1

온라인 신용카드 결제 단말기를 활용한 신용카드 결제 서비스에 있어서,

인증센터 HSM서버에서 장치인증용 공개키(PK)와 개인키(PrK)를 생성하여 저장하고, 생성된 공개키(PK)를 제조사 단말기 발급시스템에 전달하며, 제조사 단말기 발급시스템은 고유한 단말기 일련번호(SN)를 생성하고 생성된 단말기 일련번호(SN)와 상기 전달받은 공개키(PK)를 단말기에 주입(저장)하여 단말기를 발급하며, 상기 단말기 일련번호(SN)를 인증센터의 DB 서버에 등록하는 과정,

사용자가 사용자 PC를 통해 온라인으로 사용자명, 사용자 핸드폰 번호 또는 이메일 주소를 입력하면서 신용카드사 서버에 단말기 발급 서비스 신청을 하면, 신용카드사는 제조사에 단말기를 요청하고 제조사는 단말기를 신용카드사에 전달하고 단말기 장치 일련번호(SN)를 신용카드사 서버에 전달하는 과정,

신용카드사 서버가 사용자가 서비스 신청시 입력한 사용자명, 사용자 핸드폰 번호 또는 이메일주소와 단말기 일련번호를 인증서버에 전송하면 인증서버는 상기 사용자명, 사용자 핸드폰 번호 또는 이메일주소와 단말기 일련번호를 DB서버에 저장하고, 신용카드사는 단말기를 사용자에게 배송하는 과정,

을 포함하는 단말기 배포단계;

사용자가 사용자 PC에 단말기를 장착하면 사용자 PC와 단말기가 연결되며 사용자 PC에 단말기 등록창이 실행되는 과정,

사용자는 단말기 등록창을 통해 단말기 비밀번호, 사용자명, 사용자의 핸드폰번호 또는 이메일주소를 등록하고, 사용자PC는 상기 단말기 비밀번호, 사용자명, 사용자 핸드폰번호 또는 이메일 주소를 단말기에 전송하면 단말기는 상기 단말기 비밀번호, 사용자명, 사용자 핸드폰 번호 또는 이메일주소를 저장하는 과정,

단말기는 단말기 일련번호, 사용자명, 사용자 핸드폰 번호 또는 이메일주소를 입력값으로 해쉬코드1을 생성하고 단말기 일련번호, 사용자명, 사용자 핸드폰번호 또는 이메일주소, 해쉬코드1을 인증서버에 전송하는 과정,

인증서버는 전송받은 상기 단말기 일련번호, 사용자명, 사용자 핸드폰번호 또는 이메일주소를 입력값으로 해쉬코드1'을 생성하고 전송받은 해쉬코드1과 비교하여 일치하면 상기 단말기 일련번호, 사용자명, 사용자 핸드폰번호 또는 이메일주소에 대한 무결성을 검증하고, 상기 단말기 일련번호(SN)에 대응하는 인증코드(AC)를 생성하여 DB서버에 저장하고, 상기 핸드폰번호 또는 이메일 주소로 상기 인증코드(AC)를 전송하는 과정,

사용자는 핸드폰 또는 이메일로 전달받은 인증코드(AC)를 사용자 PC에 연결된 단말기에 입력하고, 단말기는 난수1(RND1)을 생성 및 저장하고, 단말기 일련번호(SN), 상기 인증코드(AC), 인증코드(AC)를 장치 인증용 공개키(PK)로 암호화하여 메세지1(m1)을 생성하고 상기 단말기 일련번호(SN)와 메세지1(m1)을 인증서버에 전송하는 과정,

인증서버는 전송받은 메시지1(m1)을 HSM서버로 전송하고 HSM서버는 저장된 개인키(PrK)로 상기 메시지1(m1)을 복호화하여 인증서버로 전송하며, 인증서버는 전달받은 복호화 메시지로 부터 단말기 일련번호(SN), 난수1(RND1), 인증코드를 추출하여 추출된 단말기 일련번호(SN)가 DB 서버에 등록되었는지 여부, 단말기 일련번호(SN)가 등록되었으면 등록된 단말기 일련번호에 대응하는 인증코드(AC)가 등록되었는지 여부, 인증코드(AC)가 등록되었으면 메시지1으로 부터 추출된 인증코드(AC)와 DB서버에 등록된 인증코드(AC)가 일치하는지 여부를 검증하는 과정,

상기 단말기 일련번호(SN)와 인증코드(AC)가 검증되면, 인증서버는 난수2(RND2)를 생성하고, 상기 난수2(RND2), 메시지1(m1)을 복호화하여 추출한 난수1(RND1), 단말기 일련번호(SN)로 부터 세션키(SK)를 생성하고, 상기 세션키(SK)로 상기 단말기 일련번호(SN), 난수1(RND1)을 암호화하여 메시지2(m2)를 생성하며, 난수2(RND2)를 인터넷망을 통해 사용자 PC에 연결된 단말기에 전송하는 과정,

단말기는 전송받은 난수2(RND2)와 단말기에 저장된 난수1(RND1)과 단말기 일련번호(SN)로 부터 세션키(SK)를 생성하여 상기 세션키(SK)로 상기 전달받은 메세지2(m2)를 복호화하여 난수1(RND1)과 단말기 일련번호(SN)를 추출하고, 단말기에 저장된 난수1(RND1)과 메시지2(m2)로 부터 복호화하여 추출한 난수1(RND1)을 비교하여 값이 일치하는지 비교하여 일치하면 단말기와 인증서버간에 암호채널을 형성하고, 상기 세션키(SK)로 암호채널 형성완

료 메시지를 암호화하여 인증서버에 전송하는 과정,

암호채널 형성완료 메시지를 받으면 인증서버는 고객명과 단말기 일련번호를 DB서버에 등록하고 단말기 등록 성공 메시지를 상기 세션키로 암호화해 단말기에 전송하면 단말기에서 상기 메시지를 복호화해서 사용자PC에 등록 성공 메시지를 전송하는 과정,

을 포함하는 단말기 등록단계;

사용자가 사용자 PC에 단말기를 장착하면 사용자 PC와 단말기가 연결되며 사용자 PC에 신용카드 등록창이 실행되는 과정,

사용자가 IC칩이 내장된 신용카드를 단말기에 삽입하면 단말기는 신용카드를 자동 인식하면서 신용카드 번호와 사용자명을 읽는 과정,

단말기에서 신용카드 번호와 단말기에 사용자명을 입력값으로 하여 해쉬코드2를 생성하고 상기 해쉬코드2, 신용카드번호, 사용자명을 세션키(SK)로 암호화해서 메시지3(m3)을 생성하고 메시지3(m3)을 인증서버에 전송하는 과정,

인증서버는 메시지3(m3)을 세션키(SK)로 복호화하여 해쉬코드2, 신용카드번호, 사용자명을 추출하고, 상기 추출된 신용카드번호와 사용자명을 입력값으로 해쉬코드2'을 생성하고 상기 추출된 해쉬코드2와 해쉬코드2'을 비교하여 메시지3(m3)의 무결성을 검증하는 과정,

인증서버는 상기 신용카드번호와 사용자명을 신용카드사 서버에 전송하면 신용카드사 서버는 상기 신용카드가 유효한 카드인지 검증하여 결과값을 인증서버에 전달하는 과정,

인증서버는 상기 신용카드가 유효한 카드로 검증결과값을 받으면 DB서버에 사용자명과 해쉬코드2를 등록하고 신용카드가 정상 등록되었다는 결과를 사용자 PC에 전송하는 과정,

