(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0022194
(43) 공개일자 2020년03월03일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *G06Q 20/38* (2012.01)
G06Q 20/40 (2012.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
H04L 9/321 (2013.01)
G06Q 20/38215 (2013.01)
(21) 출원번호 10-2018-0098034
(22) 출원일자 2018년08월22일
심사청구일자 2018년08월22일

(71) 출원인
엔에이치엔한국사이버결제 주식회사
서울특별시 구로구 디지털로26길 72 (구로동)
(72) 발명자
이창주
서울특별시 서초구 반포대로5길 54, 2층 (서초동)
(74) 대리인
특허법인 신지

전체 청구항 수 : 총 22 항

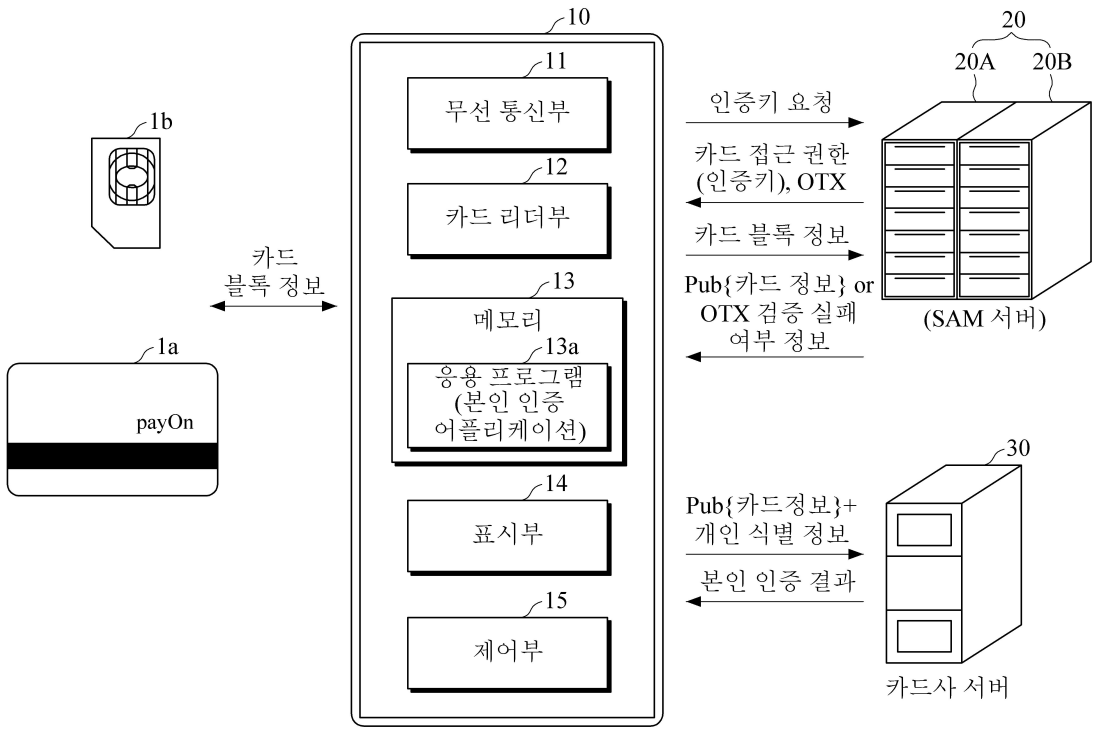
(54) 발명의 명칭 **사용자가 소지한 금융 카드 기반 본인 인증 시스템 및 방법**

(57) 요 약

본 발명은 사용자가 소지한 금융 카드 기반 본인 인증 시스템으로, 타 어플리케이션으로부터 본인 인증 요청 신호를 수신함에 따라 구동되는 본인 인증 어플리케이션에 의해 금융 카드의 접근 가능한 정보를 독출하여 보안 응용 모듈(Secure Application Module: 이하 'SAM'로 기재함) 서버로 전송한 후, SAM 서버로부터 OTX 및 사용자가

(뒷면에 계속)

