(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2011 년 4 월 28 일 (28.04.2011)

PCT

(10) 국제공개번호
WO 2011/049356 A2

(51) 국제특허분류:
G06Q 20/00 (2006.01) *H04W 12/06* (2009.01)

(21) 국제출원번호: PCT/KR2010/007171

(22) 국제출원일: 2010 년 10 월 20 일 (20.10.2010)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2009-0099794 2009 년 10 월 20 일 (20.10.2009) KR

(71) 출원인 (US 을(를) 제외한 모든 지정국에 대하여): **에스케이텔레콤 주식회사 (SK TELECOM CO., LTD.)** [KR/KR]; 서울 중구 을지로 2 가 11 번지, 100-999 Seoul (KR).

(72) 발명자; 겸
(75) 발명자/출원인 (US 에 한하여): **이원준 (LEE, Wonjun)** [KR/KR]; 서울특별시 광진구 광장동 577 현대파크빌 1009-1303, 143-815 Seoul (KR). **최승진 (CHOI, Seungjin)** [KR/KR]; 서울특별시 용산구 서빙고동 신동아아파트 16-1302, 140-751 Seoul (KR). **임동필 (LIM, Dongphil)** [KR/KR]; 서울특별시 광진구 광장동 광장 11 차 현대홈타운 1107-103, 143-210 Seoul (KR).

(74) 대리인: **이철희 (LEE, Chulhee)**; 서울 강남구 역삼동 647-13 동궁빌딩 5 층, 135-911 Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

공개:
— 국제조사보고서 없이 공개하며 보고서 접수 후 이를 별도 공개함 (규칙 48.2(g))

WO 2011/049356 A2

(54) Title: SYSTEM AND METHOD FOR PROVIDING AN AUTHENTICATION SERVICE USING A MOBILE COMMUNICATION TERMINAL

(54) 발명의 명칭 : 이동통신 단말기를 이용한 인증서비스 시스템 및 그 방법

(57) Abstract: The present invention relates to a system and method for providing an authentication service using a mobile communication terminal. The system for providing an authentication service using a mobile communication terminal according to one embodiment of the present invention comprises: a mobile communication terminal having a built-in USIM card or a built-in SIM card; a client terminal which selects the mobile communication terminal as authentication means when making a request for payment for the purchase of product; an access control server which checks whether or not the selected mobile communication terminal has subscribed to a mobile card service, and, if the mobile communication terminal has subscribed to the mobile card service, transmits, to the mobile communication terminal, a message containing a callback URL for connecting the mobile communication terminal to a WAP page for payment authentication; and a WAP server which verifies the owner of the mobile communication terminal on the basis of the USIM card or of the SIM card when the mobile communication terminal is connected to the WAP page. According to the present invention, user authentication is performed using the mobile communication terminal of a user when the user uses an online electronic commerce system, thereby overcoming the problems of spatial restrictions in using an online electronic commerce system.

(57) 요약서: 본 발명은 이동통신 단말기를 이용한 인증서비스 시스템 및 그 방법에 관한 것으로서, 본 발명의 일 실시예에 따른 이동통신 단말기를 이용한 인증서비스 시스템은, USIM 카드 또는 SIM 카드를 탑재한 이동통신 단말기; 상품 구매에 따른 대금결제 요청 시에 이동통신 단말기를 인증수단으로 선택하는 클라이언트 단말기; 선택된 이동통신 단말기의 모바일카드 가입여부를 검사하며, 이동통신 단말기가 모바일카드에 가입된 경우에 결제인증을 위한 웹페이지와 이동통신 단말기를 연결하기 위한 콜백 URL 이 포함된 문자메시지를 이동통신 단말기에 전송하는 접근제어 서버; 및 웹페이지에 이동통신 단말기가 접속하면 USIM 카드 또는 SIM 카드에 기초하여 정당 소유자에 대한 여부를 검증하는 웹 서버를 포함하는 것을 특징으로 한다. 본 발명에 의하면, 이용자가 온라인 상에서 전자상거래를 하는 경우, 이용자의 이동통신 단말기를 이용하여 이용자에 대한 인증을 수행함으로써, 온라인 상에서의 전자상거래를 이용할 수 있는 장소적 한계를 극복할 수 있게 된다.

명세서

발명의 명칭: 이동통신 단말기를 이용한 인증서비스 시스템 및 그 방법

기술분야

[1] 본 발명의 실시예는 이동통신 단말기를 이용한 인증서비스 시스템 및 그 방법에 관한 것이다. 더욱 상세하게는, 이용자가 온라인 상에서 전자상거래를 하는 경우, 이용자의 이동통신 단말기를 이용하여 이용자에 대한 인증을 수행함으로써, 온라인 상에서의 전자상거래를 이용할 수 있는 장소적 한계를 극복할 수 있도록 하며, 이동통신 단말기에 탑재된 USIM 카드를 인증수단으로 활용함으로써 인증의 신뢰성을 높일 수 있는 이동통신 단말기를 이용한 인증서비스 시스템 및 그 방법에 관한 것이다.

배경기술

[2] 인터넷의 보급이 확산됨에 따라 온라인 상에서 이루어지는 전자상거래의 규모 또한 폭발적으로 증가하고 있다. 전자상거래의 경우, 오프라인상에서의 실제 거래와는 달리 온라인 상에서 물품을 구매하거나 서비스를 이용하고, 그에 대한 대금 또는 사용료 또한 온라인 상에서 지급하는 것이 일반적이기 때문에 이용자의 실명 확인 또는 본인 여부의 확인이 무엇보다 중요하다.

[3] 이를 위하여, 종래에는 상품 거래가 이루어지는 판매자의 웹 사이트에 구매자가 가입하여 ID 및 비밀번호를 등록하도록 유도하고, 구매자에 의한 상품 구매 시 등록된 ID와 비밀번호를 확인함으로써 이용자의 본인 여부를 확인하였다.

[4] 그러나, 이와 같이 ID 및 비밀번호에 의한 이용자 인증은, 온라인 상에서 해킹하기가 쉽기 때문에, 고객의 거래를 인증하는 수단으로 사용하기에는 보안상의 문제점이 있다.

[5] 이에 대한 해결책으로 제시된 것이 인증서 즉, 전자서명(digital signature)을 통하여 이용자의 본인 여부를 확인하는 방법으로서, 디지털 ID라고도 알려진 인증서를 이용자의 단말기에 설치해두고 필요 시에 이를 인증기관에 제출하여 이용자의 본인 여부를 확인하는 방법이다. 이때, 인증서는 한국정보인증, 금융결제원 및 한국전산증권과 같은 공인된 인증기관에 의해 발행되며, 개인정보를 디지털 암호화 및 서명에 사용할 수 있도록 한 쌍의 전자 키로 이루어져 있는데, 이용자가 필요 시에 비밀키로 서명하고 인증기관에 제출하면 인증기관이 이를 확인함으로써, 이용자의 진정성을 보증한다.

[6] 그러나, 이와 같은 인증서를 이용한 방법은, 반드시 인증서를 설치한 단말기에서만 이용자가 자신을 인증할 수 있기 때문에, 이용자가 온라인을 통하여 전자상거래를 할 수 있는 장소적 제약이 따른다는 문제점이 있다.

발명의 상세한 설명

기술적 과제

[7] 전술한 문제점을 해결하기 위해 본 발명의 일 실시예는, 이용자가 온라인 상에서 전자상거래를 하는 경우, 이용자의 이동통신 단말기를 이용하여 이용자에 대한 인증을 수행함으로써, 온라인 상에서의 전자상거래를 이용할 수 있는 장소적 한계를 극복할 수 있도록 하는 이동통신 단말기를 이용한 인증서비스 시스템 및 그 방법을 제공하는 것을 목적으로 한다.

과제 해결 수단

[8] 전술한 목적을 달성하기 위한 본 발명의 일 실시예에 따른 이동통신 단말기를 이용한 인증서비스 시스템은, USIM(Universal Subscriber Identity Module) 카드 또는 SIM 카드를 탑재한 이동통신 단말기; 상품 구매에 따른 대금결제 요청 시에 이동통신 단말기를 인증수단으로 선택하는 클라이언트 단말기; 선택된 이동통신 단말기의 모바일카드 가입여부를 검사하며, 이동통신 단말기가 모바일카드에 가입된 경우에 결제인증을 위한 왑(WAP: Wireless Application Protocol)페이지와 이동통신 단말기를 연결하기 위한 콜백(call-back) URL(Uniform Resource Location)이 포함된 문자메시지를 상기 이동통신 단말기에 전송하는 접근제어 서버; 및 왑페이지에 이동통신 단말기가 접속하면 USIM 카드 또는 SIM 카드에 기초하여 정당 소유자에 대한 여부를 검증하는 왑 서버를 포함하는 것을 특징으로 한다.

[9] 여기서, 왑 서버는, 이동통신 단말기가 왑페이지를 통해 접속하면 USIM 카드 또는 SIM 카드에 저장된 정보를 읽고 표시하는 것이 바람직하다.

