(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0024994
(43) 공개일자 2018년03월08일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 9/06* (2006.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
H04L 9/0825 (2013.01)
H04L 9/0618 (2013.01)
(21) 출원번호 10-2016-0112137
(22) 출원일자 2016년08월31일
심사청구일자 2016년08월31일

(71) 출원인
주식회사 케이비저축은행
서울특별시 송파구 송파대로 260 (가락동,제일오피스텔)
(72) 발명자
이선호
경기도 수원시 팔달구 세지로 189번길 19, B동 103호 (인계동, 전원아파트)
(74) 대리인
유미특허법인

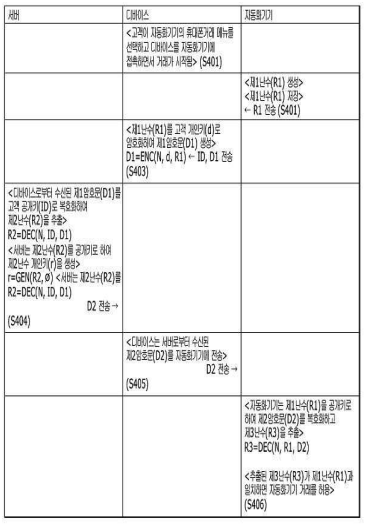
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **디바이스 및 자동화기기를 이용한 무선구간 인증 시스템 및 방법**

(57) 요 약

본 발명은 스마트폰 등 무선 디바이스에서 ATM, POS 등의 자동화기기 또는 디바이스간 데이터를 전송할 때 PKI방식의 비대칭키를 이용하여 대칭키를 이용할 때 필수 요소인 SAM을 생략하여 비용절감/시스템구축 절차 간소화/서비스 확장성 제고를 도모하고, 서버(디바이스)와 자동화기기간 무선통신 구간의 암호화 프로세스를 간소화하여 거래시간을 단축하고, 인가된 고객만 이용이 가능하도록 가용성 (Available)을 강화한 무선구간 인증 방법에 관한 것이다.

대 표 도 - 도5



(52) CPC특허분류
H04L 9/3226 (2013.01)
H04L 2209/56 (2013.01)
H04L 2209/80 (2013.01)

명 세 서

청구범위

청구항 1

고객의 디바이스를 통해 자동화기기와 서버가 통신하여 인증을 하는 비대칭키를 이용한 무선구간 인증 시스템의 무선구간 인증 방법으로서,

상기 자동화기기가 상기 디바이스의 전용ID를 읽어오는 단계

고객이 상기 자동화기기의 안내에 따라 PIN을 입력하면, 상기 자동화기기가 정당 PIN 인증 및 서버에 등록된 출금계좌번호를 가져오기 위해 랜덤값 R을 생성하고, R을 공개키인 전용ID와 PIN(P)으로 이중 암호화하여 상기 디바이스로 전송하는 단계

상기 디바이스가 내부에 저장된 공개키P에 대한 개인키p'로 수신한 값을 일차 복호화하여 일차복호화한값을 상기 서버로 전송하는 단계

상기 서버가 데이터베이스의 인터넷뱅킹 원장에 저장된 전용ID에 해당하는 출금계좌번호(A)를 추출하고, 공개키인 전용ID에 해당하는 개인키 d로 디바이스에서 전송된 일차복호화한D값을 이차복호화하여 R을 추출하는 단계

상기 서버가 개인키 d로 A와 R을 암호화하여 상기 디바이스로 전송하는 단계

상기 디바이스는 서버에서 전송된 암호화된 정보를 상기 자동화기기로 전송하는 단계

상기 자동화기기는 상기 디바이스에서 전달된 암호화된 정보(S)를 ID로 검증하여 A와 R 또는 F를 추출하고 추출된 R값이 최초에 생성한 R값과 같으면 자동화기기 거래 허용을 하는 단계를 포함하는 비대칭키를 이용한 무선구간 인증 방법.

청구항 2

제1항에 있어서,

추출된 R값이 최초에 생성한 R값과 다를 경우 상기 자동화기기가 에러메시지 출력하는 단계를 더 포함하는 비대칭키를 이용한 무선구간 인증 방법.

청구항 3

고객의 디바이스를 통해 자동화기기와 서버가 통신하여 인증을 하는 비대칭키를 이용한 무선구간 인증 시스템의 무선구간 인증 방법으로서,

동 서비스 가입시 상기 디바이스에 PIN을 등록하고 PIN에 해당하는 개인키p'와 전용ID(인터넷뱅킹ID와 1:1 매핑되는 문자열)를 생성 후 디바이스에 저장하고 서버에 전용ID와 디바이스의 고유값을 전송하여 서버에 저장하고 서버는 전용ID에 해당하는 개인키d를 생성하고 블록체인처리부에 출금계좌번호A를 d로 암호화하여 저장하고 그 저장된 주소값(H)를 서버에 저장하는 단계

상기 자동화기기가 상기 디바이스의 전용ID를 읽어오는 단계

고객이 상기 자동화기기의 안내에 따라 PIN을 입력하면, 상기 자동화기기가 정당 PIN 인증 및 서버에 등록된 출금계좌번호를 가져오기 위해 랜덤값 R을 생성하고, R을 공개키인 전용ID와 PIN(P)으로 이중 암호화하여 상기 디바이스로 전송하는 단계

상기 디바이스가 내부에 저장된 공개키P에 대한 개인키p'로 수신한 값을 일차 복호화하여 상기 자동화기기에서 입력된 PIN의 정당성 여부를 검증하는 단계

정당 PIN이 아닐 경우, 상기 디바이스는 PIN오류를 출력하는 단계

정상적으로 복호화가 될 경우, 상기 디바이스는 이차암호화값을 상기 서버로 전송하는 단계

상기 서버가 전달된 디바이스 고유값을 내부의 데이터베이스에 저장된 디바이스 고유값과 비교하는 단계

비교결과 등록된 디바이스로 판단될 경우, 상기 서버가 데이터베이스의 인터넷뱅킹 원장에 저장된 전용ID에 해당하는 출금계좌번호(A)를 추출하고, 공개키인 전용ID에 해당하는 개인키 d로 디바이스에서 전송된 D값을 이차 복호화하여 R을 추출하는 단계

상기 서버가 블록체인 처리부에 저장된 전용ID에 해당하는 출금계좌번호(A)와 블록체인 저장주소(H)를 개인키 d로 A,H,R을 암호화하여 디바이스로 전송하는 단계

등록된 디바이스가 아닐 경우 상기 서버는 오류 메시지 값(F)를 개인키 d로 암호화하여 상기 디바이스로 전송하는 단계

상기 디바이스는 서버에서 전송된 암호화된 정보를 상기 자동화기기로 전송하는 단계

상기 자동화기기가 상기 디바이스에서 전달된 S를 ID로 검증하여 H, R 또는 F를 추출하고 추출된 R값이 최초에 생성한 R값과 같고 H, R이 추출되면, 상기 블록체인 처리부에서 B를 가져와 전용ID로 복호화 후 출금계좌번호(A)를 추출하여 자동화기기 거래를 허용하는 단계를 포함하는 비대칭키를 이용한 무선구간 인증 방법.

청구항 4

제3항에 있어서,

추출된 R값이 최초에 생성한 R값과 다를 경우 상기 자동화기기가 에러메시지 출력하는 단계를 더 포함하는 비대칭키를 이용한 무선구간 인증 방법.

청구항 5

서버와 데이터를 주고 받는 디바이스에 네트워크를 통하여 연결된 자동화기기가 상기 서버를 인증하는 무선구간 인증 방법에 있어서,

상기 자동화기기가 제1난수를 생성하여 저장하고 상기 디바이스에 전송하는 단계

상기 디바이스가 고객 개인키로 상기 제1난수를 암호화한 제1암호문을 생성하여 서버에 전송하는 단계

상기 서버가 상기 제1암호문을 고객 공개키로 복호화하여 제2난수를 추출하고, 상기 제2난수를 공개키로 하여 제2난수 개인키를 생성하며, 상기 제2난수를 상기 제2난수 개인키로 암호화한 제2암호문을 생성하여 상기 디바이스를 통해 상기 자동화기기로 전송하는 단계

상기 자동화기기가 상기 제2암호문을 상기 제1난수를 공개키로 하여 복호화하고 제3난수를 추출하며, 상기 제3난수가 제1난수와 일치하면 자동화기기의 거래를 허용하는 단계

를 포함하는 무선구간 인증 방법.

