(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2016 년 10 월 6 일 (06.10.2016)

WIPO | PCT

(10) 국제공개번호
WO 2016/159462 A1

(51) 국제특허분류:
H04L 9/32 (2006.01) *G06Q 20/14* (2012.01)

(21) 국제출원번호: PCT/KR2015/009769

(22) 국제출원일: 2015 년 9 월 17 일 (17.09.2015)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2015-0047577 2015 년 4 월 3 일 (03.04.2015) KR
10-2015-0056211 2015 년 4 월 21 일 (21.04.2015) KR

(71) 출원인: **비씨카드(주) (BC CARD CO., LTD.)** [KR/KR]; 06654 서울시 서초구 효령로 275, Seoul (KR).

(72) 발명자: **이지호 (YI, Ji Ho)**; 06651 서울시 서초구 반포대로 14 길 71 1901 호, Seoul (KR).

(74) 대리인: **특허법인 하나 (HANA IP LAW FIRM)**; 06235 서울시 강남구 테헤란로 20 길 10 6 층, 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, BN, 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, IR, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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.

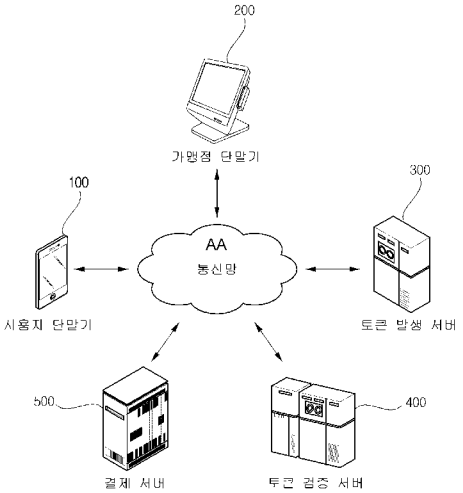
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS,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

공개:

— 국제조사보고서와 함께 (조약 제 21 조(3))

(54) **Title**: TOKEN AUTHENTICATION METHOD AND SYSTEM USING VERIFICATION VALUE GENERATED ON BASIS OF CURRENT TIME

(54) **발명의 명칭** : 현재 시간을 기초로 생성된 검증 값을 이용한 토큰 인증 방법 및 토큰 인증 시스템



100 ... User terminal
200 ... Affiliated store terminal
300 ... Token generation server
400 ... Token verification server
500 ... Payment server
AA ... Communication network

(57) **Abstract**: According to an embodiment of the present invention, there is provided a method for authenticating a token by a token authentication system, using a verification value generated on the basis of a current time. The method comprises the steps of: generating a verification value using a unique key generated on the basis of the current time, generating a virtual card number including the generated verification value and a token, and issuing the virtual card number to a user's terminal, by a token generating server; receiving an authentication request including identification information corresponding to the virtual card number through a merchant terminal recognized by the user's terminal, by a token verification server; performing authentication of the token included in the virtual card number by the token verification server by regenerating a verification value using the unique key generated on the basis of a time at which the virtual card number is generated and comparing the regenerated verification value and the verification value included in the virtual card number corresponding to the identification information; and when the authentication of the token is completed, transmitting a payment request including the token to a payment server to allow a payment to be carried out by a payment mean matched to the token, by the token verification server.

(57) 요약서:

[다음 쪽 계속]

WO 2016/159462 A1

본 발명의 일 실시예에 따르면, 토큰 인증 시스템에서 토큰을 인증하는 방법에 있어서, 토큰 발생 서버에서, 현재 시간을 기점으로 생성된 유일한 키를 이용하여 검증 값을 생성하고, 상기 생성된 검증 값과 토큰을 포함하는 가상 카드번호를 생성하여 사용자 단말기로 발급하는 단계; 토큰 검증 서버에서, 상기 가상 카드번호와 상응하는 식별 정보를 포함하는 인증 요청을, 상기 사용자 단말기로부터 인식한 가맹점 단말기를 통해 수신하는 단계; 상기 토큰 검증 서버에서, 상기 가상 카드번호의 생성 시간을 기점으로 생성된 유일한 키를 이용하여 검증 값을 재생성하고, 상기 재생성된 검증 값과 상기 식별 정보와 상응하는 가상 카드번호에 포함된 검증 값을 비교하여, 상기 가상 카드번호에 포함된 토큰에 대한 인증을 수행하는 단계; 및 상기 토큰에 대한 인증이 완료되면, 상기 토큰 검증 서버에서, 상기 토큰을 포함하는 결제 요청을 결제 서버로 전송하여, 상기 토큰과 매칭된 결제 수단으로 결제가 수행되도록 하는 단계를 포함하는, 현재 시간을 기초로 생성된 검증 값을 이용한 토큰 인증 방법이 제공된다.

명세서

발명의 명칭: 현재 시간을 기초로 생성된 검증 값을 이용한 토큰 인증 방법 및 토큰 인증 시스템

기술분야

[1] 본 발명은 현재 시간을 기초로 생성된 검증 값을 이용한 토큰 인증 방법 및 토큰 인증 시스템에 관한 것으로, 더욱 상세하게는 현재 시간을 기초로 검증 값을 생성하고, 생성된 검증 값을 이용하여 토큰을 인증하며, 토큰 인증이 완료되면 결제를 수행하고자 하는 토큰 인증 방법 및 토큰 인증 시스템에 관한 것이다.

배경기술

[2] 모바일 기기를 통한 거래에 있어서, 보안 영역에 발급되는 모바일 카드 외에 거래 복제에 대한 보안성에 취약점을 가지고 있으므로, 텍스트, 바코드, QR코드, NFC 등 다양한 형태로 결제 수단을 상용화하기 위해, 일회성 가상 카드번호인 토큰에 대한 이용이 증대되고 있다.

[3] 토큰을 이용하기 위해, 토큰 발생 서버는 새로운 토큰을 계속 생성하여 사용자 단말기로 발급하고, 해당 토큰의 유효성을 검증하기 위해 발급된 토큰을 지정된 시간 동안 데이터베이스에 저장하며, 토큰 검증 서버는 거래 승인 시점에 가맹점 단말기로부터 수신된 토큰과 데이터베이스에 일시 저장된 토큰을 비교하여, 거래의 유효성을 확인하므로, 단순한 방식으로 적절한 보안성을 제공할 수 있다.

[4] 하지만, 상술한 토큰 이용 방식은 토큰 발생 서버와 토큰 검증 서버가 동일 서버 내에 존재, 즉, 단일 시스템 구성이 필수적으로 요구되므로, 시스템 장애 등의 돌발상황에서 일관성 있는 서비스가 불가능한 문제가 있다.

[5] 또한, 토큰 이용을 위해 항상 온라인으로 토큰 발급 및 검증을 요청받고, 해당 절차를 수행해야 하는 문제도 있다.

[6] 따라서, 토큰의 발급과 인증을 위한 시스템이 물리적 또는 논리적으로 분리될 수 있는 다양한 시스템에 대한 요구가 증대되고 있으며, 상술한 문제점을 해결하기 위한 방안이 시급한 실정이다.

발명의 상세한 설명

기술적 과제

[7] 본 발명은 현재 시간을 기초로 검증 값을 생성하고, 생성된 검증 값을 이용하여 토큰을 인증하며, 토큰 인증이 완료되면 결제를 수행하고자 하는 토큰 인증 방법 및 토큰 인증 시스템을 제공하는 것을 목적으로 한다.

[8] 또한, 본 발명은 토큰이 포함된 가상 카드번호를 발급하는 장치와 토큰을 인증하는 장치가 물리적 또는 논리적으로 분리되어 있는 토큰 인증 방법 및 토큰 인증 시스템을 제공하는 것을 목적으로 한다.

[9] 또한, 본 발명은 모바일 기기를 통한 거래에서, 거래 복제에 의한 리스크를 해소하고, 거래 처리의 시스템을 간략화하며, 다양한 매체 및 환경에서 토큰을

안정하게 사용하기 위한 토큰 인증 방법 및 토큰 인증 시스템을 제공하는 것을 목적으로 한다.