[10] 또한, 이동통신 단말기는, 사용자에 대한 계좌정보 또는 신용카드정보를 저장하며, 저장된 계좌정보 또는 신용카드 정보를 왑페이지를 통해 표시시키는 것이 바람직하다.

[11] 또한, 왑 서버는, 왑페이지에 표시되는 계좌정보 또는 신용카드정보, 및 이동통신 단말기로부터 입력되는 패스워드에 기초하여 접근제어 서버에 정당 소유자에 대한 여부를 검증하는 것이 바람직하다.

[12] 전술한 목적을 달성하기 위한 본 발명의 다른 실시예에 따른 이동통신 단말기를 이용한 인증서비스 시스템은, USIM 카드 또는 SIM 카드를 탑재한 이동통신 단말기; 이동통신 단말기를 이용하여 상품 구매에 따른 대금결제 요청 시, 이동통신 단말기의 모바일카드 가입여부를 검사하며, 이동통신 단말기가 모바일카드에 가입된 경우에 결제인증을 위한 왑페이지와 이동통신 단말기를 연결하기 위한 콜백 URL이 포함된 문자메시지를 이동통신 단말기에 전송하는 접근제어 서버; 및 왑페이지에 이동통신 단말기가 접속하면 USIM 카드 또는 SIM 카드에 기초하여 정당 소유자에 대한 여부를 검증하는 왑 서버를 포함하는 것을 특징으로 한다.

[13] 전술한 목적을 달성하기 위한 본 발명에 따른 이동통신 단말기를 이용한 인증서비스 방법의 일 실시예는, 클라이언트 단말기를 이용하여 온라인

상에서의 상품 구매 시, USIM 카드 또는 SIM 카드를 탑재한 이동통신 단말기를 인증수단으로 입력받는 단계; 입력된 이동통신 단말기의 모바일카드 가입여부를 검사하는 단계; 이동통신 단말기가 모바일카드에 가입된 경우, 결제인증을 위한 왑페이지와 이동통신 단말기를 연결하기 위한 콜백 URL이 포함된 문자메시지를 이동통신 단말기에 전송하는 단계; 및 왑페이지에 이동통신 단말기가 접속하면 USIM 카드 또는 SIM 카드에 기초하여 정당 소유자에 대한 여부를 검증하는 단계를 포함하는 것을 특징으로 한다.

[14] 바람직하게는, 이동통신 단말기를 이용한 인증서비스 방법은, 이동통신 단말기가 왑페이지를 통해 접속하면 USIM 카드에 저장된 정보를 읽고 표시하는 단계를 더 포함할 수 있다.

[15] 또한, 이동통신 단말기를 이용한 인증서비스 방법은, 이동통신 단말기가, 사용자에 대한 계좌정보 또는 신용카드정보를 저장하는 단계를 더 포함할 수도 있다. 이 경우, 이동통신 단말기에 저장된 계좌정보 또는 신용카드 정보를 왑페이지를 통해 표시시키는 것이 바람직하다.

[16] 또한, 이동통신 단말기를 이용한 인증서비스 방법은, 왑페이지에 표시되는 계좌정보 또는 신용카드정보, 및 이동통신 단말기로부터 입력되는 패스워드에 기초하여 정당 소유자에 대한 여부를 검증하는 것이 바람직하다.

[17] 전술한 목적을 달성하기 위한 본 발명에 따른 이동통신 단말기를 이용한 인증서비스 방법의 다른 실시예는, USIM 카드 또는 SIM 카드를 탑재한 이동통신 단말기를 이용하여 상품 구매에 따른 대금결제 요청 시, 이동통신 단말기의 모바일카드 가입여부를 검사하는 단계; 이동통신 단말기가 모바일카드에 가입된 경우, 결제인증을 위한 왑페이지와 이동통신 단말기를 연결하기 위한 콜백 URL이 포함된 문자메시지를 이동통신 단말기에 전송하는 단계; 및 왑페이지에 이동통신 단말기가 접속하면 USIM 카드 또는 SIM 카드에 기초하여 정당 소유자에 대한 여부를 검증하는 단계를 포함하는 것을 특징으로 한다.

발명의 효과

[18] 이상에서 설명한 바와 같이 본 발명의 실시예에 의하면, 이용자가 온라인 상에서 전자상거래를 하는 경우, 이용자의 이동통신 단말기를 이용하여 이용자에 대한 인증을 수행함으로써, 온라인 상에서의 전자상거래를 이용할 수 있는 장소적 한계를 극복할 수 있도록 하며, 이동통신 단말기에 탑재된 USIM 카드를 인증수단으로 활용함으로써 이용자의 인증에 대한 신뢰성을 높일 수 있게 된다.

도면의 간단한 설명

[19] 도 1은 본 발명의 일 실시예에 따른 이동통신 단말기를 이용한 인증서비스 시스템을 개략적으로 도시한 도면이다.

[20] 도 2는 도 1의 접근제어 서버를 개략적으로 도시한 도면이다.

[21] 도 3은 도 1의 왑 서버를 개략적으로 도시한 도면이다.

[22] 도 4 및 도 5는 도 1의 이동통신 단말기를 이용한 인증서비스 시스템에 의한 인증서비스 방법의 일 실시예를 나타낸 흐름도이다.

[23] 도 6은 본 발명의 다른 실시예에 따른 이동통신 단말기를 이용한 인증서비스 시스템을 개략적으로 도시한 도면이다.

[24] 도 7 및 도 8은 도 4의 이동통신 단말기를 이용한 인증서비스 시스템에 의한 인증서비스 방법의 일 실시예를 나타낸 흐름도이다.

발명의 실시를 위한 형태

[25] 이하, 본 발명의 일부 실시예들을 예시적인 도면을 통해 상세하게 설명한다. 각 도면의 구성요소들에 참조부호를 부가함에 있어서, 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다. 또한, 본 발명의 실시예를 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략한다.

[26] 또한, 본 발명의 실시예에 대한 구성 요소를 설명하는 데 있어서, 제 1, 제 2, A, B, (a), (b) 등의 용어를 사용할 수 있다. 이러한 용어는 그 구성 요소를 다른 구성 요소와 구별하기 위한 것일 뿐, 그 용어에 의해 해당 구성 요소의 본질이나 차례 또는 순서 등이 한정되지 않는다. 어떤 구성 요소가 다른 구성요소에 "연결", "결합" 또는 "접속"된다고 기재된 경우, 그 구성 요소는 그 다른 구성요소에 직접적으로 연결되거나 접속될 수 있지만, 각 구성 요소 사이에 또 다른 구성 요소가 "연결", "결합" 또는 "접속"될 수도 있다고 이해되어야 할 것이다.

[27] 도 1은 본 발명의 일 실시예에 따른 이동통신 단말기를 이용한 인증서비스 시스템을 개략적으로 도시한 도면이다. 도면을 참조하면, 본 발명의 일 실시예에 따른 이동통신 단말기를 이용한 인증서비스 시스템은, 클라이언트 단말기(110), 유무선 망(120), 몰 서버(130), 지불서버(PG: Payment Gateway)(140), MPI(Merchant Plug-In)(150), 디렉토리 서버(160), 접근제어 서버(ACS: Access Control Server)(170), 이동통신 단말기(180) 및 왑(WAP: Wireless Application Protocol) 서버(190)를 포함한다. 여기서, 몰 서버(130), 지불서버(140), MPI(150) 및 디렉토리 서버(160)는 쇼핑몰 사이트에 구비되거나, 쇼핑몰 사이트와 연계되는 서버들로서, 이들 서버를 통합하여 쇼핑몰 서버(135)라고 명명한다.

[28] 클라이언트 단말기(110)는 유무선 망(120)을 통하여 쇼핑몰 사이트에 접속 가능하며, 접속된 쇼핑몰 사이트에서 상품 구매에 따른 대금결제를 요청하고 이동통신 단말기(180)를 인증수단으로 선택할 수 있다. 또는, 상품 구매에 따른 대금이 소정 금액 이상인 경우, 클라이언트 단말기(110)는 이동통신 단말기(180)를 인증 및 결제 수단으로 선택할 수 있다. 이때, 클라이언트 단말기(110)는 사용자로부터 구매하고자 하는 상품의 종류와 사용자 정보를 입력 받아 암호화하여 몰 서버(130)로 전달한다. 사용자 정보에는 상품 대금을

결제하고자 하는 신용카드 정보가 포함될 수 있다. 여기서, 클라이언트 단말기(110)는 통상의 PC(Personal Computer)뿐만 아니라, 유무선 망(120)을 통하여 웹 사이트에 접속이 가능한 노트북, PMP(Portable Multimedia Player), PDA(Personal Digital Assistants), 휴대폰 등의 통신 기능이 구비된 휴대용 전자기기를 포함한다.

[29] 유무선 망(120)은 인터넷을 중심으로 서로 연결되어 데이터를 송수신할 수 있는 유선망 및 무선망을 통합하여 일컫는다. 여기서, 무선망은 블루투스(Bluetooth), IrDA(Infrared Data Association) 등에 의한 근거리 무선망, CDMA(Code Division Multiple Access), WCDMA(Wideband CDMA) 등에 의한 이동통신 망, WiBro(Wireless Broadband)와 같은 무선 인터넷 망을 포함한다.

