(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0029940
(43) 공개일자 2017년03월16일

(51) 국제특허분류(Int. Cl.)
G06Q 20/40 (2012.01) *G06Q 20/34* (2012.01)
G06Q 20/38 (2012.01)
(52) CPC특허분류
G06Q 20/4012 (2013.01)
G06Q 20/34 (2013.01)
(21) 출원번호 10-2015-0127131
(22) 출원일자 2015년09월08일
심사청구일자 없음

(71) 출원인
에스케이플래닛 주식회사
경기도 성남시 분당구 판교로 264 (삼평동)
(72) 발명자
곽세병
서울특별시 성북구 돌곶이로14길 22 (석관동)
이주원
서울특별시 노원구 마들로 31, 110동 1003호 (월계동, 그랑빌아파트)
(74) 대리인
전종학, 이용하

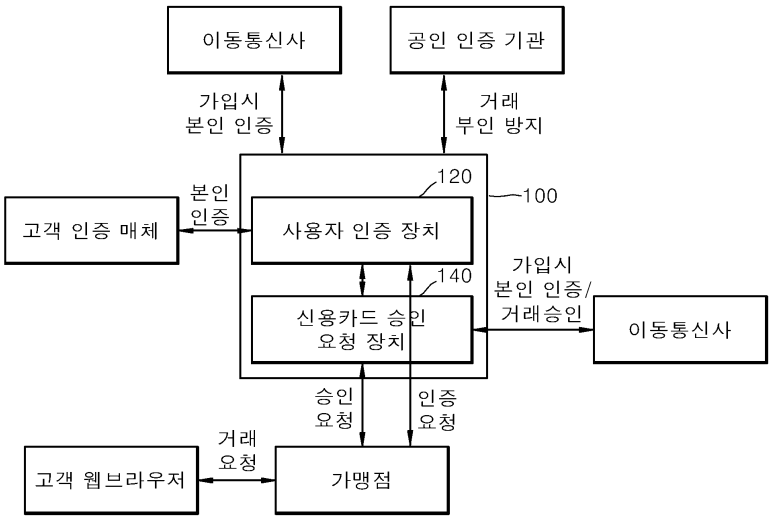
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 장치 및 방법, 그리고 시스템 및 컴퓨터 프로그램이 기록된 기록매체**

(57) 요 약

본 발명은 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 장치 및 방법, 그리고 시스템 및 컴퓨터 프로그램이 기록된 기록매체에 관한 것으로, 더욱 상세히는 웹 표준 환경에서 비대면 지급 결제가 가능하도록 구성된 웹기반 간편 결제에서 단일 결제 수단에 대해 복수의 PIN을 설정하고 해당 각 PIN에 대응되어 한도를 달리 설정하도록 하는 것으로 결제 편의성과 보안성을 모두 만족시킬 수 있도록 한 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 장치 및 방법, 그리고 시스템 및 컴퓨터 프로그램이 기록된 기록매체에 관한 것이다.

대 표 도 - 도2



(52) CPC특허분류
G06Q 20/3823 (2013.01)
G06Q 20/409 (2013.01)

명 세 서

청구범위

청구항 1

신용 카드 번호를 암호화하여 저장하고 신용 카드 인증 값을 암호화하여 정보 블록 1 및 정보 블록 2로 분할하되, 상기 정보 블록 1은 상기 정보 블록 2의 복호화를 위해 사용되고, 상기 정보 블록 1을 사용자 인증 장치로 전송하고 상기 정보 블록 1은 삭제하도록 구현되는 신용 카드 승인 요청 장치; 및

사용자 장치로부터 서로 다른 복수의 결제 PIN(personal identification number) 정보와 각 결제 PIN 정보에 대응되는 결제 한도가 설정된 설정정보를 수신하며, 상기 정보 블록 1에 대하여 상기 각 결제 PIN 정보를 기반으로 암호화하고 상기 설정정보를 기초로 암호화에 이용된 결제 PIN 정보에 대응되는 결제 한도를 설정하여 생성한 서로 다른 결제 한도가 설정된 복수의 암호화된 정보 블록 1을 저장하고, 사용자에 의한 상거래가 발생한 웹 기반 상거래 장치로부터 임시 가상 카드 번호와 결제 내역에 대한 결제 정보 수신시 상기 사용자 장치로 상기 정보 블록 1을 생성하기 위한 결제 PIN 정보를 요청하여 상기 사용자 장치로부터 수신된 결제 PIN 정보를 기반으로 복호화되는 상기 암호화된 정보 블록 1에 설정된 결제 한도와 상기 결제 정보에 따른 결제 금액을 비교하여 결제 가능 여부를 판단하고, 결제 가능시 상기 사용자 장치로부터 수신된 결제 PIN 정보를 기반으로 복호화한 정보 블록 1을 상기 신용 카드 승인 요청 장치로 전송하는 사용자 인증 장치를 포함하는 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 장치.

청구항 2

제 1항에 있어서,

상기 신용 카드 승인 요청 장치는 상기 정보 블록 1을 기반으로 상기 정보 블록 2를 복호화하여 상기 정보 블록 1 및 상기 정보 블록 2을 기반으로 암호화된 상기 신용 카드 인증 값을 복호화하고 암호화된 상기 신용 카드 번호를 복호화하며, 상기 신용카드 인증 값 및 상기 신용 카드 번호를 기반으로 신용 카드사로 전송할 승인 전문을 생성하고, 상기 승인 전문을 상기 신용 카드사로 전송하도록 구현되는 것을 특징으로 하는 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 장치.

청구항 3

제 2항에 있어서,

상기 신용 카드 번호에 대한 암호화는 HSM(hardware security module) 및 해쉬를 기반으로 수행되고,

상기 신용 카드 인증 값에 대한 암호화는 상기 HSM을 기반으로 수행되고,

상기 정보 블록 1은 상기 사용자 인증 장치에서 상기 결제 PIN 정보를 기반으로 AES(advanced encryption standard)를 통해 암호화되는 것을 특징으로 하는 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 장치.

청구항 4

제 3항에 있어서,

상기 신용 카드 승인 요청 장치는 회원 가입 절차를 통해 사용자 장치로부터 상기 신용 카드 번호 및 상기 신용 카드 인증 값을 수신하는 것을 특징으로 하는 결제 서비스 제공 장치.

청구항 5

제 1항에 있어서,

상기 사용자 인증 장치는 상기 결제 가능 여부에 따른 결제 불가시 상기 사용자 장치로 다른 결제 PIN 정보를 요청하는 것을 특징으로 하는 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 장치.

청구항 6

제 1항에 있어서,

상기 사용자 인증 장치는 상기 설정정보를 기초로 가장 높은 결제 한도에 대응되는 결제 PIN 정보를 구성하는 복수의 자리 중 사용자 장치의 선택에 따라 선택된 일부 자리의 코드를 상이한 결제 한도가 설정되는 다른 결제 PIN 정보로 이용하는 것을 특징으로 하는 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 장치.

청구항 7

신용 카드 승인 요청 장치가 신용 카드 번호를 암호화하여 저장하고, 신용 카드 인증 값을 암호화하여 정보 블록 1 및 정보 블록 2로 분할한 후 상기 정보 블록 1을 사용자 인증 장치로 전송하고 상기 정보 블록 1을 삭제하는 단계, 상기 정보 블록 1은 상기 정보 블록 2의 복호화를 위해 사용됨;

상기 사용자 인증 장치가 사용자 장치로부터 서로 다른 복수의 결제 PIN(personal identification number) 정보와 각 결제 PIN 정보에 대응되는 결제 한도가 설정된 설정정보를 수신하고, 상기 정보 블록 1에 대하여 상기 각 결제 PIN 정보를 기반으로 암호화하고 상기 설정정보를 기초로 암호화에 이용된 결제 PIN 정보에 대응되는 결제 한도를 설정하여 서로 다른 결제 한도가 설정된 복수의 암호화된 정보 블록 1을 생성한 후 저장하는 단계;

상기 사용자 인증 장치가 사용자에 의한 상거래가 발생한 웹 기반 상거래 장치로부터 임시 가상 카드 번호와 결제 내역에 대한 결제정보 수신시 상기 사용자 장치로 상기 정보 블록 1을 생성하기 위한 결제 PIN 정보를 요청하여 상기 사용자 장치로부터 수신된 결제 PIN 정보를 기반으로 복호화되는 상기 암호화된 정보 블록 1에 설정된 결제 한도와 상기 결제 정보에 따른 결제 금액을 비교하여 결제 가능 여부를 판단하는 단계; 및

상기 사용자 인증 장치가 결제 가능시 상기 사용자 장치로부터 수신된 결제 PIN 정보를 기반으로 복호화한 정보 블록 1을 상기 신용 카드 승인 요청 장치로 전송하는 단계를 포함하는 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 방법.

청구항 8

제 7항에 있어서,

상기 신용 카드 승인 요청 장치가 상기 정보 블록 1을 기반으로 상기 정보 블록 2를 복호화하여 상기 정보 블록 1 및 상기 정보 블록 2을 기반으로 암호화된 상기 신용 카드 인증 값을 복호화하고, 암호화된 상기 신용 카드 번호를 복호화하는 단계; 및

상기 신용 카드 승인 요청 장치가 상기 복호화된 신용카드 인증 값 및 상기 신용 카드 번호를 기반으로 신용 카드사로 전송할 승인 전문을 생성하고, 상기 승인 전문을 상기 신용 카드사로 전송하는 단계를 더 포함하는 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 방법.

청구항 9

제 7항 내지 제 8항 중 어느 한 항에 따른 방법을 수행하는 컴퓨터 프로그램이 기록된 기록매체.

청구항 10

회원 가입 절차를 통해 상기 신용 카드 번호 및 신용 카드 인증 값을 전송하는 사용자 장치;

상기 사용자 장치에 의한 상거래가 발생한 경우, 임시 가상 카드 번호와 결제 내역에 대한 정보를 생성하여 전송하는 웹 기반 상거래 장치; 및

상기 사용자 장치로부터 수신된 신용 카드 번호를 암호화하여 저장하고 신용 카드 인증 값을 암호화하여 정보 블록 1 및 정보 블록 2로 분할하되, 상기 정보 블록 1은 상기 정보 블록 2의 복호화를 위해 사용되고, 상기 정보 블록 1을 사용자 장치로부터 수신한 서로 다른 복수의 결제 PIN(personal identification number) 정보를 이용하여 각 결제 PIN 정보를 기반으로 암호화된 서로 다른 정보 블록 1을 저장하고, 상기 각 암호화된 정보 블록 1에 대하여 상기 사용자 장치로부터 수신된 설정정보를 기초로 서로 다른 결제 한도를 설정하며, 상기 웹 기반 상거래 장치로부터 임시 가상 카드 번호와 결제 내역에 대한 결제 정보 수신시 상기 사용자 장치로 상기 정보 블록 1을 생성하기 위한 결제 PIN 정보를 요청하고, 이를 통해 수신된 결제 PIN 정보로 복호화되는 암호화된 정보 블록 1에 설정된 결제 한도와 상기 결제 정보에 따른 결제 금액을 비교하여 결제 가능 여부를 판단하고, 결제 가능시 상기 사용자 장치로부터 수신된 결제 PIN 정보를 기반으로 복호화한 정보 블록 1과 상기 정보 블록 1을 기반으로 복호화한 상기 정보 블록 2를 기반으로 암호화된 상기 신용 카드 인증 값을 복호화하고 암호화된

상기 신용 카드 번호를 복호화하여 결제 처리하는 결제 서비스 제공 장치를 포함하는 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 장치 및 방법, 그리고 시스템 및 컴퓨터 프로그램이 기록된 기록매체에 관한 것으로, 더욱 상세히는 웹 표준 환경에서 비대면 지급 결제가 가능하도록 구성된 웹기반 간편 결제에서 단일 결제 수단에 대해 복수의 PIN을 설정하고 해당 각 PIN에 대응되어 한도를 달리 설정하도록 하는 것으로 결제 편의성과 보안성을 모두 만족시킬 수 있도록 한 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 장치 및 방법, 그리고 시스템 및 컴퓨터 프로그램이 기록된 기록매체에 관한 것이다.

배 경 기 술

[0002] 이동 통신 기술의 발전으로 휴대 전화나 PDA(personal digital assistant)와 같은 무선 디바이스의 사용이 급증하였으며, 유선 인터넷에서 행해지던 서비스도 점차 무선 인터넷 기반의 서비스로 옮겨가고 있다.

[0003] 무선 네트워크가 활성화되면서 상업, 서비스 분야에도 많은 유무선 네트워크를 이용한 다양한 서비스들이 제공되고 있다. 예를 들어, 모바일 전자 상거래인 M-커머스(mobile-commerce)는 무선 네트워크 기반의 상거래 서비스 중 하나의 예이다.

[0004] 비대면으로 상거래를 수행하기 위해서는 본인에 대한 인증 절차 및 결제 절차를 통해 비용을 지불하는 절차가 필요하다. 기존의 인증 및 결제 절차를 통한 온라인 결제 방식은 신용카드 번호, 폰 빌 등 개별적인 인증 방식을 통해서 결제를 진행하는 방식이다. 기존에 결제 방식에서는 결제 서버가 신용카드, 계좌 이체 등 결제 정보를 저장할 수가 없어서 안심 클릭이나, ISP 신용 카드 결제를 이용하거나, 간편 결제의 경우 신용카드/계좌 이체사와 협의 하에 가상 카드를 기반으로 결제를 진행하는 방식이었다. 간편 결제 제공 방식 또한 주로 앱 기반으로 제공된다. 이러한 온라인 상의 상거래를 위한 공통적인 표준 방식은 제공되지 않고 있다.

[0005] 한편, 일반적으로 기존의 결제 방식은 하나의 신용카드에 대하여 결제 한도가 단일로 설정되며, 신용카드의 결제 한도를 높이기 위해서는 카드사에 연락하여 설정을 변경해야 하는 복잡한 절차가 필요한 문제점이 있다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 한국등록특허 제10-0706894호 [발명의 명칭: 후불 결제 한도를 이용한 이동 통신 단말 스마트 카드의 사용 제어 방법과 이를 위한 이동 통신 단말 및 후불 결제한도 관리 시스템]

발명의 내용

해결하려는 과제

[0007] 본 발명의 목적은 웹 표준 환경에서 비대면 지급 결제를 위한 웹 기반 인증 결제 방법을 제공하는 동시에 단일 결제 수단에 대해서 복수의 PIN을 등록하고, 해당 PIN마다 결제에 대한 한도를 달리 설정함으로써, 결제 내용에 따라 보안성 정도가 다른 PIN을 이용하도록 하여 높은 한도에 대한 PIN 유출 위험성을 낮추고 결제 한도가 낮게 설정된 PIN은 그 구성이 상대적으로 간소하도록 하여 입력 편의성을 높이도록 함을 목적으로 한다.