[10] 본 발명의 목적들은 이상에서 언급한 목적들로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 명확하게 이해될 수 있을 것이다.

과제 해결 수단

[11] 상술한 목적을 달성하기 위한 본 발명의 일 실시예에 따르면, 토큰 인증 시스템에서 토큰을 인증하는 방법에 있어서, 토큰 발생 서버에서, 현재 시간을 기점으로 생성된 유일한 키를 이용하여 검증 값을 생성하고, 상기 생성된 검증 값과 토큰을 포함하는 가상 카드번호를 생성하여 사용자 단말기로 발급하는 단계; 토큰 검증 서버에서, 상기 가상 카드번호와 상응하는 식별 정보를 포함하는 인증 요청을, 상기 사용자 단말기로부터 인식한 가맹점 단말기를 통해 수신하는 단계; 상기 토큰 검증 서버에서, 상기 가상 카드번호의 생성 시간을 기점으로 생성된 유일한 키를 이용하여 검증 값을 재생성하고, 상기 재생성된 검증 값과 상기 식별 정보와 상응하는 가상 카드번호에 포함된 검증 값을 비교하여, 상기 가상 카드번호에 포함된 토큰에 대한 인증을 수행하는 단계; 및 상기 토큰에 대한 인증이 완료되면, 상기 토큰 검증 서버에서, 상기 토큰을 포함하는 결제 요청을 결제 서버로 전송하여, 상기 토큰과 매칭된 결제 수단으로 결제가 수행되도록 하는 단계를 포함하는, 현재 시간을 기초로 생성된 검증 값을 이용한 토큰 인증 방법이 제공된다.

[12] 상기 가상 카드번호 발급 단계는, 상기 토큰 발생 서버에서, 현재 시간을 기초로 줄리안 분 숫자를 이용하여, 상기 유일한 키를 생성하는 단계를 포함할 수 있다.

[13] 상술한 목적을 달성하기 위한 본 발명의 다른 실시예에 따르면, 토큰 인증 시스템에서 토큰을 인증하는 방법에 있어서, 사용자 단말기에서, 토큰 발생 서버로부터 키 생성 정보를 수신한 후, 상기 키 생성 정보를 통해 현재 시간을 기점으로 생성된 유일한 키를 이용하여 검증 값을 생성하고, 상기 생성된 검증 값과 토큰을 포함하는 가상 카드번호를 생성하여 상기 사용자 단말기와 연결된 토큰 저장소에 발급하는 단계; 토큰 검증 서버에서, 상기 가상 카드번호와 상응하는 식별 정보를 포함하는 인증 요청을, 상기 사용자 단말기로부터 인식한 가맹점 단말기를 통해 수신하는 단계; 상기 토큰 검증 서버에서, 상기 가상 카드번호의 생성 시간을 기점으로 생성된 유일한 키를 이용하여 검증 값을 재생성하고, 상기 재생성된 검증 값과 상기 식별 정보와 상응하는 가상 카드번호에 포함된 검증 값을 비교하여, 상기 가상 카드번호에 포함된 토큰에 대한 인증을 수행하는 단계; 및 상기 토큰에 대한 인증이 완료되면, 상기 토큰 검증 서버에서, 상기 토큰을 포함하는 결제 요청을 결제 서버로 전송하여, 상기 토큰과 매칭된 결제 수단으로 결제가 수행되도록 하는 단계를 포함하는, 현재 시간을 기초로 생성된 검증 값을 이용한 토큰 인증 방법이 제공된다.

[14] 상기 가상 카드번호 발급 단계는, 상기 사용자 단말기에서, 현재 시간을 기초로

줄리안 분 숫자를 이용하여, 상기 유일한 키를 생성하는 단계를 포함할 수 있다.

[15] 상술한 목적을 달성하기 위한 본 발명의 또 다른 실시예에 따르면, 현재 시간을 기점으로 생성된 유일한 키를 이용하여 검증 값을 생성하고, 상기 생성된 검증 값과 토큰을 포함하는 가상 카드번호를 생성하여 사용자 단말기로 발급하는 토큰 발생 서버; 상기 가상 카드번호와 상응하는 식별 정보를 상기 사용자 단말기로부터 인식하는 가맹점 단말기; 상기 인식된 식별 정보를 포함하는 인증 요청을 상기 가맹점 단말기를 통해 수신하며, 상기 가상 카드번호의 생성 시간을 기점으로 생성된 유일한 키를 이용하여 검증 값을 재생성하고, 상기 재생성된 검증 값과 상기 식별 정보와 상응하는 가상 카드번호에 포함된 검증 값을 비교하여, 상기 가상 카드번호에 포함된 토큰에 대한 인증을 수행하는 토큰 검증 서버; 및 상기 토큰에 대한 인증이 완료되면, 상기 토큰을 포함하는 결제 요청을 상기 토큰 검증 서버로부터 수신하여, 상기 토큰과 매칭된 결제 수단으로 결제를 수행하는 결제 서버를 포함하는, 토큰 인증 시스템이 제공된다.

[16] 상기 토큰 발생 서버는, 현재 시간을 기초로 줄리안 분 숫자를 이용하여, 상기 유일한 키를 생성할 수 있다.

[17] 상술한 목적을 달성하기 위한 본 발명의 또 다른 실시예에 따르면, 토큰 발생 서버로부터 키 생성 정보를 수신한 후, 상기 키 생성 정보를 통해 현재 시간을 기점으로 생성된 유일한 키를 이용하여 검증 값을 생성하고, 상기 생성된 검증 값과 토큰을 포함하는 가상 카드번호를 생성하여 토큰 저장소에 발급하는 사용자 단말기; 상기 가상 카드번호와 상응하는 식별 정보를 상기 사용자 단말기로부터 인식하는 가맹점 단말기; 상기 인식된 식별 정보를 포함하는 인증 요청을 상기 가맹점 단말기를 통해 수신하며, 상기 가상 카드번호의 생성 시간을 기점으로 생성된 유일한 키를 이용하여 검증 값을 재생성하고, 상기 재생성된 검증 값과 상기 식별 정보와 상응하는 가상 카드번호에 포함된 검증 값을 비교하여, 상기 가상 카드번호에 포함된 토큰에 대한 인증을 수행하는 토큰 검증 서버; 및 상기 토큰에 대한 인증이 완료되면, 상기 토큰을 포함하는 결제 요청을 상기 토큰 검증 서버로부터 수신하여, 상기 토큰과 매칭된 결제 수단으로 결제를 수행하는 결제 서버를 포함하는, 토큰 인증 시스템이 제공된다.

[18] 상기 사용자 단말기는, 현재 시간을 기초로 줄리안 분 숫자를 이용하여, 상기 유일한 키를 생성할 수 있다.

[19] 본 발명의 일 실시예에 따르면, 토큰이 포함된 가상 카드번호를 발급하는 장치와 토큰을 인증하는 장치가 물리적 또는 논리적으로 분리되어 있는 토큰 인증 시스템을 제공할 수 있으므로, 시스템 장애 등의 돌발상황에서도 일관성 있는 서비스를 제공할 수 있다.

[20] 또한, 본 발명의 일 실시예에 따르면, 오프라인 상에서도 사용자 단말기 자체적으로 검증 값을 생성하여, 검증 값 및 토큰을 포함하는 가상 카드번호를 발급할 수 있으므로, 항상 온라인으로 연결되어 있지 않아도 토큰이 포함된 가상 카드번호의 발급 절차가 이루어질 수 있는 효과가 있다.

[21] 본 발명의 일 실시예에 따르면, 모바일 기기를 통한 거래에서, 거래 복제에 의한 리스크를 해소하고, 거리 처리의 시스템을 간략화하며, 다양한 매체 및 환경에서 토큰 사용의 보안성을 확보할 수 있는 효과가 있다.