[30] 몰 서버(130)는 쇼핑몰 사이트에 의해 운영되는 서버로서, 클라이언트 단말기(110)로부터 암호화된 정보를 수신하며, 수신된 정보를 지불서버(140)로 전달하고, 지불서버(140)로부터 전달된 정보에 대응하는 금융정보 승인결과를 수신하여 클라이언트 단말기(110)에 전달한다.

[31] 지불서버(140)는 수신된 사용자 정보를 해당 카드사 서버(도시하지 않음)에 전송한다. 이때, MPI(150)는 지불서버(140)가 수신한 사용자 정보가 유효한지 여부를 알아보기 위하여, 지불서버(140)로부터 사용자 정보를 수신하여 디렉토리 서버(160)로 전송하며, 디렉토리 서버(160)로부터 사용자 정보에 대한 등록 여부를 수신하여 지불서버(140)로 전송한다.

[32] 디렉토리 서버(160)는 MPI(150) 및 접근제어 서버(170)와 연동한다. 즉, 몰 서버(130)로부터 사용자 정보에 대한 유효성 여부가 요청되는 경우, 디렉토리 서버(160)는 접근제어 서버(170)로부터 사용자의 등록여부를 확인(즉, 토큰의 유무를 확인)하여 몰 서버(130)에 그 결과를 전송하며, 또한 사용자 정보에 대한 인증의 요청과 응답에 대한 정보를 저장한다.

[33] 접근제어 서버(170)는 디렉토리 서버(160)로부터 사용자 정보를 전송 받아, 사용자 정보의 등록 여부를 확인한 다음, 등록 여부에 대한 결과로 소정의 토큰(CAVV: Cardholder Authentication Verification Value)을 발생시켜 디렉토리 서버(160)로 전송한다.

[34] 한편, 접근제어 서버(170)는 도 2에 도시한 바와 같이 가입 검사부(172), 콜백 메시지 전송부(174), 인증처리부(176) 및 결제금액 판단부(178)를 구비할 수 있다.

[35] 가입 검사부(172)는 클라이언트 단말기(110)로부터 이동통신 단말기(180)를 인증수단으로 선택하는 대금결제 요청신호가 수신되면, 선택된 이동통신 단말기(180)의 모바일 카드 가입여부를 검사한다. 여기서, 모바일 카드 가입이란 본 발명의 실시예에 따른 이동통신 단말기를 인증수단으로 선택할 수 있도록 하는 서비스를 말한다.

[36] 콜백 메시지 전송부(174)는 이동통신 단말기(180)가 모바일 카드에 가입된 경우, 이동통신 단말기(180)를 결제인증 왑 페이지로 연결하기 위한

콜백(call-back) URL(Uniform Resource Location)이 포함된 문자메시지를 이동통신 단말기(180)로 전송한다. 이때, 콜백 메시지 전송부(174)가 이동통신 단말기(180)로 전송하는 문자메시지에는 쇼핑몰 정보, 결제 대상인 상품의 종류, 상품 대금의 금액 등에 대한 정보가 포함될 수 있다. 또한, 결제 인증을 위한 왑 페이지는 사용자 정보에 포함되어 있는 신용카드 정보에 따라 예컨대, 카드사에 따라 다르게 설정될 수 있다. 여기서, 모바일카드 가입 여부는, 해당 이동통신 단말기(180)가 정상적인 USIM 카드 또는 SIM 카드를 탑재하고 있는지의 여부, USIM 카드 또는 SIM 카드에 계좌정보 또는 신용카드 정보를 저장하고 있는지의 여부, USIM 카드 또는 SIM 카드에 저장된 계좌정보 또는 신용카드 정보에 대응하는 은행 또는 카드사에 모바일 결제 서비스가 가입되었는지의 여부 중 적어도 하나로 수행될 수 있다.

[37] 인증 처리부(176)는 결제인증을 위한 왑 페이지와 연동하여 이동통신 단말기(180)에 대한 인증을 처리한다. 즉, 콜백 메시지 전송부(174)에 의해 전송된 문자메시지를 통하여 이동통신 단말기(180)가 결제인증을 위한 왑 페이지에 접속하면, 인증 처리부(174)는 해당 왑 페이지와 연동하여 이동통신 단말기(180)로부터 입력되는 결제계좌정보 또는 신용카드정보, 결제계좌 비밀번호 또는 신용카드 비밀번호 등에 대한 인증을 처리한다.

[38] 결제금액 판단부(178)는 클라이언트 단말기(110)로부터 수신된 대금결제 요청신호에 대응하는 결제대금이 기 설정된 금액 이하인지를 판단한다. 이때, 인증 처리부(176)는 결제금액 판단부(178)에 의한 판단 결과에 따라 인증처리를 다르게 실행할 수 있다. 예를 들어, 기준금액으로 30만원을 설정하여 두고, 결제금액 판단부(178)는 클라이언트 단말기(110)로부터 수신된 대금결제 요청신호에 대응하는 결제대금이 기준금액 이하인지를 판단하며, 인증 처리부(164)는 클라이언트 단말기(110)로부터 수신된 대금결제 요청신호에 대응하는 결제대금이 30만원 이하인 경우에는 이동통신 단말기(180)를 왑 페이지에 연결시키고 그 왑 페이지에 연동하여 인증 처리를 수행할 수 있다. 또한, 클라이언트 단말기(110)로부터 수신된 대금결제 요청신호에 대응하는 결제대금이 30만원을 초과하는 경우에는, 이동통신 단말기(180)에 기 저장된 모바일 인증서를 수신하고, 그 모바일 인증서를 인증기관에 제출하여 확인함으로써, 모바일 인증서에 기초한 인증처리를 수행할 수 있다. 여기서, 모바일 인증서는 한국정보인증, 금융결제원 및 한국전산증권과 같은 공인된 인증기관에 의해 발행되며, 개인정보를 디지털 암호화 및 서명에 사용할 수 있도록 한 쌍의 전자 키로 이루어져 있는 인증서로서, 이동통신 단말기(180)의 USIM(Universal Subscriber Identity Module) 카드 또는 SIM(Subscriber Identity Module) 카드에 저장된 인증서를 말한다.

[39] 이동통신 단말기(180)는 USIM 카드 또는 SIM를 탑재한다. USIM 카드는 3세대 이동통신, 예를 들어 WCDMA(Wideband Code Division Multiple Access)을 위한 단말기에 탑재되는 카드로서, 가입자 정보를 탑재한 SIM(Subscriber Identity

Module: 가입자 식별 모듈) 카드와 UICC(Universal IC Card)가 결합된 형태이며, 사용자 인증과 글로벌 로밍, 전자상거래 등 다양한 기능을 한 장의 카드로 구현한 것이다.

[40] USIM은 범용 가입자 식별 모듈이라고도 하는데, SIM이 이동통신 단말기의 가입자에게 인증과 요금 부과, 보안 기능 등의 다양한 서비스를 제공할 수 있도록 개인 정보를 저장한 카드 형태의 모듈인데 반하여, USIM은 SIM보다 한 단계 진화한 방식으로 가입자 인증을 하는 SIM의 역할과 교통카드나 신용카드 등의 다양한 기능이 내재된 범용 IC카드(UICC)의 기능을 겸용한다. 이때, 범용 IC카드는 다양한 다중 애플리케이션의 보안 지원을 통해 모든 개인 정보 데이터의 무결성과 보안을 보장한다.

[41] USIM은 소형 CPU(Central Processing Unit)와 메모리로 구성되는데, CPU는 암호와 및 복호화 기능으로 사용자를 식별하고, 메모리는 부가서비스를 위한 저장공간으로 이용된다. 메모리에는 사용자의 계좌정보, 신용카드나 교통카드, 또는 멤버십카드 등에 대한 정보를 저장할 수 있다. 특히, 사용자가 은행 창구 등에서 결제 직불계좌, 신용카드 등에 대한 가입 신청을 하면 은행 또는 신용카드 회사에서 카드 발급을 승인한 후 OTA(Over The Air) 기술을 이용하여 사용자의 USIM 카드 또는 SIM 카드에 계좌정보 또는 신용카드정보를 저장할 수 있게 됨으로써, 우편 등에 의한 오프라인 발급 절차를 생략하여 카드 발급절차를 단축할 수 있게 된다.

[42] 왑 서버(190)는 결제 인증을 위해 기 설정된 왑 페이지에 이동통신 단말기(180)가 접속하면, 이동통신 단말기(180)의 USIM 카드 또는 SIM 카드에 기초하여 정당 소유자에 대한 여부를 검증함으로써, 사용자 인증을 수행한다. 이를 위해, 왑 서버(190)는 도 3에 도시한 바와 같이 왑 페이지 제공부(192), 인증정보 획득부(194) 및 사용자인증 수행부(196)를 구비할 수 있다.

[43] 왑 페이지 제공부(192)는 이동통신 단말기(180)에 왑 페이지를 제공한다. 이때, 왑 페이지 제공부(192)는 접근제어 서버(170)의 콜백 메시지 전송부(174)와 연동하여 왑 페이지의 URL이 콜백 메시지로 포함되어 전송되도록 할 수 있다.