청구항 6

디바이스에 및 자동화 기기와 네트워크를 통하여 연결된 무선구간 인증 시스템으로서,

마스터 공개키와 마스터 개인키를 저장하는 데이터베이스

상기 자동화기기가 제1난수를 생성하여 저장하고 상기 디바이스에 전송하고, 상기 디바이스가 고객 개인키로 상기 제1난수를 암호화한 제1암호문을 생성하여 전송하면 이를 수신하고,

상기 제1암호문을 고객 공개키로 복호화하여 제2난수를 추출하고, 상기 제2난수를 공개키로 하여 제2난수 개인키를 생성하며, 상기 제2난수를 상기 제2난수 개인키로 암호화한 제2암호문을 생성하여 상기 디바이스를 통해 상기 자동화기기로 전송하는 서버를 포함하는 무선구간 인증 시스템.

청구항 7

제6항에 있어서,

상기 자동화기기는 상기 제2암호문을 상기 제1난수를 공개키로 하여 복호화하고 제3난수를 추출하며, 상기 제3난수가 제1난수와 일치하면 자동화기기의 거래를 허용하는 것을 특징으로 하는 무선구간 인증 시스템.

청구항 8

디바이스 및 서버와 데이터를 주고 받는 자동화기기로서,

마스터 공개키 정보를 저장하는 저장부

상기 서버 및 디바이스와 통신하기 위한 통신부

제1난수를 생성하여 상기 저장부에 저장하고 상기 디바이스에 전송하며,

상기 디바이스가 고객 개인키로 상기 제1난수를 암호화한 제1암호문을 생성하여 서버에 전송하고, 상기 서버가 상기 제1암호문을 고객 공개키로 복호화하여 제2난수를 추출하고, 상기 제2난수를 공개키로 하여 제2난수 개인키를 생성하며, 상기 제2난수를 상기 제2난수 개인키로 암호화한 제2암호문을 생성하여 상기 디바이스를 통해 전송하면, 상기 제2암호문을 상기 제1난수를 공개키로 하여 복호화하고 제3난수를 추출하며, 상기 제3난수가 제1난수와 일치하면 거래를 허용하는 제어부를 포함하는 자동화기기.

청구항 9

서버 및 자동화기기와 통신하는 디바이스에 있어서,

마스터 공개키, 고객 공개키, 고객이 지정한 비밀번호(PIN)으로 암호화된 고객 개인키중 적어도 하나의 정보를 저장하는 저장부

상기 서버 및 자동화기기와 통신하기 위한 무선 통신부

상기 자동화기기가 제1난수를 생성하여 전송하면, 상기 고객 개인키로 상기 제1난수를 암호화한 제1암호문을 생성하여 상기 서버에 전송하고, 상기 서버가 상기 제1암호문을 고객 공개키로 복호화하여 제2난수를 추출하고, 상기 제2난수를 공개키로 하여 제2난수 개인키를 생성하며, 상기 제2난수를 상기 제2난수 개인키로 암호화한 제2암호문을 생성하면 이를 상기 자동화기기로 전송하는 제어부를 포함하는 디바이스.

청구항 10

제9항에 있어서,

상기 자동화기기는 상기 제2암호문을 상기 제1난수를 공개키로 하여 복호화하고 제3난수를 추출하며, 상기 제3난수가 제1난수와 일치하면 자동화기기의 거래를 허용하는 것을 특징으로 하는 디바이스.

발명의 설명

기 술 분 야

[0001] 본 발명은 비대칭키를 이용한 무선구간 인증 방법에 관한 것으로 특히, 서비스 제공사가 고객 디바이스의 무선통신을 이용하여 포스 단말기 또는 ATM 등의 자동화기기로 소정의 거래에 관하여 안전하게 인증 데이터를 전송하는 디바이스 및 자동화기기를 이용한 무선구간 인증 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 일반적으로 전자통신 기술의 발전을 통해 무선통신이 가능한 다양한 전자기기가 금융서비스에 이용되고 있다. 개인 모바일을 통한 온라인 금융거래는 PC뱅킹을 넘어섰으며, 모바일을 통한 온라인 금융거래는 향후에도 지속 증가할 것으로 예상한다.

[0003] 모바일을 통한 오프라인 거래는 무선통신을 이용하여 ATM, 가맹점 거래가 가능하다. 실물카드를 발급하여 모바일에 저장하거나, 모바일 전용 카드를 발급하여 가맹점 결제가 가능하다.

[0004] 또한, 출금계좌를 모바일 또는 금융사 서버에 저장하여 ATM을 이용하기도 한다.

[0005] 현재 카드를 이용한 지급결제 비율은 실물카드 비율이 높지만 모바일을 통한 지급결제 비율도 높아지고 있어 향후 모바일 지급결제 비율이 실물카드 결제비율보다 높아질 것으로 예상된다.

[0006] 또한, 카드의 발급 없이 계좌이체기반의 지급결제 비율도 증가할 것으로 예상된다. 카드 이용시 필연적으로 가

맹점 수수료 등이 발생하나, 계좌이체기반의 결제는 카드 관련 비용이 없어 카드보다 낮게 수수료가 형성될 개연성이 높아 모바일을 통한 계좌이체기반의 지급결제 시장이 발전할 것으로 예상된다.

[0007] 현재 모바일을 통한 오프라인 계좌기반의 서비스는 ATM서비스가 유일하며, 계좌이체기반의 가맹점 지급결제는 없는 실정이다.

[0008] ATM서비스는 ATM에서 '휴대폰거래'와 출금/이체 등의 '서비스메뉴'를 선택하면 서버에서 계좌번호를 대칭키방식으로 암호화하여 무선통신으로 ATM으로 전송하고 ATM에서 암호화된 계좌번호를 동일 키로 복호화하여 추출된 계좌번호를 CD공동망을 이용해 거래를 완료시킨다.

[0009] 여기서, 대칭키방식은 무선통신 구간의 기밀성 확보를 위해 동일한 키를 개별은행서버 (또는 휴대폰)와 ATM 내 별도 H/W[SAM(Secure Access Module) -IC Chip]에 저장하게 된다.

[0010] 하지만, 이러한 대칭키방식 ATM서비스는 비대칭키방식과 대비해 SAM(IC- Chip)관련 적용절차가 반드시 필요하고 서버와 ATM간 상호인증 절차가 추가되며 상호 신뢰기관간만 거래가 가능하여 확장성이 부족하다는 단점이 있다.

[0011] 대칭키방식 ATM 서비스는 계좌번호를 복호화 하기 위해 자동화기기에 별도의 H/W(SAM)가 필요하고 도입된 SAM(IC칩)에 대칭키를 주입하여 자동화기기에 별도로 설치(SAM 설치 프로세스는 IC칩도입 -> 키주입 -> ATM 설치)해야 하므로 매우 복집하다. 새로운 사업자가 동 방식의 ATM 이용 요청시 상기절차의 반복이 필요하므로 비용/개발/적용절차 관련 기존 ATM에 신규사업자 진입은 불가능에 가깝다.

[0012] 또한, 서버와 ATM(IC-Chip)간의 암호화된 세션을 위해 ATM과 서버는 별도로 암호화된 통로를 만드는 절차를 수행하고 계좌번호를 전송한다. 비대칭키방식은 암호화된 통로 생성 절차 없이 바로 암호화된 계좌번호를 전송하므로 대칭키방식보다 절차가 간소하다.

[0013] 또한, 대칭키방식은 동일한 키(은행 또는 제휴기관 또는 ATM)를 이용하기 때문에 키가 유출된 경우 어디에서 유출된 지 알 수 없어 보안상 서비스를 중단하거나 모든 ATM에 장착된 동글 SAM을 다시 설치해야 하는 위험이 있다. 따라서 현재는 상호 신뢰하는 기관간(1금융권)만 서비스가 가능하므로 2금융권 등 서비스 확장에 제한이 있다.

발명의 내용

해결하려는 과제

[0014] 본 발명이 해결하고자 하는 기술적 과제는 종래의 대칭키방식 암호화의 문제를 해결하고자 하는 것으로, 스마트폰 등 무선 디바이스에서 ATM, POS 등의 자동화기기 또는 디바이스간 데이터를 전송할 때 PKI방식의 비대칭키를 이용하여 대칭키를 이용할 때 필수 요소인 SAM을 생략하여 비용절감/시스템구축 절차 간소화/서비스확장성 제고를 도모하고, 서버(디바이스)와 자동화기기간 무선통신 구간의 암호화 프로세스를 간소화하여 거래시간을 단축하고, 인가된 고객만 이용이 가능하도록 가용성 (Available)을 강화한 디바이스 및 자동화기기를 이용한 무선구간 인증 시스템 및 방법을 제공하는 것이다.