대 표 도



소지한 금융 카드에 기록된 카드 블록 정보의 접근 권한인 인증키를 획득하고, 획득한 인증키 및 OTX를 이용하여 금융 카드로부터 근거리 무선 통신 기능을 통해 독출한 암호화된 카드 블록 정보를 SAM 서버에 전송하고, SAM 서버로부터 제1 공개키에 의해 암호화된 카드 정보를 수신함에 따라 금융 카드를 발급한 카드사 서버에 전송하여 본인 인증 요청하는 이동 통신 단말과, 이동 통신 단말로부터 전송된 암호화된 카드 블록 정보를 수신함에 따라, OTX 검증이 성공함에 따라 암호화된 카드 블록 정보를 복호화하고, 복호화된 카드 블록 정보로부터 추출된 카드 번호 및 유효 기간을 포함하는 카드 정보를 해당 금융 카드를 발급한 카드사에서 배포한 제1 공개키로 암호화하여 이동 통신 단말에 전송하는 SAM 서버와, 이동 통신 단말로부터 제1 공개키로 암호화된 카드 정보를 제1 공개키와 쌍을 이루는 제1 비밀키를 이용하여 복호화하고, 카드 정보를 고객 데이터베이스와 비교하여 본인 인증한 결과를 이동 통신 단말로 통보하는 카드사 서버를 포함한다.

(52) CPC특허분류

G06Q 20/4018 (2013.01)
H04L 9/0825 (2013.01)
H04L 9/0866 (2013.01)
H04L 9/0877 (2013.01)
H04L 9/3226 (2013.01)
H04L 2209/38 (2013.01)
H04L 2209/56 (2013.01)

명 세 서

청구범위

청구항 1

타 어플리케이션으로부터 본인 인증 요청 신호를 수신함에 따라 구동되는 본인 인증 어플리케이션에 의해 금융 카드의 접근 가능한 정보를 독출하여 보안 응용 모듈(Secure Application Module: 이하 'SAM'로 기재함) 서버로 전송한 후, SAM 서버로부터 카드 블록 정보의 복호화 유효성 검증을 위한 OTX 및 사용자가 소지한 금융 카드에 기록된 카드 블록 정보의 접근 권한인 인증키를 획득하고, 획득한 인증키를 이용하여 금융 카드로부터 근거리 무선 통신 기능을 통해 독출한 암호화된 카드 블록 정보 및 OTX를 SAM 서버에 전송하고, SAM 서버로부터 제1 공개키에 의해 암호화된 카드 정보를 수신함에 따라 금융 카드를 발급한 카드사 서버에 전송하여 본인 인증 요청하고, 카드사 서버로부터 수신된 본인 인증 결과를 타 어플리케이션으로 회신하는 이동 통신 단말과,

인증키를 제공받은 이동 통신 단말로부터 전송된 암호화된 카드 블록 정보 및 OTX를 수신함에 따라, OTX 검증을 수행하여 OTX 검증이 성공함에 따라 암호화된 카드 블록 정보를 복호화하고, 복호화된 카드 블록 정보로부터 추출된 카드 번호 및 유효 기간을 포함하는 카드 정보를 해당 금융 카드를 발급한 카드사에서 배포한 제1 공개키로 암호화하여 이동 통신 단말에 전송하는 SAM 서버와,

이동 통신 단말로부터 제1 공개키로 암호화된 카드 정보를 수신함에 따라, 카드 정보를 제1 공개키와 쌍을 이루는 제1 비밀키를 이용하여 복호화하고, 카드 정보를 고객 데이터베이스와 비교하여 본인 인증한 결과를 이동 통신 단말로 통보하는 카드사 서버를 포함하는 사용자가 소지한 금융 카드 기반 본인 인증 시스템.

청구항 2

제1 항에 있어서, SAM 서버는

인증키 및 OTX를 생성하여 발급하는 인증 서버와,

카드 블록 정보를 복호화하는 암호화 서버를 포함하되,

암호화 서버는

카드 블록 정보 및 OTX가 수신됨에 따라, 인증 서버에 OTX 검증을 요청하고,

인증 서버는

검증 요청된 OTX가 자신이 발급한 OTX인지를 검증하여, 검증 결과를 암호화 서버에 회신하는 사용자가 소지한 금융 카드 기반 본인 인증 시스템.

청구항 3

제1 항에 있어서, SAM 서버는

OTX 검증이 실패함에 따라 이동 통신 단말에 본인 인증 불가 메시지를 전송하고,

이동 통신 단말은

본인 인증 불가 메시지를 타 어플리케이션으로 전송하는 사용자가 소지한 금융 카드 기반 본인 인증 시스템.

청구항 4

제2 항에 있어서, 인증 서버는

OTX 검증이 완료되면, OTX를 삭제하는 사용자가 소지한 금융 카드 기반 본인 인증 시스템.