[22] 본 발명의 효과는 상기한 효과로 한정되는 것은 아니며, 본 발명의 상세한 설명 또는 특허청구범위에 기재된 발명의 구성으로부터 추론 가능한 모든 효과를 포함하는 것으로 이해되어야 한다.

도면의 간단한 설명

[23] 도 1은 본 발명의 일 실시예에 따른 토큰 인증 시스템을 도시한 도면이다.

[24] 도 2는 본 발명의 일 실시예에 따른 토큰 인증을 통해 결제를 수행하는 과정을 도시한 도면이다.

[25] 도 3은 본 발명의 다른 실시예에 따른 토큰 인증을 통해 결제를 수행하는 과정을 도시한 도면이다.

발명의 실시를 위한 형태

[26] 이하에서는 첨부한 도면을 참조하여 본 발명을 설명하기로 한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 따라서 여기에서 설명하는 실시예로 한정되는 것은 아니다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[27] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 부재를 사이에 두고 "간접적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 구비할 수 있다는 것을 의미한다.

[28] 이하 첨부된 도면을 참고하여 본 발명의 실시예를 상세히 설명하기로 한다.

[29] 도 1은 본 발명의 일 실시예에 따른 토큰 인증 시스템을 도시한 도면이다.

[30] 도 1을 참조하면, 본 발명의 일 실시예에 따른 토큰 인증 시스템은 통신망을 통해 서로 통신 가능한 사용자 단말기(100), 가맹점 단말기(200), 토큰 발생 서버(300), 토큰 검증 서버(400) 및 결제 서버(500)를 포함할 수 있다.

[31] 먼저, 통신망은 유선 및 무선 등과 같은 그 통신 양태를 가리지 않고 구성될 수 있다. 근거리 통신망(LAN: Local Area Network), 도시권 통신망(MAN: Metropolitan Area Network), 광역 통신망(WAN: Wide Area Network) 등 다양한 통신망으로 구성될 수 있다. 바람직하게는, 본 발명에서 말하는 통신망은 이동 통신망일 수 있으며, 이와는 다른 공지의 월드와이드웹(WWW: World Wide Web) 등일 수도 있다.

[32] 사용자 단말기(100)는 휴대폰, 스마트폰, PDA(Personal Digital Assistant), PMP(Portable Multimedia Player), 태블릿 PC 등과 같이 네트워크를 통하여 외부

서버와 연결될 수 있는 모든 종류의 핸드헬드(Handheld) 기반의 무선 통신 장치를 포함할 수 있으며, 이 외에도 데스크탑 PC, 태블릿 PC, 랩탑 PC, 셋탑 박스를 포함하는 IPTV와 같이, 네트워크를 통하여 외부 서버와 연결될 수 있는 통신 장치도 포함할 수 있다.

[33] 사용자 단말기(100)는 SMS, 공인인증서, 결제 비밀번호 등의 미리 등록된 본인 인증 수단을 이용하여, 사용자 인증을 수행할 수 있다.

[34] 사용자 단말기(100)는 토큰 발생 서버(300)에서 발급한 가상 카드번호를 이용하여, 가상 카드번호와 상응하는 식별 정보를 생성할 수 있으며, 해당 식별 정보가 가맹점 단말기(200)에 인식되도록 할 수 있다. 여기서, 식별 정보는 음성, 텍스트, 바코드, QR코드, NFC 태그 정보 등 다양한 형태로 이루어질 수 있으며, 결제 수단의 정보를 포함하거나, 결제 수단과 대응되는 특정 정보를 포함할 수도 있다.

[35] 즉, 사용자 단말기(100)는 가상 카드번호와 상응하는 식별 정보를 이용하여, 음성, 텍스트, 바코드, QR코드, NFC 등 다양한 결제 수단으로 활용될 수 있도록 할 수 있으며, 식별 정보가 가맹점 단말기(200)에 인식되게 하여, 식별 정보와 상응하는 미리 등록된 결제 수단을 통해 결제가 요청될 수 있다.

[36] 가맹점 단말기(200)는 결제 서버(500)를 운영하는 사업자(예를 들면, 카드사)의 제휴 가맹점에 설치된 단말기로서, POS 단말기일 수 있으며, POS 단말기에는 POS 값이 미리 발급되어 있을 수 있다. 여기서, POS 값은 카드 시스템에서 제휴 서비스 처리를 위한 서비스 코드 값으로 플라스틱 카드의 일부 영역(예를 들면, TRACK2 영역)에 발급될 수 있다.

[37] 본 발명의 일 실시예에 따르면, 실제 카드에 POS 값이 발급된 영역은 카드번호, 유효기간, 서비스코드(CVC), RPU등으로 구성될 수 있고, 가상 카드번호, 토큰 유효기간, 서비스코드(CVC), 검증 값 등으로 구성될 수도 있다.

[38] 가맹점 단말기(200)는 사용자 단말기(100)로부터 가상 카드번호와 상응하는 식별 정보를 인식할 수 있다.

[39] 예를 들어, 가맹점 단말기(200)는 사용자 단말기(100)에 디스플레이 되고 있는 바코드, QR 코드 등의 식별 정보를 인식할 수 있으며, 사용자 단말기(100)가 일정 거리 내에 위치하면, 근거리 통신을 통해 NFC 태그 등의 식별 정보를 인식할 수도 있다.

[40] 가맹점 단말기(200)는 사용자 단말기(100)로부터 인식한 식별 정보를 포함하는 인증 요청을 토큰 검증 서버(400)로 전송할 수 있다. 이 때, 가맹점 단말기(200)는 식별 정보와 상응하는 미리 등록된 결제 수단을 통한 결제가 수행되기 위해, 인증 요청을 토큰 검증 서버(400)로 전송할 수 있다.

[41] 토큰 발생 서버(300)는 현재 시간을 기점으로 생성된 유일한 키를 이용하여 검증 값을 생성할 수 있다. 이 때, 토큰 발생 서버(300)는 사용자 단말기(100)에서 사용자 인증이 완료된 이후, 검증 값을 생성할 수 있다.

[42] 본 발명의 일 실시예에 따르면, 검증 값은 결제의 유효성을 검증하기 위해, 가상

카드번호의 생성 또는 인증 요청 시마다 암호화적인 연산 및 해쉬 연산을 통해서 생성되는 해쉬 값으로, 토큰 검증 서버(400)에서 토큰이 정상적으로 발행되었는지 확인하는데 활용될 수 있다.

[43] 또한, 검증 값의 길이는 미리 정해진 자리 미만으로 사용될 수 있도록 설정될 수 있는데, 이 경우, 미리 정해진 자리 이외에 위치하는 숫자는 사용되지 않을 수 있다. 예를 들어, 검증 값의 앞 5자리만 사용될 수 있도록 설정되어 있는데, 검증 값이 8자리인 경우, 앞 5자리만 사용되고, 뒤 3자리는 사용되지 않을 수 있다.

[44] 이하에서는, 토큰 발생 서버(300)가 결제 서버(500)와 연결되어 검증 값을 생성하는 과정을 설명하지만, 이에 제한되지 않으며, 토큰 발생 서버(300)가 결제 서버(500)에 포함되어, 결제 서버(500)에서 토큰 발생 서버(300)의 기능을 수행할 수도 있다.

[45] 먼저, 토큰 발생 서버(300)는 사용자에게 미리 발급된 결제 수단(예를 들면, 카드)에 대한 정보를 관리하는 결제 서버(500)로부터 마스터키를 획득할 수 있다. 이 때, 결제 서버(500)는 결제 수단을 이용하기 위해 미리 회원으로 등록된 사용자 별로 마스터키를 생성하여 관리할 수 있는데, 예를 들어, 결제 서버(500)가 카드사 서버인 경우, 카드사 서버는 카드 회원으로 등록된 사용자 별로 마스터키를 생성하여 관리할 수 있다.

[46] 본 발명의 일 실시예에 따르면, 마스터키는 사용자에게 발급된 결제 수단의 식별번호(예를 들면, 카드번호)와 매칭되는 고유키로, 검증 값 생성시 암호화 과정에서 활용될 수 있다.