과제의 해결 수단

[0015] 상술한 과제를 해결하기 위한 본 발명의 특징에 따른 비대칭키를 이용한 무선구간 인증 방법은,

[0016] 고객의 디바이스를 통해 자동화기기와 서버가 통신하여 인증을 하는 비대칭키를 이용한 무선구간 인증 시스템의 무선구간 인증 방법으로서,

[0017] 동 서비스 가입시 상기 디바이스에 PIN을 등록하고 PIN에 해당하는 개인키p'와 전용ID(인터넷뱅킹ID와 1:1 매핑되는 문자열)를 생성 후 디바이스에 저장하고 서버에 전용ID와 디바이스의 고유값을 전송하여 서버에 저장하고 서버는 전용ID에 해당하는 개인키d를 생성하는 단계(서비스가입 단계);

[0018] 상기 자동화기기가 상기 디바이스의 전용ID(금융사 식별)를 읽어오는 단계

[0019] 고객이 상기 자동화기기에서 '휴대폰거래'를 선택하고 현금출금 등 '서비스메뉴'를 선택하고 상기 자동화기기의 안내에 따라 PIN을 입력하면, 상기 자동화기기가 정당 PIN 인증 및 서버에 등록된 출금계좌번호를 가져오기 위해 랜덤값 R을 생성하고, R을 공개키인 전용ID와 PIN(P)으로 이중 암호화하여 상기 디바이스로 전송하는 단계[1차암호화[2차암호화(R,ID)], P];

[0020] 상기 디바이스가 수신된 이중암호화값을 내부에 저장된 공개키 P에 대한 개인키 p'로 1차 복호화하고 복호화 값

인 이차 암호화값(R,ID)을 상기 서버로 전송하는 단계

[0021] 상기 서버가 전달된 디바이스 고유값(통신시 자동전달)을 내부의 데이터베이스에 저장된 디바이스 고유값과 비교하는 단계

[0022] 비교결과 등록된 디바이스로 판단될 경우, 상기 서버가 데이터베이스의 인터넷뱅킹 원장에 저장된 전용ID에 해당하는 출금계좌번호(A)를 추출하고, 공개키인 전용ID에 해당하는 개인키 d로 디바이스에서 이차 암호화값을 이차 복호화하여 R을 추출하는 단계

[0023] 상기 서버가 개인키 d로 A와 R을 암호화하여 상기 디바이스로 전송하는 단계

[0024] 상기 디바이스는 서버에서 전송된 암호화된 정보를 상기 자동화기기로 전송하는 단계

[0025] 상기 자동화기기는 상기 디바이스에서 개인키d로 암호화된 정보(S)를 ID로 복호화하여 A와 R을 추출하고 추출된 R값이 최초에 생성한 R값과 같으면 자동화기기 거래 표시하는 단계를 포함한다.

[0026] 상기 방법은, 추출된 R값이 최초에 생성한 R값과 다를 경우 상기 자동화기기가 에러메시지 출력하는 단계를 더 포함한다.

[0027] 상술한 과제를 해결하기 위한 본 발명의 다른 특징에 따른 비대칭키를 이용한 무선구간 인증 방법은,

[0028] 동 서비스 가입시 상기 디바이스에 PIN을 등록하고 PIN에 해당하는 개인키p'와 전용ID(인터넷뱅킹ID와 1:1 매핑되는 문자열)를 생성 후 디바이스에 저장하고 서버에 전용ID와 디바이스의 고유값을 전송하여 서버에 저장하고 서버는 전용ID에 해당하는 개인키d를 생성하고 블록체인처리부에 출금계좌번호A를 d로 암호화하여 저장하고 그 저장된 주소값(H)를 서버에 저장하는 단계

[0029] 상기 자동화기기가 상기 디바이스의 전용ID(금융사 식별)를 읽어오는 단계

[0030] 고객이 상기 자동화기기에서 '휴대폰거래'를 선택하고 현금출금 등 '서비스메뉴'를 선택하고 상기 자동화기기의 안내에 따라 PIN을 입력하면, 상기 자동화기기가 정당 PIN 인증 및 서버에 등록된 출금계좌번호를 가져오기 위해 랜덤값 R을 생성하고, R을 공개키인 전용ID와 PIN(P)으로 이중 암호화하여 상기 디바이스로 전송하는 단계[1차암호화[2차암호화(R,ID)], P];

[0031] 상기 디바이스가 수신된 이중암호화값을 내부에 저장된 공개키 P에 대한 개인키 p'로 1차 복호화하고 복호화 값인 이차 암호화값(R,ID)을 상기 서버로 전송하는 단계

[0032] 상기 서버가 전달된 디바이스 고유값(통신시 자동전달)을 내부의 데이터베이스에 저장된 디바이스 고유값과 비교하는 단계

[0033] 비교결과 등록된 디바이스로 판단될 경우, 공개키인 전용ID에 해당하는 개인키 d로 디바이스에서 이차 암호화값을 이차 복호화하여 R을 추출하는 단계

[0034] 상기 서버가 블록체인 처리부에 저장된 전용ID에 해당하는 출금계좌번호(A)와 블록체인 저장주소(H)를 개인키 d로 A,H,R을 암호화하여 디바이스로 전송하는 단계

[0035] 상기 디바이스는 서버에서 전송된 암호화된 정보를 상기 자동화기기로 전송하는 단계

[0036] 상기 자동화기기가 상기 디바이스에서 개인키d로 암호화된 정보(S)를 ID로 복호화하여 H, R을 추출하고 추출된 R값이 최초에 생성한 R값과 같으면, 상기 블록체인 처리부에서 B를 가져와 전용ID로 복호화 후 출금계좌번호(A)를 추출하여 자동화기기 거래를 표시하는 단계를 포함한다.

[0037] 상기 방법은, 추출된 R값이 최초에 생성한 R값과 다를 경우 상기 자동화기기가 에러메시지 출력하는 단계를 더 포함한다.

[0038] 상술한 과제를 해결하기 위한 본 발명의 다른 특징에 따른 비대칭키를 이용한 무선구간 인증 방법은,

[0039] 서버와 데이터를 주고 받는 디바이스에 네트워크를 통하여 연결된 자동화기기가 상기 서버를 인증하는 무선구간 인증 방법에 있어서,

[0040] 상기 자동화기기가 제1난수를 생성하여 저장하고 상기 디바이스에 전송하는 단계

[0041] 상기 디바이스가 고객 개인키로 상기 제1난수를 암호화한 제1암호문을 생성하여 서버에 전송하는 단계

[0042] 상기 서버가 상기 제1암호문을 고객 공개키로 복호화하여 제2난수를 추출하고, 상기 제2난수를 공개키로 하여

제2난수 개인키를 생성하며, 상기 제2난수를 상기 제2난수 개인키로 암호화한 제2암호문을 생성하여 상기 디바이스를 통해 상기 자동화기기로 전송하는 단계

[0043] 상기 자동화기기가 상기 제2암호문을 상기 제1난수를 공개키로 하여 복호화하고 제3난수를 추출하며, 상기 제3난수가 제1난수와 일치하면 자동화기기의 거래를 허용하는 단계

[0044] 를 포함한다.

[0045] 상술한 과제를 해결하기 위한 본 발명의 다른 특징에 따른 비대칭키를 이용한 무선구간 인증 시스템은,

[0046] 디바이스에 및 자동화 기기와 네트워크를 통하여 연결된 무선구간 인증 시스템으로서,

[0047] 마스터 공개키와 마스터 개인키를 저장하는 데이터베이스

[0048] 상기 자동화기기가 제1난수를 생성하여 저장하고 상기 디바이스에 전송하고, 상기 디바이스가 고객 개인키로 상기 제1난수를 암호화한 제1암호문을 생성하여 전송하면 이를 수신하고,

[0049] 상기 제1암호문을 고객 공개키로 복호화하여 제2난수를 추출하고, 상기 제2난수를 공개키로 하여 제2난수 개인키를 생성하며, 상기 제2난수를 상기 제2난수 개인키로 암호화한 제2암호문을 생성하여 상기 디바이스를 통해 상기 자동화기기로 전송하는 서버를 포함한다.

[0050] 상기 자동화기기는 상기 제2암호문을 상기 제1난수를 공개키로 하여 복호화하고 제3난수를 추출하며, 상기 제3난수가 제1난수와 일치하면 자동화기기의 거래를 허용하는 것을 특징으로 한다.