청구항 5

제2 항에 있어서, 인증 서버는

OTX에 기록된 생성시간을 체크하여 OTX 생성시간으로부터 일정시간이 경과되었을 경우, OTX 검증 실패 결과를 회신하는 사용자가 소지한 금융 카드 기반 본인 인증 시스템.

청구항 6

제1 항에 있어서, 이동 통신 단말은

사용자의 개인 식별 번호(Personal Identification Number: PIN)를 추가 획득하고, 개인 식별 정보를 카드 정보와 함께 카드사 서버에 전송하여 추가 인증 요청하고,

카드사 서버는

카드 정보와 함께 개인 식별 번호가 추가 수신됨에 따라, 이를 추가 인증하는 카드사 서버를 포함하는 사용자가 소지한 금융 카드 기반 본인 인증 시스템.

청구항 7

제6항에 있어서, 개인 식별 번호는

사용자의 주민 번호 또는 사용자가 소지한 휴대 단말의 번호인 사용자가 소지한 금융 카드 기반 본인 인증 시스템.

청구항 8

제1항에 있어서, 이동 통신 단말은

제1 공개키에 의해 암호화된 카드 정보를 이동 통신 단말만이 보유한 제2 비밀키로 추가 암호화하여 카드사 서버에 전송하여 본인 인증 요청하고,

카드사 단말은

추가 암호화된 카드 정보를 제2 비밀키와 쌍을 이루는 제2 공개키로 복호화한 후, 제1 비밀키로 복호화하는 사용자가 소지한 금융 카드 기반 본인 인증 시스템.

청구항 9

제1항에 있어서, 이동 통신 단말은

사용자로부터 입력받은 본인 인증 허용 시간을 카드사 서버에 전송하여 미리 등록하고,

카드사 서버는

사용자별로 미리 설정된 본인 인증 허용 시간을 등록하고, 본인 인증 요청 수신시, 해당 사용자의 본인 인증 허용 시간을 검출하고, 본인 인증 허용 시간을 기반으로 본인 인증 요청이 유효한지를 판단하고, 본인 인증 요청이 유효하지 않을 경우 본인 인증 불가 메시지를 이동 통신 단말에 전송하는 사용자가 소지한 금융 카드 기반 본인 인증 시스템.

청구항 10

근거리 무선 통신 기능이 탑재된 이동 통신 단말에서 실행되는 본인 인증 어플리케이션에서 구현되는 사용자가 소지한 금융 카드 기반 본인 인증 방법에 있어서,

타 어플리케이션으로부터 본인 인증 요청 신호가 수신됨에 따라 금융 카드의 접근 가능한 정보를 독출하여 보안 응용 모듈(Secure Application Module: 이하 'SAM'로 기재함) 서버에 전송하는 단계와,

SAM 서버로부터 카드 블록 정보의 복호화 유효성 검증을 위한 OTX 및 사용자가 소지한 금융 카드에 기록된 카드 블록 정보의 접근 권한인 인증키를 획득하는 단계와,

획득된 인증키를 이용하여 금융 카드에 기록된 암호화된 카드 블록 정보를 근거리 무선 통신 기능 기능을 통해 독출하는 단계와,

독출된 암호화된 카드 블록 정보 및 OTX를 SAM 서버에 전송하는 단계와,

SAM 서버로부터 금융 카드를 발급한 카드사에서 배포한 제1 공개키로 암호화된 카드 번호 및 유효 기간을 포함하는 카드 정보를 수신함에 따라, 금융 카드를 발급한 카드사 서버에 전송하여 본인 인증 요청하는 단계와,

카드사 서버로부터 회신된 본인 인증 결과를 타 어플리케이션으로 회신하는 단계를 포함하는 사용자가 소지한 금융 카드 기반 본인 인증 방법.

청구항 11

제10 항에 있어서, 본인 인증 요청하는 단계는

사용자의 개인 식별 번호(Personal Identification Number: PIN)를 추가 획득하고, 개인 식별 정보를 카드 정보와 함께 카드사 서버에 전송하여 추가 인증 요청하는 단계를 포함하는 사용자가 소지한 금융 카드 기반 본인 인증 방법.

청구항 12

제11항에 있어서, 개인 식별 번호는

사용자의 주민 번호 또는 사용자가 소지한 휴대 단말의 번호인 사용자가 소지한 금융 카드 기반 본인 인증 방법.

청구항 13

제10항에 있어서, 본인 인증 요청하는 단계는

암호화키 분배 서버로부터 이동 통신 단말만이 보유할 암호화키인 제2 비밀키를 미리 분배받는 단계와,

제1 공개키에 의해 암호화된 카드 정보를 이동 통신 단말만이 보유한 제2 비밀키로 추가 암호화하는 단계를 더 포함하는 사용자가 소지한 금융 카드 기반 본인 인증 방법.