[0008] 또한, 본 발명의 다른 목적은 사용자 장치에서 결제시 발생하는 다양한 침해 유형에 대한 보안성을 제공함을 그 목적으로 한다.

과제의 해결 수단

[0009] 본 발명의 실시예에 따른 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 장치는 신용 카드 번호를 암호화하여 저장하고 신용 카드 인증 값을 암호화하여 정보 블록 1 및 정보 블록 2로 분할하되, 정보 블록 1은 정보 블록 2의 복호화를 위해 사용되고, 정보 블록 1을 사용자 인증 장치로 전송하고 정보 블록 1은 삭제하도록 구현

되는 신용 카드 승인 요청 장치 및 사용자 장치로부터 서로 다른 복수의 결제 PIN(personal identification number) 정보와 각 결제 PIN 정보에 대응되는 결제 한도가 설정된 설정정보를 수신하며, 정보 블록 1에 대하여 각 결제 PIN 정보를 기반으로 암호화하고 설정정보를 기초로 암호화에 이용된 결제 PIN 정보에 대응되는 결제 한도를 설정하여 생성한 서로 다른 결제 한도가 설정된 복수의 암호화된 정보 블록 1을 저장하고, 사용자에 의한 상거래가 발생한 웹 기반 상거래 장치로부터 임시 가상 카드 번호와 결제 내역에 대한 결제 정보 수신시 사용자 장치로 정보 블록 1을 생성하기 위한 결제 PIN 정보를 요청하여 사용자 장치로부터 수신된 결제 PIN 정보를 기반으로 복호화되는 암호화된 정보 블록 1에 설정된 결제 한도와 결제 정보에 따른 결제 금액을 비교하여 결제 가능 여부를 판단하고, 결제 가능시 사용자 장치로부터 수신된 결제 PIN 정보를 기반으로 복호화한 정보 블록 1을 신용 카드 승인 요청 장치로 전송하는 사용자 인증 장치를 포함할 수 있다.

[0010] 본 발명과 관련된 일 예로서, 신용 카드 승인 요청 장치는 정보 블록 1을 기반으로 정보 블록 2를 복호화하여 정보 블록 1 및 정보 블록 2을 기반으로 암호화된 신용 카드 인증 값을 복호화하고 암호화된 신용 카드 번호를 복호화하며, 신용카드 인증 값 및 신용 카드 번호를 기반으로 신용 카드사로 전송할 승인 전문을 생성하고, 승인 전문을 신용 카드사로 전송하도록 구현되는 것을 특징으로 할 수 있다.

[0011] 본 발명과 관련된 일 예로서, 신용 카드 번호에 대한 암호화는 HSM(hardware security module) 및 해쉬를 기반으로 수행되고, 신용 카드 인증 값에 대한 암호화는 HSM을 기반으로 수행되고, 정보 블록 1은 사용자 인증 장치에서 결제 PIN 정보를 기반으로 AES(advanced encryption standard)를 통해 암호화되는 것을 특징으로 할 수 있다.

[0012] 본 발명과 관련된 일 예로서, 신용 카드 승인 요청 장치는 회원 가입 절차를 통해 사용자 장치로부터 신용 카드 번호 및 신용 카드 인증 값을 수신하는 것을 특징으로 할 수 있다.

[0013] 본 발명과 관련된 일 예로서, 사용자 인증 장치는 결제 가능 여부에 따른 결제 불가시 사용자 장치로 다른 결제 PIN 정보를 요청하는 것을 특징으로 할 수 있다.

[0014] 본 발명과 관련된 일 예로서, 사용자 인증 장치는 설정정보를 기초로 가장 높은 결제 한도에 대응되는 결제 PIN 정보를 구성하는 복수의 자리 중 사용자 장치의 선택에 따라 선택된 일부 자리의 코드를 상이한 결제 한도가 설정되는 다른 결제 PIN 정보로 이용하는 것을 특징으로 할 수 있다.

[0015] 본 발명의 실시예에 따른 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 방법은 신용 카드 승인 요청 장치가 신용 카드 번호를 암호화하여 저장하고, 신용 카드 인증 값을 암호화하여 정보 블록 1 및 정보 블록 2로 분할한 후 정보 블록 1을 사용자 인증 장치로 전송하고 정보 블록 1을 삭제하는 단계, 정보 블록 1은 정보 블록 2의 복호화를 위해 사용됨과, 사용자 인증 장치가 사용자 장치로부터 서로 다른 복수의 결제 PIN(personal identification number) 정보와 각 결제 PIN 정보에 대응되는 결제 한도가 설정된 설정정보를 수신하고, 정보 블록 1에 대하여 각 결제 PIN 정보를 기반으로 암호화하고 설정정보를 기초로 암호화에 이용된 결제 PIN 정보에 대응되는 결제 한도를 설정하여 서로 다른 결제 한도가 설정된 복수의 암호화된 정보 블록 1을 생성한 후 저장하는 단계와, 사용자 인증 장치가 사용자에 의한 상거래가 발생한 웹 기반 상거래 장치로부터 임시 가상 카드 번호와 결제 내역에 대한 결제정보 수신시 사용자 장치로 정보 블록 1을 생성하기 위한 결제 PIN 정보를 요청하여 사용자 장치로부터 수신된 결제 PIN 정보를 기반으로 복호화되는 암호화된 정보 블록 1에 설정된 결제 한도와 결제 정보에 따른 결제 금액을 비교하여 결제 가능 여부를 판단하는 단계 및 사용자 인증 장치가 결제 가능시 사용자 장치로부터 수신된 결제 PIN 정보를 기반으로 복호화한 정보 블록 1을 신용 카드 승인 요청 장치로 전송하는 단계를 포함할 수 있다.

[0016] 본 발명과 관련된 일 예로서, 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 방법은 신용 카드 승인 요청 장치가 정보 블록 1을 기반으로 정보 블록 2를 복호화하여 정보 블록 1 및 정보 블록 2을 기반으로 암호화된 신용 카드 인증 값을 복호화하고, 암호화된 신용 카드 번호를 복호화하는 단계 및 신용 카드 승인 요청 장치가 복호화된 신용카드 인증 값 및 신용 카드 번호를 기반으로 신용 카드사로 전송할 승인 전문을 생성하고, 승인 전문을 신용 카드사로 전송하는 단계를 더 포함할 수 있다.

[0017] 본 발명의 실시예에 따른 기록매체에는 상술한 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 방법을 수행하는 컴퓨터 프로그램이 저장될 수 있다.

[0018] 본 발명의 실시예에 따른 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 시스템은 회원 가입 절차를 통해 신용 카드 번호 및 신용 카드 인증 값을 전송하는 사용자 장치와, 사용자 장치에 의한 상거래가 발생한 경우, 임시 가상 카드 번호와 결제 내역에 대한 정보를 생성하여 전송하는 웹 기반 상거래 장치 및 사용자 장치

로부터 수신된 신용 카드 번호를 암호화하여 저장하고 신용 카드 인증 값을 암호화하여 정보 블록 1 및 정보 블록 2로 분할하되, 정보 블록 1은 정보 블록 2의 복호화를 위해 사용되고, 정보 블록 1을 사용자 장치로부터 수신한 서로 다른 복수의 결제 PIN(personal identification number) 정보를 이용하여 각 결제 PIN 정보를 기반으로 암호화된 서로 다른 정보 블록 1을 저장하고, 각 암호화된 정보 블록 1에 대하여 사용자 장치로부터 수신된 설정정보를 기초로 서로 다른 결제 한도를 설정하며, 웹 기반 상거래 장치로부터 임시 가상 카드 번호와 결제 내역에 대한 결제 정보 수신시 사용자 장치로 정보 블록 1을 생성하기 위한 결제 PIN 정보를 요청하고, 이를 통해 수신된 결제 PIN 정보로 복호화되는 암호화된 정보 블록 1에 설정된 결제 한도와 결제 정보에 따른 결제 금액을 비교하여 결제 가능 여부를 판단하고, 결제 가능시 사용자 장치로부터 수신된 결제 PIN 정보를 기반으로 복호화한 정보 블록 1과 정보 블록 1을 기반으로 복호화한 정보 블록 2를 기반으로 암호화된 신용 카드 인증 값을 복호화하고 암호화된 신용 카드 번호를 복호화하여 결제 처리하는 결제 서비스 제공 장치를 포함할 수 있다.

발명의 효과

[0019] 본 발명은 웹 표준 환경에서 비대면 지급 결제를 위한 웹 기반 인증 결제 방법을 제공하는 동시에 단일 결제 수단에 대한 서로 다른 결제 한도에 따른 PIN을 달리 설정하도록 하고, 해당 PIN 입력 정보를 통해 한도를 달리 적용할 수 있으며, 소액 결제 한도의 PIN을 간단하게 설정하는 것으로 소액에 대한 결제 편의성을 높일 수 있고, 소액 결제 한도보다 높은 일반 한도에 대한 PIN의 전체 노출을 줄일 수 있어 보안성을 높이는 효과가 있다.

[0020] 또한, 본 발명은 고객에게는 결제 이용 편의성 및 안전한 결제를 제공하고 글로벌 웹 표준에 맞춘 결제 서비스를 제공함으로써 다른 국가에서도 본 발명의 실시예에 따른 결제 서비스를 기반으로 결제를 진행할 수 있는 동시에 사용자 장치에서 결제시 발생하는 다양한 침해 유형을 방지하여 높은 보안성을 제공하는 효과가 있다.

도면의 간단한 설명

[0021] 도 1은 본 발명의 실시예에 따른 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 시스템의 구성 환경도.

도 2는 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 시스템을 구성하는 결제 서비스 제공 장치의 동작 개념도.

도 3은 본 발명의 실시예에 따른 사용자 회원 가입 절차를 나타낸 개념도.

도 4는 본 발명의 실시예에 따른 사용자 회원 가입 절차를 나타낸 흐름도.

도 5는 본 발명의 실시예에 따른 신용 카드 승인 요청 장치 및 사용자 인증 장치에서 신용 카드 번호와 신용 카드 인증값을 암호화하는 방법에 대한 개념도.

도 6은 사용자에 의한 웹 기반 상거래 발생시 본 발명의 실시예에 따른 결제 서비스 제공 장치의 결제 PIN의 입력에 따른 결제 절차를 나타낸 흐름도.

도 7은 본 발명의 실시예에 따른 결제 PIN의 입력에 따른 결제 절차를 나타낸 개념도.

도 8은 본 발명의 실시예에 따른 결제 서비스 제공 장치의 설정정보에 따른 서로 다른 결제 PIN 구성에 대한 예시도.

발명을 실시하기 위한 구체적인 내용

[0022] 본 발명에서 사용되는 기술적 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아님을 유의해야 한다. 또한, 본 발명에서 사용되는 기술적 용어는 본 발명에서 특별히 다른 의미로 정의되지 않는 한, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 의미로 해석되어야 하며, 과도하게 포괄적인 의미로 해석되거나, 과도하게 축소된 의미로 해석되지 않아야 한다. 또한, 본 발명에서 사용되는 기술적인 용어가 본 발명의 사상을 정확하게 표현하지 못하는 잘못된 기술적 용어일 때에는, 당업자가 올바르게 이해할 수 있는 기술적 용어로 대체되어 이해되어야 할 것이다. 또한, 본 발명에서 사용되는 일반적인 용어는 사전에 정의되어 있는 바에 따라, 또는 전후 문맥상에 따라 해석되어야 하며, 과도하게 축소된 의미로 해석되지 않아야 한다.

[0023] 또한, 본 발명에서 사용되는 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한 복수의 표현을 포함한다. 본 발명에서, "구성된다" 또는 "포함한다" 등의 용어는 발명에 기재된 여러 구성 요소들, 또는 여러 단계를 반

드시 모두 포함하는 것으로 해석되지 않아야 하며, 그 중 일부 구성 요소들 또는 일부 단계들은 포함되지 않을 수도 있고, 또는 추가적인 구성 요소 또는 단계들을 더 포함할 수 있는 것으로 해석되어야 한다.

[0024] 또한, 본 발명에서 사용되는 제 1, 제 2 등과 같이 서수를 포함하는 용어는 구성 요소들을 설명하는데 사용될 수 있지만, 구성 요소들은 용어들에 의해 한정되어서는 안 된다. 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제 1 구성 요소는 제 2 구성 요소로 명명될 수 있고, 유사하게 제 2 구성 요소도 제 1 구성 요소로 명명될 수 있다.

[0025] 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 실시 예를 상세히 설명하되, 도면 부호에 관계없이 동일하거나 유사한 구성 요소는 동일한 참조 번호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다.

[0026] 또한, 본 발명을 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다. 또한, 첨부된 도면은 본 발명의 사상을 쉽게 이해할 수 있도록 하기 위한 것일 뿐, 첨부된 도면에 의해 본 발명의 사상이 제한되는 것으로 해석되어서는 아니 됨을 유의해야 한다.

[0027] 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 실시예를 상세히 설명하되, 도면 부호에 관계없이 동일하거나 유사한 구성 요소는 동일한 참조 번호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다.

[0028] 또한, 본 발명을 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다. 또한, 첨부된 도면은 본 발명의 사상을 쉽게 이해할 수 있도록 하기 위한 것일 뿐, 첨부된 도면에 의해 본 발명의 사상이 제한되는 것으로 해석되어서는 아니 됨을 유의해야 한다.

[0029] 기존에 네트워크 기반의 결제 방법에서는 결제 서버가 결제 정보를 저장하지 못함에 따라서 매번 결제 정보를 입력해야 하는 불편함이 존재하였다. 기존의 간편 결제의 경우도 결제사가 가상 카드 번호 기반으로 결제를 할 경우 별도의 카드사와 전용 회선 연결을 통해서 결제 규격을 정의하여 결제해야 하는 등 불편함이 존재하고 전 카드사 및 은행 등 발행인(issuer)와 연동하는데 많은 시간이 소요되어 서비스 확산에 어려움이 있었다.