을 포함하는 신용카드 등록단계;

사용자가 온라인 쇼핑몰 서버에 접속하여 상품을 선택하고 결제요청을 하면 사용자 PC에 결제방식을 선택창이 뜨는 과정,

사용자가 결제방식 선택창에 온라인 신용카드 결제 단말기를 활용한 신용카드 결제 서비스(이하, 스마트결제)를 선택하면, 사용자PC는 PG사 서버에 스마트결제를 요청하고 스마트결제창이 실행되는 과정,

사용자는 단말기를 사용자 PC에 연결하고 해당 사용자PC에서 상기 단말기를 최초 사용하는 경우 스마트결제창에 단말기 비밀번호 입력을 요구하는 창이 뜨고 사용자가 단말기 비밀번호를 입력하면 사용자가 입력한 비밀번호와 단말기에 저장된 비밀번호를 비교하여 일치하면 단말기가 사용자PC와 연결되는 과정,

사용자가 IC칩이 내장된 신용카드를 단말기에 삽입하면 단말기는 상기 신용카드를 자동 인식하며, 신용카드번호와 사용자명을 읽고, 신용카드번호와 사용자명을 입력값으로 해쉬코드2를 생성하는 과정,

스마트결제창에 신용카드 비밀번호 입력창이 뜨면 사용자는 신용카드 비밀번호를 입력하고 단말기는 사용자가 입력한 신용카드 비밀번호와 신용카드에 등록된 신용카드 비밀번호가 일치하는지 여부를 검증하는 과정,

상기 신용카드 비밀번호가 검증되면 단말기는 신용카드번호와 사용자명을 입력값으로 생성한 상기 해쉬코드2를 인증서버에 전송하고, 인증서버는 상기 전송받은 해쉬코드2가 DB서버에 등록었는지, 등록이 되었다면 값이 일치하는지 비교하여 값이 일치하면 신용카드 등록을 확인하고 신용카드 등록확인 메시지를 단말기에 전송하는 과정,

단말기가 신용카드 등록확인 메시지를 받으면, 난수3(RND3)을 생성하고, 난수3(RND3)과 단말기 일련번호(SN)을 공개키(PK)로 암호화하여 메시지3(m3)을 생성하여, 상기 메시지3(m3)과 단말기 일련번호(SN)를 인증서버로 전송하는 과정,

인증서버는 전송받은 상기 메시지3(m3)을 HSM서버에 전달하고, HSM서버는 개인키(PrK)로 메시지3(m3)을 복호화하여 인증서버에 전달하는 과정,

인증서버는 메시지3(m3)을 복호화하여 추출된 단말기 일련번호(SN)를 DB서버에 등록된 단말기 일련번호(SN)와 비교하여 일치하는지 검증하는 과정,

상기 단말기 일련번호(SN)가 검증되면, 인증서버는 난수4(RND4)를 생성하고 난수3(RND3), 난수4(RND4), 단말기

일련번호(SN)로 부터 세션키2(SK2)를 생성하고, 상기 세션키2(SK2)로 단말기 일련번호(SN)와 난수4(RND4)를 암호화하여 메시지4(m4)를 생성하고, 상기 메시지4(m4)와 난수4(RND4)를 단말기에 전송하는 과정,

단말기는 전달받은 상기 난수4(RND4)와 단말기 일련번호(SN), 난수3(RND3)을 이용하여 세션키2(SK2)를 생성하고, 상기 세션키2(SK2)로 메시지4(m4)를 복호화하여 추출된 난수1(RND1)이 단말기에서 생성된 난수1(RND1)과 값이 일치하면 단말기와 인증서버간에 암호채널2을 형성하는 과정,

상기 암호채널2가 형성되면, 단말기는 거래전문을 생성하고 인증서버에 상기 거래전문을 전송하는 과정,

인증서버는 전송받은 거래전문을 신용카드사 서버에 전송하고 신용카드사 서버는 상기 거래전문을 참조하여 결제를 진행하고 결제처리결과를 온라인쇼핑몰 서버에 전송하는 과정,

온라인쇼핑몰은 신용카드사 서버로부터 결제처리결과를 받고 결제처리결과를 사용자 PC에 전송하면, 사용자 PC의 스마트결제창에 결제처리 결과를 표시하는 과정,

을 포함하는 신용카드 결제단계;

를 포함하는 것을 특징으로 하는 온라인 신용카드 결제 단말기를 활용한 신용카드 결제 서비스.

명 세 서

기 술 분 야

[0001] 본 발명은 사용자 인증에 속한 기술분야로 구체적으로 온라인 신용카드 결제 단말기를 활용한 신용카드 결제 서비스에 관한 것이다.

배 경 기 술

[0002] 인터넷뱅킹에 못지 않게 신용카드를 이용한 온라인 결제는 매년 수조원에 이를 만큼 빈번하게 이루어지고 있다. 기존에 온라인에서 신용카드를 이용한 결제는 신용카드 번호, 신용카드 결제비밀번호, 신용카드 인증번호만 있으면 결제가 가능하다. 위의 온라인 신용카드 결제에 필요한 정보들은 사용자 PC에 설치된 키로깅 프로그램과 같은 악성 프로그램에 의해 쉽게 노출이 되며, 실제 신용카드 결제 관련 금융사고는 매년 수천여 건에 이를 만큼 심각한 문제가 되고 있으나 이를 위한 뚜렷한 해결책 또한 없는 것이 사실이다. 위의 악성 프로그램을 탐지하기 위해 PC에 방화벽,백신,키보드 해킹방지 프로그램과 같은 각종 보안프로그램을 설치해도 알려진 해킹 프로그램을 방지하는 데는 효과가 있으나 알려지지 않은 변종 악성 프로그램에 실시간으로 대처하는 것은 불가능하다.

발명의 내용

해결하려는 과제

[0003] 상술한 종래의 문제점을 해결하기 위해 본 발명은 신용카드 결제 단말기를 발급하고 사용자가 온라인 신용카드 거래시, 상기 신용카드 결제 단말기를 통해 인증 서버에 접속하여 본인 인증을 하고 신용카드 결제 단말기와 인증 서버 간의 암호채널을 형성하고 상기 암호채널을 통해 결제정보를 송수신하여 안전한 온라인 신용카드 결제가 가능하도록 하는 것을 목적으로 한다.

과제의 해결 수단

[0004] 상술한 목적을 달성하기 위해, 본 발명은 인증센터 HSM서버에서 장치인증용 공개키(PK)와 개인키(PrK)를 생성하여 저장하고, 생성된 공개키(PK)를 제조사 단말기 발급시스템에 전달하며, 제조사 단말기 발급시스템은 고유한 단말기 일련번호(SN)를 생성하고 생성된 단말기 일련번호(SN)와 상기 전달받은 공개키(PK)를 단말기에 주입(저장)하여 단말기를 발급하며, 상기 단말기 일련번호(SN)를 인증센터의 DB 서버에 등록하는 과정, 사용자가 사용자 PC를 통해 온라인으로 사용자명, 사용자 핸드폰 번호 또는 이메일 주소를 입력하면서 신용카드사 서버에 단말기 발급 서비스 신청을 하면, 신용카드사는 제조사에 단말기를 요청하고 제조사는 단말기를 신용카드사에 전달하고 단말기 장치 일련번호(SN)를 신용카드사 서버에 전달하는 과정, 신용카드사 서버가 사용자가 서비스 신청시 입력한 사용자명, 사용자 핸드폰 번호 또는 이메일주소와 단말기 일련번호를 인증서버에 전송하면 인증서버는 상기 사용자명, 사용자 핸드폰 번호 또는 이메일주소와 단말기 일련번호를 DB서버에 저장하고, 신용카드사는 단말기를 사용자에게 배송하는 과정을 포함하는 단말기 배포단계; 사용자가 사용자 PC에 단말기를 장착하면