[0051] 상술한 과제를 해결하기 위한 본 발명의 다른 특징에 따른 자동화기기는,

[0052] 디바이스 및 서버와 데이터를 주고 받는 자동화기기로서,

[0053] 마스터 공개키 정보를 저장하는 저장부

[0054] 상기 서버 및 디바이스와 통신하기 위한 통신부

[0055] 제1난수를 생성하여 상기 저장부에 저장하고 상기 디바이스에 전송하며,

[0056] 상기 디바이스가 고객 개인키로 상기 제1난수를 암호화한 제1암호문을 생성하여 서버에 전송하고, 상기 서버가 상기 제1암호문을 고객 공개키로 복호화하여 제2난수를 추출하고, 상기 제2난수를 공개키로 하여 제2난수 개인키를 생성하며, 상기 제2난수를 상기 제2난수 개인키로 암호화한 제2암호문을 생성하여 상기 디바이스를 통해 전송하면, 상기 제2암호문을 상기 제1난수를 공개키로 하여 복호화하고 제3난수를 추출하며, 상기 제3난수가 제1난수와 일치하면 거래를 허용하는 제어부를 포함한다.

[0057] 상술한 과제를 해결하기 위한 본 발명의 다른 특징에 따른 디바이스는,

[0058] 서버 및 자동화기기와 통신하는 디바이스에 있어서,

[0059] 마스터 공개키, 고객 공개키, 고객이 지정한 비밀번호(PIN)으로 암호화된 고객 개인키중 적어도 하나의 정보를 저장하는 저장부

[0060] 상기 서버 및 자동화기기와 통신하기 위한 무선 통신부

[0061] 상기 자동화기기가 제1난수를 생성하여 전송하면, 상기 고객 개인키로 상기 제1난수를 암호화한 제1암호문을 생성하여 상기 서버에 전송하고, 상기 서버가 상기 제1암호문을 고객 공개키로 복호화하여 제2난수를 추출하고, 상기 제2난수를 공개키로 하여 제2난수 개인키를 생성하며, 상기 제2난수를 상기 제2난수 개인키로 암호화한 제2암호문을 생성하면 이를 상기 자동화기기로 전송하는 제어부를 포함한다.

[0062] 상기 자동화기기는 상기 제2암호문을 상기 제1난수를 공개키로 하여 복호화하고 제3난수를 추출하며, 상기 제3난수가 제1난수와 일치하면 자동화기기의 거래를 허용하는 것을 특징으로 한다.

발명의 효과

[0063] 본 발명의 실시예에서는 스마트폰 등 무선 디바이스에서 ATM, POS 등의 자동화기기 또는 디바이스간 데이터를 전송할 때 PKI방식의 비대칭키를 이용하여 대칭키를 이용할 때 필수 요소인 SAM을 생략하여 비용절감/시스템구축 절차 간소화/서비스 확장성 제고를 도모하고, 디바이스와 자동화기기간 무선통신 구간의 암호화 프로세스를 간소화하여 거래시간을 단축시키고, 인가된 고객만 이용이 가능하도록 가용성 (Available)을 강화한 디바이스

및 자동화기기를 이용한 무선구간 인증 시스템 및 방법을 제공할 수 있다.

도면의 간단한 설명

[0064] 도 1은 본 발명의 제1 실시예에 따른 비대칭키를 이용한 무선구간 인증 시스템의 구성도이다.

도 2는 도 1의 자동화기기의 구성도이다.

도 3은 도 1의 디바이스의 구성도이다.

도 4은 본 발명의 제1 실시예에 따른 비대칭키를 이용한 무선구간 인증 방법의 동작 흐름도이다.

도 5는 본 발명의 제2 실시예에 따른 비대칭키를 이용한 무선구간 인증 방법의 동작 흐름도이다.

도 6a 및 도 6b는 본 발명의 제3 실시예에 따른 비대칭키를 이용한 무선구간 인증 방법의 동작 흐름도이다.

도 7은 본 발명의 제4 실시예에 따른 비대칭키를 이용한 무선구간 인증 시스템의 구성도이다.

도 8은 본 발명의 제4 실시예에 따른 비대칭키를 이용한 무선구간 인증 방법의 동작 시스템의 동작 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0065] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시 예를 가질 수 있는 바, 특정 실시 예들을 도면에 예시하고 발명을 실시하기 위한 구체적인 내용을 상세하게 설명하고자 한다.

[0066] 그러나, 이는 본 발명을 특정한 실시 형태에 한정하는 데 사용하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함하는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[0067] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다.

[0068] 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0069] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다.

[0070] 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다

[0071] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다.

[0072] 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0073] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다.

[0074] 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0075] 이하, 본 발명에 따른 바람직한 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0076] 도 1은 본 발명의 제1 실시예에 따른 비대칭키를 이용한 무선구간 인증 시스템의 구성도이고, 도 2는 도 1의 자동화기기의 구성도이다.

[0077] 도 1을 참조하면, 고객의 디바이스(300)는 자동화기기(300)와 RF등와이파이등 근건리 무선으로 연결되고, 디바이스별 고유값(기기일련번호, USIM일련번호, 전화번호 등)이 저장되어 있다. 또한, 전용ID와 공개키 PIN에 대응하는 개인키P'를 내부 메모리에 저장한다.

[0078] 서버(110)는 디바이스별 고유값(기기일련번호, USIM일련번호, 전화번호 등)과 전용ID, 출금계좌번호를 데이터베이스(120)의 인터넷뱅킹 원장에 저장한다.

[0079] 또한, 서버(110)는 공개키인 전용ID에 해당하는 개인키 d를 저장한다.

[0080] 전용ID는 인증을 위한 아이디로서 PIN으로 생성하며, 인터넷뱅킹 ID와 1:1로 매핑되는 (특수)문자+숫자열로 이루어지고, 유출되더라도 실제 인터넷뱅킹 ID는 알 수 없으며 공개키 역할을 한다.

[0081] PIN(Personel Identification Number)은 고객이 미리 등록하는 4~6자리 숫자열로 비밀번호의 일종으로 공개키 역할을 한다.

[0082] d는 ID로 생성되는 개인키로 서버(110)에서만 생성 가능하다.

[0083] P'는 PIN으로 생성되는 개인키이다.

[0084] R은 자동화기기(ATM)에서 생성하는 일회용 난수값으로 자동화기기(200)와 서버(110)간 상호인증용으로 이용된다.

[0085] ENC는 Encryption(암호화)를 의미한다.

[0086] DEC는 Decryption(복호화)를 의미한다.

[0087] A(Account)는 출금계좌번호이다.

[0088] 블록체인(BC, Blockchain)은 인터넷상에 분산화된 거래장부로 MS에서는 서비스형태로 제공 중이며, 여기에 한정하지 않고, 본 발명의 서버(110)에서 또는 다른 서버에서 구현될 수 있다.

[0089] 도 2를 참조하면, 자동화 기기(200)는 표시부(210), 입력부(220), 제어부(230), 통신부(240), 저장부(250)를 포함한다.

[0090] 입력부(220)는 키패드나 터치장치 등의 입력수단으로서 사용자의 선택을 입력받아 제어부(230)로 전달한다.

[0091] 통신부(240)는 유선통신망 또는 무선통신망 등을 이용하여 디바이스(300) 또는 블록체인 처리부와의 통신 기능을 수행한다.

[0092] 표시부(210)는 정보를 표시한다.

[0093] 제어부(230)는 입력부(220) 선택에 따라 인증에 관련된 프로세스를 수행하며, 서버(110)로부터 수신되는 정보를 상기 표시부(210)에 표시하는 기능을 수행할 수도 있다.

[0094] 저장부(250)는 인증과 관련된 제어프로그램을 저장하며, 상기 제어프로그램은 상기 제어부(230)에서 실행된다.

[0095] 자동화기기(200)는 ATM 또는 포스 단말기일 수 있으며, 필요에 따라 다른 기능부를 추가로 포함한다.

[0096] 도 3을 참조하면, 디바이스(300)는 표시부(310), 입력부(320), 제어부(330), 무선통신부(340), 저장부(350)를 포함한다.

[0097] 입력부(320)는 키패드나 터치장치 등의 입력수단으로서 사용자의 선택을 입력받아 제어부(330)로 전달한다.

[0098] 무선통신부(340)는 무선통신망 또는 근거리 통신 등을 이용하여 자동화기기(200) 또는 서버와의 통신 기능을 수행한다.

[0099] 표시부(310)는 정보를 표시한다.