[47] 토큰 발생 서버(300)는 마스터키를 이용하여 카드키를 생성할 수 있다. 여기서, 카드키는 카드 별로 검증 또는 사용자 인증을 위해 활용될 수 있다.

[48] 토큰 발생 서버(300)는 카드키를 이용하여 세션키를 생성할 수 있다. 이 때, 토큰 발생 서버(300)는 줄리안 분 숫자를 이용하여, 각 분과 추가 데이터를 이용하여 별도의 세션키를 생성할 수 있다.

[49] 본 발명의 일 실시예에 따르면, 줄리안 분 숫자는 줄리안 일자를 분으로 확대한 것으로, 줄리안 일자란 특정한 연도의 시작으로부터 경과된 일수를 의미하는데, 예를 들어, 2015년 1월 15일에 대한 줄리안 일자는 "15"일 수 있다.

[50] 즉, 줄라인 분 숫자는 특정한 연도의 시작으로부터 경과된 분의 숫자를 의미하며, 예를 들어, 2015년 1월 15일에 대한 줄리안 분 숫자는 15일, 24시간, 60분에 해당하는 각각의 숫자를 곱하여 계산되는 "21600"일 수 있다.

[51] 토큰 발생 서버(300)는 사용자 인증이 완료된 현재 시간을 기초로, 줄리안 분 숫자를 이용하여 유일한 키인 세션키를 생성할 수 있으며, 생성된 세션키를 이용하여 검증 값을 생성할 수 있다. 즉, 토큰 발생 서버(300)는 현재 시간을 기점으로 생성된 유일한 키를 이용하여 검증 값을 생성할 수 있다.

[52] 토큰 발생 서버(300)는 생성된 검증 값과 토큰을 포함하는 가상 카드번호를 생성하여, 생성된 가상 카드번호를 사용자 단말기(100)로 발급할 수 있다.

[53] 본 발명의 일 실시예에 따르면, 토큰은 결제 서비스에서 사용될 수 있도록

지정된 가상의 카드번호로, 미리 설정된 토큰 유효기간이 만료되기 전까지 사용 가능한 일회성 토큰일 수 있으며, 토큰 유효기간은 YYMM 형식으로, 지원되는 토큰의 길이에 따라 0부터 4자리까지 사용될 수 있다. 예를 들어, 가상 카드번호는 총 21자리일 수 있으며, 토큰이 16자리, 검증 값이 5자리로 가상 카드번호가 구성될 수 있지만, 이에 제한되지 않으며, 다양한 형식으로 가상 카드번호가 구성될 수도 있다.

[54] 토큰 검증 서버(400)는 가맹점 단말기(200)로부터 인증 요청을 수신할 수 있으며, 토큰 생성 시간을 기점으로 생성된 유일한 키를 이용하여 검증 값을 재생성할 수 있다.

[55] 검증 값 재생성 시, 토큰 검증 서버(400)는 토큰 발생 서버(300)에서 가상 카드번호를 생성한 시간을 기초로, 상술한 바와 같이, 줄리안 분 숫자를 이용하여 유일한 키인 세션키를 생성하는 과정을 통해 검증 값을 재생성할 수 있다.

[56] 토큰 검증 서버(400)는 재생성된 검증 값과 가상 카드번호에 포함된 검증 값, 즉, 토큰 발생 서버(300)에서 생성한 검증 값을 비교하여, 토큰에 대한 인증을 수행할 수 있다. 이 때, 토큰 발생 서버(300)에서 생성된 검증 값과 토큰 검증 서버(400)에서 생성된 검증 값은 동일하거나, 서로 대응되는 값으로, 토큰 검증 서버(400)는 검증 값들을 비교하여, 비교 결과 일치하거나 대응되는 것으로 확인되면, 토큰에 대한 인증을 완료할 수 있다.

[57] 예를 들어, 가상 카드번호에 유효기간이 3분으로 설정되어 있는데, 토큰 발생 서버(300)에서 10시 5분에 현재 시간을 기초로 제1 검증 값을 생성하여, 제1 검증 값과 토큰을 포함하는 가상 카드번호를 발급한 이후, 10시 8분에 토큰 검증 서버(400)에서 가맹점 단말기(200)로부터 인증 요청을 수신하였다고 가정한다.

[58] 먼저, 토큰 검증 서버(400)는 10시 5분부터 유효기간 3분 내에 있는 10시 7분을 기초로 제2 검증 값을 생성하여, 제1 검증 값과 제2 검증 값을 비교할 수 있으며, 이 경우 제1 검증 값은 10시 5분을 기초로 생성되었고, 제2 검증 값은 10시 7분을 기초로 생성되었으므로, 비교 결과가 일치하지 않을 수 있다.

[59] 이후, 토큰 검증 서버(400)는 10시 7분보다 1분 빠른 10시 6분을 기초로 제2 검증 값을 생성하여, 제1 검증 값과 제2 검증 값을 비교할 수 있으며, 이 경우도 비교 결과가 일치하지 않을 수 있다.

[60] 이후, 토큰 검증 서버(400)는 10시 6분보다 1분 빠른 10시 5분을 기초로 제2 검증 값을 생성하여, 제1 검증 값과 제2 검증 값을 비교할 수 있으며, 이 경우에는 제 1 검증 값과 제 2 검증 값 모두 10시 5분을 기초로 생성되었으므로, 비교 결과가 일치하여, 토큰에 대한 인증이 완료될 수 있다.

[61] 즉, 토큰 검증 서버(400)는 인증 요청이 수신된 시점부터 가상 카드번호에 설정된 유효기간까지 시간을 1분씩 빠르게 하여, 각각의 시간을 기초로 검증 값을 생성하면서, 비교해가는 과정을 통해 토큰에 대한 인증을 수행할 수 있다.

[62] 이에 따라, 토큰을 포함하는 가상 카드번호의 생성과 토큰에 대한 인증 시, 기초

데이터와 알고리즘만 알고 있으면, 검증 값 생성이 가능하기 때문에, 하나의 주체에 의해서 생성 또는 검증할 필요가 없으므로, 도 1에 도시된 바와 같이, 토큰 발생 서버(300)와 토큰 검증 서버(400)의 분리가 가능할 수 있다. 그러나, 이에 제한되지 않으며, 토큰 발생 서버(300)와 토큰 검증 서버(400)는 하나의 통합 서버로 구현될 수도 있음은 물론이다.

[63] 토큰에 대한 인증을 완료하면, 토큰 검증 서버(400)는 결제 요청을 결제 서버(500)로 전송할 수 있다. 이 때, 토큰 검증 서버(400)는 가맹점 단말기(200)로부터 수신한 인증 요청에 포함된 식별 정보를 이용하여, 식별 정보와 상응하는 가상 카드번호에 포함된 토큰을 확인할 수 있으며, 해당 토큰을 포함하는 결제 요청을 결제 서버(500)로 전송할 수 있다.

[64] 결제 서버(500)는 토큰에 대한 인증을 완료한 토큰 검증 서버(400)로부터 토큰을 포함하는 결제 요청을 수신할 수 있으며, 토큰과 매칭된 결제 수단을 확인하여, 해당 결제 수단으로 결제를 수행할 수 있다.

[65] 결제 서버(500)는 결제가 완료되면, 결제 완료 내역을 사용자 단말기(100) 또는 가맹점 단말기(200)로 전송할 수 있다.

[66] 도 2는 본 발명의 일 실시예에 따른 토큰 인증을 통해 결제를 수행하는 과정을 도시한 도면이다.

[67] 도 2에서는 토큰 발생 서버(300) 및 토큰 검증 서버(400)에서 각각 동작을 수행하는 과정을 도시하고 있지만, 이에 제한되지 않으며, 토큰 발생 서버(300)와 토큰 검증 서버(400)가 하나의 통합 서버로 이루어져 동작을 수행할 수 있고, 결제 서버(500)에 토큰 발생 서버(300)와 토큰 검증 서버(400)가 모두 포함되어 있어, 결제 서버(500)에서 모든 동작을 수행할 수도 있다.