사용자 PC와 단말기가 연결되며 사용자 PC에 단말기 등록창이 실행되는 과정, 사용자는 단말기 등록창을 통해 단말기 비밀번호, 사용자명, 사용자의 핸드폰번호 또는 이메일주소를 등록하고, 사용자PC는 상기 단말기 비밀번호, 사용자명, 사용자 핸드폰번호 또는 이메일 주소를 단말기에 전송하면 단말기는 상기 단말기 비밀번호, 사용자명, 사용자 핸드폰 번호 또는 이메일주소를 저장하는 과정, 단말기는 단말기 일련번호, 사용자명, 사용자 핸드폰 번호 또는 이메일주소를 입력값으로 해쉬코드1을 생성하고 단말기 일련번호, 사용자명, 사용자 핸드폰번호 또는 이메일주소, 해쉬코드1을 인증서버에 전송하는 과정, 인증서버는 전송받은 상기 단말기 일련번호, 사용자명, 사용자 핸드폰번호 또는 이메일주소를 입력값으로 해쉬코드1'을 생성하고 전송받은 해쉬코드1과 비교하여 일치하면 상기 단말기 일련번호, 사용자명, 사용자 핸드폰번호 또는 이메일주소에 대한 무결성을 검증하고, 상기 단말기 일련번호(SN)에 대응하는 인증코드(AC)를 생성하여 DB서버에 저장하고, 상기 핸드폰번호 또는 이메일주소로 상기 인증코드(AC)를 전송하는 과정, 사용자는 핸드폰 또는 이메일로 전달받은 인증코드(AC)를 사용자 PC에 연결된 단말기에 입력하고, 단말기는 난수1(RND1)을 생성 및 저장하고, 단말기 일련번호(SN), 상기 인증코드(AC), 인증코드(AC)를 장치 인증용 공개키(PK)로 암호화하여 메세지1(m1)을 생성하고 상기 단말기 일련번호(SN)와 메세지1(m1)을 인증서버에 전송하는 과정, 인증서버는 전송받은 메시지1(m1)을 HSM서버로 전송하고 HSM서버는 저장된 개인키(PrK)로 상기 메시지1(m1)을 복호화하여 인증서버로 전송하며, 인증서버는 전달받은 복호화 메시지로 부터 단말기 일련번호(SN), 난수1(RND1), 인증코드를 추출하여 추출된 단말기 일련번호(SN)가 DB서버에 등록되었는지 여부, 단말기 일련번호(SN)가 등록되었으면 등록된 단말기 일련번호에 대응하는 인증코드(AC)가 등록되었는지 여부, 인증코드(AC)가 등록되었으면 메시지1으로 부터 추출된 인증코드(AC)와 DB서버에 등록된 인증코드(AC)가 일치하는지 여부를 검증하는 과정, 상기 단말기 일련번호(SN)와 인증코드(AC)가 검증되면, 인증서버는 난수2(RND2)를 생성하고, 상기 난수2(RND2), 메시지1(m1)을 복호화하여 추출한 난수1(RND1), 단말기 일련번호(SN)로 부터 세션키(SK)를 생성하고, 상기 세션키(SK)로 상기 단말기 일련번호(SN), 난수1(RND1)을 암호화하여 메시지2(m2)를 생성하며, 난수2(RND2)를 인터넷망을 통해 사용자 PC에 연결된 단말기에 전송하는 과정, 단말기는 전송받은 난수2(RND2)와 단말기에 저장된 난수1(RND1)과 단말기 일련번호(SN)로 부터 세션키(SK)를 생성하여 상기 세션키(SK)로 상기 전달받은 메세지2(m2)를 복호화하여 난수1(RND1)과 단말기 일련번호(SN)를 추출하고, 단말기에 저장된 난수1(RND1)과 메시지2(m2)로 부터 복호화하여 추출한 난수1(RND1)을 비교하여 값이 일치하는지 비교하여 일치하면 단말기와 인증서버간에 암호채널을 형성하고, 상기 세션키(SK)로 암호채널 형성완료 메시지를 암호화하여 인증서버에 전송하는 과정, 암호채널 형성완료 메시지를 받으면 인증서버는 고객명과 단말기 일련번호를 DB서버에 등록하고 단말기 등록 성공 메시지를 상기 세션키로 암호화해 단말기에 전송하면 단말기에서 상기 메시지를 복호화해서 사용자PC에 등록 성공 메시지를 전송하는 과정을 포함하는 단말기 등록단계; 사용자가 사용자 PC에 단말기를 장착하면 사용자 PC와 단말기가 연결되며 사용자 PC에 신용카드 등록창이 실행되는 과정, 사용자가 IC칩이 내장된 신용카드를 단말기에 삽입하면 단말기는 신용카드를 자동 인식하면서 신용카드 번호와 사용자명을 읽는 과정, 단말기에서 신용카드 번호와 단말기에 사용자명을 입력값으로 하여 해쉬코드2를 생성하고 상기 해쉬코드2, 신용카드번호, 사용자명을 세션키(SK)로 암호화해서 메시지3(m3)을 생성하고 메시지3(m3)을 인증서버에 전송하는 과정, 인증서버는 메시지3(m3)을 세션키(SK)로 복호화하여 해쉬코드2, 신용카드번호, 사용자명을 추출하고, 상기 추출된 신용카드번호와 사용자명을 입력값으로 해쉬코드2'을 생성하고 상기 추출된 해쉬코드2와 해쉬코드2'을 비교하여 메시지3(m3)의 무결성을 검증하는 과정, 인증서버는 상기 신용카드번호와 사용자명을 신용카드사 서버에 전송하면 신용카드사 서버는 상기 신용카드가 유효한 카드인지 검증하여 결과값을 인증서버에 전달하는 과정, 인증서버는 상기 신용카드가 유효한 카드로 검증결과값을 받으면 DB서버에 사용자명과 해쉬코드2를 등록하고 신용카드가 정상 등록되었다는 결과를 사용자 PC에 전송하는 과정을 포함하는 신용카드 등록단계; 사용자가 온라인 쇼핑몰 서버에 접속하여 상품을 선택하고 결제요청을 하면 사용자 PC에 결제방식을 선택창이 뜨는 과정, 사용자가 결제방식 선택창에 온라인 신용카드 결제 단말기를 활용한 신용카드 결제 서비스(이하, 스마트결제)를 선택하면, 사용자PC는 PG사 서버에 스마트결제를 요청하고 스마트결제창이 실행되는 과정, 사용자는 단말기를 사용자 PC에 연결하고 해당 사용자PC에서 상기 단말기를 최초 사용하는 경우 스마트결제창에 단말기 비밀번호 입력을 요구하는 창이 뜨고 사용자가 단말기 비밀번호를 입력하면 사용자가 입력한 비밀번호와 단말기에 저장된 비밀번호를 비교하여 일치하면 단말기가 사용자PC와 연결되는 과정, 사용자가 IC칩이 내장된 신용카드를 단말기에 삽입하면 단말기는 상기 신용카드를 자동 인식하며, 신용카드번호와 사용자명을 읽고, 신용카드번호와 사용자명을 입력값으로 해쉬코드2를 생성하는 과정, 스마트결제창에 신용카드 비밀번호 입력창이 뜨면 사용자는 신용카드 비밀번호를 입력하고 단말기는 사용자가 입력한 신용카드 비밀번호와 신용카드에 등록된 신용카드 비밀번호가 일치하는지 여부를 검증하는 과정, 상기 신용카드 비밀번호가 검증되면 단말기는 신용카드번호와 사용자명을 입력값으로 생성한 상기 해쉬코드2를 인증서버에 전송하고, 인증서버는 상기 전송받은 해쉬코드2가 DB서버에 등록었는지, 등록이 되었다면 값이 일치하는지 비교하여 값이 일치하면 신용카드 등록을 확인하고 신용카드 등록확인 메시지를 단말기에 전송하는