[0100] 제어부(330)는 입력부(320) 선택에 따라 인증에 관련된 프로세스를 수행하며, 서버(110) 또는 자동화기기(200)기로부터 수신되는 정보를 상기 표시부(210)에 표시하는 기능을 수행할 수도 있다.

[0101] 저장부(350)는 인증과 관련된 제어프로그램을 저장하며, 상기 제어프로그램은 상기 제어부(330)에서 실행된다.

[0102] 이러한 구성을 가진 본 발명의 실시예에 따른 비대칭키를 이용한 무선구간 인증 방법에 대해 설명하기로 한다.

[0103] 도 4는 본 발명의 제1 실시예에 따른 비대칭키를 이용한 무선구간 인증 방법의 동작 흐름도이다.

[0104] 먼저, 사용자는 이용기기 등록을 한다. 고객이 모바일뱅킹 가입 또는 무선통신으로 자동화기기(200)를 이용할 수 있는 서비스(예시 '모바일 현금카드서비스') 가입 시 고객의 디바이스(300)에서 PIN(Personel Identification Number)을 등록하고, 자동화기기(200)에서 이용할 출금계좌번호를 선택한다.

[0105] 디바이스(300)는 PIN으로 생성되는 전용 ID(인터넷뱅킹 ID가 아닌 PIN(P)을 통해 새롭게 생성되는 ID로 인터넷뱅킹 ID와 1:1로 매핑)와 출금계좌번호를 서버(110)에 송신하고 전용ID와 공개키 PIN에 대응하는 개인키P'를 내부 메모리에 저장한다. 이하에서 ID는 별도의 언급이 없으면 전용 ID이다.

[0106] 서버(110)는 디바이스(300)에서 수신된 디바이스별 고유값(기기일련번호, USIM일련번호, 전화번호 등)과 ID, 출금계좌번호를 인터넷뱅킹 원장에 등록한다.

[0107] 이렇게 서비스 가입이 된 상태에서, 고객은 필요에 따라 인증이 필요한 계좌이체나 다른 금융서비스를 이용함, 이때 인증 방법을 설명하면 다음과 같다.

[0108] 도 4를 참조하면, 고객은 디바이스(300)로 무선통신을 통해 자동화기기(300)와 통신을 연결하고, 자동화기기(200)는 디바이스(300)의 전용ID를 읽어온다(S300).

[0109] 그리고 고객이 자동화기기(200)의 안내에 따라 PIN을 입력하면 자동화기기(200)는 정당 PIN 인증 및 서버(110)에 등록된 출금계좌번호를 가져오기 위해 랜덤값 R을 생성하고, R을 공개키인 전용ID와 PIN(P)으로 이중 암호화하여 디바이스(300)로 전송한다(S310). 이때 전송값은 [C=ENC(ENC(R,ID),P)]이다.

[0110] 그러면, 고객의 디바이스(300)는 내부에 저장된 공개키P에 대한 개인키p'로 수신한 C값을 일차 복호화하여 이차 암호화값(D)을 서버(110)로 전송한다(S320). 이때의 전송값(D)는 다음과 같다.

[0111] D=ENC(R,ID)

[0112] 그러면, 서버(110)는 디바이스에서 자동으로 전달된 디바이스 고유값을 내부의 데이터베이스(120)에 저장된 디바이스 고유값과 비교한다.

[0113] 비교결과 등록된 디바이스(300)로 판단될 경우, 서버(110)는 데이터베이스(120)의 인터넷뱅킹 원장에 저장된 전용ID에 해당하는 출금계좌번호(A)를 추출하고, 공개키인 전용ID에 해당하는 개인키 d로 디바이스(300)에서 전송된 D값을 이차복호화하여 R을 추출한다.

[0114] 그리고 나서, 서버(110)는 개인키 d로 A와 R을 암호화하여 디바이스(300)로 전송한다(S330).

[0115] 이때 전송값(S)는 다음과 같다. S=ENC(AllR,d)

[0116] 한편, 등록된 디바이스(300)가 아닐 경우 서버(110)는 오류 메시지 값(F)를 개인키 d로 암호화하여 디바이스(300)로 전송한다. 이때의 전송값(S)는 다음과 같다. S=ENC(F, d)

[0117] 다음, 디바이스(300)는 서버(110)에서 전송된 S를 자동화기기(200)로 전송한다(S340).

[0118] 그러면, 자동화기기(200)는 디바이스(300)에서 전달된 S를 ID로 검증하여 A와 R 또는 F를 추출하고 추출된 R값이 최초에 생성한 R값과 같으면 자동화기기(200) 거래 허용을 한다. 즉 인증을 하게 된다. 이 경우 A를 CD 공동망으로 전송한다.

[0119] 한편, 추출된 R값이 최초에 생성한 R값과 다를 경우 자동화기기(200)는 에러메시지 출력한다.

[0120] P'와 ID가 디바이스(300)에 저장되지만 ID가 유출되더라도, 실제 인터넷 뱅킹 ID를 유츄할 수 없으며, P'는 1차 복호화용으로만 이용되므로 유출되더라도 의미가 없다.

[0121] 사실상 PIN과 인증된 (USIM, 기기일련번호, SMS_ARS 인증 등) 디바이스에서만 거래가 가능하므로(앱의 위변조 확인 여부는 모바일뱅킹프로그램의 기본 보안적용사항으로 복제폰 또는 위변조 앱에서는 근본적으로 이용이 불가능하다) 복제폰만으로 거래가 불가하여 보안성이 강화된다.

[0122] 이와 같이 본 발명의 제1 실시예에서는 자동화기기(200)를 이용하여 인증을 하므로 별도 H/W가 불필요하고, 프로세스가 간소화되며, PIN/디바이스 인증으로 가용성을 강화할 수 있다.

[0123] 이러한 본 발명의 제1 실시예는 다양한 변형이 가능하며, 변형예중 블록체인을 이용한 변형예에 관하여 설명한다.

[0124] 도 5는 본 발명의 제2 실시예에 따른 비대칭키를 이용한 무선구간 인증 방법의 동작흐름도이다.

[0125] 먼저 서버(110)에는 마스터 공개키(N)와 마스터 개인키(∅)가 저장되어 있다. 그리고, 디바이스(300)에는 마스터 공개키(N), 고객 공개키(ID), 고객 개인키(d)가 저장되어 있다.

[0126] 그리고, 자동화기기(200)에는 마스터 공개키(N)가 저장되어 있다.

[0127] 도 5를 참조하면, 고객이 자동화기기(200)의 휴대폰거래 메뉴를 선택하고 디바이스(300)를 자동화기기(200)에 접촉하면서 거래가 시작된다(S401). 이때 자동화기기(200)가 디바이스(300)에 내장된 nfc 칩등을 인식할 수도 있고, 서로 근거리 통신을하여 인식을 할 수도 있다.

[0128] 그리고 나서 자동화기기(200)의 제어부(230)는 제1난수(R1)를 생성하고 내부의 저장부(250)에 저장하고, 디바이스(300)로 전송한다(S402).

[0129] 다음, 디바이스(300)의 제어부(330)는 제1난수(R1)를 고객 개인키(d)로 암호화하여 제1암호문(D1)을 생성한다.

[0130] D1=ENC(N, d, R1)

[0131] 그리고 나서, 디바이스(300)의 제어부(330)는 아이디와 제1 암호문(ID, D1)을 서버(110)로전송한다(S403).

[0132] 그러면, 서버(110는 디바이스(300)로부터 수신된 제1암호문(D1)를 고객 공개키(ID)로 복호화하여 제2난수(R2)을 추출한다.

[0133] R2=DEC(N, ID, D1)

[0134] 그리고 서버(110)는 제2난수(R2)를 공개키로 하여 제2난수 개인키(r)을 생성한다.

[0135] r=GEN(R2,∅)

[0136] 다음, 서버(110)는 제2난수(R2)를 제2난수 개인키(r)로 암호화하여 제2암호문(D2)을 생성한다.

[0137] D2=ENC(N, r, R2)

[0138] 그리고 서버(110)는 생성된 제2 암호문(D2)을 디바이스(300)로 전송한다(S404).

[0139] 그러면, 디바이스(300)는 서버(110)로부터 수신된 제2암호문(D2)를 자동화기기에 전송한다(S405).

[0140] 다음, 자동화기기(200)는 제1난수(R1)을 공개키로 하여 제2암호문(D2)를 복호화하고 제3난수(R3)을 추출한다.

[0141] R3=DEC(N, R1, D2)

[0142] 그리고 추출된 제3난수(R3)가 제1난수(R1)과 일치하면, 자동화기기(200)는 자동화기기 거래를 허용한다(S406).