[44] 인증정보 획득부(194)는 제공된 왑 페이지를 통해 접속한 이동통신 단말기(180)가 결제를 요청하는 경우, 이동통신 단말기(180)에 탑재된 USIM 카드 또는 SIM 카드에 기초하여 결제 인증을 위한 인증정보를 획득한다. 이때, 인증정보 획득부(194)는 웹 페이지를 통해 이동통신 단말기(180)의 사용자로부터 PIN(Personal Identification Number) 정보 등을 입력받으며, 이동통신 단말기(180)의 USIM 카드 또는 SIM 카드로부터 계좌정보 또는 신용카드정보 등을 획득하도록 구현될 수 있다.

[45] 사용자 인증 수행부(196)는 인증정보 획득부(194)에 의해 획득된 인증정보에 기초하여 사용자 인증을 수행한다. 이때, 사용자 인증 수행부(196)는 웹 페이지를 통해 이동통신 단말기(180)의 사용자로부터 PIN 정보, 계좌정보 또는 신용카드정보에 대한 패스워드 등을 수신하며, 수신된 정보를 이동통신

단말기(180)의 USIM 카드 또는 SIM 카드로부터 수신한 정보와 비교함으로써 사용자 인증을 수행할 수 있다. 또는, 사용자 인증 수행부(196)는 웹 페이지를 통해 이동통신 단말기(180)로부터 수신한 PIN 정보, 패스워드 등과 함께 USIM 카드 또는 SIM 카드로부터 수신한 계좌정보 또는 신용카드정보를 접근제어 서버(170)에 제출하고 정당사용자 여부를 확인함으로써 사용자에 대한 인증을 수행할 수도 있다.

[46] 도 4 및 도 5는 도 1의 이동통신 단말기를 이용한 인증서비스 시스템의 일 실시예에 의한 인증서비스 방법을 나타낸 흐름도이다. 도면을 참조하여 본 발명의 일 실시예에 따른 이동통신 단말기를 이용한 인증서비스 시스템의 기능 및 동작을 상세하게 설명한다.

[47] 도면을 참조하면, 클라이언트 단말기(110)는 유무선 망(120)을 통하여 쇼핑몰 서버(135)에 접속하여 상품 구매에 따른 대금결제를 요청하고 이동통신 단말기(180)를 인증수단으로 선택할 수 있다. 또는, 상품 구매에 따른 대금이 소정 금액 이상인 경우, 클라이언트 단말기(110)는 이동통신 단말기(180)를 인증 및 결제 수단으로 선택할 수 있다. 이때, 클라이언트 단말기(110)는 사용자로부터 구매하고자 하는 상품의 종류와 사용자 정보를 입력 받아 암호화하여 쇼핑몰 서버(135)로 전달한다(단계 1). 사용자 정보에는 상품 대금을 결제하고자 하는 신용카드 정보가 포함될 수 있다.

[48] 쇼핑몰 서버(135)는 클라이언트 단말기(110)로부터의 결제 요청신호에 대응하여, 접근제어 서버(170)에 본 발명에 따른 인증서비스에 상응하는 서비스의 가입을 요청하며, 그에 대응하는 응답신호를 수신할 수 있다(단계 2, 단계 3). 도면에는 이를 안심클릭으로 명명하였다. 이로써, 쇼핑몰 서버(135)는 클라이언트 단말기(110)와 접근제어 서버(170) 사이에서 원활하게 정보 전달을 수행할 수 있게 되며, 클라이언트 단말기(110)에 이동통신 단말기(180)를 인증수단, 또는 인증 및 결제 수단으로 선택할 수 있도록 하는 인증창을 구동시킬 수 있게 된다(단계 4).

[49] 클라이언트 단말기(110)는 단계 4에 의해 구동된 인증창을 통하여 이동통신 단말기(180)를 인증수단, 또는 인증 및 결제으로 선택할 수 있다. 이동통신 단말기(180)를 인증수단으로 하는 인증요청 신호는 접근제어 서버(170)로 전송된다(단계 5). 여기서, 쇼핑몰 서버(135)에 의해 수행되는 절차는 전술한 바와 동일하므로, 이하에서는 그 설명을 생략한다.

[50] 접근제어 서버(170)는 디렉토리 서버(160)로부터 수신한 사용자 정보 및 이동통신 단말기(180)의 USIM 카드 또는 SIM 카드에 기초하여 해당 이동통신 단말기(180)의 모바일카드 가입여부를 검사한다(단계 6). 이때, 접근제어 서버(170)는 사용자 정보 및 이동통신 단말기(180)의 USIM 카드 또는 SIM 카드에 기초하여 해당하는 카드사 서버(도시하지 않음)에 인증서비스 가입여부를 문의할 수도 있다. 또한, 접근제어 서버(170)는 USIM 카드 또는 SIM 카드에 기초하여 이동통신 단말기(180)의 고유정보를 인식하고, 사용자로부터

PIN(Personal Identification Number) 정보를 수신함으로써, 이동통신 단말기(180)에 대한 정당 사용자의 여부를 확인할 수도 있다.

[51] 이동통신 단말기(180)가 인증서비스에 가입된 경우, 접근제어 서버(170)는 결제 인증을 위해 기 설정된 왑 페이지와 이동통신 단말기(180)를 연동하기 위한 콜백 URL이 포함된 문자메시지를 이동통신 단말기(180)로 전송한다(단계 7). 이때, 접근제어 서버(170)가 이동통신 단말기(180)로 전송하는 문자메시지에는 쇼핑몰 정보, 결제 대상인 상품의 종류, 상품 대금의 금액 등에 대한 정보가 포함될 수 있다. 또한, 결제 인증을 위한 왑 페이지는 사용자 정보에 포함되어 있는 신용카드 정보에 따라 즉, 카드사에 따라 다르게 설정될 수 있다.

[52] 왑 서버(190)에 의해 제공된 왑 페이지에 이동통신 단말기(180)가 접속하면(단계 8), 왑 서버(190)는 이동통신 단말기(180)의 USIM 카드 또는 SIM 카드에 기초하여, 접근제어 서버(170)에 이동통신 단말기(180)의 정당 소유자인지를 문의하고 그에 대한 응답신호를 수신함으로써, 사용자 인증을 수행한다(단계 9, 단계 10).

[53] 또한, 왑 서버(190)는 이동통신 단말기(180)에 대하여, USIM 카드 또는 SIM 카드 정보를 요청하며, 그 정보를 이동통신 단말기(180)의 화면에 표시시키는 것이 바람직하다(단계 11). 이와 같은 화면에 표시되는 정보는 사용자가 결제 수단으로 이용하고자 하는 계좌정보 또는 신용카드 정보가 포함되는 것이 바람직하다. 이때, 이동통신 단말기(180)가 사용자에 대한 계좌정보 또는 신용카드 정보를 저장하고 있지 않은 경우, 이동통신 단말기(180)는 클라이언트 단말기(110)에 사용자에 대한 계좌정보 또는 신용카드 정보를 문의하고 그에 대한 응답신호를 수신할 수 있다(단계 12, 단계 13).

[54] 왑 서버(190)에 의해 이동통신 단말기(180)의 화면에 표시된 정보에 기초하여 이동통신 단말기(180)의 사용자가 계좌번호 또는 신용카드 정보에 대한 패스워드를 입력하면(단계 14), 왑 서버(190)는 이동통신 단말기(180)로부터 수신된 패스워드에 기초하여 접근제어 서버(170)에 본인인증을 확인하며, 그 결과를 다시 이동통신 단말기(180)로 전송한다(단계 15, 단계 16). 이때, 접근제어 서버(170)는 본인 인증의 결과를 쇼핑몰 서버(135)에 전송하는 것이 바람직하다(단계 17). 이로써, 쇼핑몰 서버(135)는 VAN(Value Added Network)(200)을 통해 결제에 대한 승인 요청을 하고, 그 응답신호를 받을 수 있게 된다(단계 18, 단계 19). 여기서, VAN(200)은 부가가치 망으로서, 쇼핑몰 서버(135)와 결제 서버(도시하지 않음)를 연결하며, 상품 대금에 대한 정산 요청 및 그 결과를 전달함으로써, 사용자의 신용카드 정보에 의해 지급된 과금이 쇼핑몰 서버(135)에 정상적으로 정산될 수 있도록 한다. 이와 같은 과정이 완료되면, 접근제어 서버(170)는 그에 대한 결과를 이동통신 단말기(180)에 문자메시지로 전송함으로써, 최종적인 승인 결과를 통지하는 것이 바람직하다(단계 20).

[55] 도 6은 본 발명의 다른 실시예에 따른 이동통신 단말기를 이용한 인증서비스

시스템을 개략적으로 도시한 도면이다. 여기서, 이동통신 단말기(480)는 유무선 망(120)을 통하여 쇼핑몰 서버(135)에 접속하여 상품을 구매할 수 있으며, 그에 대한 인증 수단으로 자신을 선택할 수 있다. 즉, 이 경우의 이동통신 단말기(480)는 도 1의 클라이언트 단말기(110)의 기능과 이동통신 단말기(180)의 기능을 동시에 수행할 수 있다. 이때, 이동통신 단말기(480) 이외의 각각의 다른 구성요소는, 도 1의 각각의 다른 구성요소와 그 기능 및 동작이 동일하므로, 이에 대한 상세한 설명은 생략한다.