과정, 단말기가 신용카드 등록확인 메시지를 받으면, 난수3(RND3)을 생성하고, 난수3(RND3)과 단말기 일련번호(SN)을 공개키(PK)로 암호화하여 메시지3(m3)을 생성하여, 상기 메시지3(m3)과 단말기 일련번호(SN)를 인증서버로 전송하는 과정, 인증서버는 전송받은 상기 메시지3(m3)을 HSM서버에 전달하고, HSM서버는 개인키(PrK)로 메시지3(m3)을 복호화하여 인증서버에 전달하는 과정, 인증서버는 메시지3(m3)을 복호화하여 추출된 단말기 일련번호(SN)를 DB서버에 등록된 단말기 일련번호(SN)와 비교하여 일치하는지 검증하는 과정, 상기 단말기 일련번호(SN)가 검증되면, 인증서버는 난수4(RND4)를 생성하고 난수3(RND3), 난수4(RND4), 단말기 일련번호(SN)로 부터 세션키2(SK2)를 생성하고, 상기 세션키2(SK2)로 단말기 일련번호(SN)와 난수4(RND4)를 암호화하여 메시지4(m4)를 생성하고, 상기 메시지4(m4)와 난수4(RND4)를 단말기에 전송하는 과정, 단말기는 전달받은 상기 난수4(RND4)와 단말기 일련번호(SN), 난수3(RND3)을 이용하여 세션키2(SK2)를 생성하고, 상기 세션키2(SK2)로 메시지4(m4)를 복호화하여 추출된 난수1(RND1)이 단말기에서 생성된 난수1(RND1)과 값이 일치하면 단말기와 인증서버간에 암호채널2을 형성하는 과정, 상기 암호채널2가 형성되면, 단말기는 거래전문을 생성하고 인증서버에 상기 거래전문을 전송하는 과정, 인증서버는 전송받은 거래전문을 신용카드사 서버에 전송하고 신용카드사 서버는 상기 거래전문을 참조하여 결제를 진행하고 결제처리결과를 온라인쇼핑몰 서버에 전송하는 과정, 온라인쇼핑몰은 신용카드사 서버로부터 결제처리결과를 받고 결제처리결과를 사용자 PC에 전송하면, 사용자 PC의 스마트 결제창에 결제처리 결과를 표시하는 과정을 포함하는 신용카드 결제단계;를 포함하는 것을 특징으로 하는 온라인 신용카드 결제 단말기를 활용한 신용카드 결제 서비스를 제공한다.

발명의 효과

[0005] 본 발명에 의하면, 온라인 신용카드 결제 단말기를 활용한 신용카드 결제 서비스를 이용하는 사용자는 안전하게 온라인 신용카드 결제를 할 수 있는 효과가 있다. 보다 구체적으로 신용카드결제가 되기 위해서 등록된 단말기와 신용카드를 소지하고 단말기 비밀번호와 신용카드 비밀번호를 알고 있어야 한다. 단말기와 인증서버는 단말기 발급시 생성된 공개키와 개인키를 이용해 상호인증을 하고 상호인증이 완료되면 암호통신을 위해 세션키를 공유하게 되며 세션키를 이용하여 암호채널을 형성하고 신용카드 결제에 필요한 정보(신용카드 번호, 신용카드 비밀번호, 사용자명 등)을 암호통신 한다. 이로 인해 PC 또는 네트웍상의 악성코드 또는 악의적목적을 가진 해커에 의해 정보가 유출되지 않고 안전하게 신용카드 거래를 할 수 있는 효과가 있다.

도면의 간단한 설명

[0006] 도1는 단말기 발급 및 배포단계를 나타낸 도면이다.

도2과 도3는 단말기 등록단계를 나타낸 도면이다.

도4는 신용카드 등록과정을 나타낸 도면이다.

도5와 도6는 신용카드 결제과정을 나타낸 도면이다.

도7은 단말기의 바람직한 실시예를 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

[0007] 이하 첨부된 도면을 참조하여, 본 발명의 바람직한 실시 예에 따라 본 발명을 상세히 설명하기로 한다.

[0008] 온라인 신용카드 결제 단말기를 활용한 신용카드 결제 서비스를 설명하기에 앞서 단말기 구현의 바람직한 실시예를 설명하기로 한다.

[0009] 도7은 단말기의 바람직한 실시예를 나타낸 도면이다. 단말기는

[0010] 단말기는 인터페이스부, 제어부, 스마트카드리더부, 보안칩(난수발생기,키생성부,저장부,암복호화부)로 구성된다.

[0011] 인터페이스부는 단말기와 사용자PC를 연결하여 데이터를 주고 받을수 있게 하며, USB, 시리얼포트, 병렬포트, 블루투스 등 다양한 연결방식을 사용하는 것이 가능하며, USB를 사용하는 것이 바람직하다.

[0012] 보안칩은 난수발생기, 키생성부, 저장부, 암복호화부를 포함한다. 난수발생기에서는 난수를 생성하며,저장부는 상기 난수, 개인키, 세션키, 단말기 일련번호 및 데이터등을 저장하며, 암복호화부에서는 데이터를 암호화/복호화를 수행한다. 보안칩은 스마트카드로 구현하는것이 바람직하다. 제어부와 보안칩은는 ISO7816 인터페이스로 연결되는 것이 바람직하다. 보안칩에 저장된 데이터는 외부로 유출이 불가능하다.

[0013] 스마트카드 리더부는 IC칩 형태의 신용카드를 삽입하고 신용카드와 제어부를 연결하여 상호간 데이터를 송수신하게 한다.

[0014] 제어부는 인터페이스부, 스마트카드리더부, 보안칩을 연결하여 상호간 데이터를 송수신하게 한다.

[0015] 이하 도1 ~ 도6을 참조하여, 본 발명의 바람직한 실시 예에 따른 온라인 신용카드 결제 단말기를 활용한 신용카드 결제 서비스에 대해 상세하게 설명한다.

[0016] 도1는 단말기 발급 및 배포단계를 나타낸 도면이다.

[0017] 도1를 참고로 배포단계를 상세히 설명한다.