[0030] 이하, 본 발명의 실시예에서는 고객의 이용 편의성과 보안성을 제고하며, 글로벌 웹 표준에 맞춘 결제 서비스 제공 장치, 시스템 및 방법을 제시함과 아울러 웹 기반 결제 환경에서 단일 결제 수단에 대응되어 복수의 결제 한도가 설정 가능하여 보안성을 높이는 동시에 결제 편의성을 향상시킬 수 있는 결제 서비스 제공 장치, 시스템 및 방법에 대해 개시한다.

[0031] 웹 표준이란 특정 단말기 운영 환경(예를 들어, ActiveX, Java, Adobe Air)에 존속하지 않고 별도 Plug-in 설치 없이 다종의 운영 환경 간의 호환성을 위해 제정된 국제 웹 표준 기술을 의미한다.

[0032] 예를 들어, 웹 표준은 W3C(World Wide Web Consortium)에서 제정한 HTML5와 같은 차세대 개방형 기술일 수 있다.

[0033] 이하, 본 발명의 실시예에서 개시하는 웹 표준의 의미는 HTML5 표준 기술로만 한정되지 않으며, 그 외 다양한 다종의 운영 환경 간의 호환성을 확보하기 위한 DOM, JavaScript 등 다양한 웹 구동 기술들을 포함할 수 있다.

[0034] 이하, 본 발명의 실시예에 따른 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 장치, 시스템 및 방법은 고객의 이용 편의성과 보안성 제고를 위해 국내 전자 금융 거래 규제가 요구하는 보안성을 준수하면서도 온라인 인증 결제 시 매번 민감한 개인 정보 및 결제 정보를 입력, 통신해야 하는 불편함과 위험성을 개선할 수 있다.

[0035] 또한, 본 발명의 실시예에 따른 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 장치, 시스템 및 방법은 글로벌 표준에 맞춘 결제 서비스로서 서비스 경쟁력 강화를 위해 글로벌 표준에 맞게 설계된 일반 인증 거래(2D 인증 결제)에 본인 인증을 추가하여 거래 안정성을 높인 본인 인증 거래(3D 인증 결제)일 수 있다.

[0036] 또한, 본 발명의 실시예에 따른 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 장치, 시스템 및 방법은 개인 단말의 플랫폼, OS(operating system)에 상관없이 거래 인증 및 승인 서비스의 제공이 가능하도록 확장성과 상호 호환성을 고려한 공통 프로세스를 제공할 수 있다.

[0037] 더하여, 본 발명의 실시예에 따른 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 장치, 시스템 및 방법은 단일 결제 수단에 대해서 복수의 PIN을 등록하고, 해당 PIN마다 결제에 대한 한도를 달리 설정함으로써, 결제 내용에 따라 보안성 정도가 다른 PIN을 이용하도록 하여 높은 한도에 대한 PIN 유출 위험성을 낮추고 결제 한도가 낮게 설정된 PIN은 그 구성이 상대적으로 간소하도록 하여 입력 편의성을 높일 수 있다.

[0038] 이하, 구체적인 본 발명의 실시예에 따른 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 장치, 시스템

및 방법이 개시된다.

[0039] 도 1은 본 발명의 실시예에 따른 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 시스템의 구성 환경도이며, 도 2는 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 시스템을 구성하는 결제 서비스 제공 장치의 동작 개념도이다.

[0040] 도 1에 도시된 바와 같이, 본 발명의 실시예에 따른 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 시스템은 통신망을 통해 연결되는 사용자 장치(10), 웹 기반 상거래 장치(200) 및 결제 서비스 제공 장치(100)를 포함할 수 있다.

[0041] 한편, 도 2를 참조하여 복수 한도 선택을 지원하는 웹 기반 결제 서비스에 대한 동작 프로세스를 설명하면, 결제 서비스 제공 장치(100)는 물리적으로 분리된 별도의 하위 장치를 포함하는 구조로 구현될 수 있다.

[0042] 즉, 결제 서비스 제공 장치(100)는 신용카드 승인 요청 장치(140)와 사용자 인증 장치(120)를 포함할 수 있다.

[0043] 신용카드 승인 요청 장치(140)는 신용 카드사와 인증 거래를 수행하기 위한 서버일 수 있다.

[0044] 사용자 인증 장치(120)는 사용자의 본인 인증을 담당하는 서버일 수 있다. 사용자 인증 장치(120)는 가맹점으로부터 사용자가 가입을 한 경우, 본인 여부를 이동 통신사의 휴대폰 본인 확인서비스(SMS-OTP)를 통해 본인 인증을 수행할 수 있다.

[0045] 그리고 사용자 인증 장치(120)는 웹 브라우저를 통해 사용자로부터 신용 카드 정보를 수신하고, PIN(personal identification number) 번호를 수신하여 저장 및 관리할 수 있다.

[0046] 구체적으로 사용자 인증 장치(120)는 아래와 같은 동작을 수행할 수 있다.

[0047] 사용자 인증 장치(120)는 사용자의 회원 등록 과정에서 웹 브라우저를 통해 수신한 사용자의 개인 정보(이름, 생년월일, 성별, 국적, 휴대폰 번호, 이동통신사, 이메일)를 기반으로 이동 통신사 본인 인증 또는 iPin 본인 인증을 수행할 수 있다. 본인 인증의 결과로 받은 CI(connecting information)/DI(duplication information) 개인 정보는 모두 사용자 인증 장치(120)의 데이터베이스에 암호화하여 저장 관리될 수 있다.

[0048] 사용자가 사용자 인증 장치(120)에 로그인한 경우, 사용자 인증 장치(120)는 사용자에 의해 이미 등록된 신용 카드 정보(카드 ID)들을 추출하여 임시 생성한 암호화 키로 암호화하여 임시 가상 카드 번호를 생성할 수 있다.

[0049] 또한, 사용자 인증 장치(120)는 사용자의 거래 진행 환경 정보(접속 IP(internet protocol), 위치 정보, User Agent), 거래 내용(거래 내역), 회원 정보, 결제 정보 등을 데이터베이스에 암호화하여 저장할 수 있다.

[0050] 또한, 사용자 인증 장치(120)는 신용 카드 승인 요청 장치(140)로부터 전달받은 정보 블록 1(사용자에 의해 신용 카드 승인 요청 장치(140)에 등록된 신용 카드의 승인시 필요한 인증 값을 난독화하여 2개의 정보로 분리한 것 가운데 1개의 정보 블록)을 회원이 입력한 결제 PIN을 기반으로 암호화하여 저장할 수 있다.

[0051] 또한, 사용자 인증 장치(120)는 거래 승인 요청시에 회원이 입력한 결제 PIN으로 복호화한 정보 블록 1을 신용 카드 승인 요청 장치(140)로 전송할 수 있다.

[0052] 구체적으로 신용 카드 승인 요청 장치(140)는 아래와 같은 동작을 수행할 수 있다.

[0053] 사용자가 신용 카드를 서비스에 등록시 신용 카드의 유효성을 평가하기 위하여 신용 카드사에 승인 여부를 확인하기 위한 신용 카드 인증에 필요한 정보(신용 카드 번호, 유효 기간, 카드 비밀 번호 앞 2자리, 생년월일)를 사용자 장치(10)를 이용하여 신용 카드 승인 요청 장치(140)에 일시적으로 전송할 수 있다.

[0054] 신용 카드 승인 요청 장치(140)가 승인 결과 신용 카드의 유효성을 확인하면 일반적인 VAN의 정보 처리 절차와 같이 신용 카드 인증에 필요한 정보(일례로, 신용 카드 번호)는 HSM(hardware security module)을 통해 하드웨어적으로 암호화되고 이에 대응하는 카드 ID가 생성되어 신용 카드 승인 요청 장치(140)에 저장될 수 있다.

[0055] 신용 카드의 인증에 필요한 정보 중 유효 기간, 카드 비밀 번호 앞 2자리, 생년 월일을 포함하는 신용 카드 인증 값은 2개의 정보 블록으로 난독화되어 분리되며 2개의 정보 블록 각각은 모두 별도의 HSM 장비로 암호화될 수 있다.

[0056] 2개의 정보 블록 각각에 대한 암호화 절차시 정보 블록 1의 HSM 암호화 결과로 생성된 값이 정보 블록 2의 암호화 키로 사용할 수 있다. 따라서, 정보 블록 1이 없으면 정보 블록 2에 접근할 수 없도록 연쇄적인 암호화가 수행될 수 있다.

[0057] 생성된 2개의 정보 블록 중 정보 블록 1은 사용자 인증 장치(120)로 전송되며 전송 후 정보 블록 1은 신용 카드 승인 요청 장치(140)에서 삭제될 수 있다.

[0058] 인증 결제 방법을 수행하기 위한 사용자 장치는 웹 브라우저를 통해 인증 및 결제 절차를 수행할 수 있다. 사용자 장치(10)에서 구동되는 웹 브라우저는 웹 표준을 지원하는 브라우저로서 사용자의 결제 및 인증을 위해 필요한 입력 값(예를 들어, PIN, 전화번호 등)을 수신하며, 입력 값을 보안 채널(예를 들어, SSL(secure socket layer))을 통해 사용자 인증 장치(120)로 전송할 수 있다.

[0059] 사용자 장치(10)에는 인증 결제 방법을 수행하기 위한 인증 결제 어플리케이션이 설치될 수 있다. 예를 들어, 인증 결제 어플리케이션은 웹 브라우저에서 실시되는 비대면 결제의 보안성을 제공하는 JavaScript 기반의 Web App(Application)일 수 있다.

[0060] 인증 결제 어플리케이션에서는 신규 회원 가입, 로그인, 인증 화면, 결제 화면을 기반으로 한 인증 결제 절차가 수행될 수 있으며, 사용자로부터 입력 정보를 처리하며, 결제 서비스 제공 장치(100)를 통해 인증 절차 및 결제 절차를 진행할 수 있다.

[0061] 인증 결제 어플리케이션은 E2E 보안(사용자와 서버간의 구간보호), 가상 키보드(사용자의 입력값 보호), 페이지 난독화(웹 페이지의 데이터 암호화) 기능을 제공할 수 있다.

[0062] 상술한 구성에서, 사용자 인증 장치(120)는 사용자 장치(10)로 결제에 이용할 결제 PIN을 요청하며, 도시된 바와 같이 분리된 정보 블록 1에 대하여 사용자 장치로부터 수신된 결제 PIN을 암호화키로 이용하여 AES(advanced encryption standard) 기반으로 암호화할 수 있다.

[0063] 이때, 사용자 인증 장치(120)는 사용자 장치(10)로부터 상이한 결제 한도 금액(이하, 결제 한도)에 대응되는 복수의 결제 PIN을 수신할 수 있으며, 각 결제 PIN에 대응되어 설정될 결제 한도에 대한 설정정보를 사용자 장치(10)로부터 수신할 수 있다.

[0064] 일례로, 사용자 인증 장치(120)는 사용자 장치(10)로부터 일반 결제 한도(총 한도, 일회 결제 한도, 일일 결제 한도 등)에 대응되는 결제 PIN 1과 소액 결제 한도(일반 결제 한도보다 낮게 설정된 결제 한도)에 대응되는 결제 PIN 2와 결제 PIN 1 및 2에 각각 대응되는 상이한 결제 한도가 설정된 설정정보를 수신하고, 결제 PIN 1을 이용하여 정보 블록 1을 AES 기반으로 암호화하여 제 1 암호화 정보 블록 1을 생성하고, 결제 PIN 2를 이용하여 정보 블록 1을 AES 기반으로 암호화하여 제 2 암호화 정보 블록 1을 생성할 수 있다.

[0065] 또한, 사용자 인증 장치(120)는 설정정보를 기초로 결제 PIN 1을 통해 생성한 제 1 암호화 정보 블록 1에 대하여 일반 결제 한도를 설정하고, 결제 PIN 2를 통해 생성한 제 2 암호화 정보 블록 1에 대하여 소액 결제 한도를 설정하여 저장할 수 있다.

[0066] 이때, 사용자 인증 장치(120)는 각 암호화 정보 블록 1에 대하여 별도의 한도 식별자를 부여하고, 각 한도 식별자에 대응되는 결제 한도를 한도 식별자와 매칭하여 생성한 매칭정보를 데이터베이스에 저장할 수도 있다. 여기서, 정보 블록 1의 암호화시 부여된 한도 식별자도 함께 정보 블록 1과 암호화될 수 있다.

[0067] 또한, 사용자 인증 장치(120)는 정보 블록 1을 결제 PIN을 통해 암호화시 결제 한도에 대한 데이터를 정보 블록 1과 함께 암호화하여 결제 한도가 설정되어 암호화된 정보 블록 1을 생성할 수도 있다.

[0068] 이에 따라, 사용자 인증 장치(120)는 각 결제 PIN을 이용하여 정보 블록 1을 암호화하여 서로 다른 암호화된 정보 블록 1을 생성하여 저장할 수 있으며, 설정정보를 기초로 각 암호화된 정보 블록 1에 대하여 암호화에 이용된 결제 PIN에 대응되는 결제 한도를 설정할 수 있다.

[0069] 이후, 사용자 인증 장치(120)는 사용자 장치(10)에 의한 웹 기반 상거래 장치(200)를 통한 상거래가 발생한 경우 웹 기반 상거래 장치(200)로부터 임시 가상 카드 번호와 결제 내역에 대한 결제 정보를 수신하고, 결제 정보 수신시 사용자 장치로 정보 블록 1을 생성하기 위한 결제 PIN을 요청할 수 있다.

[0070] 이에 따라, 사용자 인증 장치(120)는 사용자 장치(10)로부터 결제 PIN을 수신하고, 복수의 암호화된 정보 블록 1 중에서 수신된 결제 PIN으로 복호화되는 정보 블록 1을 식별할 수 있다.

[0071] 일례로, 사용자 인증 장치(120)는 사용자 장치(10)로부터 결제 PIN 2를 수신한 경우 해당 결제 PIN 2로 복호화되는 제 2 암호화 정보 블록 1을 식별하고, 제 2 암호화 정보 블록 1에 설정된 소액 결제 한도를 확인할 수 있다.

[0072] 이후, 사용자 인증 장치(120)는 확인된 결제 한도를 결제 정보에 따른 결제 내역과 비교하여 결제 한도를 초과하는지 여부에 따라 결제 가능 여부를 결정할 수 있으며, 결제 가능시 복호화된 정보 블록 1을 신용 카드 승인 요청 장치로 전송할 수 있다.