[56] 도 7 및 도 8은 도 4의 이동통신 단말기를 이용한 인증서비스 시스템에 의한 인증서비스 방법의 일 실시예를 나타낸 흐름도이다.

[57] 도면을 참조하면, 이동통신 단말기(180)는 유무선 망(120)을 통하여 쇼핑몰 서버(135)에 접속하여 상품 구매에 따른 대금결제를 요청하고 자신을 인증수단으로 선택할 수 있다. 이때, 이동통신 단말기(180)는 사용자로부터 구매하고자 하는 상품의 종류와 사용자 정보를 입력 받아 암호화하여 쇼핑몰 서버(135)로 전달한다(단계 1). 사용자 정보에는 상품 대금을 결제하고자 하는 신용카드 정보가 포함될 수 있다.

[58] 이때, 쇼핑몰 서버(135)는 클라이언트 단말기(110)로부터의 결제 요청신호에 대응하여, 접근제어 서버(170)에 본 발명에 따른 인증서비스에 상응하는 서비스의 가입을 요청하며, 그에 대응하는 응답신호를 수신할 수 있다(단계 2, 단계 3). 이로써, 쇼핑몰 서버(135)는 이동통신 단말기(180)와 접근제어 서버(170) 사이에서 원활하게 정보 전달을 수행할 수 있게 되며, 이동통신 단말기(180)를 인증수단으로 선택할 수 있도록 하는 인증창을 구동시킬 수 있게 된다(단계 4).

[59] 이동통신 단말기(180)는 단계 4에 의해 구동된 인증창을 통하여 이동통신 단말기(180)를 인증수단으로 선택할 수 있다. 이동통신 단말기(180)를 인증수단으로 하는 인증요청 신호는 접근제어 서버(170)로 전송된다(단계 5).

[60] 접근제어 서버(170)는 디렉토리 서버(160)로부터 수신한 사용자 정보 및 이동통신 단말기(180)의 USIM 카드 또는 SIM 카드에 기초하여 해당 이동통신 단말기(180)의 모바일카드 가입여부를 검사한다(단계 6). 이때, 접근제어 서버(170)는 사용자 정보 및 이동통신 단말기(180)의 USIM 카드 또는 SIM 카드에 기초하여 해당하는 카드사 서버(도시하지 않음)에 모바일카드 가입여부를 문의할 수도 있다. 또한, 접근제어 서버(170)는 USIM 카드 또는 SIM 카드에 기초하여 이동통신 단말기(180)의 고유정보를 인식하고, 사용자로부터 PIN 정보를 수신함으로써, 이동통신 단말기(180)에 대한 정당 사용자의 여부를 확인할 수도 있다.

[61] 이동통신 단말기(180)가 모바일카드에 가입된 경우, 접근제어 서버(170)는 결제 인증을 위해 기 설정된 왑 페이지와 이동통신 단말기(180)를 연동하기 위한 콜백 URL이 포함된 문자메시지를 이동통신 단말기(180)로 전송한다(단계 7). 여기서, 결제 인증을 위한 왑 페이지는 사용자 정보에 포함되어 있는 신용카드 정보에 따라 즉, 카드사에 따라 다르게 설정될 수 있다.

[62] 왑 서버(190)에 의해 제공된 왑 페이지에 이동통신 단말기(180)가 접속하면(단계 8), 왑 서버(190)는 이동통신 단말기(180)의 USIM 카드 또는 SIM 카드에 기초하여, 접근제어 서버(170)에 이동통신 단말기(180)의 정당 소유자인지를 문의하고 그에 대한 응답신호를 수신함으로써, 사용자 인증을 수행한다(단계 9).

[63] 또한, 왑 서버(190)는 이동통신 단말기(180)에 대하여, USIM 카드 또는 SIM 카드 정보를 요청하며, 그 정보를 이동통신 단말기(180)의 화면에 표시시키는 것이 바람직하다(단계 10). 이와 같은 화면에 표시되는 정보는 사용자가 결제 수단으로 이용하고자 하는 계좌정보 또는 신용카드 정보가 포함되는 것이 바람직하다.

[64] 왑 서버(190)에 의해 이동통신 단말기(180)의 화면에 표시된 정보에 기초하여 이동통신 단말기(180)의 사용자가 계좌번호 또는 신용카드 정보에 대한 패스워드를 입력하면(단계 11), 왑 서버(190)는 이동통신 단말기(180)로부터 수신된 패스워드에 기초하여 접근제어 서버(170)에 본인인증을 확인하며, 그 결과를 다시 이동통신 단말기(180)로 전송한다(단계 12, 단계 13). 이때, 접근제어 서버(170)는 본인 인증의 결과를 쇼핑몰 서버(135)에 전송하는 것이 바람직하다(단계 14). 이로써, 쇼핑몰 서버(135)는 VAN(Value Added Network)(200)을 통해 결제에 대한 승인 요청을 하고 그 응답신호를 받을 수 있게 된다(단계 15, 단계 16). 이와 같은 과정이 완료되면, 접근제어 서버(170)는 그에 대한 결과를 이동통신 단말기(180)에 문자메시지로 전송함으로써, 최종적인 승인 결과를 통지하는 것이 바람직하다(단계 17).

[65] 한편, 전술한 절차는 이동통신 단말기(180)를 이용하여 결제하고자 하는 결제 대금이 소정 금액 이하인 경우에만 사용하며, 결제 대금이 소정 금액을 초과하는 경우에는 모바일 인증서를 통해 결제가 수행되도록 구현될 수 있다. 즉, 이동통신 단말기(180)에 탑재된 USIM 카드 또는 SIM 카드에 모바일 인증서를 저장하고, 이동통신 단말기(180)가 상품 구매에 따른 인증 및 결제 수단으로 선택된 경우, 접근제어 서버(170)는 결제 대금이 기 설정된 금액 이하인 경우에는 전술한 인증처리를 수행하고 기 설정된 금액을 초과하는 경우에는 모바일 인증서를 인증기관에 확인하여 인증처리를 하도록 구현될 수 있다. 이로써, 결제 서버는 결제대금이 기 설정된 금액 이하인 경우에는 모바일 카드에 의한 결제처리를 수행하며, 결제대금이 기 설정된 금액을 초과하는 경우에는 모바일 인증서에 의한 결제처리를 수행하게 된다.

[66] 이상에서, 본 발명의 실시예를 구성하는 모든 구성 요소들이 하나로 결합하거나 결합하여 동작하는 것으로 설명되었다고 해서, 본 발명이 반드시 이러한 실시예에 한정되는 것은 아니다. 즉, 본 발명의 목적 범위 안에서라면, 그 모든 구성 요소들이 하나 이상으로 선택적으로 결합하여 동작할 수도 있다. 또한, 그 모든 구성 요소들이 각각 하나의 독립적인 하드웨어로 구현될 수 있지만, 각 구성 요소들의 그 일부 또는 전부가 선택적으로 조합되어 하나 또는

복수 개의 하드웨어에서 조합된 일부 또는 전부의 기능을 수행하는 프로그램 모듈을 갖는 컴퓨터 프로그램으로서 구현될 수도 있다. 그 컴퓨터 프로그램을 구성하는 코드들 및 코드 세그먼트들은 본 발명의 기술 분야의 당업자에 의해 용이하게 추론될 수 있을 것이다. 이러한 컴퓨터 프로그램은 컴퓨터가 읽을 수 있는 저장매체(Computer Readable Media)에 저장되어 컴퓨터에 의하여 읽혀지고 실행됨으로써, 본 발명의 실시예를 구현할 수 있다. 컴퓨터 프로그램의 저장매체로서는 자기 기록매체, 광 기록매체, 캐리어 웨이브 매체 등이 포함될 수 있다.

[67] 또한, 이상에서 기재된 "포함하다", "구성하다" 또는 "가지다" 등의 용어는, 특별히 반대되는 기재가 없는 한, 해당 구성 요소가 내재할 수 있음을 의미하는 것이므로, 다른 구성 요소를 제외하는 것이 아니라 다른 구성 요소를 더 포함할 수 있는 것으로 해석되어야 한다. 기술적이거나 과학적인 용어를 포함한 모든 용어들은, 다르게 정의되지 않는 한, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미가 있다. 사전에 정의된 용어와 같이 일반적으로 사용되는 용어들은 관련 기술의 문맥상의 의미와 일치하는 것으로 해석되어야 하며, 본 발명에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[68] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 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

[69] 이상에서 설명한 바와 같이 본 발명의 실시예는 이동통신 분야, 이동통신 단말기를 이용한 대금결제 시스템분야 등에 적용되어, 이용자가 온라인 상에서 전자상거래를 하는 경우, 이용자의 이동통신 단말기를 이용하여 이용자에 대한 인증을 수행함으로써, 온라인 상에서의 전자상거래를 이용할 수 있는 장소적 한계를 극복할 수 있도록 하며, 이동통신 단말기에 탑재된 USIM 카드를 인증수단으로 활용함으로써 이용자의 인증에 대한 신뢰성을 높일 수 있는 효과를 발생시키는 매우 유용한 발명이다.