[0018] 인증센터 HSM서버에서 장치인증용 공개키(PK)와 개인키(PrK)를 생성하여 저장하고(S101), 생성된 공개키(PK)를 제조사 단말기 발급시스템에 전달하면(S102), 제조사 단말기 발급시스템은 고유한 단말기 일련번호(SN)를 생성하고 생성된 단말기 일련번호(SN)와 상기 전달받은 공개키(PK)를 단말기에 주입(저장)하여 단말기를 발급하며(S103), 상기 단말기 일련번호(SN)는 인증센터의 DB 서버에 등록한다.(S104)

[0019] 사용자가 사용자 PC를 통해 온라인으로 사용자명, 사용자 핸드폰 번호 또는 이메일 주소를 입력하면서 신용카드사 서버에 단말기 발급 서비스 신청을 하면(S105), 신용카드사는 제조사에 단말기를 요청하고(S106) 제조사는 단말기를 신용카드사에 전달하고 단말기 장치 일련번호(SN)를 신용카드사 서버에 전달한다.(S107)

[0020] 신용카드사 서버가 사용자가 서비스 신청시 입력한 사용자 정보(사용자명, 사용자 핸드폰 번호 또는 이메일주소)와 단말기 일련번호를 인증서버에 전송하면 인증서버는 상기 사용자명, 사용자 핸드폰 번호 또는 이메일주소와 단말기 일련번호를 DB서버에 저장하고(S108), 신용카드사는 단말기를 사용자에게 배송한다.(S109)

[0021] 도2과 도3는 단말기 등록단계를 나타낸 도면이다.

[0022] 도2를 참고로 단말기 등록단계 중 인증코드 전달까지 과정를 상세히 설명한다.

[0023] 사용자가 사용자 PC에 단말기를 장착하면 사용자 PC와 단말기가 연결되며 사용자 PC에 단말기 등록창이 실행된다.(S201)

[0024] 사용자는 단말기 등록창을 통해 단말기 비밀번호와 사용자정보(사용자명, 사용자의 핸드폰번호 또는 이메일주소 등)를 등록한다.(S202)

[0025] 사용자PC는 상기 단말기 비밀번호, 사용자 정보(사용자명, 사용자 핸드폰번호 또는 이메일 주소 등)를 단말기에 전송한다.(S203)

[0026] 단말기는 상기 단말기 비밀번호, 사용자정보(사용자명, 사용자 핸드폰 번호 또는 이메일주소 등)를 저장한다.(S204)

[0027] 단말기는 단말기 일련번호, 사용자명, 사용자 핸드폰 번호 또는 이메일주소를 입력값으로 해쉬코드1을 생성한다.(S205)

[0028] 단말기는 단말기 일련번호, 사용자정보(사용자명, 사용자 핸드폰번호 또는 이메일주소 등), 해쉬코드1을 인증서버에 전송한다.(S206)

[0029] 인증서버는 전송받은 상기 단말기 일련번호, 사용자정보(사용자명, 사용자 핸드폰번호 또는 이메일주소 등)를 입력값으로 해쉬코드1'을 생성하고 전송받은 상기 해쉬코드1과 비교하여 일치하면 상기 단말기 일련번호, 사용자정보(사용자명, 사용자 핸드폰번호 또는 이메일주소 등)가 변조되지 않았다는 무결성을 검증한다.(S207)

[0030] 인증서버는 상기 단말기 일련번호(SN)에 대응하는 인증코드(AC)를 생성하여 DB서버에 저장하고, 상기 핸드폰번호 또는 이메일 주소로 상기 인증코드(AC)를 전송한다.(S208)

[0031] 도3를 참고로 인증코드 전달 이후부터 단말기 등록까지 과정를 상세히 설명한다.

[0032] 사용자는 핸드폰 또는 이메일로 전달받은 인증코드(AC)를 사용자 PC에 연결된 단말기에 입력한다.(S209)

[0033] 단말기는 난수1(RND1)을 생성 및 저장하고, 단말기 일련번호(SN), 상기 인증코드(AC), 난수1(RND1)을 장치 인증용 공개키(PK)로 암호화하여 메세지1(m1)을 생성하고 상기 단말기 일련번호(SN)와 메세지1(m1)을 인증서버에 전송한다.(S210)

[0034] 상기 난수1(RND1)은 단말기의 보안칩(스마트카드IC) 내부에서 생성되고 저장되기 때문에 외부로 유출될 수 없고 단말기 내부에서 안전하게 관리된다.

[0035] 인증서버는 전송받은 메시지1(m1)을 HSM서버로 전송하고 HSM서버는 저장된 개인키(PrK)로 상기 메시지1(m1)을 복호화하여 인증서버로 전송한다.(S211)

[0036] 인증서버는 전달받은 메시지1(m1)의 복호화 메시지로부터 단말기 일련번호(SN), 난수1(RND1), 인증코드(AC)를 추출하여 추출된 단말기 일련번호(SN)가 DB 서버에 등록되었는지 여부, 단말기 일련번호(SN)가 등록되었으면 등록된 단말기 일련번호에 대응하는 인증코드(AC)가 등록되었는지 여부, 인증코드(AC)가 등록되었으면 메시지1(m1)으로 부터 추출된 인증코드(AC)와 DB서버에 등록된 인증코드(AC)가 일치하는지 여부를 검증한다.(S212)

[0037] 상기 단말기 일련번호(SN)와 인증코드(AC)가 검증되면, 인증서버는 난수2(RND2)를 생성하고, 상기 난수2(RND2), 메시지1(m1)을 복호화하여 추출한 난수1(RND1), 단말기 일련번호(SN)로부터 세션키(SK)를 생성하고, 상기 세션키(SK)로 상기 단말기 일련번호(SN), 난수1(RND1)을 암호화하여 메시지2(m2)를 생성하며, 상기 메시지2(m2)와 난수2(RND2)를 인터넷망을 통해 사용자 PC에 연결된 단말기에 전송한다.(S213)

[0038] 상기 세션키를 생성하는 방법은 다양하게 사용할 수 있다. 예를 들어 단말기 일련번호(SN)와 난수2(RND2)를 난수1(RND1)로 암호화하여 세션키(SK)를 생성할 수 있고 특정 알고리즘을 적용하여 단말기 일련번호(SN), 난수1(RND1), 난수2(RND2)을 뒤섞어서 세션키(SK)를 생성할 수 있다.

[0039] 단말기는 전송받은 난수2(RND2)와 단말기에 저장된 난수1(RND1)과 단말기 일련번호(SN)로 부터 세션키(SK)를 생성하여 상기 세션키(SK)로 상기 전달받은 메세지2(m2)를 복호화하여 난수1(RND1)과 단말기 일련번호(SN)를 추출하고, 단말기에 저장된 난수1(RND1)과 메시지2(m2)로 부터 복호화하여 추출한 난수1(RND1)을 비교하여 값이 일치하는지 비교하여 일치하면 단말기와 인증서버간에 암호채널을 형성하고, 상기 세션키(SK)로 암호채널 형성완료 메시지를 암호화하여 인증서버에 전송한다.(S214)

[0040] 암호채널 형성완료 메시지를 받으면 인증서버는 고객명과 단말기 일련번호를 DB서버에 등록하고 단말기 등록 성공 메시지를 상기 세션키(SK)로 암호화해 단말기에 전송하면 단말기에서 상기 메시지를 복호화해서 사용자PC에 등록 성공 메시지를 전송한다.(S215)

[0041] 도4는 신용카드 등록과정을 나타낸 도면이다.