청구항 14

제10항에 있어서,

사용자로부터 입력받은 본인 인증 허용 시간을 카드사 서버에 전송하여 미리 등록하는 단계를 더 포함하는 사용자가 소지한 금융 카드 기반 본인 인증 방법.

청구항 15

제 10항에 있어서,

SAM 서버로부터 OTX 검증이 실패함에 따른 본인 인증 불가 메시지를 수신함에 따라, 본인 인증 불가 메시지를 타 어플리케이션으로 전송하는 단계를 더 포함하는 사용자가 소지한 금융 카드 기반 본인 인증 방법.

청구항 16

보안 응용 모듈(Secure Application Module : 이하 'SAM'로 기재함) 서버에서의 사용자가 소지한 금융 카드 기반 본인 인증 방법에 있어서,

이동 통신 단말로부터 금융 카드의 접근 가능한 정보와 함께 금융 카드에 기록된 카드 블록 정보의 접근 권한인 인증키 발급이 요청됨에 따라, 이동 통신 단말로부터 전송된 정보를 통해 사용자를 인증한 후 이동 통신 단말로 카드 블록 정보의 복호화 유효성 검증을 위한 OTX 및 인증키를 제공하는 단계와,

이동 통신 단말로부터 OTX 및 암호화된 카드 블록 정보가 전송됨에 따라, OTX 검증을 수행하는 단계와,

OTX 검증이 성공할 경우, 암호화된 카드 블록 정보를 복호화하는 단계와,

복호화된 카드 블록 정보로부터 카드 번호 및 유효 기간을 포함하는 카드 정보를 추출하는 단계와,

추출된 카드 정보를 해당 금융 카드를 발급한 카드사에서 배포한 제1 공개키로 암호화하는 단계와,

암호화된 카드 정보를 이동 통신 단말에 전송하는 단계를 포함하는 사용자가 소지한 금융 카드 기반 본인 인증 방법.

청구항 17

제16항에 있어서,

OTX 검증이 실패할 경우, 이동 통신 단말에 복호화 불가 메시지를 전송하는 단계를 더 포함하는 사용자가 소지한 금융 카드 기반 본인 인증 방법.

청구항 18

제16항에 있어서, OTX 검증을 수행하는 단계는

검증 요청된 OTX가 자신이 발급한 OTX인지를 검증하는 사용자가 소지한 금융 카드 기반 본인 인증 방법.

청구항 19

제16항에 있어서, OTX 검증을 수행하는 단계는

OTX 검증이 완료되면, OTX를 삭제하는 사용자가 소지한 금융 카드 기반 본인 인증 방법.

청구항 20

제16항에 있어서, OTX 검증을 수행하는 단계는

OTX에 기록된 생성시간을 체크하여 OTX 생성시간으로부터 일정시간이 경과되었을 경우, OTX 검증 실패 결과를 회신하는 사용자가 소지한 금융 카드 기반 본인 인증 방법.

청구항 21

제 10항 내지 15항 중 어느 한 항에 기재된 사용자가 소지한 금융 카드 기반 본인 인증 방법을 수행하는 본인 인증 어플리케이션이 소프트웨어 상태로 프로그램화되어 저장되는 메모리를 포함하거나, 하드웨어 상태로 사용

자가 소지한 금융 카드 기반 본인 인증 방법을 수행하는 프로세스 정보가 저장된 칩으로 구성되어, 자체 구비된 프로세싱 PC의 CPU를 통해 메모리에 저장되거나 칩으로 구성된 사용자가 소지한 금융 카드 기반 본인 인증 방법을 수행하는 이동 통신 단말.

청구항 22

보안 응용 모듈(Secure Application Module: SAM)이 소프트웨어 상태로 프로그램화되어 메모리에 저장되거나, 하드웨어 상태로 보안 응용 모듈(Secure Application Module: SAM) 정보가 저장된 칩으로 구성되어, 자체 구비된 프로세싱 PC의 CPU를 통해 별도의 무선 통신 수단을 통해 이동 통신 단말을 통해 무선 통신을 수행함으로써, 제16항 내지 제20항 중 어느 한 항에 기재된 사용자가 소지한 금융 카드 기반 본인 인증 방법을 처리하는 보안 응용 모듈(Secure Application Module: SAM) 서버.