[68] 먼저, S201 단계에서, 사용자 단말기(100)는 SMS, 공인인증서, 결제 비밀번호 등의 본인 인증 수단으로 사용자 인증을 수행할 수 있다.

[69] S202 단계에서, 사용자 단말기(100)는 사용자 인증이 완료된 것을 알려주기 위한 사용자 인증 완료 정보를 토큰 발생 서버(300)로 전송할 수 있다. 이 때, S201 단계에서, 사용자 단말기(100)가 결제 비밀번호 등으로 결제 서버(500)를 통해 사용자 인증을 수행한 경우, 토큰 발생 서버(300)는 결제 서버(500)로부터 사용자 인증 완료 정보를 수신할 수도 있다.

[70] 토큰 발생 서버(300)는 S202 단계에서 수신된 사용자 인증 완료 정보를 이용하여, 사용자 단말기(100)에서 사용자 인증이 완료된 것을 확인할 수 있다.

[71] S203 단계에서, 토큰 발생 서버(300)는 현재 시간을 기초로, 해당 시간 기점으로 유일한 키인 세션키를 생성할 수 있고, 세션키와 사용자 정보 또는 결제 정보 등을 이용하여 검증 값을 생성할 수 있으며, 토큰, 검증 값 등을 포함하는 가상 카드번호를 생성할 수 있다.

[72] 예를 들어, 토큰 발생 서버(300)는 사용자에게 발급된 실제 카드번호와 대응되는 16자리 토큰과 현재 시간을 기초로 생성된 5자리 검증 값을 포함하는 21자리 가상 카드번호를 생성할 수 있다.

[73] 토큰 발생 서버(300)에서 가상카드 번호 생성 시, Cryptogram version 값, 거래 구분 값, PAN, PAN 유효기간, MD 키 등이 이용되거나 생성될 수 있다.

[74] 본 발명의 일 실시예에 따르면, Cryptogram version 값은 결제 서비스를 위한 검증 값 생성 및 인증을 위한 암호화 및 사용되는 데이터의 종류 및 길이를 지정한 값이며, 가상 카드번호가 발급되는 환경에 따라 가장 효율적인 암호화 형식을 지정하고 버전으로 구분된 값일 수 있다.

[75] 본 발명의 일 실시예에 따르면, 거래 구분 값은 결제 서비스의 거래 종류에 대한 구분을 위한 코드 값으로, 결제 수단 별로 별도로 부여된 코드 값일 수 있다.

[76] 본 발명의 일 실시예에 따르면, PAN은 토큰과 매칭된 실제 카드번호이고, PAN 유효기간은 실제카드에 설정된 카드 유효기간으로 YYMM형식일 수 있으며, MD 키는 마스터 데리베이션 키로 HSM(High Speed Memory)에 보관될 수 있다.

[77] S204 단계에서, 토큰 발생 서버(300)는 S203 단계에서 생성한 가상 카드번호를 사용자 단말기(100)로 발급하여 전송할 수 있다.

[78] S205 단계에서, 사용자 단말기(100)는 토큰 발생 서버(300)로부터 발급받은 가상 카드번호를 이용하여, 가상 카드번호와 상응하는 식별 정보를 생성할 수 있다. 즉, 사용자 단말기(100)는 음성, 텍스트, 바코드, QR코드, NFC 등 다양한 결제 수단으로 활용될 수 있도록, 가상 카드번호와 상응하는 식별 정보를 생성할 수 있다.

[79] S206 단계에서, 사용자 단말기(100)는 가맹점 단말기(200)로 식별 정보를 전송할 수 있으며, 가맹점 단말기(200)는 해당 식별 정보를 인식할 수 있다.

[80] 구체적으로, 사용자 단말기(100)가 근거리 무선 통신 등을 이용하여, NFC 태그 등의 식별 정보를 가맹점 단말기(200)로 직접 전송하면, 가맹점 단말기(200)는 해당 식별 정보를 인식할 수 있고, 사용자 단말기(100)가 바코드, QR 코드 등의 식별 정보를 화면에 디스플레이 하면, 가맹점 단말기(200)이 가맹점 단말기(200)와 연결된 판독기를 이용하여 식별 정보를 인식할 수도 있다.

[81] S207 단계에서, 가맹점 단말기(200)는 사용자 단말기(100)로부터 인식한 식별 정보를 포함하는 인증 요청을 토큰 검증 서버(400)로 전송할 수 있다. 이 때, 가맹점 단말기(200)는 VAN 또는 직승인 방식으로 토큰 검증 서버(400)에 인증 요청을 전송할 수 있다.

[82] S208 단계에서, 토큰 검증 서버(400)는 S203 단계에서 생성된 가상 카드번호의 생성 시간을 기초로, 해당 시간 기점으로 유일한 키를 생성한 후, 생성된 유일한 키를 이용하여 검증 값을 재생성할 수 있다.

[83] 이후, 토큰 검증 서버(400)는 S207 단계에서 수신된 인증 요청에 포함되어 있는 식별 정보와 상응하는 가상 카드번호를 확인하여, 가상 카드번호에 포함된 검증 값과 재생성된 검증 값을 비교하여 토큰에 대한 인증을 수행할 수 있다. 이 때, 토큰 검증 서버(400)는 검증 값들이 일치하는 경우 토큰에 대한 인증을 완료하여, 결제를 위한 거래를 허용할 수 있다.

[84] 본 발명의 일 실시예에 따르면, 토큰 인증 시 사용되는 데이터는 토큰, 토큰

유효기간, 줄리안 분 숫자, 검증 값, POS값, Cryptogram version 값, 거래 구분 값 등일 수 있다.

[85] S209 단계에서, 토큰 검증 서버(400)는 토큰에 대한 인증이 완료되면, S207 단계에서 토큰을 포함하는 결제 요청을 결제 서버(500)로 전송할 수 있다.

[86] S210 단계에서, 결제 서버(500)는 S209 단계에서 수신된 결제 요청에 따라, 결제 요청에 포함된 토큰을 확인하여, 토큰과 매칭된 결제 수단으로 결제를 수행할 수 있다.

[87] 이후, 결제 서버(500)는 결제 완료 내역을 사용자 단말기(100) 또는 가맹점 단말기(200)로 전송할 수 있다.

[88] 도 3은 본 발명의 다른 실시예에 따른 토큰 인증을 통해 결제를 수행하는 과정을 도시한 도면이다.

[89] 도 3에서는 사용자 단말기(100)에서 가상 카드번호를 생성하는 과정을 도시하고 있는데, 도 2에서의 설명과 중복되는 내용은 생략하기로 한다.

[90] 먼저, S301 단계에서, 사용자 단말기(100)는 S201 단계와 같이, 사용자 인증을 수행할 수 있다.

[91] 사용자 단말기(100)에 보안성이 확보된 안전한 토큰 저장소가 구비되어 있거나, 사용자 단말기(100)와 토큰 저장소가 연결되어 있는 경우, 사용자 인증이 완료되더라도 토큰 발생 서버(300)는 가상 카드번호를 직접 생성하지 않고, 토큰 발급을 요청하는 과정만 수행할 수 있다. 예를 들어, 토큰 발생 서버(300)는 키 생성 시 필요한 기초 데이터인 키 생성 정보만을 사용자 단말기(100)로 전송할 수 있다.

[92] S302 단계에서, 사용자 단말기(100)는 S203 단계에서 토큰 발생 서버(300)가 수행한 동작, 즉, 현재 시간을 기초로 줄리안 분 숫자를 이용하여, 유일한 키를 생성할 수 있으며, 생성된 유일한 키를 이용하여 검증 값을 생성하고, 검증 값 및 토큰을 포함하는 가상 카드번호를 생성할 수 있으며, 생성된 가상 카드번호를 토큰 저장소에 발급할 수 있다.