[0042] 사용자가 사용자 PC에 단말기를 장착하면 사용자 PC와 단말기가 연결되며 사용자 PC에 신용카드 등록창이 실행된다.(S301)

[0043] 사용자가 IC칩이 내장된 신용카드를 단말기에 삽입하면 단말기는 신용카드를 자동 인식하면서 신용카드 번호와 사용자명을 읽는다.(S302)

[0044] 단말기는 신용카드 번호와 단말기에 사용자명을 입력값으로 하여 해쉬코드2를 생성하고 상기 해쉬코드2, 신용카드번호, 사용자명을 세션키(SK)로 암호화해서 메시지3(m3)을 생성하고 메시지3(m3)을 인증서버에 전송한다.(S303)

[0045] 인증서버는 메시지3(m3)을 세션키(SK)로 복호화하여 해쉬코드2, 신용카드번호, 사용자명을 추출하고, 상기 추출된 신용카드번호와 사용자명을 입력값으로 해쉬코드2'을 생성하고 상기 추출된 해쉬코드2와 해쉬코드2'을 비교하여 메시지3(m3)의 무결성을 검증한다.(S304)

[0046] 인증서버는 상기 신용카드번호와 사용자명을 신용카드사 서버에 전송하면 신용카드사 서버는 상기 신용카드가 유효한 카드인지 검증하여 결과값을 인증서버에 전달한다.(S305)

[0047] 인증서버는 상기 신용카드가 유효한 카드로 검증결과값을 받으면 DB서버에 사용자명과 해쉬코드2를 등록하고 신용카드가 정상 등록되었다는 결과를 사용자 PC에 전송한다.(S306)

[0048] 도5와 도6는 신용카드 결제과정을 나타낸 도면이다.

[0049] 사용자가 온라인 쇼핑몰 서버에 접속하여 상품을 선택하고 결제요청을 하면 사용자 PC에 결제방식을 선택창이 뜬다.(S401)

[0050] 사용자가 결제방식 선택창에 온라인 신용카드 결제 단말기를 활용한 신용카드 결제 서비스(이하, 스마트결제)를

선택하면, 사용자PC는 PG사 서버에 스마트결제를 요청하고 스마트결제창이 실행된다.(S402)

[0051] 사용자는 단말기를 사용자 PC에 연결하고 해당 사용자PC에서 상기 단말기를 최초 사용하는 경우 스마트결제창에 단말기 비밀번호 입력을 요구하는 창이 뜨고 사용자가 단말기 비밀번호를 입력하면 사용자가 입력한 비밀번호와 단말기에 저장된 비밀번호를 비교하여 일치하면 단말기가 사용자PC와 연결된다.(S403)

[0052] 만일, 단말기 비밀번호가 일정회수(5회 등) 이상 틀리게 되면 자동으로 단말기가 잠기게 되는 것이 바람직하다. 단말기가 잠기게 되면 사용자는 단말기를 사용할 수 없게 된다.

[0053] 사용자가 IC칩이 내장된 신용카드를 단말기에 삽입하면 단말기는 상기 신용카드를 자동 인식하며, 신용카드번호와 사용자명을 읽고, 신용카드번호와 사용자명을 입력값으로 해쉬코드2를 생성한다.(S404)

[0054] 스마트결제창에 신용카드 비밀번호 입력창이 뜨면 사용자는 신용카드 비밀번호를 입력하고 단말기는 사용자가 입력한 신용카드 비밀번호와 신용카드에 등록된 신용카드 비밀번호가 일치하는지 여부를 검증한다.(S405)

[0055] 상기 신용카드 비밀번호가 검증되면 단말기는 신용카드번호와 사용자명을 입력값으로 생성한 상기 해쉬코드2를 인증서버에 전송하고, 인증서버는 상기 전송받은 해쉬코드2가 DB서버에 등록었는지, 등록이 되었다면 값이 일치하는지 비교하여 값이 일치하면 신용카드 등록을 확인하고 신용카드 등록확인 메시지를 단말기에 전송한다.(S406)

[0056] 단말기가 신용카드 등록확인 메시지를 받으면, 난수3(RND3)을 생성하고, 난수3(RND3)과 단말기 일련번호(SN)을 공개키(PK)로 암호화하여 메시지3(m3)을 생성하여, 상기 메시지3(m3)과 단말기 일련번호(SN)를 인증서버로 전송한다.(S407)

[0057] 인증서버는 전송받은 상기 메시지3(m3)을 HSM서버에 전달하고, HSM서버는 개인키(PrK)로 메시지3(m3)을 복호화하여 인증서버에 전달한다.(S408)

[0058] 인증서버는 메시지3(m3)을 복호화하여 추출된 단말기 일련번호(SN)를 DB서버에 등록된 단말기 일련번호(SN)와 비교하여 일치하는지 검증한다.(S409)

[0059] 상기 단말기 일련번호(SN)가 검증되면, 인증서버는 난수4(RND4)를 생성하고 난수3(RND3), 난수4(RND4), 단말기 일련번호(SN)로 부터 세션키2(SK2)를 생성하고, 상기 세션키2(SK2)로 단말기 일련번호(SN)와 난수4(RND4)를 암호화하여 메시지4(m4)를 생성하고, 상기 메시지4(m4)와 난수4(RND4)를 단말기에 전송한다.(S410)

[0060] 단말기는 전달받은 상기 난수4(RND4)와 단말기 일련번호(SN), 난수3(RND3)을 이용하여 세션키2(SK2)를 생성하고, 상기 세션키2(SK2)로 메시지4(m4)를 복호화하여 추출된 난수1(RND1)이 단말기에서 생성된 난수1(RND1)과 값이 일치하면 단말기와 인증서버간에 암호채널2을 형성한다.(S411)

[0061] 상기 암호채널2가 형성되면, 단말기는 거래전문을 생성하고 인증서버에 상기 거래전문을 전송한다.(S412)

[0062] 인증서버는 전송받은 거래전문을 신용카드사 서버에 전송하고 신용카드사 서버는 상기 거래전문을 참조하여 결제를 진행하고 결제처리결과를 온라인쇼핑몰 서버에 전송한다.(S413)

[0063] 온라인쇼핑몰은 신용카드사 서버로부터 결제처리결과를 받고 결제처리결과를 사용자 PC에 전송하면, 사용자 PC의 스마트결제창에 결제처리 결과를 표시한다.(S414)

[0064] 이상 첨부된 도면을 참고로 본 발명의 바람직한 실시 예를 통해 설명하였지만, 본 발명은 이에 한정되지 않고 다양한 변화와 변경 및 균등물을 사용할 수 있다. 따라서 본 발명은 상기 실시 예를 적절히 변형하여 응용할 수 있고, 이러한 응용도 하기 특허청구범위에 기재된 기술적 사상을 바탕으로 하는 한 본 발명의 권리범위에 속하게 됨은 당연하다 할 것이다.

산업상 이용가능성

[0065] 본 발명은 안전한 온라인 신용카드 결제 서비스가 필요한 산업분야에 광범위하게 이용될 수 있다.