[0143] 상기 과정에서 ENC(N, d, M) 은 공개키 암호의 일례로써, M^d mod N 와 같은 RSA암호 연산이 될 수 있다.

[0144] 그리고, DEC(N, e, C)은 공개키 복호의 일례로써 C^e mod N와 같은 RSA암호 연산이 될 수 있다.

[0145] 여기서 (d, e)는 상호 개인키, 공개키 관계에 있다.

[0146] ENC와 DEC의 관계를 보면 C=ENC(N, d, M) 라면 M=DEC(N, e, C)의 관계에 있다.

[0147] 또한, GEN(e, ∅)는 공개키암호에서 공개키에 대응되는 개인키를 생성하는 일례로써 1/e mod ∅ 과 같은 수학적 연산이 될 수 있다.

[0148] 상기 제2 실시예에 덧붙여 디바이스에는 고객 개인키(d)가 고객이 지정한 비밀번호(PIN)으로 암호화되어 저장되어 있을 수 있다. 이 경우, 확장흐름도에서는 자동화기기에서 PIN을 입력받아 처리하는 방법이 추가되어 질 수 있다

[0149] 이러한 변형예를 설명한다.

[0150] 도 6a 및 도 6b는 본 발명의 제3 실시예에 따른 비대칭키를 이용한 무선구간 인증 방법의 동작흐름도이다.

[0151] 도 6a 및 도 6b를 참조하면, 먼저 서버(110)에는 마스터 공개키(N)와 마스터 개인키(∅)가 저장되어 있다. 그리고, 디바이스(300)에는 마스터 공개키(N), 고객 공개키(ID), 고객 개인키(d)가 저장되어 있다. 또한, 디바이스(300)에는 고객이 지정한 비밀번호(PIN)으로 암호화된 고객 개인키(dE)가 저장되어 있다. 이때,

dE=ENC_S(PIN, d)

[0152] 그리고, 자동화기기(200)에는 마스터 공개키(N)가 저장되어 있다.

[0153] 도 6a 및 도 6b를 참조하면, 고객이 자동화기기(200)의 휴대폰거래 메뉴를 선택하고 디바이스(300)를 자동화기기(200)에 접촉하면서 거래가 시작된다(S411). 이때 자동화기기(200)가 디바이스(300)에 내장된 nfc 칩등을 인식할 수도 있고, 서로 근거리 통신을하여 인식을 할 수도 있다.

[0154] 그리고 나서 자동화기기(200)의 제어부(230)는 고객 비밀번호(PIN)를 입력받는다.

[0155] 그리고 자동화기기(200)의 제어부(230)는 제1난수(R1)를 생성하고 내부의 저장부(250)에 저장하고, 디바이스(300)로 제1난수와 고객비밀번호(R1, PIN)를 전송한다(S412).

[0156] 다음, 디바이스(300)의 제어부(330)는 암호화된 고객 개인키(dE)를 고객 비밀번호(PIN)으로 복호화하여 고객 개인키(d)를 추출한다.

[0157] d=DEC_S(PIN, dE)

[0158] 그리고, 디바이스(300)의 제어부(330)는 제1난수(R1)를 고객 개인키(d)로 암호화하여 제1암호문(D1)을 생성한다.

[0159] D1=ENC(N, d, R1)

[0160] 그리고 나서, 디바이스(300)의 제어부(330)는 아이디와 제1 암호문(ID, D1)을 서버(110)로전송한다(S413).

[0161] 그러면, 서버(110는 디바이스(300)로부터 수신된 제1암호문(D1)를 고객 공개키(ID)로 복호화하여 제2난수(R2)을 추출한다.

[0162] R2=DEC(N, ID, D1)

[0163] 그리고 서버(110)는 제2난수(R2)를 공개키로 하여 제2난수 개인키(r)을 생성한다.

[0164] r=GEN(R2, ∅)

[0165] 다음, 서버(110)는 제2난수(R2)를 제2난수 개인키(r)로 암호화하여 제2암호문(D2)을 생성한다.

[0166] D2=ENC(N, r, R2)

[0167] 그리고 서버(110)는 생성된 제2 암호문(D2)을 디바이스(300)로 전송한다(S414).

[0168] 그러면, 디바이스(300)는 서버(110)로부터 수신된 제2암호문(D2)를 자동화기기에 전송한다(S415).

[0169] 다음, 자동화기기(200)는 제1난수(R1)을 공개키로 하여 제2암호문(D2)를 복호화하고 제3난수(R3)을 추출한다.

[0170] R3=DEC(N, R1, D2)

[0171] 그리고 추출된 제3난수(R3)가 제1난수(R1)과 일치하면, 자동화기기(200)는 자동화기기 거래를 허용한다(S416).

[0172] 상기 과정에서 ENC_S(K, d)는 대칭키 암호의 일례로서 AES, SEED, 3DES등 다양한 대칭키 암호를 사용할 수 있다.

[0173] 그리고, DEC_S(K, dE)는 대칭키 복호의 일례로서 ENC_S에서 사용한 동일한 대칭키 암호를 사용할 수 있다.

[0174] ENC_S와 DEC_S의 관계를 보면 dE=ENC_S(K, d) 이면 d=DEC_S(K, dE)의 관계가 있다.

[0175] 또 다른 실시예에 대하여 설명하면 다음과 같다.

[0176] 도 7은 본 발명의 제4 실시예에 따른 비대칭키를 이용한 무선구간 인증 시스템의 구성도이다.

[0177] 제4 실시예에서는 디바이스(300)에 ID와 p'만 저장해둔다.

[0178] 도 7을 참조하면, 본 발명의 제4 실시예에 따른 비대칭키를 이용한 무선구간 인증 시스템은, 서버(110), 블록체인 처리부, 자동화기기(200)를 포함한다.

[0179] 이러한 구성은 제1 실시예와 유사하며, 블록체인 처리부(500)가 추가되었으며, 서버(110)에서 암호화된 계좌번호 정보를 블록체인에 등록하고 자동화기기(200)에서 확인하는 방식이다.

[0180] 이러한 제4 실시예에 따른 비대칭키를 이용한 무선구간 인증 시스템의 동작을 설명하면 다음과 같다.

[0181] 도 8은 본 발명의 제4 실시예에 따른 비대칭키를 이용한 무선구간 인증 방법의 동작 시스템의 동작 흐름도이다.

[0182] 이용 기기 등록 절차는 제1 실시예와 동일하므로 상세한 설명은 생략한다.

[0183] 도 8를 참조하면, 고객은 디바이스(300)로 무선통신을 통해 자동화기기(300)와 통신을 연결하고, 자동화기기(200)는 디바이스(300)의 전용ID를 읽어온다(S500).

[0184] 그리고 고객이 자동화기기(200)의 안내에 따라 PIN을 입력하면 자동화기기(200)는 정당 PIN 인증 및 서버(110)에 등록된 출금계좌번호를 가져오기 위해 랜덤값 R을 생성하고, R을 공개키인 전용ID와 PIN(P)으로 이중 암호화하여 디바이스(300)로 전송한다(S510). 이때 전송값은 C=ENC(ENC(R,ID),P)이다.

[0185] 그러면, 고객의 디바이스(300)는 내부에 저장된 공개키P에 대한 개인키p'로 수신한 C값을 일차 복호화하여 이차 암호화값(D)을 서버(110)로 전송한다(S520). 이때의 전송값(D)는 다음과 같다.

[0186] D=ENC(R,ID)

[0187] 그러면, 서버(110)는 전달된 디바이스 고유값을 내부의 데이터베이스(120)에 저장된 디바이스 고유값과 비교한다.

[0188] 비교결과 등록된 디바이스(300)로 판단될 경우, 서버(110)는 데이터베이스(120)의 인터넷뱅킹 원장에 저장된 전용ID에 해당하는 출금계좌번호(A)를 추출하고, 공개키인 전용ID에 해당하는 개인키 d로 디바이스(300)에서 전송된 D값을 이차복호화하여 R을 추출한다.

[0189] 그리고 나서, 서버(110)는 블록체인에 저장된 전용ID에 해당하는 출금계좌번호(A)와 블록체인 저장주소(H)를 개인키 d로 H,R을 암호화하여 디바이스(300)로 전송한다(S530).

[0190] 이때 전송값(S)는 다음과 같다. S=ENC(HllR,d)

[0191] 다음, 디바이스(300)는 서버(110)에서 전송된 S를 자동화기기(200)로 전송한다(S540).