[70]

[71] CROSS-REFERENCE TO RELATED APPLICATION

[72] 본 특허출원은 2009년 10월 20일 한국에 출원한 특허출원번호 제 10-2009-0099794 호에 대해 미국 특허법 119(a)조(35 U.S.C § 119(a))에 따라

우선권을 주장하면, 그 모든 내용은 참고문헌으로 본 특허출원에 병합된다.
아울러, 본 특허출원은 미국 이외에 국가에 대해서도 위와 동일한 동일한 이유로 우선권을 주장하면 그 모든 내용은 참고문헌으로 본 특허출원에 병합된다.

청구범위

[청구항 1] USIM(Universal Subscriber Identity Module) 카드 또는 SIM 카드를 탑재한 이동통신 단말기;
상품 구매에 따른 대금결제 요청 시에 상기 이동통신 단말기를 인증수단으로 선택하는 클라이언트 단말기;
선택된 상기 이동통신 단말기의 모바일카드 가입여부를 검사하며, 상기 이동통신 단말기가 상기 모바일카드에 가입된 경우에 결제인증을 위한 왑(WAP: Wireless Application Protocol)페이지와 상기 이동통신 단말기를 연결하기 위한 콜백(call-back) URL(Uniform Resource Location)이 포함된 문자메시지를 상기 이동통신 단말기에 전송하는 접근제어 서버; 및
상기 왑페이지에 상기 이동통신 단말기가 접속하면 상기 USIM 카드 또는 상기 SIM 카드에 기초하여 정당 소유자에 대한 여부를 검증하는 왑 서버
를 포함하는 것을 특징으로 하는 이동통신 단말기를 이용한 인증서비스 시스템.

[청구항 2] 클라이언트 단말기로부터 이동통신 단말기를 인증수단으로 선택하는 대금결제 요청신호가 수신되면, 선택된 상기 이동통신 단말기의 모바일카드 가입여부를 검사하는 가입 검사부;
상기 이동통신 단말기가 상기 모바일카드에 가입된 경우, 상기 이동통신 단말기를 결제인증 왑 페이지로 연결하기 위한 콜백 URL이 포함된 문자메시지를, 상기 이동통신 단말기로 전송하는 콜백 메시지 전송부; 및
상기 결제인증 왑 페이지와 연동하여 상기 이동통신 단말기에 대한 인증을 처리하는 인증처리부
를 포함하는 것을 특징으로 하는 접근제어 서버.

[청구항 3] 제 2항에 있어서,
상기 대금결제 요청신호에 대응하는 결제대금이 기 설정된 금액 이하인지를 판단하는 결제금액 판단부
를 더 포함하며,
상기 대금결제 요청신호에 대응하는 결제대금이 상기 기 설정된 금액을 초과하는 경우, 상기 인증처리부는 상기 이동통신 단말기에 저장된 모바일 인증서에 기초하여 인증처리를 수행하는 것을 특징으로 하는 접근제어 서버.

[청구항 4] 이동통신 단말기에 왑 페이지를 제공하는 왑 페이지 제공부;
제공된 상기 왑 페이지를 통해 상기 이동통신 단말기가 결제를 요청하는 경우, 상기 이동통신 단말기에 탑재된 USIM 카드 또는

SIM 카드에 기초하여 결제 인증을 위한 인증정보를 획득하는 인증정보 획득부; 및

상기 인증정보 획득부에 의해 획득된 인증정보에 기초하여 사용자 인증을 수행하는 사용자 인증 수행부

를 포함하는 것을 특징으로 하는 왑 서버.

[청구항 5] 제 4항에 있어서,

상기 인증정보 획득부는 상기 이동통신 단말기로부터 계좌정보 또는 신용카드정보, 및 그에 대응하는 패스워드를 수신하며,

상기 사용자 인증 수행부는 상기 인증정보 획득부를 통해 수신한 정보에 기초하여 사용자 인증을 수행하는 것을 특징으로 하는 왑 서버.

[청구항 6] 클라이언트 단말기를 이용하여 온라인 상에서의 상품 구매 시,

USIM 카드 또는 SIM 카드를 탑재한 이동통신 단말기를 인증수단으로 입력받는 단계;

입력된 상기 이동통신 단말기의 모바일카드 가입여부를 검사하는 단계;

상기 이동통신 단말기가 상기 모바일카드에 가입된 경우, 결제인증을 위한 왑페이지와 상기 이동통신 단말기를 연결하기 위한 콜백 URL이 포함된 문자메시지를 상기 이동통신 단말기에 전송하는 단계;

상기 왑페이지에 상기 이동통신 단말기가 접속하면 상기 USIM 카드 또는 상기 SIM 카드에 기초하여 정당 소유자에 대한 여부를 검증하는 단계; 및

검증된 상기 정당 소유자에 대하여, 상기 왑페이지를 통해 상기 이동통신 단말기로부터 수신되는 계좌정보 또는 신용카드정보에 기초하여 대금결제를 처리하는 단계

를 포함하는 것을 특징으로 하는 이동통신 단말기를 이용한 인증서비스 방법.

[청구항 7] 제 6항에 있어서,

상기 이동통신 단말기에 저장된 계좌정보 또는 신용카드 정보를 상기 왑페이지를 통해 표시하는 것을 특징으로 하는 이동통신 단말기를 이용한 인증서비스 방법.

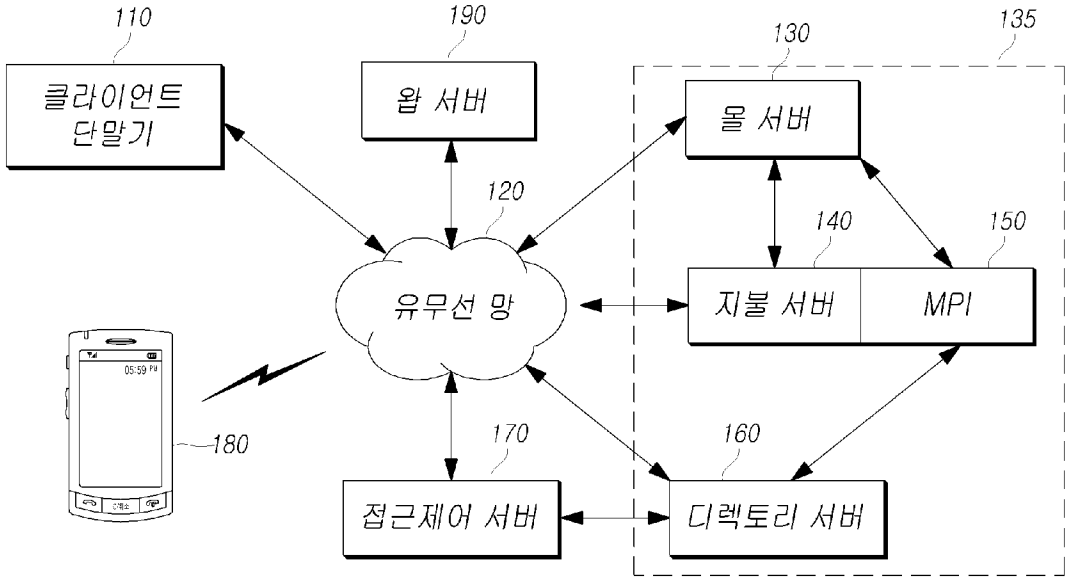
[청구항 8] 제 6항에 있어서,

상기 왑페이지를 통해 계좌정보 또는 상기 신용카드정보, 및 패스워드를 입력받으며, 상기 이동통신 단말기로부터 입력되는 정보에 기초하여 정당 사용자에 대한 인증처리를 하는 것을 특징으로 하는 이동통신 단말기를 이용한 인증서비스 방법.

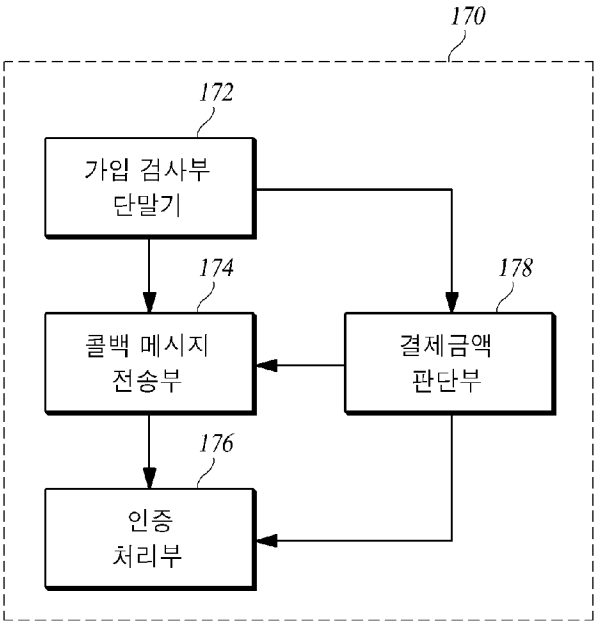
[청구항 9] USIM 카드 또는 SIM 카드를 탑재한 이동통신 단말기를 이용하여

상품 구매에 따른 대금결제 요청 시, 상기 이동통신 단말기의 모바일카드 가입여부를 검사하는 단계;
상기 이동통신 단말기가 상기 모바일카드에 가입된 경우, 결제인증을 위한 왑페이지와 상기 이동통신 단말기를 연결하기 위한 콜백 URL이 포함된 문자메시지를 상기 이동통신 단말기에 전송하는 단계;
상기 왑페이지에 상기 이동통신 단말기가 접속하면 상기 USIM 카드 또는 상기 SIM 카드에 기초하여 정당 소유자에 대한 여부를 검증하는 단계; 및
검증된 상기 정당 소유자에 대하여, 상기 왑페이지를 통해 상기 이동통신 단말기로부터 수신되는 계좌정보 또는 신용카드정보에 기초하여 대금결제를 처리하는 단계
를 포함하는 것을 특징으로 하는 이동통신 단말기를 이용한 인증서비스 방법.