발명의 설명

기 술 분 야

[0001] 본 발명은 본인 인증 기술에 관한 것으로, 특히 사용자가 소지한 금융 카드 기반 본인 인증 시스템 및 방법에 관한 것이다.

배 경 기 술

[0003] 현재 유무선통신 기술의 발달과, 언제 어디서나 유무선통신망에 접속할 수 있는 휴대통신단말기들의 발달로 유비쿼터스 컴퓨팅 환경이 구축되었다.

[0004] 이와 같이 유비쿼터스 컴퓨팅 환경이 구축됨에 따라 오프라인상에 수행되던 무수히 많은 일들이 온라인으로 이루어지고 있다. 그 중 대표적인 것들로는 은행의 인터넷뱅킹 및 모바일 뱅킹, 공공기관의 주민등록등본 발급, 쇼핑몰 등의 온라인 본인 인증 등이 될 수 있을 것이다.

[0005] 그러나 온라인상에서 어떠한 행위를 하기 위해서는 그 행위를 하는 주체가 그 행위의 정당한 주체인지를 판단하여야 한다.

[0006] 이러한 주체, 즉 사용자 본인인지를 확인하기 위한 본인인증이 필요하게 되어 다양한 방식의 본인인증 방식들이 개발되어 적용되고 있다. 이러한 본인인증 방식으로는 지식기반 인증 방식, 생체기반 인증 방식 및 소지기반 인증 방식 등이 있을 수 있을 것이다.

[0007] 지식기반 인증 방식으로는 아이디 및 패스워드 인증 방식, 개인식별번호(Personal Identification Number:PIN) 인증 방식 및 아이핀 인증방식 등이 있다. 그리고 생체기반 인증 방식으로는 지문, 음성, 홍채 및 정맥 인식 등을 이용한 인증 방식들이 있다. 또한, 소지기반 인증 방식으로는 일회용 패스워드(One Time Password: OTP) 인증 방식, 핸드폰, 휴대폰 및 스마트폰으로 불리는 이동 통신 단말을 이용한 SMS 승인번호 인증 방식 및 ARS 인증 방식 등이 있다.

[0008] 이 중 보안성이 높은 소지기반 인증 방식이 많이 적용되고 있으나, ARS 인증 방식의 경우 인증 시점에서 사용자의 소지로 간주되는 유무선 전화기가 도용될 가능성이 있고, OTP 인증 방식은 분실 시 도용될 수 있으며, 이동통신 단말을 이용한 SMS 인증 또한, 메모리 해킹을 통해 승인번호가 유출될 수 있는 문제점이 있다.

발명의 내용

해결하려는 과제

[0010] 따라서, 이러한 문제점을 해결하기 위해 보다 더 강력한 보안성이 있으면서도 간편하게 인증을 수행할 수 있는 인증 방식으로, 이동 통신 단말의 근거무선통신(Near Field Communication: NFC)을 이용하여 사용자들이 소지하는 금융카드의 접촉에 의한 카드 대면 인증과, 금융카드의 고유 식별정보(Unique ID: UID) 및 개인식별번호(Personal Identification Number: PIN)를 이용하여 카드정보의 노출없이 본인인증의 보안성을 높이면서도 본인

인증을 간편하게 수행할 수 있는 본인 인증 시스템 및 방법을 제공한다.

과제의 해결 수단

[0012] 본 발명은 카드사 서버를 포함하는 사용자가 소지한 금융 카드 기반 본인 인증 시스템으로, 타 어플리케이션으로부터 본인 인증 요청 신호를 수신함에 따라 구동되는 본인 인증 어플리케이션에 의해 금융 카드의 접근 가능한 정보를 독출하여 보안 응용 모듈(Secure Application Module: 이하 'SAM'로 기재함) 서버로 전송한 후, SAM 서버로부터 OTX 및 사용자가 소지한 금융 카드에 기록된 카드 블록 정보의 접근 권한인 인증키를 획득하고, 획득한 인증키 및 OTX를 이용하여 금융 카드로부터 근거리 무선 통신 기능을 통해 독출한 암호화된 카드 블록 정보를 SAM 서버에 전송하고, SAM 서버로부터 제1 공개키에 의해 암호화된 카드 정보를 수신함에 따라 금융 카드를 발급한 카드사 서버에 전송하여 본인 인증 요청하고, 카드사 서버로부터 수신된 본인 인증 결과를 타 어플리케이션으로 회신하는 이동 통신 단말과, OTX 및 인증키를 제공받은 이동 통신 단말로부터 전송된 암호화된 카드 블록 정보를 수신함에 따라, OTX 검증을 수행하고, OTX 검증이 성공함에 따라 암호화된 카드 블록 정보를 복호화하고, 복호화된 카드 블록 정보로부터 추출된 카드 번호 및 유효 기간을 포함하는 카드 정보를 해당 금융 카드를 발급한 카드사에서 배포한 제1 공개키로 암호화하여 이동 통신 단말에 전송하는 SAM 서버와, 이동 통신 단말로부터 제1 공개키로 암호화된 카드 정보를 수신함에 따라, 카드 정보를 제1 공개키와 쌍을 이루는 제1 비밀키를 이용하여 복호화하고, 카드 정보를 고객 데이터베이스와 비교하여 본인 인증한 결과를 이동 통신 단말로 통보하는 카드사 서버를 포함한다.