[93] 가상 카드번호 생성 시, 사용자 단말기(100)는 미리 토큰 발생 서버(300)로부터 수신한 키 생성 정보를 이용하여, 자체적으로 검증 값을 생성할 수 있으므로, 거래 요청 시마다 토큰 발생 서버(300)로부터 생성된 검증 값을 수신하지 않아도 되기 때문에, 오프라인 상에서도 가상 카드번호를 생성할 수 있다.

[94] S303 단계에서, 사용자 단말기(100)는 S205 단계와 같이, 가상 카드번호와 상응하는 식별 정보를 생성할 수 있다.

[95] S304 단계에서, 사용자 단말기(100)는 S206 단계와 같이, 가맹점 단말기(200)로 식별 정보를 전송할 수 있다.

[96] S305 단계에서, 가맹점 단말기(200)는 S207 단계와 같이, 식별 정보를 포함하는 인증 요청을 토큰 검증 서버(400)로 전송할 수 있다.

[97] S306 단계에서, 토큰 검증 서버(400)는 S208 단계와 같이, 토큰에 대한 인증을 수행할 수 있다.

[98] S307 단계에서, 토큰 검증 서버(400)는 S209 단계와 같이, 결제 요청을 결제 서버(500)로 전송할 수 있다.

[99] S308 단계에서, 결제 서버(500)는 S210 단계와 같이, 결제 요청에 따라 결제를 수행할 수 있다.

[100] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

[101] 본 발명의 범위는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

서열목록 Free Text

[102] 100 : 사용자 단말기

[103] 200 : 가맹점 단말기

[104] 300 : 토큰 발생 서버

[105] 400 : 토큰 검증 서버

[106] 500 : 결제 서버

청구범위

[청구항 1] 토큰 인증 시스템에서 토큰을 인증하는 방법에 있어서,
토큰 발생 서버에서, 현재 시간을 기점으로 생성된 유일한 키를 이용하여 검증 값을 생성하고, 상기 생성된 검증 값과 토큰을 포함하는 가상 카드번호를 생성하여 사용자 단말기로 발급하는 단계;
토큰 검증 서버에서, 상기 가상 카드번호와 상응하는 식별 정보를 포함하는 인증 요청을, 상기 사용자 단말기로부터 인식한 가맹점 단말기를 통해 수신하는 단계;
상기 토큰 검증 서버에서, 상기 가상 카드번호의 생성 시간을 기점으로 생성된 유일한 키를 이용하여 검증 값을 재생성하고, 상기 재생성된 검증 값과 상기 식별 정보와 상응하는 가상 카드번호에 포함된 검증 값을 비교하여, 상기 가상 카드번호에 포함된 토큰에 대한 인증을 수행하는 단계; 및
상기 토큰에 대한 인증이 완료되면, 상기 토큰 검증 서버에서, 상기 토큰을 포함하는 결제 요청을 결제 서버로 전송하여, 상기 토큰과 매칭된 결제 수단으로 결제가 수행되도록 하는 단계를 포함하는, 현재 시간을 기초로 생성된 검증 값을 이용한 토큰 인증 방법.

[청구항 2] 제1항에 있어서,
상기 가상 카드번호 발급 단계는,
상기 토큰 발생 서버에서, 현재 시간을 기초로 줄리안 분 숫자를 이용하여, 상기 유일한 키를 생성하는 단계를 포함하는, 현재 시간을 기초로 생성된 검증 값을 이용한 토큰 인증 방법.

[청구항 3] 토큰 인증 시스템에서 토큰을 인증하는 방법에 있어서,
사용자 단말기에서, 토큰 발생 서버로부터 키 생성 정보를 수신한 후, 상기 키 생성 정보를 통해 현재 시간을 기점으로 생성된 유일한 키를 이용하여 검증 값을 생성하고, 상기 생성된 검증 값과 토큰을 포함하는 가상 카드번호를 생성하여 상기 사용자 단말기와 연결된 토큰 저장소에 발급하는 단계;
토큰 검증 서버에서, 상기 가상 카드번호와 상응하는 식별 정보를 포함하는 인증 요청을, 상기 사용자 단말기로부터 인식한 가맹점 단말기를 통해 수신하는 단계;
상기 토큰 검증 서버에서, 상기 가상 카드번호의 생성 시간을 기점으로 생성된 유일한 키를 이용하여 검증 값을 재생성하고, 상기 재생성된 검증 값과 상기 식별 정보와 상응하는 가상 카드번호에 포함된 검증 값을 비교하여, 상기 가상 카드번호에 포함된 토큰에 대한 인증을 수행하는 단계; 및

상기 토큰에 대한 인증이 완료되면, 상기 토큰 검증 서버에서, 상기 토큰을 포함하는 결제 요청을 결제 서버로 전송하여, 상기 토큰과 매칭된 결제 수단으로 결제가 수행되도록 하는 단계를 포함하는, 현재 시간을 기초로 생성된 검증 값을 이용한 토큰 인증 방법.

[청구항 4] 제3항에 있어서,
상기 가상 카드번호 발급 단계는,
상기 사용자 단말기에서, 현재 시간을 기초로 줄리안 분 숫자를 이용하여, 상기 유일한 키를 생성하는 단계를 포함하는, 현재 시간을 기초로 생성된 검증 값을 이용한 토큰 인증 방법.

[청구항 5] 현재 시간을 기점으로 생성된 유일한 키를 이용하여 검증 값을 생성하고, 상기 생성된 검증 값과 토큰을 포함하는 가상 카드번호를 생성하여 사용자 단말기로 발급하는 토큰 발생 서버;
상기 가상 카드번호와 상응하는 식별 정보를 상기 사용자 단말기로부터 인식하는 가맹점 단말기;
상기 인식된 식별 정보를 포함하는 인증 요청을 상기 가맹점 단말기를 통해 수신하며, 상기 가상 카드번호의 생성 시간을 기점으로 생성된 유일한 키를 이용하여 검증 값을 재생성하고, 상기 재생성된 검증 값과 상기 식별 정보와 상응하는 가상 카드번호에 포함된 검증 값을 비교하여, 상기 가상 카드번호에 포함된 토큰에 대한 인증을 수행하는 토큰 검증 서버; 및
상기 토큰에 대한 인증이 완료되면, 상기 토큰을 포함하는 결제 요청을 상기 토큰 검증 서버로부터 수신하여, 상기 토큰과 매칭된 결제 수단으로 결제를 수행하는 결제 서버를 포함하는, 토큰 인증 시스템.