부호의 설명

[0066] 100 : 인증서버 200 : HSM서버

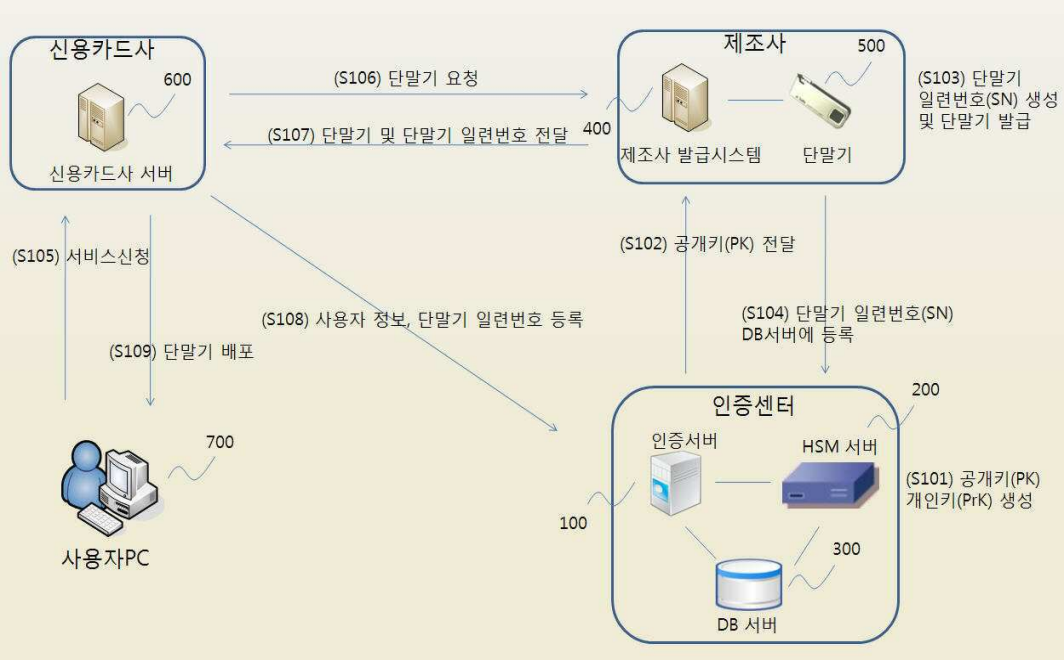
300 : DB서버 400 : 제조사 발급시스템

500 : 단말기 600 : 신용카드사 서버

700 : 사용자PC

도면

도면1

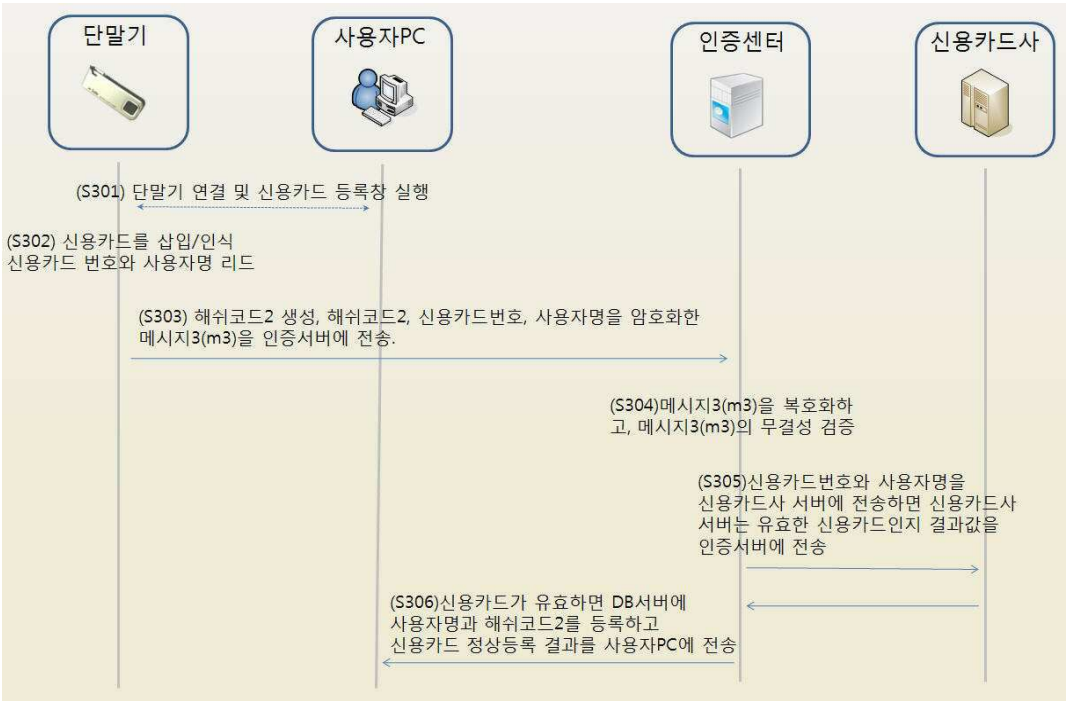


도면2

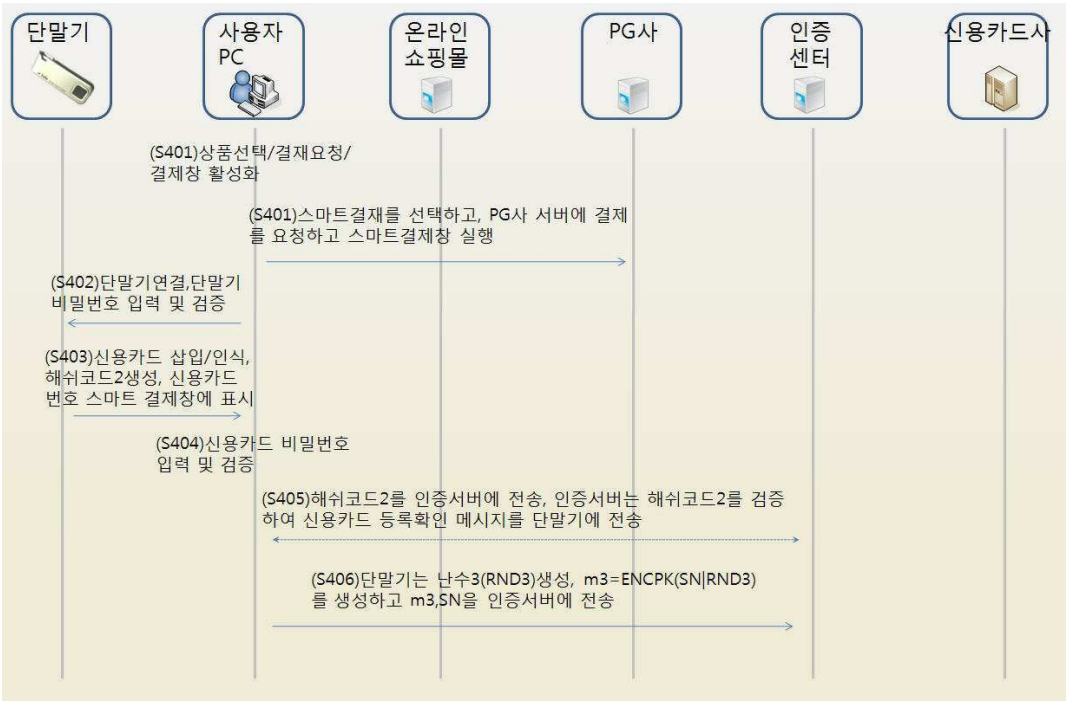
도면3


단말기
사용자PC
인증센터
(S209) 인증코드(AC) 입력
(S210) 단말기일련번호(SN), 메시지1(m1)=ENCPK(SN|AC|RND1) 을 인증서버에 전송
(S211) 메시지1(m1)을 HSM 서버에 전달하여 복호화
(S212) 단말기 일련번호(SN), 난수1(RND1), 인증코드(AC)검증
(S213) 난수2(RND2),메시지2(m2)=ENC2SK(SN|RND1)를 단말기에 전송
(S214) 메시지2(m2)에 대한 검증이 완료되면 단말기와 인증서버 사이에 암호채널을 형성하고, 암호채널 형성완료 메시지를 암호화하여 전송
(S215) 인증서버는 단말기를 등록하고 단말기 등록 성공 메시지를 전송