[0013] 본 발명은 근거리 무선 통신 기능이 탑재된 이동 통신 단말에서 실행되는 본인 인증 어플리케이션에서 구현되는 사용자가 소지한 금융 카드 기반 본인 인증 방법으로, 근거리 무선 통신 기능이 탑재된 이동 통신 단말에서 실행되는 본인 인증 어플리케이션에서 구현되는 사용자가 소지한 금융 카드 기반 본인 인증 방법에 있어서, 타 어플리케이션으로부터 본인 인증 요청 신호가 수신됨에 따라 금융 카드의 접근 가능한 정보를 독출하여 보안 응용 모듈(Secure Application Module: 이하 'SAM'로 기재함) 서버에 전송하는 단계와, SAM 서버로부터 OTX 및 사용자가 소지한 금융 카드에 기록된 카드 블록 정보의 접근 권한인 인증키를 획득하는 단계와, 획득된 OTX 및 인증키를 이용하여 금융 카드에 기록된 암호화된 카드 블록 정보를 근거리 무선 통신 기능 기능을 통해 독출하는 단계와, 독출된 암호화된 카드 블록 정보를 SAM 서버에 전송하는 단계와, SAM 서버로부터 금융 카드를 발급한 카드사에서 배포한 제1 공개키로 암호화된 카드 번호 및 유효 기간을 포함하는 카드 정보를 수신함에 따라, 금융 카드를 발급한 카드사 서버에 전송하여 본인 인증 요청하는 단계와, 카드사 서버로부터 회신된 본인 인증 결과를 타 어플리케이션으로 회신하는 단계를 포함한다.

[0014] 본 발명은 보안 응용 모듈(Secure Application Module : 이하 'SAM'로 기재함) 서버에서의 사용자가 소지한 금융 카드 기반 본인 인증 방법으로, 이동 통신 단말로부터 금융 카드의 접근 가능한 정보와 함께 금융 카드에 기록된 카드 블록 정보의 접근 권한인 인증키 발급이 요청됨에 따라, 이동 통신 단말로부터 전송된 정보를 통해 사용자를 인증한 후 이동 통신 단말로 OTX 및 인증키를 제공하는 단계와, 이동 통신 단말로부터 암호화된 카드 블록 정보가 전송됨에 따라, OTX 검증을 수행하는 단계와, OTX 검증이 성공할 경우, 암호화된 카드 블록 정보를 복호화하는 단계와, 복호화된 카드 블록 정보로부터 카드 번호 및 유효 기간을 포함하는 카드 정보를 추출하는 단계와, 추출된 카드 정보를 해당 금융 카드를 발급한 카드사에서 배포한 제1 공개키로 암호화하는 단계와, 암호화된 카드 정보를 이동 통신 단말에 전송하는 단계를 포함한다.

발명의 효과

[0016] 본 발명은 이동 통신 단말의 NFC를 이용하여 사용자가 소지한 금융카드의 접촉에 의해 획득되는 금융카드 정보에 의해 금융카드 소지기반의 금융카드 대면 인증을 수행함으로써 보안성을 높일 수 있는 효과를 갖는다.

[0017] 본 발명은 금융카드의 대면 인증을 위한 금융카드의 카드정보 획득 시 보안응용모듈(Secure Application Module: SAM) 서버를 이용하여 금융카드의 유효성 검사 및 카드정보의 암호화 통신을 수행하므로 보안성을 향상시킬 수 있는 효과를 갖는다.

도면의 간단한 설명

[0019] 도 1은 본 발명의 일 실시 예에 따른 사용자가 소지한 금융 카드 기반 본인 인증 시스템의 구성을 나타낸 도면이다.