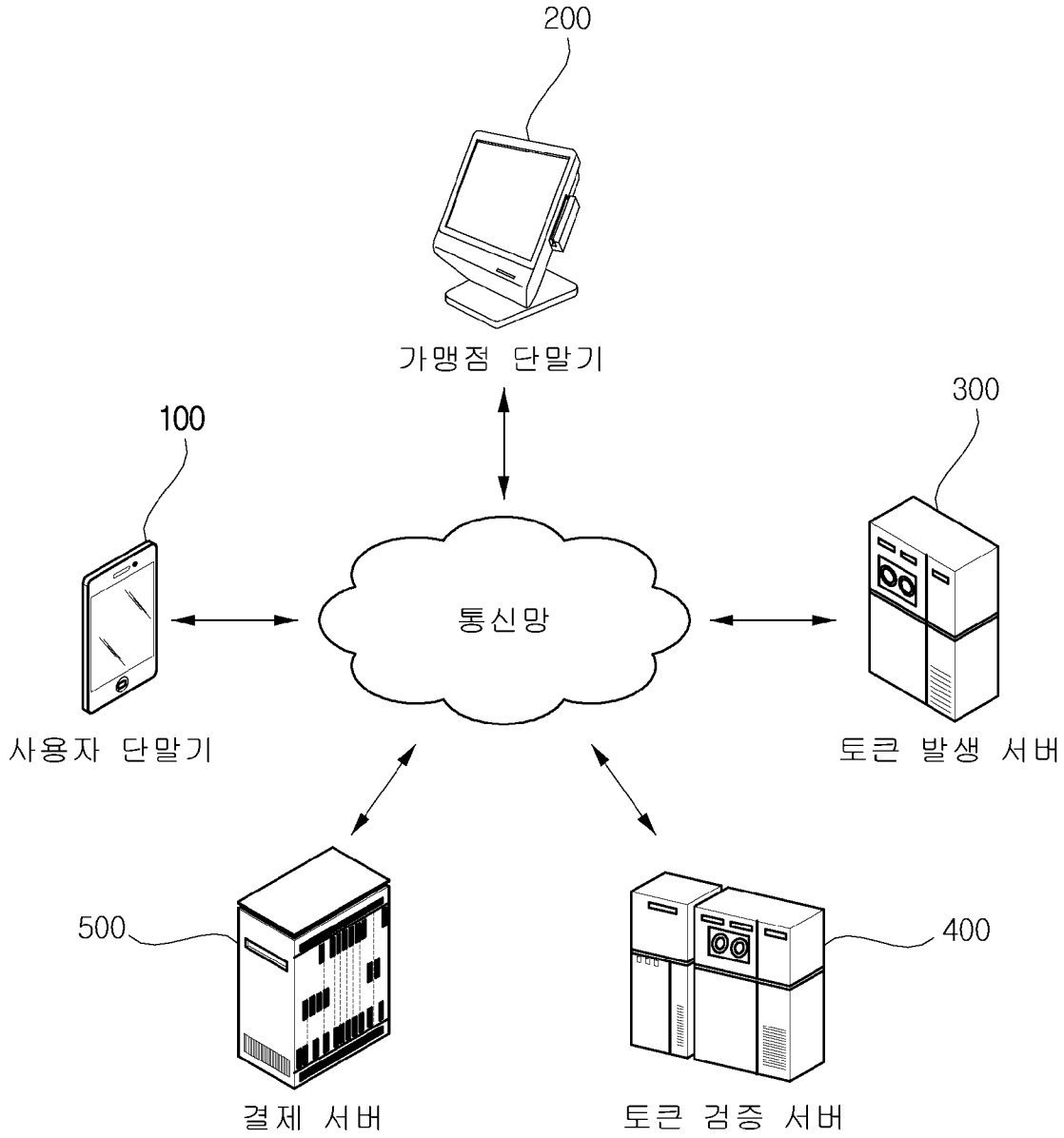
[청구항 6] 제5항에 있어서,
상기 토큰 발생 서버는, 현재 시간을 기초로 줄리안 분 숫자를 이용하여, 상기 유일한 키를 생성하는, 토큰 인증 시스템.

[청구항 7] 토큰 발생 서버로부터 키 생성 정보를 수신한 후, 상기 키 생성 정보를 통해 현재 시간을 기점으로 생성된 유일한 키를 이용하여 검증 값을 생성하고, 상기 생성된 검증 값과 토큰을 포함하는 가상 카드번호를 생성하여 토큰 저장소에 발급하는 사용자 단말기;
상기 가상 카드번호와 상응하는 식별 정보를 상기 사용자 단말기로부터 인식하는 가맹점 단말기;
상기 인식된 식별 정보를 포함하는 인증 요청을 상기 가맹점 단말기를 통해 수신하며, 상기 가상 카드번호의 생성 시간을 기점으로 생성된 유일한 키를 이용하여 검증 값을 재생성하고, 상기 재생성된 검증 값과 상기 식별 정보와 상응하는 가상 카드번호에 포함된 검증 값을 비교하여, 상기 가상 카드번호에

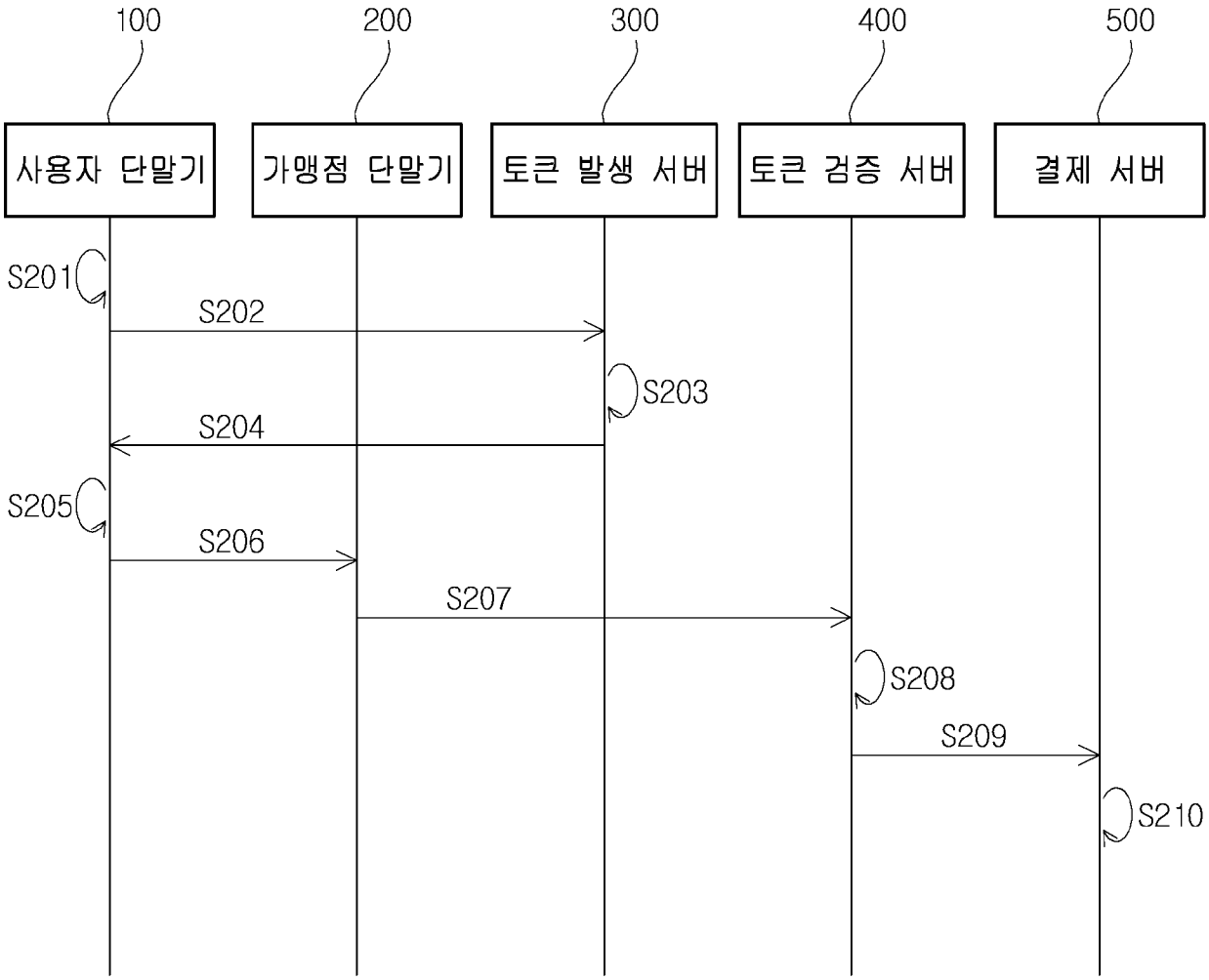
포함된 토큰에 대한 인증을 수행하는 토큰 검증 서버; 및
상기 토큰에 대한 인증이 완료되면, 상기 토큰을 포함하는 결제 요청을 상기 토큰 검증 서버로부터 수신하여, 상기 토큰과 매칭된 결제 수단으로 결제를 수행하는 결제 서버를 포함하는, 토큰 인증 시스템.

[청구항 8] 제7항에 있어서,
상기 사용자 단말기는, 현재 시간을 기초로 줄리안 분 숫자를 이용하여, 상기 유일한 키를 생성하는, 토큰 인증 시스템.