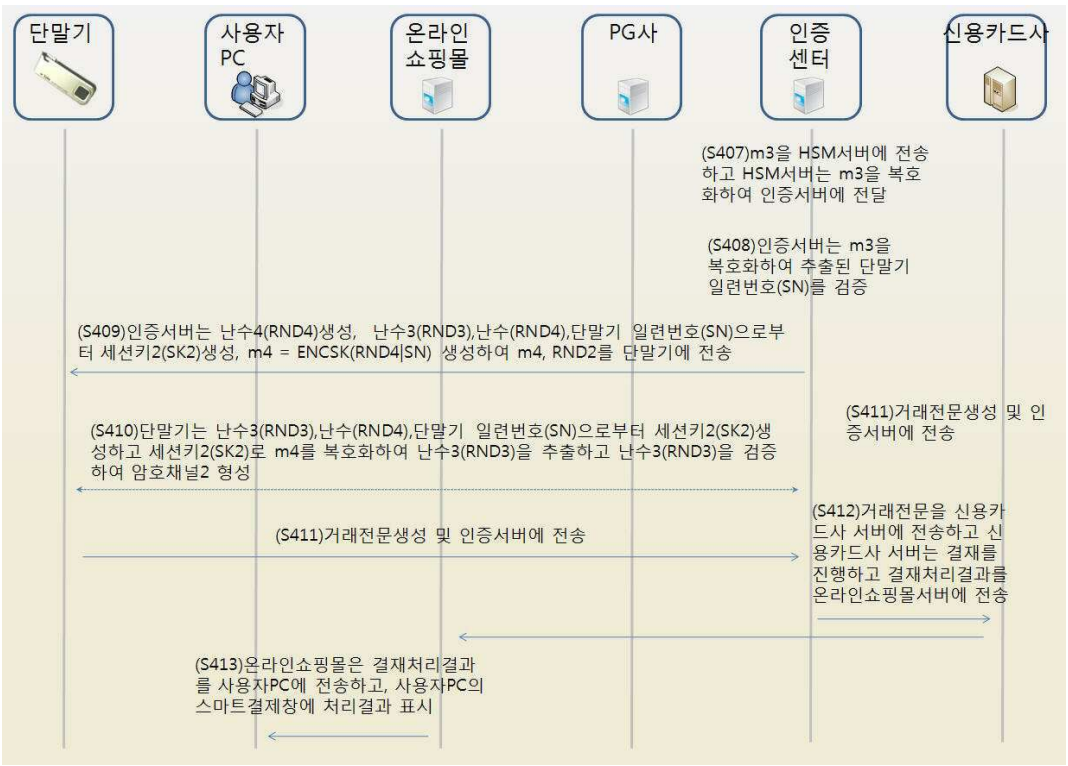
도면4


단말기
사용자PC
인증센터
신용카드사
(S301) 단말기 연결 및 신용카드 등록창 실행
(S302) 신용카드를 삽입/인식
신용카드 번호와 사용자명 리드
(S303) 해쉬코드2 생성, 해쉬코드2, 신용카드번호, 사용자명을 암호화한 메시지3(m3)을 인증서버에 전송.
(S304)메시지3(m3)을 복호화하고, 메시지3(m3)의 무결성 검증
(S305)신용카드번호와 사용자명을 신용카드사 서버에 전송하면 신용카드사 서버는 유효한 신용카드인지 결과값을 인증서버에 전송
(S306)신용카드가 유효하면 DB서버에 사용자명과 해쉬코드2를 등록하고 신용카드 정상등록 결과를 사용자PC에 전송

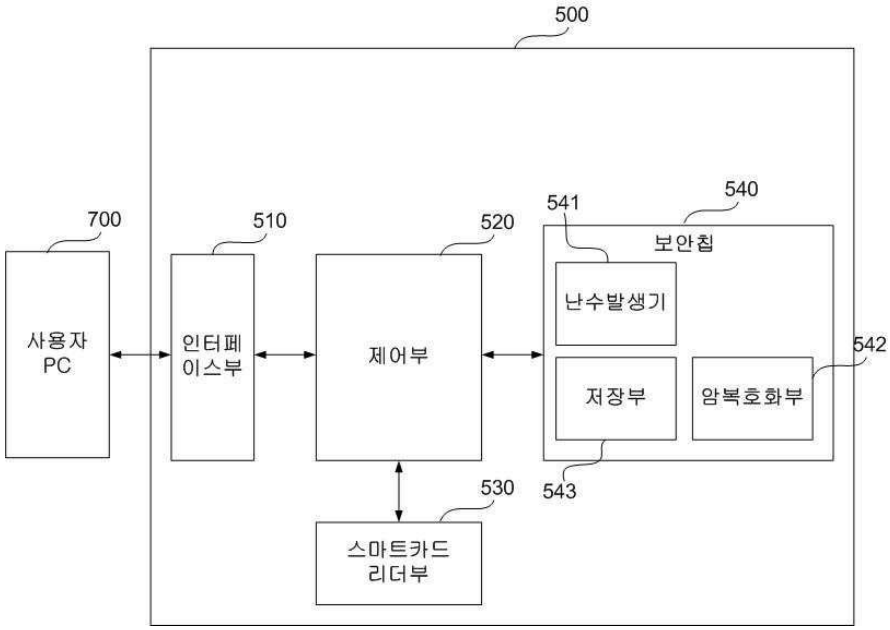
도면5


단말기
사용자 PC
온라인 쇼핑몰
PG사
인증 센터
신용카드사
(S401)상품선택/결재요청/ 결제창 활성화
(S401)스마트결재를 선택하고, PG사 서버에 결제를 요청하고 스마트결제창 실행
(S402)단말기연결,단말기 비밀번호 입력 및 검증
(S403)신용카드 삽입/인식, 해쉬코드2생성, 신용카드 번호 스마트 결제창에 표시
(S404)신용카드 비밀번호 입력 및 검증
(S405)해쉬코드2를 인증서버에 전송, 인증서버는 해쉬코드2를 검증하여 신용카드 등록확인 메시지를 단말기에 전송
(S406)단말기는 난수3(RND3)생성, m3=ENCPK(SN|RND3)를 생성하고 m3,SN을 인증서버에 전송

도면6


단말기
사용자 PC
온라인 쇼핑몰
PG사
인증 센터
신용카드사
(S407)m3을 HSM서버에 전송하고 HSM서버는 m3을 복호화하여 인증서버에 전달
(S408)인증서버는 m3을 복호화하여 추출된 단말기 일련번호(SN)를 검증
(S409)인증서버는 난수4(RND4)생성, 난수3(RND3),난수(RND4),단말기 일련번호(SN)으로부터 세션키2(SK2)생성, m4 = ENCSK(RND4|SN) 생성하여 m4, RND2를 단말기에 전송
(S411)거래전문생성 및 인증서버에 전송
(S410)단말기는 난수3(RND3),난수(RND4),단말기 일련번호(SN)으로부터 세션키2(SK2)생성하고 세션키2(SK2)로 m4를 복호화하여 난수3(RND3)을 추출하고 난수3(RND3)을 검증하여 암호채널2 형성
(S411)거래전문생성 및 인증서버에 전송
(S412)거래전문을 신용카드사 서버에 전송하고 신용카드사 서버는 결재를 진행하고 결재처리결과를 온라인쇼핑몰서버에 전송
(S413)온라인쇼핑몰은 결재처리결과를 사용자PC에 전송하고, 사용자PC의 스마트결제창에 처리결과 표시

도면7


500
700
사용자 PC
510
인터페이스부
520
제어부
530
스마트카드 리더부
540
보안칩
541
난수발생기
542
암복호화부
543
저장부