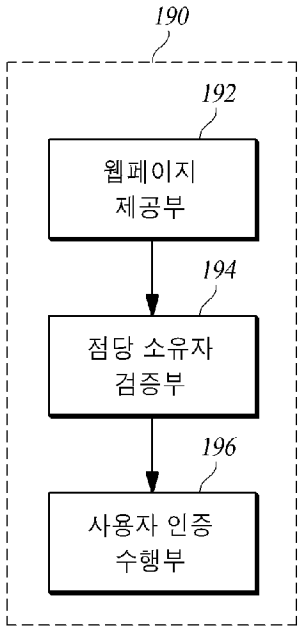
[Fig. 1]


110
클라이언트 단말기
190
왑 서버
130
135
올 서버
120
140
150
유무선 망
지불 서버
MPI
180
170
160
접근제어 서버
디렉토리 서버

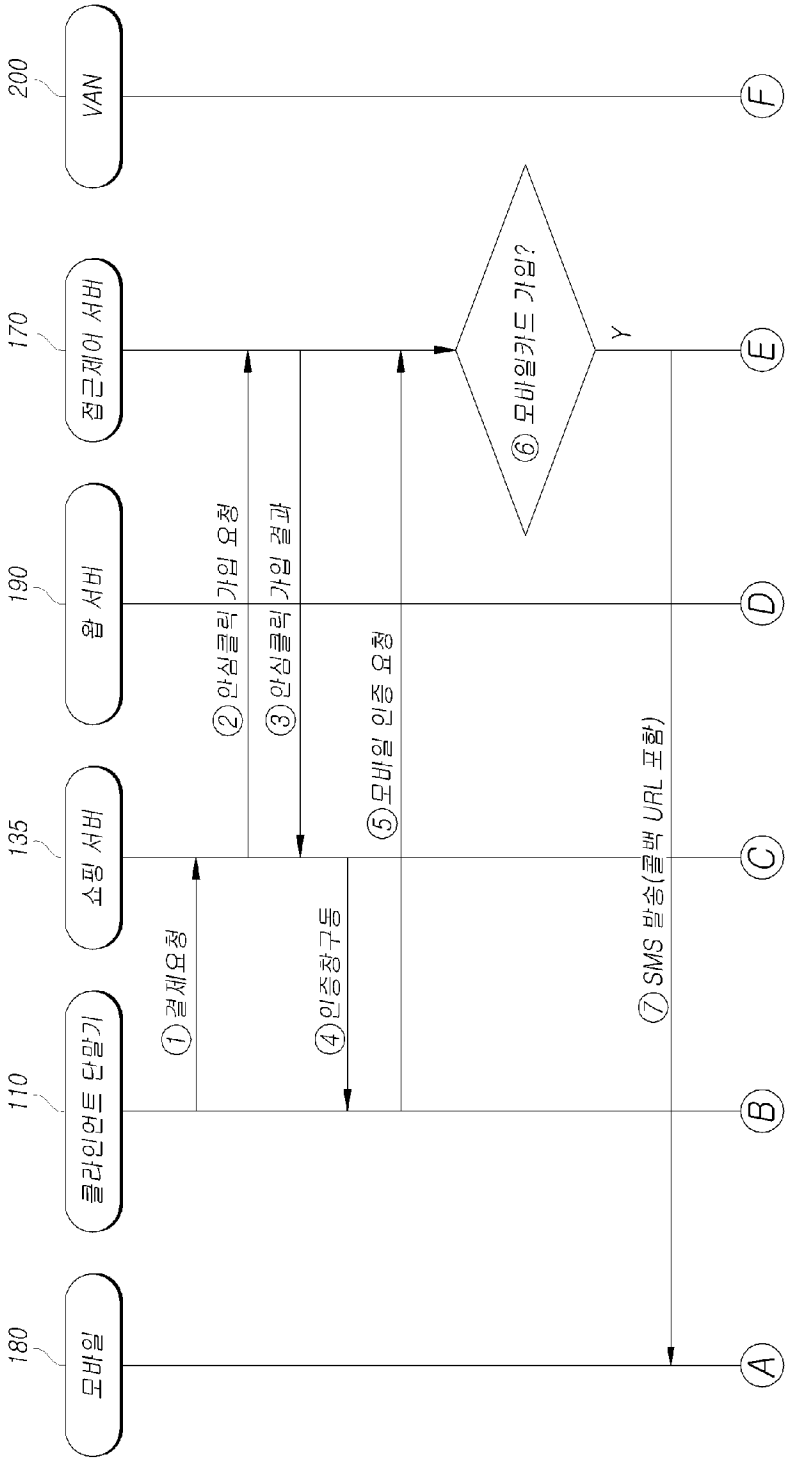
[Fig. 2]


170
172
가입 검사부 단말기
174
178
콜백 메시지 전송부
결제금액 판단부
176
인증 처리부

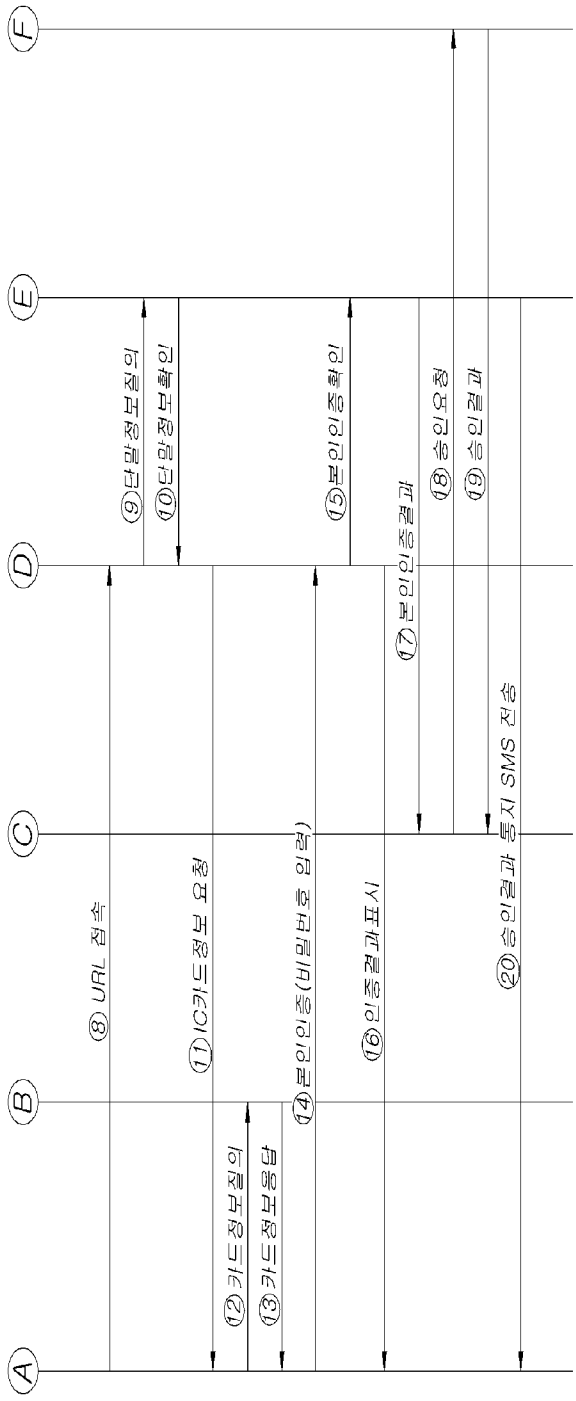
[Fig. 3]