[0073] 이때, 사용자 인증 장치(120)는 결제 정보에 포함된 임시 가상 카드 번호를 복호화하고, 복호화된 임시 가상 카드 번호에 대응되는 카드 ID를 조회하여 추출하며, 해당 추출된 카드 ID를 상술한 복호화된 정보 블록 1과 함께 신용카드 승인 요청 장치(140)로 전송할 수 있다.

[0074] 한편, 사용자 인증 장치(120)는 결제 내역이 확인된 결제 한도를 초과하는 경우 결제 불가로 판단하고, 사용자 장치(10)로 다른 결제 PIN을 요청할 수 있다.

[0075] 또한, 사용자 인증 장치(120)는 결제 가능 여부에 대한 결제 가능 여부 정보를 사용자 장치(10) 및 웹 기반 상거래 장치(200)로 전송하여 결제 진행 여부를 판단할 수 있도록 제공한다.

[0076] 한편, 신용카드 승인 요청 장치(140)는 사용자 인증 장치(120)로부터 수신한 정보 블록 1을 기반으로 정보 블록 2를 복호화하고, 복호화된 정보 블록 1 및 정보 블록 2를 기반으로 암호화된 신용 카드 인증 값을 복호화하며, 사용자 인증 장치(120)로부터 수신된 카드 ID에 대응되는 암호화된 신용 카드 번호를 복호화할 수 있다. 이때, 신용카드 승인 요청 장치는 신용 카드 번호의 암호화에 이용한 HSM를 기반으로 암호화된 신용 카드 번호를 복호화할 수 있다.

[0077] 이에 따라, 신용카드 승인 요청 장치(140)는 복호화된 신용 카드 인증 값 및 신용 카드 번호를 기반으로 신용카드사 서버로 전송할 승인 전문을 생성하고, 승인 전문을 신용 카드사 서버로 전송할 수 있으며, 신용 카드사 서버로부터 승인 결과를 수신한 후 웹 기반 상거래 장치(200)로 전송하여 결제 처리를 완료할 수 있다.

[0078] 이때, 신용카드 승인 요청 장치(140)는 사용자 인증 장치(120)로부터 웹 기반 상거래 장치(200)가 제공한 결제 정보를 수신하고, 해당 결제 정보와 상술한 신용 카드 인증 값 및 신용 카드 번호를 기반으로 승인 전문을 생성할 수 있다. 여기서, 사용자 인증 장치(120)로부터 신용카드 승인 요청 장치(140)에 제공되는 결제 정보에는 결제 내역에 대한 정보만이 포함될 수 있다.

[0079] 이와 같이, 본 발명은 사용자가 결제 승인 요청시 결제 PIN 만으로 결제 한도를 용이하게 선택할 수 있도록 하며, 이에 따라 결제 한도가 가장 높은 결제 PIN의 반복 사용을 최소화하여 결제 PIN의 노출에 따른 보안 위협을 방지할 수 있다.

[0080] 상술한 바에 따라, 본 발명은 결제 서비스 제공 장치와 카드사 서버간 신용카드 관련 정보가 교환되도록 하여 온라인 인증 결제시 결제정보의 송수신을 최소화할 수 있으며, 신용카드와 관련된 정보를 복수의 정보 블럭으로 분리 관리하여 보안성을 크게 향상시킬 수 있다.

[0081] 더하여, 본 발명은 기존의 결제 처리 시스템과 달리 단일 결제 수단에 대하여 복수의 결제 한도를 허용하고, 결제 PIN 만으로 용이하게 결제 한도를 복수로 설정할 수 있을 뿐 아니라 결제 한도 판단을 카드사 서버가 아닌 결제 서비스 제공 장치에서 수행할 수 있으므로 사용자의 결제 한도 설정에 대한 편의성을 높일 수 있다.

[0082] 이때, 본 발명은 가장 높은 결제 한도에 대한 PIN의 복잡도를 높여 설정하도록 지원하고, 소액 결제 한도에 대해서는 복잡도가 낮은 PIN을 설정할 수 있도록 지원하여 결제 편의성을 크게 향상시킬 수 있다.

[0083] 한편, 상술한 구성에서 사용자 장치(10)는 통신 기능을 구비한 스마트 폰(Smart Phone), 휴대 단말기(Portable Terminal), 이동 단말기(Mobile Terminal), 개인 정보 단말기(Personal Digital Assistant: PDA), PMP(Portable Multimedia Player) 단말기, 텔레매틱스(Telematics) 단말기, 내비게이션(Navigation) 단말기, 개인용 컴퓨터(Personal Computer), 노트북 컴퓨터, 슬레이트 PC(Slate PC), 태블릿 PC(Tablet PC), 울트라북(ultrabook), 웨어러블 디바이스(Wearable Device, 예를 들어, 워치형 단말기(Smartwatch), 글래스형 단말기(Smart Glass), HMD(Head Mounted Display) 등 포함), 와이브로(Wibro) 단말기, IPTV(Internet Protocol Television) 단말기, 스마트 TV, 디지털방송용 단말기, AVN(Audio Video Navigation) 단말기, A/V(Audio/Video) 시스템, 플렉시블 단말기(Flexible Terminal) 등과 같은 다양한 단말기를 포함할 수 있다.

[0084] 또한, 상술한 통신망의 일례로 무선랜(Wireless LAN: WLAN), DLNA(Digital Living Network Alliance), 와이브로(Wireless BroaDB(400)and: Wibro), 와이맥스(World Interoperability for Microwave Access: Wimax), GSM(Global System for Mobile communication), CDMA(Code Division Multi Access), CDMA2000(Code Division Multi Access 2000), EV-DO(Enhanced Voice-Data Optimized or Enhanced Voice-Data Only), WCDMA(Wideband CDMA), HSDPA(High Speed Downlink Packet Access), HSUPA(High Speed Uplink Packet Access), IEEE 802.16,

롱 텀 에볼루션(Long Term Evolution: LTE), LTE-A(Long Term Evolution-Advanced), 광대역 무선 이동 통신 서비스(Wireless Mobile BroaDB(400)and Service: WMBS), 블루투스(Bluetooth), RFID(Radio Frequency Identification), 적외선 통신(Infrared Data Association: IrDA), UWB(Ultra Wideband), 지그비(ZigBee), 인접 자장 통신(Near Field Communication: NFC), 초음파 통신(Ultra Sound Communication: USC), 가시광 통신(Visible Light Communication: VLC), 와이 파이(Wi-Fi), 와이 파이 다이렉트(Wi-Fi Direct) 등과 같은 무선 통신망이 포함될 수 있으며, 전력선 통신(Power Line Communication: PLC), USB 통신, 이더넷(Ethernet), 시리얼 통신(serial communication), 광/동축 케이블 등과 같은 유선 통신망이 포함될 수도 있다.

[0085] 또한, 상술한 결제 서비스 제공 장치(100)와, 웹 기반 상거래 장치(200)는 웹 서버, 데이터베이스 서버, 프록시 서버 등과 같은 다양한 서버의 형태로 구현될 수 있다.

[0086] 또한, 결제 서비스 제공 장치(100) 및 웹 기반 상거래 장치(200)에는 네트워크 부하 분산 메커니즘, 내지 서비스 장치가 인터넷 또는 다른 네트워크 상에서 동작할 수 있도록 하는 다양한 소프트웨어 중 하나 이상이 설치될 수 있으며, 이를 통해 컴퓨터화된 시스템으로 구현될 수 있다.

[0087] 또한, 네트워크는 http 네트워크일 수 있으며, 전용 회선(private line), 인트라넷 또는 임의의 다른 네트워크일 수 있다. 나아가, 각 결제 서비스 제공 장치 및 웹 기반 상거래 장치(100, 200)와 사용자 장치(10)의 연결은 데이터가 임의의 해커 또는 다른 제3자에 의한 공격을 받지 않도록 보안 네트워크로 연결될 수 있다. 또한, 결제 서비스 제공 장치 및 웹 기반 상거래 장치(100, 200)는 복수의 데이터베이스 서버를 포함할 수 있으며, 이러한 데이터베이스 서버가 분산 데이터베이스 서버 아키텍쳐를 비롯한 임의의 유형의 네트워크 연결을 통해 각 서비스 제공 장치와 별도로 연결되는 방식으로 구현될 수 있다.

[0088] 한편, 사용자 장치(10)는 입력부, 표시부, 통신부, 저장부, 음성 출력부, 제어부와 같은 다양한 구성부로 구성될 수 있다.

[0089] 입력부는 사용자에 의한 버튼 조작 또는 임의의 기능 선택에 따른 신호를 수신하거나, 디스플레이되는 화면을 터치/스크롤하는 등의 조작에 의해 생성된 명령 또는 제어 신호를 수신하거나, 사용자에 의해 입력된 정보에 대응하는 신호를 수신하며, 키 패드(Key Pad), 돔 스위치 (Dome Switch), 터치 패드(정압/정전), 터치 스크린(Touch Screen), 조그 휠, 조그 스위치, 조그 셔틀(Jog Shuttle), 마우스(mouse), 스타일러스 펜(Stylus Pen), 터치 펜(Touch Pen) 등의 다양한 장치가 사용될 수 있다.

[0090] 더하여, 표시부는 제어부의 제어에 의해 저장부에 저장된 사용자 인터페이스 및/또는 그래픽 사용자 인터페이스를 이용하여 다양한 메뉴 화면 등과 같은 다양한 콘텐츠를 표시할 수 있다. 여기서, 표시부에 표시되는 콘텐츠는 다양한 텍스트 또는 이미지 데이터(각종 정보 데이터 포함)와 아이콘, 리스트 메뉴, 콤보 박스 등의 데이터를 포함하는 메뉴 화면 등을 포함한다. 또한, 표시부는 터치 스크린 일 수 있다.

[0091] 이때, 사용자의 터치 제스쳐를 감지하기 위한 터치 센서가 포함될 수 있다. 터치 센서는 정전식이나, 감압식, 압전식 등과 같은 다양한 형태 중 하나일 수 있다. 정전식인 경우 터치 스크린 표면에 코팅된 유전체를 이용하여, 사용자의 신체 일부가 터치 스크린 표면에 터치되었을 때 사용자의 인체로 여기되는 미세 전기를 감지하여 터치 좌표가 산출된다. 감압식인 경우 터치 스크린에 두 개의 전극 판이 내장되며, 사용자가 화면을 터치하면 터치된 위치의 상하 전극 판이 접촉되어 전류가 흐르게 되며, 이러한 전류의 흐름이 감지되어 터치 좌표가 산출된다.

[0092] 이외에도, 사용자 장치(10)가 펜 입력 기능을 지원할 수 있으며, 이 경우 사용자의 신체 일부가 아닌 펜과 같은 입력 수단을 활용한 사용자의 제스쳐도 감지될 수 있다. 예로서, 입력 수단이 코일을 내부에 포함하는 스타일러스 펜인 경우, 사용자 장치(10)는 스타일러스 펜 내부의 코일에 의해 변화되는 자기장을 감지하기 위한 자기장 감지 센서를 포함할 수 있다. 이 경우 사용자의 터치 제스쳐 뿐만 아니라 호버링(hovering)과 같은 사용자의 근접 제스쳐도 감지할 수 있다.

[0093] 또한, 표시부는 액정 디스플레이(Liquid Crystal Display: LCD), 박막 트랜지스터 액정 디스플레이(Thin Film Transistor-Liquid Crystal Display: TFT LCD), 유기 발광 다이오드(Organic Light-Emitting Diode: OLED), 플렉시블 디스플레이(Flexible Display), 3차원 디스플레이(3D Display), 전자잉크 디스플레이(e-ink display), LED(Light Emitting Diode) 중에서 적어도 하나의 형태로 구현될 수 있으며, 이를 위한 구동회로, 백라이트 유닛 등을 함께 포함할 수 있다.

[0094] 또한, 표시부는 입체영상을 표시하는 입체 디스플레이부로서 구성될 수 있다.

[0095] 입체 디스플레이부에는 스테레오스코픽 방식(안경 방식), 오토 스테레오스코픽 방식(무안경 방식), 프로젝션 방식(홀로그래픽 방식) 등의 3차원 디스플레이 방식이 적용될 수 있다.

[0096] 또한, 표시부는 제어부의 제어에 의해 결제 서비스 제공 장치(100)로부터 발급된 임시 가상 카드 번호 또는 상품권이나 쿠폰 등에 대한 정보 등을 표시한다.

[0097] 음성 출력부는 제어부에 의해 소정 신호 처리된 신호에 포함된 음성 정보를 출력한다. 여기서, 음성 출력부에는 리시버, 스피커, 버저 등이 포함될 수 있다.

[0098] 또한, 음성 출력부는 제어부에 의해 생성된 안내 음성을 출력한다.

[0099] 또한, 음성 출력부는 제어부에 의해 결제 서비스 제공 장치(100)로부터 발급된 임시 가상 카드 번호 또는 상품권이나 쿠폰 등에 대한 정보에 대응하는 음성 정보를 출력한다.

[0100] 통신부는 상술한 유/무선 통신망을 통해 내부의 임의의 구성 요소 또는 외부의 임의의 적어도 하나의 단말기와 통신 연결한다. 이때, 외부의 임의의 단말기는 네트워크 서비스 시스템, 서버 등을 포함할 수 있다.

[0101] 제어부는 저장부에 저장된 프로그램 및 데이터를 이용하여 사용자 장치(10)의 전반적인 제어 기능을 실행한다. 제어부는 RAM, ROM, CPU, GPU, 버스를 포함할 수 있으며, RAM, ROM, CPU, GPU 등은 버스를 통해 서로 연결될 수 있다. CPU는 저장부에 액세스하여, 저장부에 저장된 O/S(Operating System)를 이용하여 부팅을 수행할 수 있으며, 저장부에 저장된 각종 프로그램, 컨텐츠, 데이터 등을 이용하여 다양한 동작을 수행할 수 있다.

[0102] 또한, 저장부는 사용자 장치(10)가 동작하는데 필요한 데이터와 프로그램 등을 저장한다.

[0103] 즉, 저장부는 사용자 장치(10)에서 구동되는 다수의 응용 프로그램(application program 또는 애플리케이션), 사용자 장치(10)의 동작을 위한 데이터들, 명령어들을 저장할 수 있다. 이러한 응용 프로그램 중 적어도 일부는 무선 통신을 통해 외부 서버로부터 다운로드 될 수 있다. 또한 이러한 응용 프로그램 중 적어도 일부는 사용자 장치(10)의 기본적인 기능(예를 들어, 전화 착신, 발신 기능, 메시지 수신, 발신 기능)을 위하여 출고 당시부터 사용자 장치(10)상에 존재할 수 있다. 한편, 응용 프로그램은 사용자장치 저장부에 저장되고, 사용자 장치(10)에 설치되어, 사용자장치 제어부에 의하여 사용자 장치(10)의 동작(또는 기능)을 수행하도록 구동될 수 있다.