[0192] 그러면, 자동화기기(200)는 디바이스(300)에서 전달된 S를 ID로 검증하여 H, R을 추출하고 추출된 R값이 최초에 생성한 R값과 같고 H, R이 추출되면, 블록체인 처리부에서 B를 가져와 전용ID로 복호화 후 출금계좌번호(A)를 추출하여 자동화기기(200) 거래를 허용한다(S550).

[0193] 한편, 추출된 R값이 최초에 생성한 R값과 다를 경우 자동화기기(200)는 에러메시지 출력한다.

[0194] 본 발명의 실시예에서는 인가된 고객만 자동화기기(200) 거래가 가능하여 가용성이 강화되며, 자동화기기(200)에 별도의 키를 저장하지 않아 기존 대칭키방식보다 보안성이 강화하고, 대칭키를 저장하기 위한 별도 H/W가 필요하지 않아 비용절감 및 서비스 확장이 용이하고, 디바이스(300)와 자동화기기(200)간 데이터전달 프로세스가 단순해지는 효과가 있다.

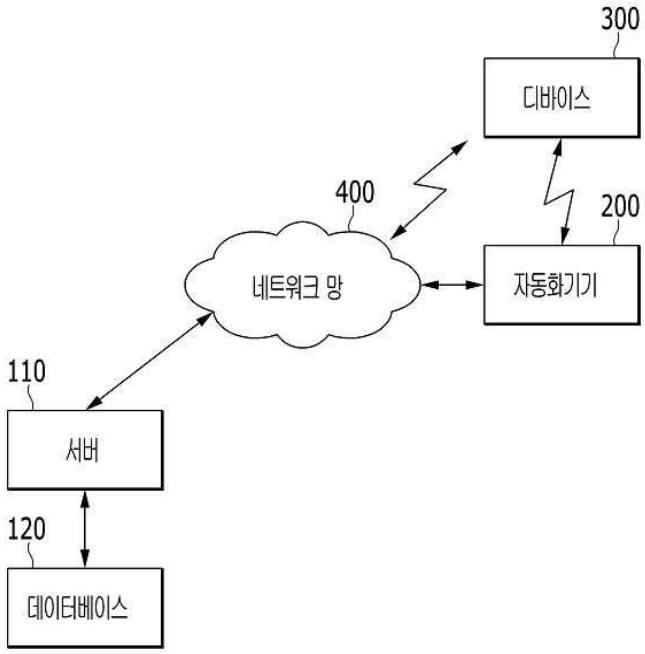
[0195] 또한, 본 발명의 실시예에서는 계좌이체기반 결제시스템에서도 응용이 가능하여 향후 다양한 무선환경에서 체크/신용 카드등의 발급 없이도 간편하고 안전한 방식으로 계좌기반 금융거래가 가능하다.

[0196] 이상에서 설명한 본 발명의 실시예는 장치 및 방법을 통해서만 구현이 되는 것은 아니며, 본 발명의 실시예의 구성에 대응하는 기능을 실현하는 프로그램 또는 그 프로그램이 기록된 기록 매체를 통해 구현될 수도 있으며, 이러한 구현은 앞서 설명한 실시예의 기재로부터 본 발명이 속하는 기술분야의 전문가라면 쉽게 구현할 수 있는 것이다.

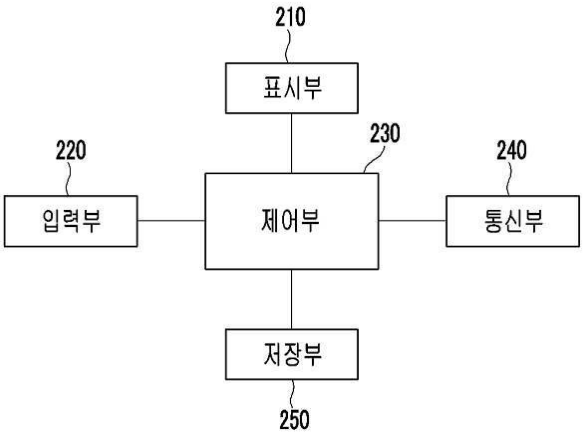
[0197] 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

도면

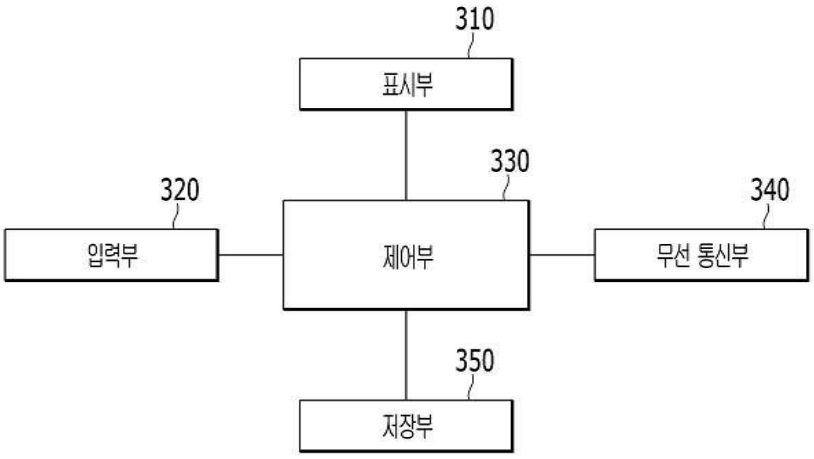
도면1


300
디바이스
400
200
네트워크 망
자동화기기
110
서버
120
데이터베이스

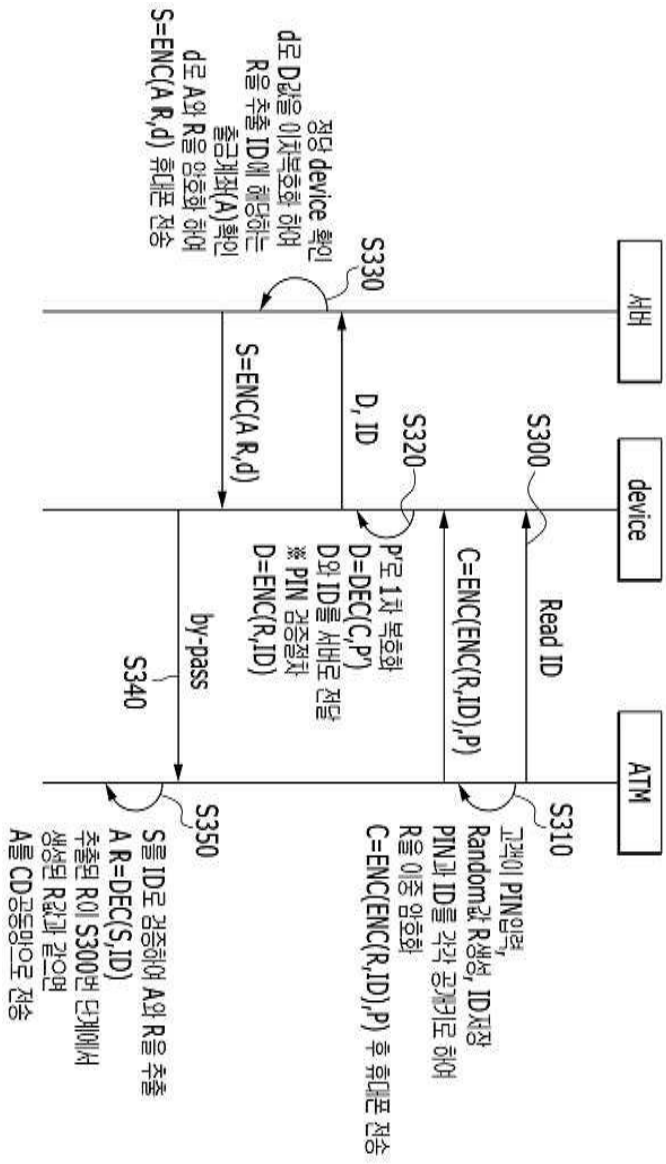
도면2


210
표시부
230
220
240
입력부
제어부
통신부
저장부
250

도면3


310
표시부
330
320
340
입력부
제어부
무선 통신부
350
저장부

도면4


서버
device
ATM
S330
정당 device 확인
d로 D값을 이차복호화 하여
R을 추출 ID에 해당하는
출금계좌(A)확인
d로 A와 R을 암호화 하여
S=ENC(A R,d) 휴대폰 전송
S=ENC(A R,d)
D, ID
S320
P'로 1차 복호화
D=DEC(C,P')
D와 ID를 서버로 전달
※ PIN 검증절차
D=ENC(R,ID)
S300
C=ENC(ENC(R,ID),P)
Read ID
by-pass
S340
S310
고객이 PIN입력, P
Random값 R생성, ID저장
PIN과 ID를 각각 공개키로 하여
R을 이중 암호화
C=ENC(ENC(R,ID),P) 후 휴대폰 전송
S350
S을 ID로 검증하여 A와 R을 추출
A R=DEC(S,ID)
추출된 R이 S300번 단계에서
생성된 R값과 같으면
A를 CD공동망으로 전송