도 2는 본 발명의 일 실시 예에 따른 카드사 서버의 블록 구성도이다.

도 3은 본 발명의 일 실시 예에 따른 사용자가 소지한 금융 카드 기반 본인 인증 방법을 설명하기 위한 신호 흐름도이다.

도 4는 본 발명의 다른 실시 예에 따른 사용자가 소지한 금융 카드 기반 본인 인증 방법을 설명하기 위한 신호 흐름도이다.

도 5는 본 발명의 실시 예에 따라 SAM 서버에서 이동 통신 단말로 인증키가 제공되는 과정을 설명하기 위한 신호 흐름도이다.

도 6은 본 발명의 또 다른 실시 예에 따른 카드사 서버의 인증 방법을 설명하기 위한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0020] 이하 첨부된 도면을 참조하여, 바람직한 실시 예에 따른 사용자가 소지한 금융 카드 기반 본인 인증 시스템 및 방법에 대해 상세히 설명하면 다음과 같다. 여기서, 동일한 구성에 대해서는 동일부호를 사용하며, 반복되는 설명, 발명의 요지를 불필요하게 흐릴 수 있는 공지 기능 및 구성에 대한 상세한 설명은 생략한다. 발명의 실시형태는 당업계에서 평균적인 지식을 가진 자에게 본 발명을 보다 완전하게 설명하기 위해서 제공되는 것이다. 따라서, 도면에서의 요소들의 형상 및 크기 등은 보다 명확한 설명을 위해 과장될 수 있다.

[0021] 첨부된 블록도의 각 블록과 흐름도의 각 단계의 조합들은 컴퓨터 프로그램인스트럭션들(실행 엔진)에 의해 수행될 수도 있으며, 이들 컴퓨터 프로그램 인스트럭션들은 범용 컴퓨터, 특수용 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서에 탑재될 수 있으므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서를 통해 수행되는 그 인스트럭션들이 블록도의 각 블록 또는 흐름도의 각 단계에서 설명된 기능들을 수행하는 수단을 생성하게 된다.

[0022] 이들 컴퓨터 프로그램 인스트럭션들은 특정 방식으로 기능을 구현하기 위해 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 지향할 수 있는 컴퓨터 이용가능 또는 컴퓨터 판독 가능 메모리에 저장되는 것도 가능하므로, 그 컴퓨터 이용가능 또는 컴퓨터 판독 가능 메모리에 저장된 인스트럭션들은 블록도의 각 블록 또는 흐름도의 각 단계에서 설명된 기능을 수행하는 인스트럭션 수단을 내포하는 제조 품목을 생산하는 것도 가능하다.

[0023] 그리고 컴퓨터 프로그램 인스트럭션들은 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에 탑재되는 것도 가능하므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에서 일련의 동작 단계들이 수행되어 컴퓨터로 실행되는 프로세스를 생성해서 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 수행하는 인스트럭션들은 블록도의 각 블록 및 흐름도의 각 단계에서 설명되는 기능들을 실행하기 위한 단계들을 제공하는 것도 가능하다.

[0024] 또한, 각 블록 또는 각 단계는 특정된 논리적 기능들을 실행하기 위한 하나 이상의 실행 가능한 인스트럭션들을 포함하는 모듈, 세그먼트 또는 코드의 일부를 나타낼 수 있으며, 몇 가지 대체 실시 예들에서는 블록들 또는 단계들에서 언급된 기능들이 순서를 벗어나서 발생하는 것도 가능함을 주목해야 한다. 예컨대, 잇달아 도시되어 있는 두 개의 블록들 또는 단계들은 사실 실질적으로 동시에 수행되는 것도 가능하며, 또한 그 블록들 또는 단계들이 필요에 따라 해당하는 기능의 역순으로 수행되는 것도 가능하다.

[0025] 이하, 첨부 도면을 참조하여 본 발명의 실시 예를 상세하게 설명한다. 그러나 다음에 예시하는 본 발명의 실시 예는 여러 가지 다른 형태로 변형될 수 있으며, 본 발명의 범위가 다음에 상술하는 실시 예에 한정되는 것은 아니다. 본 발명의 실시 예는 당업계에서 통상의 지식을 가진 자에게 본 발명을 보다 완전하게 설명하기 위하여 제공된다.

[0027] 도 1은 본 발명의 일 실시 예에 따른 사용자가 소지한 금융 카드 기반 본인 인증 시스템의 구성을 나타낸 도면이다.