[0104] 또한, 저장부는 플래시 메모리 타입, 하드 디스크 타입, 멀티미디어 카드 마이크로 타입, 카드 타입의 메모리(예를 들면, SD 또는 XD 메모리 등), 자기 메모리, 자기 디스크, 광디스크, 램(RAM), SRAM, 롬(ROM), EEPROM, PROM 중 적어도 하나의 저장매체를 포함할 수 있다. 또한, 사용자 장치(10)는 인터넷상에서 사용자장치 저장부의 저장 기능을 수행하는 웹 스토리지를 운영하거나, 또는 웹 스토리지와 관련되어 동작할 수도 있다.

[0105] 또한, 저장부는 제어부의 제어에 의해 결제 서비스 제공 장치(100)로부터 발급된 임시 가상 카드 번호 또는 쿠폰이나 상품권에 대한 정보 등을 저장한다.

[0106] 또한, 사용자 장치(10)는 해당 사용자 장치(10)에 연결되는 모든 외부기기와의 인터페이스 역할을 수행하는 인터페이스부(미도시)를 더 포함할 수도 있다.

[0107] 예를 들면, 인터페이스부는 유/무선 헤드셋 포트(Headset Port), 외부 충전기 포트, 유/무선 데이터 포트, 메모리 카드(Memory Card) 포트, 식별 모듈이 구비된 장치를 연결하는 포트, 오디오 I/O(Input/Output) 포트, 비디오 I/O(Input/Output) 포트, 이어폰 포트 등으로 구성될 수 있다. 여기서, 식별 모듈은 사용자 장치(10)의 사용 권한을 인증하기 위한 각종 정보를 저장한 칩으로서, 사용자 인증 모듈(User Identity Module: UIM), 가입자 인증 모듈(Subscriber Identity Module: SIM), 범용 사용자 인증 모듈(Universal Subscriber Identity Module: USIM) 등을 포함할 수 있다. 또한, 식별 모듈이 구비된 장치는 스마트 카드(Smart Card) 형식으로 제작될 수 있다. 따라서, 식별 모듈은 포트를 통하여 사용자 장치(10)와 연결될 수 있다. 이와 같은 인터페이스부는 외부 기기로부터 데이터를 수신하거나 전원을 수신하여 사용자 장치(10) 내부의 각 구성 요소에 전달하거나 사용자 장치(10) 내부의 데이터가 외부 기기로 전송되도록 한다.

[0108] 또한, 인터페이스부는 사용자 장치(10)가 외부 크래들(Cradle)과 연결될 때 크래들로부터의 전원이 해당 사용자 장치(10)에 공급되는 통로가 되거나, 사용자에 의해 크래들에서 입력되는 각종 명령 신호가 해당 사용자 장치(10)로 전달되는 통로가 될 수 있다. 크래들로부터 입력되는 각종 명령 신호 또는 해당 전원은 사용자 장치(10)가 크래들에 정확히 장착되었음을 인지하기 위한 신호로 동작될 수도 있다.

[0109] 또한, 사용자 장치(10)는 사용자에 의한 버튼 조작 또는 임의의 기능 선택에 따른 신호를 수신하거나, 디스플레이되는 화면을 터치/스크롤하는 등의 조작에 의해 생성된 명령 또는 제어 신호를 수신하기 위한 입력부(미도

시)를 더 포함할 수도 있다.

[0110] 이하, 상술한 구성을 참고하여 본 발명의 실시예에 따른 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 시스템의 상세 실시예를 이하 도면을 통해 설명한다.

[0111] 도 3은 본 발명의 실시예에 따른 사용자 회원 가입 절차를 나타낸 개념도이다.

[0112] 도 3을 참조하면, 사용자가 기존의 회원이고, 웹 기반 상거래 장치(또는 웹 기반 상거래 서버)가 ID 비연동 가맹 장치인 경우. 사용자는 등록된 회원 ID를 기반으로 웹 어플리케이션에 대한 인증을 수행하고, 인증 DLP(data loss prevention) 절차로 리다이렉트될 수 있다. 웹 기반 상거래 장치와 다른 웹 기반 상거래 장치 간의 ID 연동이 되는 경우, 회원 정보 조회 절차를 거쳐 연동 ID를 기반으로 인증 DLP 절차가 수행될 수 있다.

[0113] 인증 DLP 절차에서는 결제 수단 리스트 제공, 결제 PIN 입력 및 FDS(fraud detection system)에 의한 추가 인증(ARS(automatic response system), SMS(short message service)-OTP(one time password) 및 App 인증)이 수행될 수 있다.

[0114] 사용자가 기존의 회원이 아닌 경우, 약관 동의, 본인 인증, 결제 정보 등록, 결제 PIN 등록, 설정정보 등록 등을 통해 신규 가입 절차를 진행할 수 있다.

[0115] 인증 DLP 절차를 통해 인증이 완료된 경우, 승인 절차가 진행될 수 있다.

[0116] 도 4는 본 발명의 실시예에 따른 사용자 회원 가입 절차를 나타낸 흐름도이다.

[0117] 사용자 인증 장치는 사용자부터 인증 결제 서비스 가입 요청 및 회원 정보를 수신하고 이동 통신사를 통해 사용자에 대한 본인 인증을 수행할 수 있다. 또한, 본인 인증 이후, 사용자는 사용자 인증 장치 및 신용 카드 승인 요청 장치를 통해 신용 카드(카드 번호 및 CAV(card authentication value))를 등록할 수 있다. 신용 카드의 유효성을 확인받고 결제를 위한 정보는 암호화되어 사용자 인증 장치 및 신용 카드 승인 요청 장치 각각에 저장할 수 있다.

[0118] 본 발명의 실시예에 따르면, 회원의 신용 카드 속성에 따라 다양한 본인 인증 방법을 통해 회원 계정을 등록할 수 있다. 모든 회원 계정은 비금융사에 의한 본인 확인 방법과 금융사에 의한 본인 확인 방법을 모두 수행하여 본인 확인을 수행할 수 있다.

[0119] 도 4를 참조하면, 사용자는 웹 기반 상거래 장치(예를 들어, 대표 가맹점의 웹 사이트를 운영하는 서버)로 결제 요청을 할 수 있다(단계 S300).

[0120] 사용자는 웹 기반 상거래 장치를 통해 결제 방법으로서 본 발명의 실시예에 따른 복수 한도 선택을 지원하는 웹 기반 결제 서비스 방법에 따른 간편 결제를 선택하고 간편 결제를 요청할 수 있다.

[0121] 웹 기반 상거래 장치는 사용자의 가입 내역을 조회하고 사용자가 신규 회원인지 여부에 대해 확인할 수 있다(단계 S305). 웹 기반 상거래 장치는 회원 데이터베이스를 기반으로 간편 결제를 요청한 사용자가 이미 간편 결제 절차의 진행이 가능한 회원인지 여부를 판단할 수 있다. 회원 데이터베이스에 사용자의 가입 내역이 존재하는 경우, 사용자의 간편 결제 절차의 진행이 가능하다고 판단할 수 있다. 반대로, 회원 데이터베이스에 사용자의 가입 내역이 존재하지 않는 경우, 사용자가 간편 결제 절차의 진행이 가능하지 않고 사용자의 간편 결제 절차에 대한 신규 가입이 필요하다고 판단할 수 있다. 이하, 사용자의 간편 결제 절차에 대한 신규 가입이 필요한 경우를 가정하여 설명한다.

[0122] 웹 기반 상거래 장치는 간편 결제 절차를 위한 신규 회원 등록 절차의 진행을 사용자 인증 장치로 요청할 수 있다(단계 S310). 사용자 인증 장치는 우선 신규 회원 등록 절차의 진행을 요청한 웹 기반 상거래 장치에 대한 유효성을 인증할 수 있고, 약관 동의 화면과 회원 정보 입력 화면을 별도의 웹 페이지에 출력하여 사용자 장치로 전송할 수 있다.

[0123] 사용자 장치는 간편 결제 서비스 페이지에 약관 동의, 회원 정보, 결제 PIN, 설정정보 등을 입력하여 사용자 인증 장치로 전송할 수 있다(단계 S315). 사용자 장치는 회원 정보를 입력할 수 있다(단계 S320). 회원 정보는 이메일, 서비스 사용 ID/패스워드, 사용자 장치(예를 들어, 휴대용 단말기)의 가입 정보를 포함할 수 있다. 사용자 장치의 가입 정보는 본인 인증에 필요한 사용자 장치의 번호, 성명, 생년월일, 성별, 국적 등을 포함할 수 있다.

[0124] 사용자 인증 장치는 사용자로부터 입력받은 사용자 장치의 본인 인증 정보를 휴대폰 본인 확인 서비스 대행사

(신용평가사)를 통해 이동 통신사로 전달할 수 있다(단계 S325).

[0125] 이동 통신사는 본인 확인 서비스 대행사로부터 수신한 사용자 장치의 본인 인증 정보를 기반으로 사용자 장치로 SMS 인증 번호를 전송할 수 있다(단계 S330).

[0126] 사용자 장치는 수신한 SMS 인증 번호를 사용자 인증 장치로 전송할 수 있다(단계 S335).

[0127] 사용자 인증 장치는 수신한 SMS 인증 번호를 본인 확인 서비스 대행사를 통해 이동 통신사로 전송하여 사용자에 대한 인증을 요청할 수 있다(단계 S340).

[0128] 이동 통신사는 사용자 인증 장치로부터 수신한 SMS 인증 번호를 기반으로 사용자 확인을 수행한 결과(예를 들어, CI/DI)를 본인 확인 서비스 대행사를 통해 사용자 인증 장치로 전송할 수 있다(단계 S345).

[0129] 사용자 인증 장치는 사용자 장치를 통해 사용자에게 결제 수단에 대한 정보 입력을 요청할 수 있다(단계 S350). 사용자 인증 장치는 중요 정보에 대해서는 스크린 키보드, 안티 바이러스 프로그램 공지 등 사용자 환경 정보를 함께 공지하고 사용자로부터 공지에 대한 확인을 요청할 수 있다.

[0130] 사용자 장치는 결제 수단에 대한 정보를 입력할 수 있다. 사용자 장치는 사용자 인증 장치로 신용 카드 정보를 전송할 수 있다(단계 S355). 사용자 장치를 통해 사용자 인증 장치로 전송되는 신용 카드 정보는 신용 카드 승인 요청 장치로부터 제공받은 암호화키로 암호화되어 전송될 수 있다.

[0131] 사용자 인증 장치는 암호화되어 전송된 사용자의 신용 카드 정보를 신용 카드 승인 요청 장치로 전송할 수 있다(단계 S360).

[0132] 신용 카드 승인 요청 장치는 암호화되어 전송된 사용자의 신용 카드 정보를 복호화하고 신용 카드사 서버에 승인 요청 전문을 전송할 수 있다(단계 S365).

[0133] 신용 카드사 서버는 승인계를 통해 사용자의 신용 카드 정보의 유효성을 확인할 수 있고, 승인 결과를 신용카드 승인 요청 장치로 전송할 수 있다(단계 S370).

[0134] 신용카드 승인 요청 장치는 신용 카드 승인 결과를 토대로 신용 카드 번호와 신용 카드 인증 값을 암호화할 수 있다. 예를 들어, 신용 카드 번호는 HSM을 기반으로 암호화되어 신용카드 승인 요청 장치에 저장될 수 있다. 신용 카드 승인 요청 장치는 신용 카드 번호의 식별을 위하여 카드 ID를 생성하여 함께 저장할 수 있다.

[0135] 또한, 신용카드 승인 요청 장치는 신용 카드 인증 값(유효 기간, 카드 비밀번호 앞 두자리, 생년 월일)은 2개로 나뉘어져 정보 블록 1과 정보 블록 2로 분리될 수 있다. 정보 블록 1은 물리적으로 격리된 사용자 인증 장치로 전송될 수 있다(단계 S375). 정보 블록 1은 사용자 인증 장치로 전송된 이후 신용 카드 승인 요청 장치에서 삭제될 수 있다. 전술한 바와 같이 신용 카드 승인 요청 장치에서는 사용자 인증 장치로부터 전송된 정보 블록 1을 기반으로 한 정보 블록 2로의 접근이 수행될 수 있다.

[0136] 전술한 바와 같이 정보 블록 1은 사용자 인증 장치에서 사용자에 의해 입력된 결제 PIN을 기반으로 암호화되어 저장될 수 있다.

[0137] 사용자 인증 장치는 사용자 장치로 결제 PIN을 요청할 수 있다(단계 S380).

[0138] 사용자 장치는 결제 PIN을 암호화하여 사용자 인증 장치로 전송할 수 있다(단계 S385).

[0139] 이때, 사용자 장치는 사용자 입력에 따라 서로 상이한 복수의 결제 한도 설정을 위한 복수의 결제 PIN을 생성하고, 각 결제 PIN에 대응되는 결제 한도에 대한 설정정보를 생성하여 사용자 인증 장치로 전송할 수 있다.

[0140] 이에 따라, 사용자 인증 장치는 각 결제 PIN을 기반으로 정보 블록 1을 암호화하여 서로 다른 복수의 암호화된 정보 블록 1을 생성할 수 있으며(단계 S390), 설정정보를 기초로 각 암호화된 정보 블록 1에 대하여 암호화에 이용된 결제 PIN에 대응되는 결제 한도를 설정할 수 있다(단계 S395).

[0141] 이때, 사용자 인증 장치는 암호화 완료 및 결제 한도 설정 완료 이후 암호화 전의 정보 블록 1과 설정정보는 삭제할 수 있다.

[0142] 도 5는 본 발명의 실시예에 따른 신용 카드 승인 요청 장치 및 사용자 인증 장치에서 신용 카드 번호와 신용 카드 인증값을 암호화하는 방법에 대한 개념도이다.

[0143] 도 5를 참조하면, 신용카드의 PAN(primary account number)(400)은 HSM 및 Hash를 기반으로 암호화될 수 있다. 암호화된 PAN 정보는 카드 ID와 매칭되어 신용 카드 승인 요청 장치에 저장될 수 있다.

[0144] 또한, 신용카드 승인 요청 장치는 카드 ID를 사용자 인증 장치로 전송하며, 사용자 인증 장치는 해당 카드 ID를 저장할 수 있다.