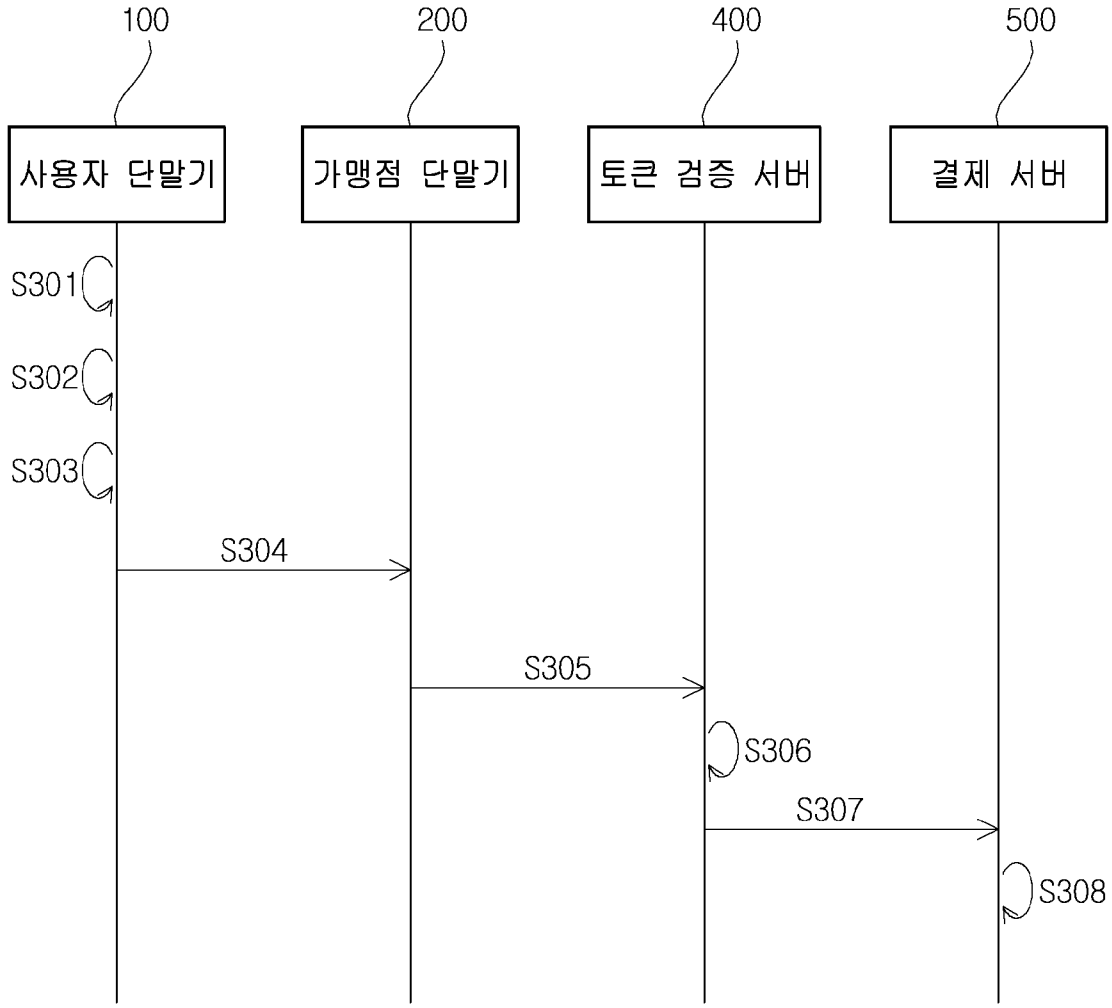
[Fig. 1]



[Fig. 2]


100
200
300
400
500
사용자 단말기
가맹점 단말기
토큰 발생 서버
토큰 검증 서버
결제 서버
S201
S202
S203
S204
S205
S206
S207
S208
S209
S210

[Fig. 3]


100
200
400
500
사용자 단말기
가맹점 단말기
토큰 검증 서버
결제 서버
S301
S302
S303
S304
S305
S306
S307
S308

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2015/009769

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i, G06Q 20/14(2012.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 9/32; G06Q 20/40; G06Q 20/20; G06F 17/60; G06Q 20/32; H04L 9/20; G06Q 20/16; G06Q 20/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: token, authentication, key, time, verification value, virtual card number, payment server, franchise terminal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 10-2014-0077013 A (SK PLANET CO., LTD.) 23 June 2014 See paragraphs [0021], [0090]-[0095]; and figure 4.	1-8
Y	KR 10-1009914 B1 (GROCKINFO CO., LTD.) 20 January 2011 See paragraphs [0030]-[0037]; and figures 4-5.	1-8
A	KR 10-2008-0062525 A (LANGUAGE & INTERFACE SOFT CO., LTD.) 03 July 2008 See paragraph [0015]; and figure 1.	1-8
A	KR 10-2005-0097624 A (CHOI, Jun Su) 10 October 2005 See paragraphs [0060]-[0064]; and figure 4.	1-8
A	US 2001-0047335 A1 (ARNDT, Martin et al.) 29 November 2001 See paragraphs [0053]-[0058]; and figure 1.	1-8

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 JANUARY 2016 (21.01.2016)	**22 JANUARY 2016 (22.01.2016)**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2015/009769

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2014-0077013 A	23/06/2014	WO 2014-092286 A1	19/06/2014
KR 10-1009914 B1	20/01/2011	NONE	
KR 10-2008-0062525 A	03/07/2008	KR 10-0858552 B1	12/09/2008
KR 10-2005-0097624 A	10/10/2005	NONE	
US 2001-0047335 A1	29/11/2001	AU 2001-50540 A1	12/11/2001
		AU 5054001 A	12/11/2001
		EP 1279149 A2	29/01/2003
		GB 2361790 A	31/10/2001
		WO 01-84509 A2	08/11/2001
		WO 01-84509 A3	16/05/2002

국 제 조 사 보 고 서

국제출원번호
PCT/KR2015/009769

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 9/32(2006.01)i, G06Q 20/14(2012.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04L 9/32; G06Q 20/40; G06Q 20/20; G06F 17/60; G06Q 20/32; H04L 9/20; G06Q 20/16; G06Q 20/14

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 토큰, 인증, 키, 시간, 검증 값, 가상 카드번호, 결제 서버, 가맹점 단말기

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	KR 10-2014-0077013 A (에스케이플래닛 주식회사) 2014.06.23 단락 [0021], [0090]-[0095]; 및 도면 4 참조.	1-8
Y	KR 10-1009914 B1 ((주)지락인포메이션) 2011.01.20 단락 [0030]-[0037]; 및 도면 4-5 참조.	1-8
A	KR 10-2008-0062525 A ((주)엘엔아이소프트) 2008.07.03 단락 [0015]; 및 도면 1 참조.	1-8
A	KR 10-2005-0097624 A (최준수) 2005.10.10 단락 [0060]-[0064]; 및 도면 4 참조.	1-8
A	US 2001-0047335 A1 (MARTIN ARNDT 등) 2001.11.29 단락 [0053]-[0058]; 및 도면 1 참조.	1-8

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2016년 01월 21일 (21.01.2016)	2016년 01월 22일 (22.01.2016)

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)
팩스 번호 +82-42-472-7140

심사관
김도원
전화번호 +82-42-481-5560

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2015/009769

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2014-0077013 A	2014/06/23	WO 2014-092286 A1	2014/06/19
KR 10-1009914 B1	2011/01/20	없음	
KR 10-2008-0062525 A	2008/07/03	KR 10-0858552 B1	2008/09/12
KR 10-2005-0097624 A	2005/10/10	없음	
US 2001-0047335 A1	2001/11/29	AU 2001-50540 A1	2001/11/12
		AU 5054001 A	2001/11/12
		EP 1279149 A2	2003/01/29
		GB 2361790 A	2001/10/31
		WO 01-84509 A2	2001/11/08
		WO 01-84509 A3	2002/05/16