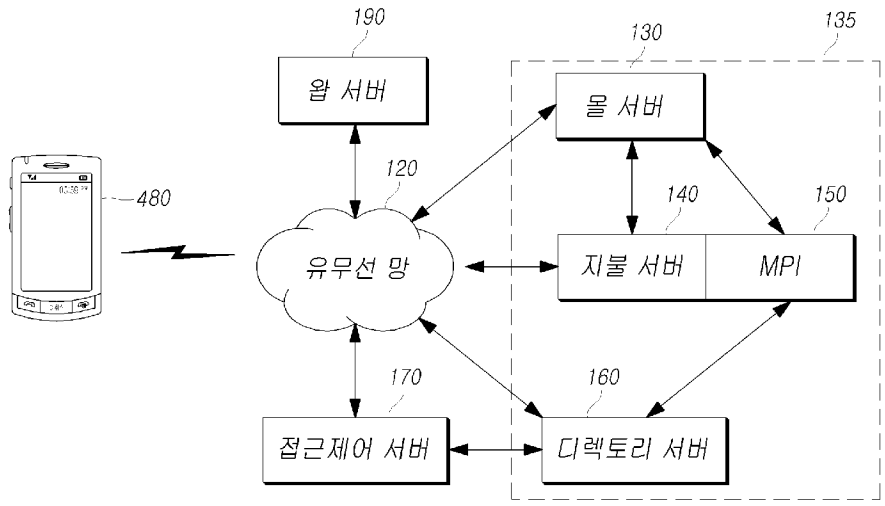
[Fig. 4]


200
VAN
170
접근제어 서버
190
왑 서버
135
쇼핑 서버
110
클라이언트 단말기
180
모바일
F
E
D
C
B
A
⑥ 모바일키드 가입?
Y
② 안심클릭 가입 요청
③ 안심클릭 가입 결과
⑤ 모바일 인증 요청
① 결제요청
④ 인증창구동
⑦ SMS 발송(콜백 URL 포함)

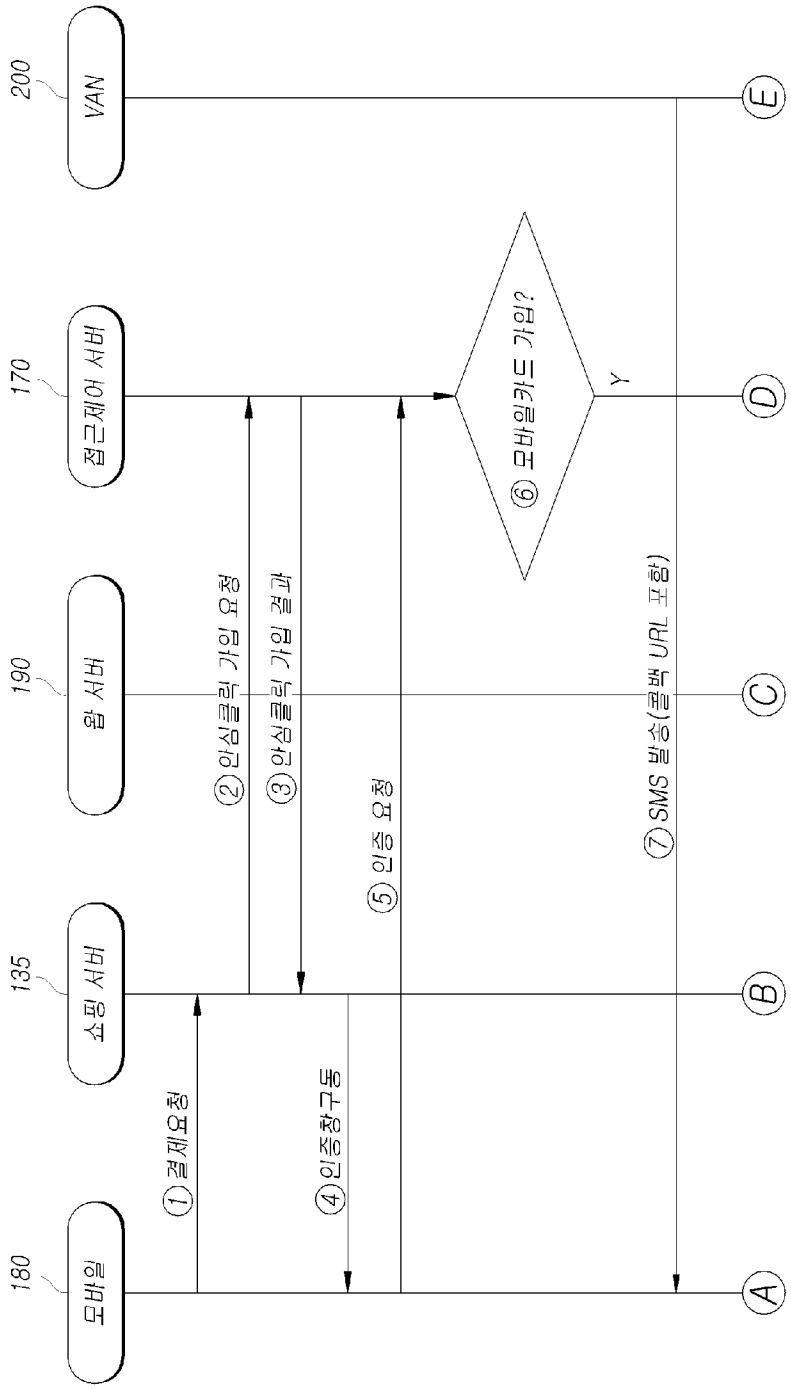
[Fig. 5]


F
E
D
C
B
A
⑧ URL 접속
⑨단말정보질의
⑩단말정보확인
⑪IC카드정보 요청
⑫ 카드정보질의
⑬카드정보응답
⑭본인인증(비밀번호 입력)
⑮본인인증확인
⑯ 인증결과표시
⑰ 본인인증결과
⑱ 승인요청
⑲ 승인결과
⑳ 승인결과 통지 SMS 전송

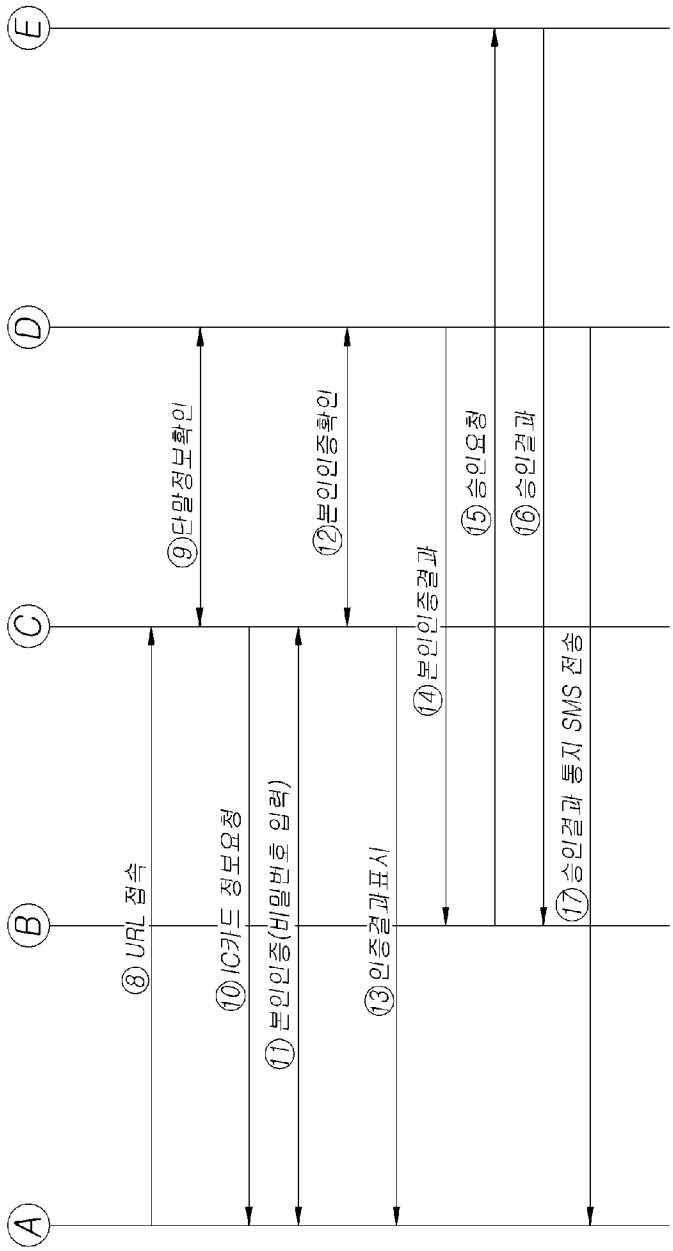
[Fig. 6]


190
130
135
왑 서버
몰 서버
480
120
140
150
유무선 망
지불 서버
MPI
170
160
접근제어 서버
디렉토리 서버

[Fig. 7]


200
VAN
170
접근제어 서버
190
왑 서버
135
쇼핑 서버
180
모바일
① 결제요청
② 안심클릭 가입 요청
③ 안심클릭 가입 결과
④ 인증창 구동
⑤ 인증 요청
⑥ 모바일카드 가입?
Y
⑦ SMS 발송(콜백 URL 포함)
A
B
C
D
E

[Fig. 8]


E
D
C
B
A
⑨단말정보확인
⑫본인인증확인
⑮승인요청
⑯승인결과
⑭본인인증결과
⑧URL 접속
⑩IC카드 정보요청
⑪본인인증(비밀번호 입력)
⑬인증결과표시
⑰승인결과 통지 SMS 전송