[0145] 이때, 사용자 인증 장치는 카드 ID를 임시 생성한 암호화 키로 암호화하여 임시 가상 카드 번호를 생성하고, 해당 임시 가상 카드 번호를 사용자 장치로 전송할 수 있다.

[0146] 신용카드의 신용 카드 인증값(card authentication value, CAV)(405)은 파트1(410)과 파트2(420)로 분리될 수 있다. 파트1(410)에 대응되는 CAV 정보는 HSM을 기반으로 암호화되어 정보 블록 1(430)로 생성되어 사용자 인증 장치로 전송될 수 있다. 파트2(420)는 정보 블록 1(430)을 초기 암호값을 사용하여 HSM을 기반으로 암호화한 정보 블록 2(440)로 생성될 수 있다.

[0147] 한편, 사용자 인증 장치는 신용카드 승인 요청 장치로부터 정보 블록 1(430) 수신시 사용자 장치로 결제에 이용할 결제 PIN을 요청하며, 도시된 바와 같이 분리된 정보 블록 1(430)에 대하여 사용자 장치로부터 수신된 결제 PIN을 암호화키로 이용하여 AES(450) 기반으로 암호화할 수 있다.

[0148] 이때, 사용자 인증 장치는 정보 블록 1(430)을 AES(450) 기반으로 암호화하는데 있어서, BEK(block encryption key)를 사용할 수 있다. BEK은 사용자 장치로부터 입력된 사용자 PIN을 기반으로 생성된 키일 수 있다.

[0149] 또한, 사용자 인증 장치는 사용자 장치로부터 상이한 결제 한도 금액(이하, 결제 한도)에 대응되는 복수의 결제 PIN을 수신할 수 있으며, 각 결제 PIN에 대응되어 설정될 결제 한도에 대한 설정정보를 사용자 장치로부터 수신할 수 있다.

[0150] 일례로, 사용자 인증 장치는 사용자 장치로부터 일반 결제 한도(총 한도, 일회 결제 한도, 일일 결제 한도 등)에 대응되는 결제 PIN 1과 소액 결제 한도(일반 결제 한도보다 낮게 설정된 결제 한도)에 대응되는 결제 PIN 2와 결제 PIN 1 및 2에 각각 대응되는 상이한 결제 한도가 설정된 설정정보를 수신하고, 결제 PIN 1을 이용하여 정보 블록 1을 AES(450) 기반으로 암호화하여 제 1 암호화 정보 블록 1(461)을 생성하고, 결제 PIN 2를 이용하여 정보 블록 1을 AES(450) 기반으로 암호화하여 제 2 암호화 정보 블록 1(462)을 생성할 수 있다.

[0151] 또한, 사용자 인증 장치는 설정정보를 기초로 결제 PIN 1을 통해 생성한 제 1 암호화 정보 블록 1(461)에 대하여 일반 결제 한도를 설정하고, 결제 PIN 2를 통해 생성한 제 2 암호화 정보 블록 1(462)에 대하여 소액 결제 한도를 설정할 수 있다.

[0152] 이에 따라, 사용자 인증 장치는 각 결제 PIN을 이용하여 정보 블록 1을 암호화하여 서로 다른 암호화된 정보 블록 1(461, 462)을 생성하여 저장할 수 있으며, 설정정보를 기초로 각 암호화된 정보 블록 1(461, 462)에 대하여 암호화에 이용된 결제 PIN에 대응되는 결제 한도를 설정할 수 있다.

[0153] 상술한 구성에서, 사용자 인증 장치는 이미 결제 PIN을 설정한 사용자 장치가 이미 설정한 결제 PIN 및 결제 한도를 변경하고자 하는 경우 본인 확인 서비스 대행사 및 이동 통신사와 통신망을 통해 연동하여 본인 인증 후 상술한 구성을 반복하여 변경된 복수의 결제 PIN 각각에 대응되는 암호화된 정보 블록 1을 생성하고, 각 암호화된 정보 블록 1에 대하여 결제 한도를 설정하여 저장하며 기존 복수의 암호화된 정보 블록 1은 삭제할 수 있다.

[0154] 이를 통해, 사용자는 용이하게 결제 PIN과 결제 한도를 변경할 수 있다.

[0155] 도 6은 사용자에 의한 웹 기반 상거래 발생시 본 발명의 실시예에 따른 결제 서비스 제공 장치의 결제 PIN의 입력에 따른 결제 절차를 나타낸 흐름도이다.

[0156] 도 6을 참조하면, 사용자가 본 발명의 실시예에 따른 간편 결제 절차를 선택한 경우(단계 S500), 웹 기반 상거래 장치는 사용자 인증 장치로 결제를 요청할 수 있다(단계 S505). 웹 기반 상거래 장치는 사용자에 의해 선택된 임시 가상 카드 번호와 결제 내역(품목, 가맹점 명, 금액, 거래 일시 등)을 포함하는 결제 정보를 사용자 인증 장치로 전달하여 거래 인증 요청을 진행할 수 있다.

[0157] 사용자 인증 장치는 임시 가상 카드 번호가 거래 유효 시간 이내에 도착했는지 여부에 대해 확인할 수 있다. 또한, 사용자 인증 장치는 임시 가상 카드 번호를 기반으로 사용자의 카드 ID에 대한 정보를 조회하여 사용자의 카드 ID에 대한 정보를 획득할 수 있다(단계 S510).

[0158] 일례로, 사용자 인증 장치는 임시 가상 카드 번호를 복호화하여 복호화된 임시 가상 카드 번호에 대응되는 카드 ID에 대한 정보를 조회하여 추출할 수 있다.

[0159] 사용자 인증 장치는 사용자 장치로 기존에 설정한 결제 PIN에 대한 정보를 입력하도록 요청할 수 있다(단계

S515). 사용자 인증 장치는 사용자 장치로 결제 PIN의 입력을 요청하기 위한 화면을 제공할 수 있다. 결제 PIN의 입력을 요청하기 위한 화면 상에서는 입력될 결제 PIN에 대한 보안을 위해 스크린 키보드 적용과 안티바이러스 백신 프로그램의 사용에 대한 안내 정보가 제공될 수 있다.

[0160] 사용자는 사용자 장치를 통해 결제 PIN을 입력할 수 있다(단계 S520).

[0161] 이때, 사용자는 기존에 설정한 복수의 결제 PIN 중 어느 하나를 입력하여 결제 한도를 선택할 수 있다.

[0162] 사용자 인증 장치는 결제 내역(품목, 가맹점 명, 금액, 거래 일시 등)을 확인하고 이미 암호화하여 저장한 복수의 암호화된 정보 블록 1 중에서 어느 하나를 사용자 장치로부터 수신된 결제 PIN으로 복호화할 수 있다(단계 S525).

[0163] 또한, 사용자 인증 장치는 결제 PIN으로 복호화되는 암호화된 정보 블록 1에 대응되어 설정된 결제 한도를 확인할 수 있다(단계 S530).

[0164] 이때, 사용자 인증 장치는 복호화되는 암호화된 정보 블록 1에 부여된 한도 식별자를 식별하고, 상술한 매칭정보를 기초로 한도 식별자에 매칭된 결제 한도를 확인할 수도 있다.

[0165] 이후, 사용자 인증 장치는 확인된 결제 한도가 웹 기반 상거래 장치로부터 수신된 결제 정보에 따른 결제 금액을 초과하는지 여부에 따른 결제 가능 여부를 판단할 수 있다(단계 S535).

[0166] 즉, 사용자 인증 장치는 결제 금액이 결제 한도를 초과하는 경우 결제 불가로 판단하여 결제 승인 불가에 대한 정보를 웹 기반 상거래 장치로 전송하고, 웹 기반 상거래 장치는 결제 불가를 사용자 장치로 통보할 수 있다.

[0167] 이때, 사용자 인증 장치는 결제 승인 불가에 대한 정보를 웹 기반 상거래 장치에 앞서 사용자 장치로 우선 전송하고, 결제 금액 이상의 결제 한도에 대응되는 결제 PIN을 재입력하도록 사용자 장치에 요청할 수도 있다.

[0168] 또한, 사용자 인증 장치는 결제 한도 이내의 결제 금액으로 판단되어 결제 가능한 것으로 판단한 경우 복호화된 정보 블록 1을 신용카드 승인 요청장치로 전송할 수 있다.

[0169] 이에 앞서, 사용자 인증 장치는 결제 가능 판단시 정보 블록 1을 신용카드 승인 요청장치로 전송하기 이전에 가맹점에 의한 거래 위변조를 막기 위해 거래 연동 일회용 인증 값(거래 인증값)을 생성할 수 있다(단계 S540).

[0170] 사용자 인증 장치는 거래 연동 일회용 인증 값을 웹 기반 상거래 장치로 전송할 수 있다(단계 S545).

[0171] 웹 기반 상거래 장치는 결제 내역, 임시 가상 카드 번호, 거래 연동 일회용 인증 값을 신용카드 승인 요청 장치로 전송하여 결제 승인을 요청할 수 있다(단계 S550).

[0172] 여기서, 단계 S540 내지 단계 S550 대신 사용자 인증 장치가 단계 S535 이후, 본인 인증을 성공 후 직접 신용카드 승인 요청 장치로 결제 승인을 요청할 수 있다(단계 S555).

[0173] 한편, 신용카드 승인 요청 장치는 결제 내역과 회원 정보 등을 통해 거래 연동 일회용 인증값을 직접 생성하고, 직접 생성한 거래 연동 일회용 인증값과 웹 기반 상거래 장치로부터 수신한 거래 연동 일회용 인증값을 비교할 수 있다(단계 S560). 이러한 비교 절차를 기반으로 웹 기반 상거래 장치로부터 수신한 결제 내역에 대한 위변조의 발생 여부가 검증될 수 있다.

[0174] 신용카드 승인 요청 장치는 사용자 인증 장치로 거래 연동 일회용 인증값을 전송하고, 정보 블록 1을 요청할 수 있다(단계 S565).

[0175] 사용자 인증 장치는 거래 연동 일회용 인증값을 검증하고(단계 S570), 거래 연동 일회용 인증값이 검증된 경우, 정보 블록 1을 신용카드 승인 요청 장치로 전송할 수 있다(단계 S575).

[0176] 또한, 사용자 인증 장치는 임시 가상 카드 번호를 통해 추출된 카드 ID를 정보 블록 1과 함께 신용카드 승인 요청 장치로 전송할 수 있다.

[0177] 이때, 사용자 인증 장치 및 신용카드 승인 요청 장치는 상술한 거래 연동 일회용 인증값의 생성 및 검증 과정 없이 정보 블록 1 및 카드 ID를 송수신할 수도 있음은 물론이다.

[0178] 신용 카드 승인 요청 장치는 사용자 인증 장치로부터 수신한 정보 블록 1을 기반으로 정보 블록 2를 복호화하고, 복호화된 정보 블록 1 및 정보 블록 2를 기반으로 암호화된 신용 카드 인증 값을 복호화할 수 있다.

[0179] 또한, 신용 카드 승인 요청 장치는 사용자 인증 장치로부터 수신한 카드 ID에 대응되는 암호화된 신용 카드 번호를 복호화할 수 있다.

[0180] 이에 따라, 신용 카드 승인 요청 장치는 복호화된 신용 카드 인증 값과 신용 카드 번호를 기초로 승인 요청 정보를 생성하여 신용 카드사로 전송할 수 있다(단계 S580). 예를 들어, 승인 요청 정보는 정보 블록 1과 정보 블록 2 및 신용 카드 번호를 기반으로 하드웨어 암호화 장비(HSM)를 통해 생성된 승인 전문일 수 있다.

[0181] 이때, 신용카드 승인 요청 장치는 사용자 인증 장치로부터 웹 기반 상거래 장치가 제공한 결제 정보를 수신할 수 있으며, 해당 결제 정보와 상술한 신용 카드 인증 값 및 신용 카드 번호를 기반으로 승인 요청 정보(승인 전문)을 생성할 수 있다.

[0182] 신용 카드 승인 요청 장치는 신용카드사 서버로 승인 요청 정보를 전송할 수 있고(단계 S585), 신용 카드사 서버는 승인 요청 정보를 수신하고 승인 결과를 신용 카드 승인 요청 장치로 전송할 수 있다(단계 S590). 신용 카드 승인 요청 장치는 승인 결과를 웹 기반 상거래 장치로 전송할 수 있다(단계 S595).

[0183] 상술한 구성을 토대로, 본 발명의 실시예에 따른 결제 서비스 제공 장치는 결제 처리를 완료할 수 있으며, 사용자가 원하는 결제 한도 내에서 결제가 이루어지도록 지원할 수 있다.

[0184] 도 7은 본 발명의 실시예에 따른 결제 PIN의 입력에 따른 결제 절차를 나타낸 개념도이다.

[0185] 도 7을 참조하면, 웹 기반 상거래 장치(600)는 사용자에 의해 선택된 임시 가상 카드 번호와 결제 내역(품목, 가맹점 명, 금액, 거래 일시 등)을 포함하는 결제 정보를 사용자 인증 장치(620)로 전달하여 거래 인증 요청을 진행할 수 있다.

[0186] 사용자 인증 장치(620)는 임시 가상 카드 번호를 기준으로 사용자의 카드 ID에 대한 정보를 조회하여 사용자의 카드 ID에 대한 정보를 획득할 수 있다. 사용자의 카드 ID에 대한 정보는 신용 카드 승인 요청 장치(640)로 전달될 수 있다. 신용 카드 승인 요청 장치(640)는 카드 ID에 대한 정보를 기반으로 암호화된 신용 카드 번호를 조회하고 암호화된 신용 카드 번호를 복호화하여 고객의 결제 정보로서 사용할 수 있다.

[0187] 신용 카드 승인 요청 장치(640)에서 암호화된 신용 카드 번호에 대한 복호화는 사용자 인증 장치(620)로부터 수신한 정보 블록 1을 기반으로 복호화한 정보 블록 2를 기반으로 수행되거나 HSM을 기반으로 복호화가 수행될 수 있다.

[0188] 사용자 인증 장치(620)는 사용자 장치로 회원 가입시 설정한 결제 PIN에 대한 정보를 입력하도록 요청할 수 있다. 사용자는 사용자 장치를 통해 원하는 결제 한도에 대응되는 결제 PIN을 입력할 수 있다.