도면5

서버	디바이스	자동화기기
	<고객이 자동화기기의 휴대폰거래 메뉴를 선택하고 디바이스를 자동화기기에 접촉하면서 거래가 시작됨> (S401)	
		<제1난수(R1) 생성> <제1난수(R1) 저장> ← R1 전송 (S401)
	<제1난수(R1)를 고객 개인키(d)로 암호화하여 제1암호문(D1) 생성> D1=ENC(N, d, R1) ← ID, D1 전송 (S403)	
<디바이스로부터 수신된 제1암호문(D1)를 고객 공개키(ID)로 복호화하여 제2난수(R2)을 추출> R2=DEC(N, ID, D1) <서버는 제2난수(R2)를 공개키로 하여 제2난수 개인키(r)을 생성> r=GEN(R2, ø) <서버는 제2난수(R2)를 R2=DEC(N, ID, D1) D2 전송 → (S404)		
	<디바이스는 서버로부터 수신된 제2암호문(D2)를 자동화기기에 전송> D2 전송 → (S405)	
		<자동화기기는 제1난수(R1)을 공개키로 하여 제2암호문(D2)를 복호화하고 제3난수(R3)을 추출> R3=DEC(N, R1, D2) <추출된 제3난수(R3)가 제1난수(R1)과 일치하면 자동화기기 거래를 허용> (S406)

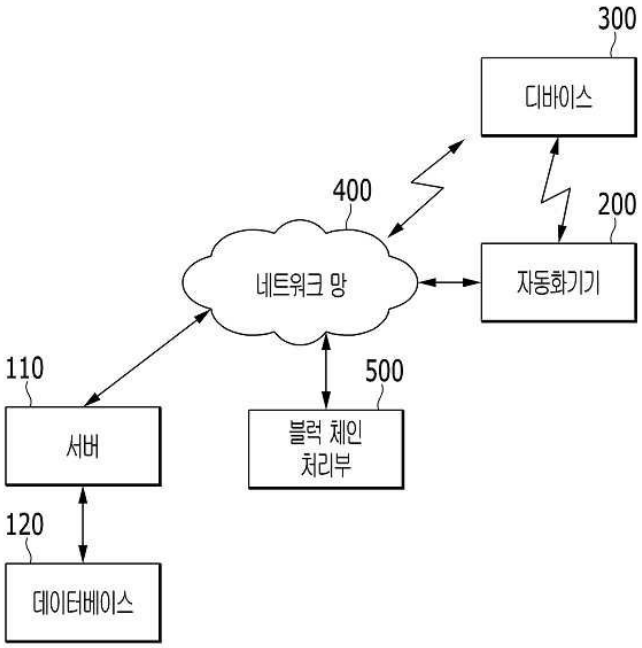
도면6a

서버	디바이스	자동화기기
	고객이 지정한 비밀번호(PIN)으로 암호화된 고객 개인키=dE dE=ENC_S(PIN, d) <고객이 자동화기기의 휴대폰거래 메뉴를 선택하고 디바이스를 자동화기기에 접촉하면서 거래가 시작됨> (S411)	
		<고객 비밀번호(PIN) 입력> <제1난수(R1) 생성> <제1난수(R1) 저장> ← R1, PIN 전송 (S412)
	<암호화된 고객 개인키(dE)를 고객 비밀번호(PIN)으로 복호화하여 고객 개인키(d)를 추출> d=DEC_S(PIN, dE) <제1난수(R1)를 고객 개인키(d)로 암호화하여 제1암호문(D1) 생성> D1=ENC(N, d, R1) ← ID, D1 전송 (S413)	
<디바이스로부터 수신된 제1암호문(D1)를 고객 공개키(ID)로 복호화하여 제2난수(R2)을 추출> R2=DEC(N, ID, D1) <서버는 제2난수(R2)를 공개키로 하여 제2난수 개인키(r)을 생성> r=GEN(R2, ø) <서버는 제2난수(R2)를 제2난수 개인키(r)로 암호화하여 제2암호문(D2) 생성> D2=ENC(N, r, R2) D2 전송 → (S414)		

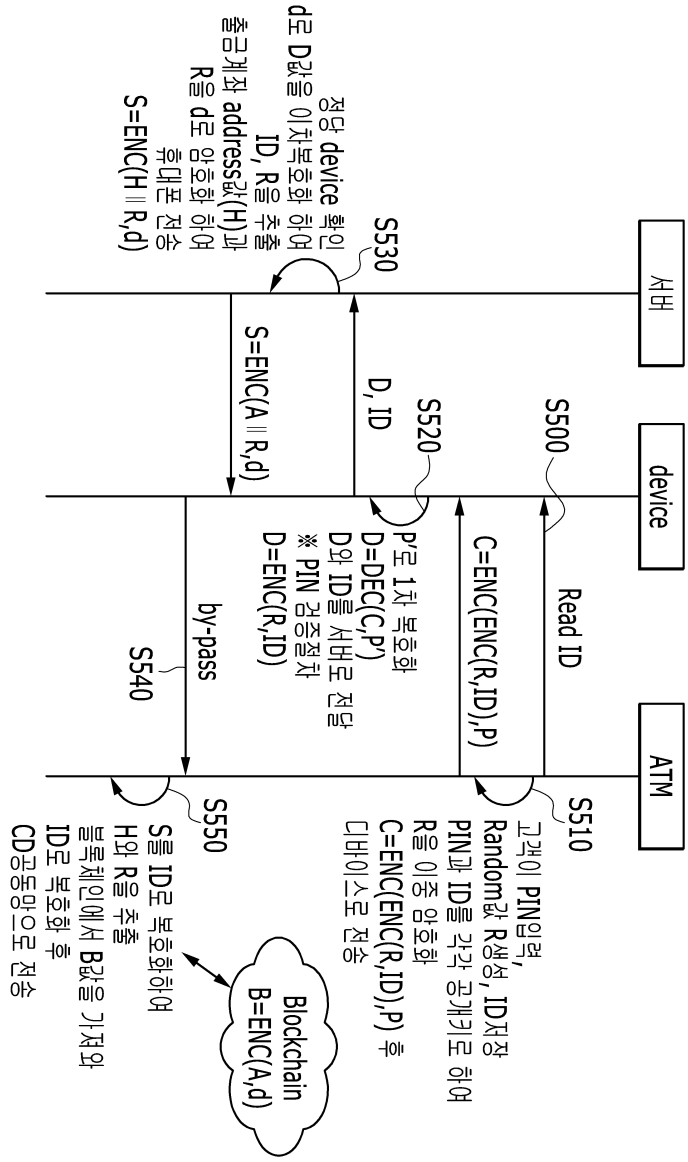
도면6b

	<디바이스는 서버로부터 수신된 제2암호문(D2)를 자동화기기에 전송> D2 전송 → (S415)	
		<자동화기기는 제1난수(R1)을 공개키로 하여 제2암호문(D2)를 복호화하고 제3난수(R3)을 추출> R3=DEC(N, R1, D2) <추출된 제3난수(R3)가 제1난수(R1)과 일치하면 자동화기기 거래를 허용> (S416)

도면7



도면8


서버
device
ATM
S530
정당 device 확인
d로 D값을 이차복호화 하여
ID, R을 추출
출금계좌 address값(H)과
R을 d로 암호화 하여
휴대폰 전송
S=ENC(H‖R,d)
S=ENC(A‖R,d)
D, ID
S520
P'로 1차 복호화
D=DEC(C,P')
D와 ID를 서버로 전달
※ PIN 검증절차
D=ENC(R,ID)
S500
C=ENC(ENC(R,ID),P)
Read ID
S540
by-pass
S510
고객이 PIN입력,
Random값 R생성, ID저장
PIN과 ID를 각각 공개키로 하여
R을 이중 암호화
C=ENC(ENC(R,ID),P) 후
디바이스로 전송
S550
S을 ID로 복호화하여
H와 R을 추출
블록체인에서 B값을 가져와
ID로 복호화 후
CD공동망으로 전송
Blockchain
B=ENC(A,d)