[0189] 사용자 인증 장치(620)는 회원 가입시에 암호화하여 저장한 암호화된 복수의 정보 블록 1 중에서 사용자가 원하는 결제 한도에 대응되는 결제 PIN으로 암호화된 정보 블록 1을 사용자 장치로부터 수신된 결제 PIN을 통해 복호화할 수 있다.

[0190] 또한, 사용자 인증 장치(620)는 복호화된 정보 블록 1에 대응되어 설정된 결제 한도와 결제 정보에 따른 결제 금액을 비교하여 결제 금액이 결제 한도 이내인 경우 결제가 가능한 것으로 판단하여 이후 절차를 진행할 수 있다.

[0191] 신용카드 승인 요청 장치(640)는 사용자 인증 장치(620)로 거래 인증값을 전송하고, 정보 블록 1을 요청할 수 있다. 사용자 인증 장치(620)는 거래 인증값을 검증하고, 거래 인증값이 검증되고 결제 한도와 결제 금액의 비교를 통해 결제 가능한 것으로 판단한 경우, 복호화된 정보 블록 1을 신용카드 승인 요청 장치(640)로 전송할 수 있다.

[0192] 신용 카드 승인 요청 장치(640)는 사용자 인증 장치(620)로부터 수신한 복호화된 정보 블록 1을 기반으로 정보 블록 2를 복호화할 수 있다. 신용 카드 승인 요청 장치(640)는 복호화된 정보 블록 1 및 정보 블록 2를 기반으로 신용 카드 인증 값을 생성할 수 있다.

[0193] 이에 따라, 신용 카드 승인 요청 장치(640)는 신용 카드 인증 값과 신용 카드 번호를 기반으로 승인 요청 정보를 생성하여 신용 카드사 서버로 전송할 수 있다.

[0194] 이때, 신용카드 승인 요청 장치(640)는 사용자 인증 장치(620)로부터 웹 기반 상거래 장치(600)가 제공한 결제 정보를 정보 블록 1과 함께 수신할 수 있으며, 해당 결제 정보와 상술한 신용 카드 인증 값 및 신용 카드 번호를 기반으로 승인 요청 정보(승인 전문)을 생성할 수 있다.

[0195] 신용 카드 승인 요청 장치(640)는 신용카드사 서버로 승인 요청 정보를 전송할 수 있고, 신용 카드사 서버는 승인 요청 정보를 수신하고 승인 결과를 신용 카드 승인 요청 장치(640)로 전송할 수 있다. 신용 카드 승인 요청 장치(640)는 승인 결과를 웹 기반 상거래 장치(600)로 전송할 수 있다.

[0196] 상술한 구성에서, 결제 서비스 제공 장치는 사용자가 서로 다른 결제 한도에 각각 대응되는 결제 PIN의 복잡도를 상이하게 설정할 수 있도록 지원하여, 결제 한도가 가장 높은 결제 PIN에 대해서는 높은 복잡도를 가진 결제 PIN이 설정되도록 하고, 결제 한도가 낮은 소액 결제에 대해서는 복잡도가 낮은 결제 PIN이 설정되도록 하여 결제 한도가 높은 결제 PIN의 보안성을 높이고, 결제 한도가 낮은 결제 PIN을 통해 결제 편의성을 제공할 수 있는데 이를 도 8을 통해 설명한다.

[0197] 도시된 바와 같이, 결제 서비스 제공 장치에 포함된 사용자 인증 장치는 사용자 장치로부터 수신된 설정정보를 기초로 결제 한도가 가장 높은 결제 PIN 정보를 구성하는 복수의 자리 중 사용자 장치의 선택에 따라 선택된 일부 자리의 코드를 결제 PIN 정보와 상이한 결제 한도에 대응되는 다른 결제 PIN 정보로 이용할 수 있다.

[0198] 예를 들어, 도시된 바와 같이 결제 PIN 정보인 PIN 1을 구성하는 복수의 자리(8자리) 중 일부(4자리)에 해당하는 다른 결제 PIN 정보인 PIN 2를 입력하면 소액결제만 가능하도록 하고, 전체 PIN 1(8자리)을 입력하면 일반 한도 결제가 가능하도록 할 수 있다.

[0199] 이를 통해, 달리 설정되는 복수의 결제 PIN은 일반 한도에 대한 PIN 정보가 더 복잡하고 소액 한도에 대한 PIN 정보는 더 간소할 수 있으며, 필요하다면 일반 한도에 대한 PIN은 소액한도에 대한 PIN을 포함하는 형태로 구성할 수도 있다. 따라서, 소액 결제는 입력 횟수를 줄이기 위해 일반 한도에 대한 PIN 중 일부를 입력하는 것으로 구성할 수 있다.

[0200] 이상에서 설명된 사용자 장치, 결제 서비스 제공 장치, 웹 기반 상거래 장치 및 각종 서버는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다.

[0201] 또한, 실시예들에서 설명된 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPA(field programmable array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다.

[0202] 사용자 장치, 결제 서비스 제공 장치, 웹 기반 상거래 장치 및 각종 서버는 운영 체제(OS: Operating System) 및 운영 체제상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 실행할 수 있다. 또한, 사용자 장치, 결제 서비스 제공 장치, 웹 기반 상거래 장치 및 각종 서버는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다.

[0203] 이해의 편의를 위하여, 구성요소는 각각 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다.

[0204] 예를 들어, 사용자 장치, 결제 서비스 제공 장치, 웹 기반 상거래 장치 및 각종 서버는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0205] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 사용자 장치, 결제 서비스 제공 장치, 웹 기반 상거래 장치 및 각종 서버를 원하는 대로 동작하도록 하거나 독립적으로 또는 결합적으로(collectively) 명령할 수 있다.

[0206] 소프트웨어 및/또는 데이터는, 사용자 장치, 결제 서비스 제공 장치, 웹 기반 상거래 장치 및 각종 서버에 의하여 해석되거나 사용자 장치, 결제 서비스 제공 장치, 웹 기반 상거래 장치 및 각종 서버에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 구체화(embody)될 수 있다.

[0207] 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0208] 본 발명의 실시예에 따른 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 방법은 컴퓨터 프로그램으로 작성 가능하며, 컴퓨터 프로그램을 구성하는 코드들 및 코드 세그먼트들은 당해 분야의 컴퓨터 프로그래머에 의하여 용이하게 추론될 수 있다. 또한, 해당 컴퓨터 프로그램은 컴퓨터가 읽을 수 있는 정보저장매체(computer readable media)에 저장되고, 컴퓨터나 본 발명의 실시예에 따른 결제 서비스 제공 장치, 웹 기반 상거래 장치, 사용자 장치 등에 의하여 읽혀지고 실행됨으로써 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 방법을 구현할 수 있다.

[0209] 정보저장매체는 자기 기록매체, 광 기록매체 및 캐리어 웨이브 매체를 포함한다. 본 발명의 실시예에 따른 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 방법을 구현하는 컴퓨터 프로그램은 결제 서비스 제공 장치, 웹 기반 상거래 장치, 사용자 장치 등의 내장 메모리에 저장 및 설치될 수 있다. 또는, 본 발명의 실시예에 따른 복수 한도 선택을 지원하는 웹 기반 결제 서비스 제공 방법을 구현하는 컴퓨터 프로그램을 저장 및 설치한 스마트 카드 등의 외장 메모리가 인터페이스를 통해 결제 서비스 제공 장치, 웹 기반 상거래 장치, 사용자 장치 등에 장착될 수도 있다.

[0210] 본 명세서에 기술된 다양한 장치 및 구성부는 하드웨어 회로(예를 들어, CMOS 기반 로직 회로), 펌웨어, 소프트웨어 또는 이들의 조합에 의해 구현될 수 있다. 예를 들어, 다양한 전기적 구조의 형태로 트랜지스터, 로직게이트 및 전자회로를 활용하여 구현될 수 있다.

[0211] 전술된 내용은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 수정 및 변형이 가능할 것이다. 따라서, 본 발명에 개시된 실시예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

산업상 이용가능성

[0212] 본 발명은 웹 표준 환경에서 비대면 지급 결제를 위한 웹 기반 인증 결제 방법을 제공하는 동시에 단일 결제 수단에 대한 서로 다른 결제 한도에 따른 PIN을 달리 설정하도록 하고, 해당 PIN 입력 정보를 통해 한도를 달리 적용할 수 있으며, 소액 결제 한도의 PIN을 간단하게 설정하는 것으로 소액에 대한 결제 편의성을 높일 수 있고, 소액 결제 한도보다 높은 일반 한도에 대한 PIN의 전체 노출을 줄일 수 있어 보안성을 높이는 것으로서, 다양한 온라인 결제 또는 비대면 결제 시스템에 광범위하게 적용될 수 있다.

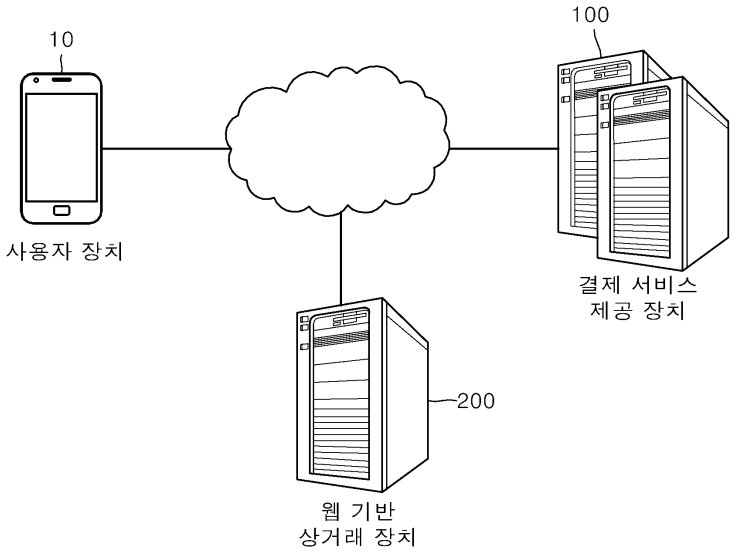
부호의 설명

[0213] 100: 결제 서비스 제공 장치 120: 사용자 인증 장치

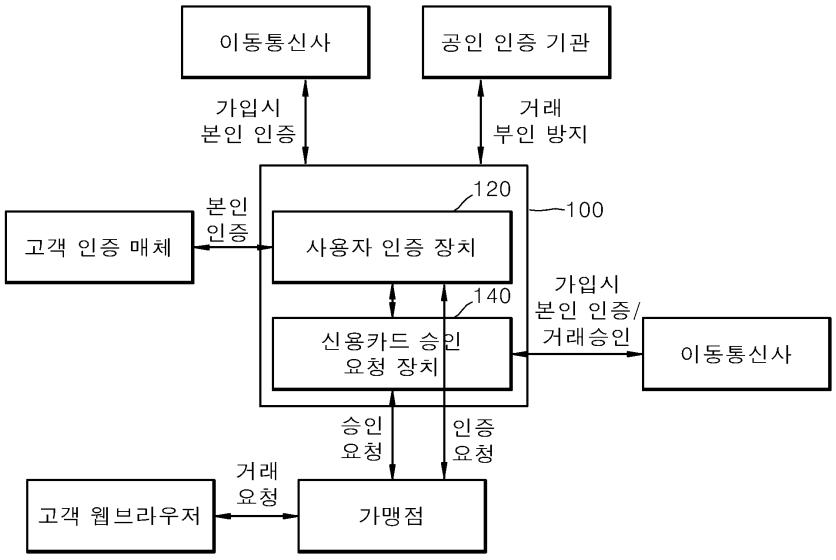
140: 신용카드 승인 요청 장치

도면

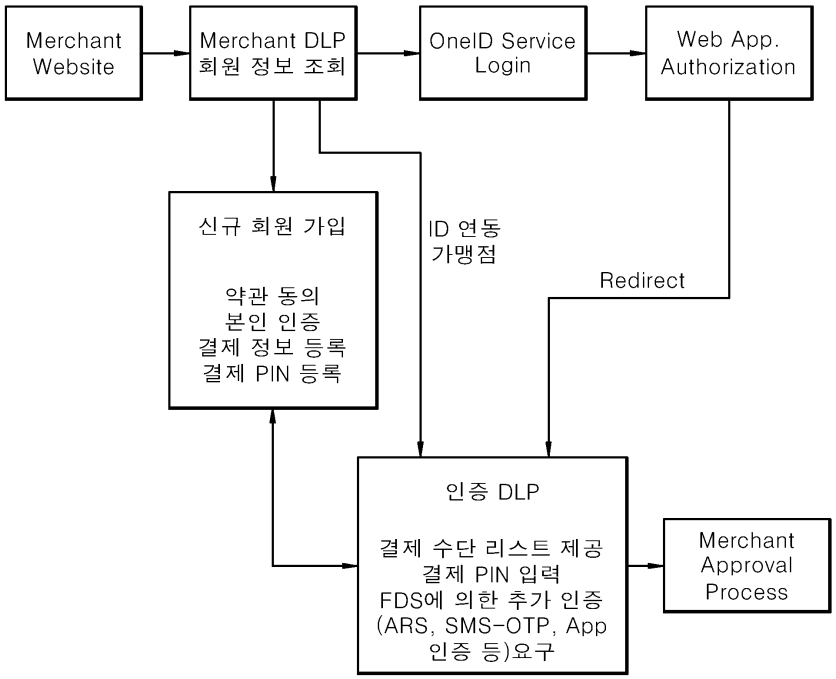
도면1


10
사용자 장치
100
결제 서비스
제공 장치
200
웹 기반
상거래 장치

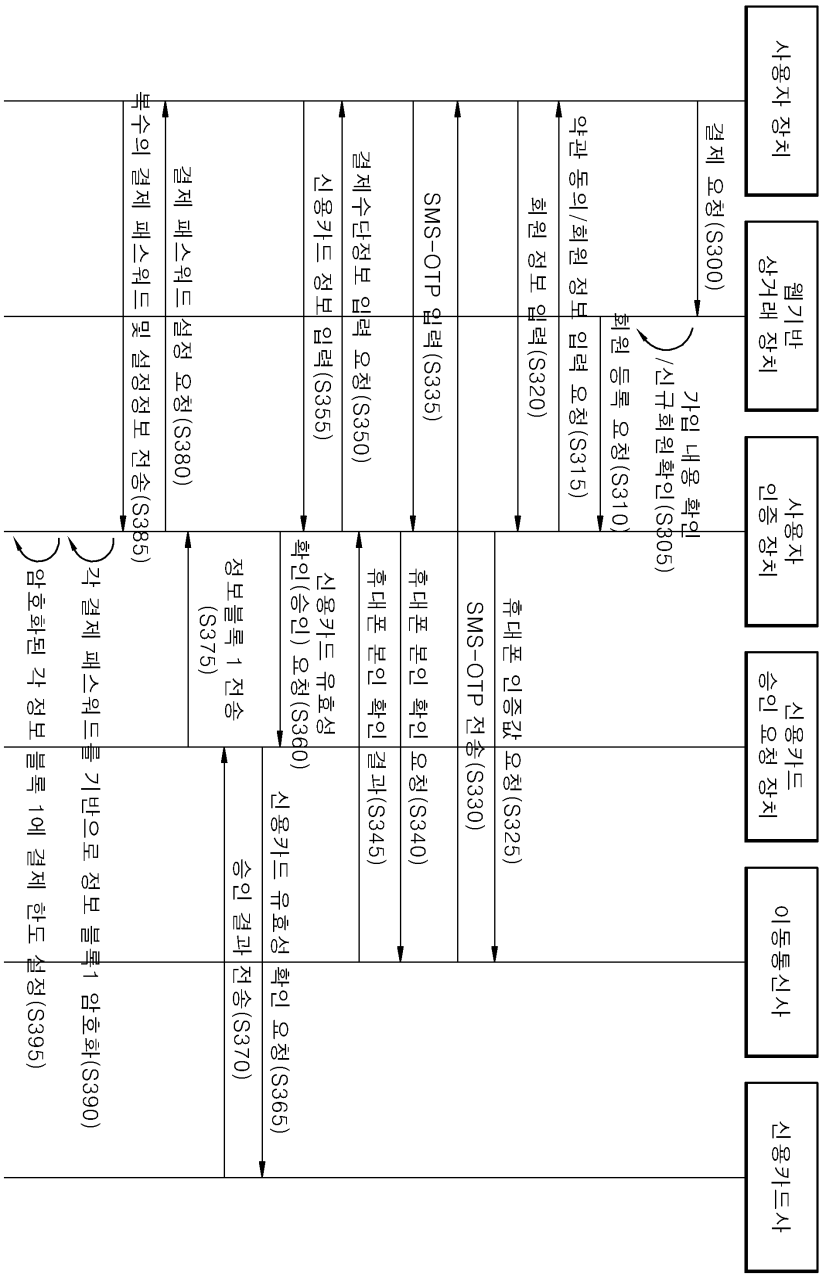
도면2


이동통신사
공인 인증 기관
가입시
본인 인증
거래
부인 방지
120
100
본인
인증
고객 인증 매체
사용자 인증 장치
140
가입시
본인 인증/
거래승인
신용카드 승인
요청 장치
이동통신사
승인
요청
인증
요청
거래
요청
고객 웹브라우저
가맹점

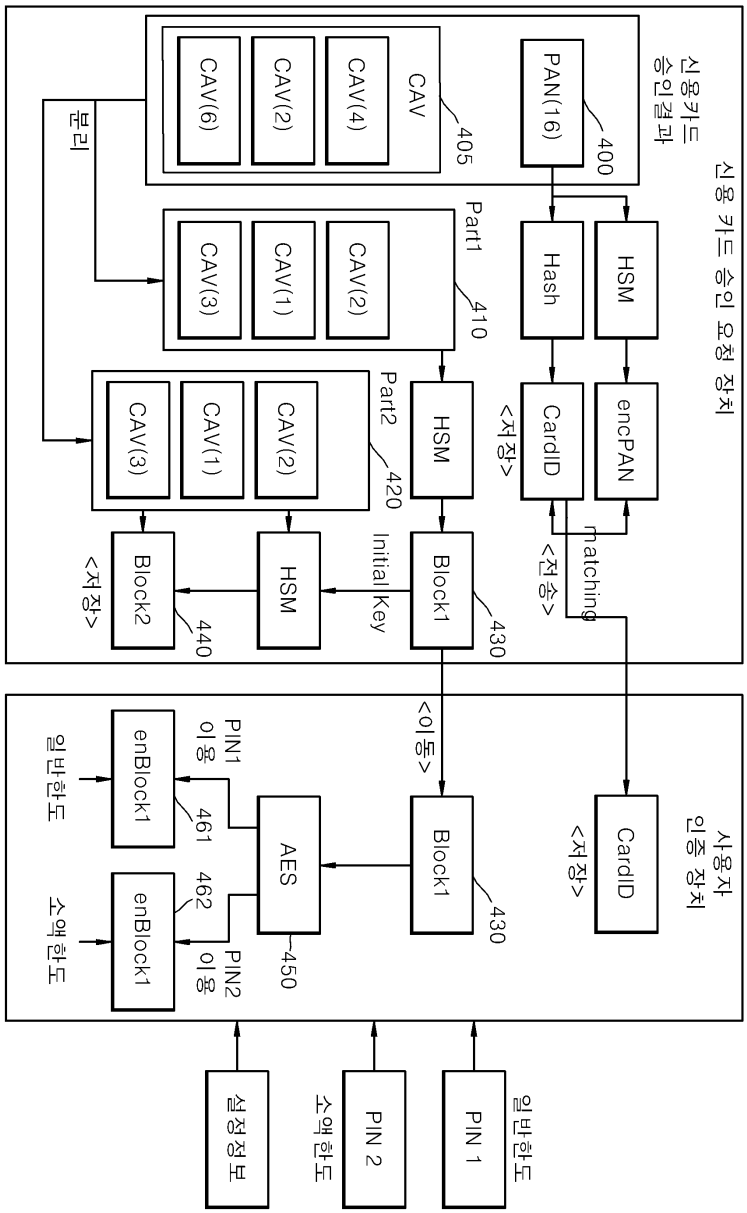
도면3


Merchant Website
Merchant DLP 회원 정보 조회
OneID Service Login
Web App. Authorization
신규 회원 가입
약관 동의
본인 인증
결제 정보 등록
결제 PIN 등록
ID 연동 가맹점
Redirect
인증 DLP
결제 수단 리스트 제공
결제 PIN 입력
FDS에 의한 추가 인증
(ARS, SMS-OTP, App 인증 등)요구
Merchant Approval Process

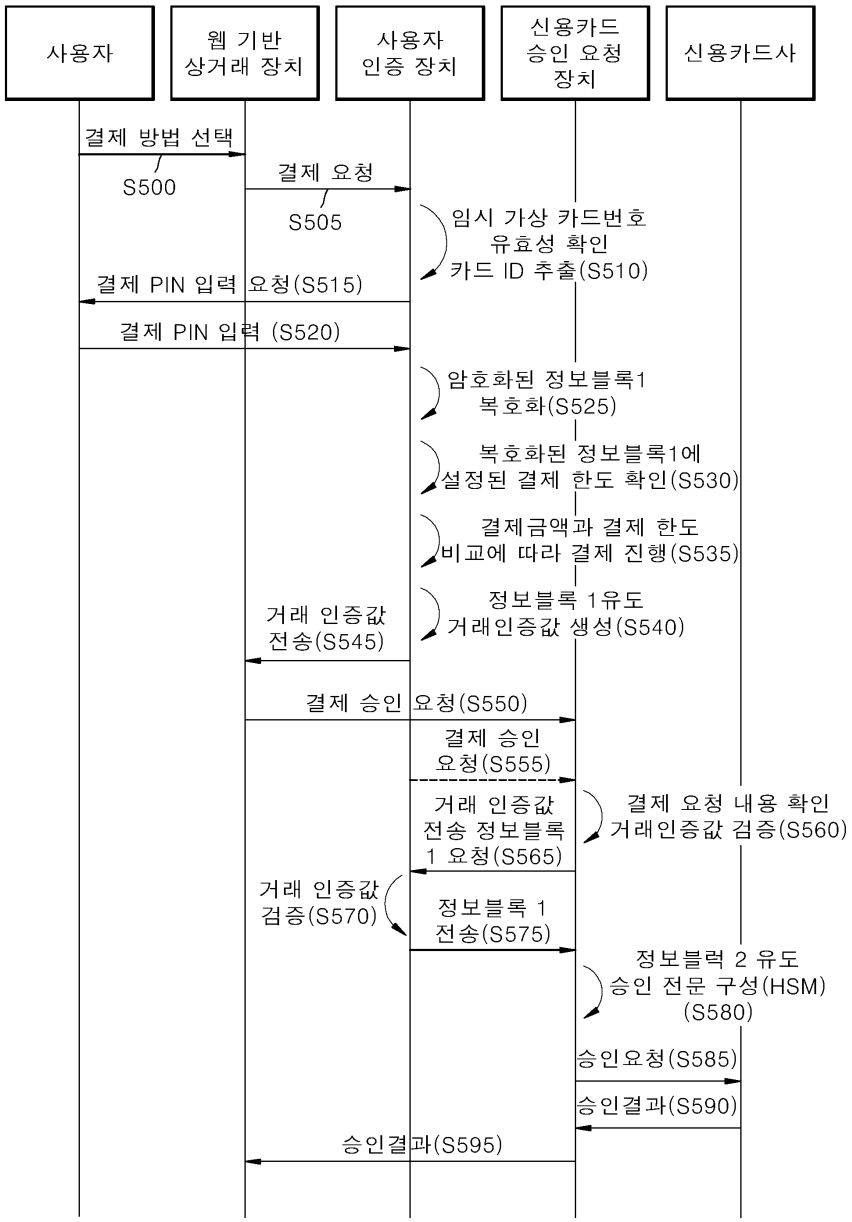
도면4


사용자 장치
웹기반 상거래 장치
사용자 인증 장치
신용카드 승인 요청 장치
이동통신사
신용카드사
결제 요청(S300)
가입 내용 확인 /신규회원확인(S305)
회원 등록 요청(S310)
약관 동의/회원 정보 입력 요청(S315)
회원 정보 입력(S320)
휴대폰 인증값 요청(S325)
SMS-OTP 전송(S330)
SMS-OTP 입력(S335)
휴대폰 본인 확인 요청(S340)
휴대폰 본인 확인 결과(S345)
결제수단정보 입력 요청(S350)
신용카드 정보 입력(S355)
신용카드 유효성 확인(승인) 요청(S360)
신용카드 유효성 확인 요청(S365)
승인 결과 전송(S370)
정보블록 1 전송 (S375)
결제 패스워드 설정 요청(S380)
복수의 결제 패스워드 및 설정정보 전송(S385)
각 결제 패스워드를 기반으로 정보 블록1 암호화(S390)
암호화된 각 정보 블록 1에 결제 한도 설정(S395)

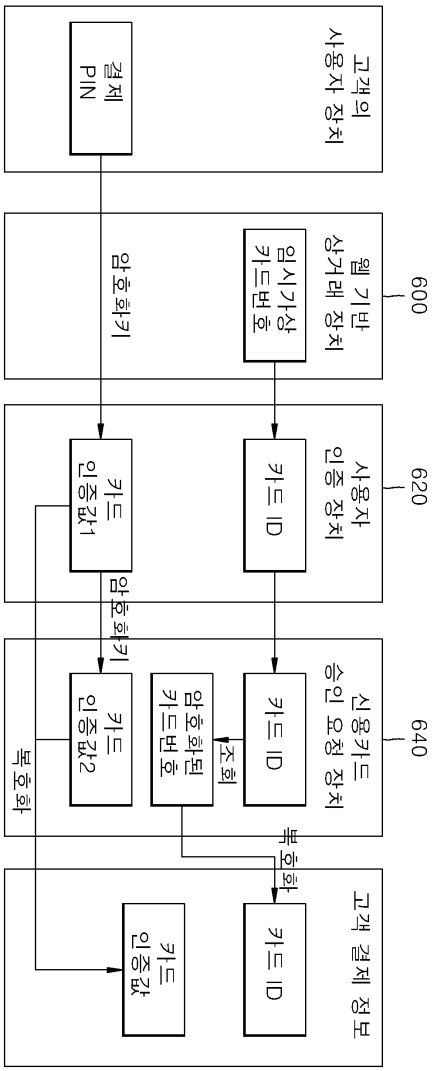
도면5


신용 카드 승인 요청 장치
신용카드 승인결과
PAN(16)
400
CAV
CAV(6)
CAV(2)
CAV(4)
405
분리
Part1
CAV(3)
CAV(1)
CAV(2)
410
Part2
CAV(3)
CAV(1)
CAV(2)
420
Hash
HSM
CardID
<저장>
encPAN
matching
<전송>
HSM
Block1
430
Initial Key
HSM
Block2
440
<저장>
<이동>
사용자 인증 장치
CardID
<저장>
Block1
430
AES
450
enBlock1
461
PIN1 이용
일반한도
enBlock1
462
PIN2 이용
소액한도
설정정보
PIN 2
소액한도
PIN 1
일반한도

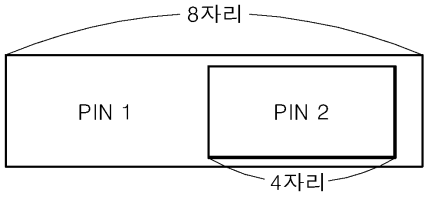
도면6


사용자
웹 기반 상거래 장치
사용자 인증 장치
신용카드 승인 요청 장치
신용카드사
결제 방법 선택
S500
결제 요청
S505
임시 가상 카드번호 유효성 확인 카드 ID 추출(S510)
결제 PIN 입력 요청(S515)
결제 PIN 입력 (S520)
암호화된 정보블록1 복호화(S525)
복호화된 정보블록1에 설정된 결제 한도 확인(S530)
결제금액과 결제 한도 비교에 따라 결제 진행(S535)
정보블록 1유도 거래인증값 생성(S540)
거래 인증값 전송(S545)
결제 승인 요청(S550)
결제 승인 요청(S555)
결제 요청 내용 확인 거래인증값 검증(S560)
거래 인증값 전송 정보블록 1 요청(S565)
거래 인증값 검증(S570)
정보블록 1 전송(S575)
정보블럭 2 유도 승인 전문 구성(HSM) (S580)
승인요청(S585)
승인결과(S590)
승인결과(S595)

도면7


고객의 사용자 장치
결제 PIN
웹 기반 상거래 장치
600
암호화키
임시가상 카드번호
사용자 인증 장치
620
카드 인증값1
카드 ID
암호화키
신용카드 승인 요청 장치
640
카드 인증값2
암호화된 카드번호
카드 ID
조회
복호화
복호화
고객 결제 정보
카드 인증값
카드 ID

도면8


8자리
PIN 1
PIN 2
4자리