[0028] 도 1을 참조하면, 사용자가 소지한 금융 카드 기반 본인 인증 시스템은 사용자가 소지한 금융 카드(1a, 1b), 이동 통신 단말(10), 보안응용모듈(Secure Application Module: 이하 'SAM'이라 기재함) 서버(20) 및 카드사 서

버(30)를 포함한다.

[0029] 이동 통신 단말(10), SAM 서버(20) 및 카드사 서버(30)는 유무선 데이터 통신망(미도시)을 통해 연결될 것이다. 여기서, 유무선 데이터 통신망은 와이파이(WiFi)망이 포함된 인터넷망과, 3G(Third Generation) WCDMA 방식, 4세대(4Generation:4G=Long Term Evolution(LTE))망 및 5세대 이동통신(5Generation Networks)을 포함하는 이동통신망이 결합되어 있는 통신망이다.

[0030] 본 발명에 따른 사용자가 소지한 금융 카드 기반 본인 인증은 사용자에게 임의의 서비스를 제공하기 위해 기관, 업체 및 매장 등에서 본인 인증 이벤트가 발생됨에 따라 이루어진다. 여기서, 기관은 온라인 및 오프라인의 은행, 증권사 및 보험사 등의 금융기관, 동사무소, 구청, 시청, 금융본인 인증원 등과 같은 관공서 등이 될 수 있으며, 업체는 인터넷 쇼핑몰 운영 업체, 다수의 매장을 가지는 오프라인 업체 등이 될 수 있을 것이다.

[0031] 금융 카드(1a, 1b)는 일반적인 신용카드, 교통카드 등과 같이 이동 통신 단말(10)과 접촉 또는 비접촉식으로 연결되어 금융 서비스, 교통서비스 등을 수행할 수 있는 모든 종류의 카드를 포함한다. 일 예로, 실물 신용 카드(1a) 및 모바일 카드(1b) 등이 포함될 수 있는데, 이러한 금융 카드(1a, 1b)에는 1 이상의 칩(Chip)이 내장되어 있으며, 이동 통신 단말(10)와 근거리 무선통신에 의하여 비접촉식으로 연결되어 데이터를 주고 받을 수 있는 RF 방식의 카드일 수 있다. 여기서, 근거리 무선통신은 RF, 적외선 통신, PAN 통신, 블루투스 통신 등 제한이 없으나, NFC(Near Field Communication) 프로토콜을 따르는 통신 방식인 것이 바람직하다. 또한, 이러한 금융 카드(1a, 1b)의 칩 내부에는 OS(Operation System)(미도시) 및 저장공간(미도시)이 구비되고, 저장공간은 2 이상의 섹터로 구분되어 각 섹터에는 보안정도에 따른 계층적인 카드 관련 정보가 저장될 수 있다. 이동 통신 단말(10)로부터 RF 방식으로 인증키가 전달됨에 따라, 금융 카드(1a, 1b)의 칩 내부에는 OS(Operation System)는 인증키를 이용한 인증 알고리즘을 수행하여, 각 섹터들에 저장된 카드 관련 정보를 RF 방식으로 이동 통신 단말(10)로 전달하여 줄 수 있다. 이에 대한 상세한 설명은 도 5를 참조하여 후술하기로 한다.

[0032] 이동 통신 단말(10)은 금융 카드(1a, 1b)와 SAM 서버(20) 또는 카드사 서버(30)를 연결시켜 금융 카드 소지 기반의 본인 인증 채널을 제공하는 통신 단말기로서, 일반적인 휴대폰, 스마트 폰 등의 개인 무선 통신 단말기일 수 있으나 그에 한정되는 것은 아니다. 즉, 이동 통신 단말(10)은 이러한 개인의 무선 통신 단말기에 한정되는 것은 아니며, 카드에 접속하여 카드에 저장된 정보들을 이용하여 해당되는 서비스를 중개해주는 단말로서, 기존의 VAN 통신망과 연결된 일반적인 신용카드 단말기 등과 같이 기타 다른 형태의 모든 무선 카드 단말기 또는 동글 단말기일수도 있을 것이다.

[0033] 이러한 이동 통신 단말(10)에는 본 발명에 의한 금융 카드(1a, 1b)를 소지한 사용자의 본인 인증을 위한 본인 인증 어플리케이션이 응용 프로그램(13a)으로서 설치될 수 있다. 본 발명에 따라, 이동 통신 단말(10)은 SAM 서버(20) 및 카드사 서버(30) 등과 무선 인터넷 통신을 수행하는 무선 통신부(11), 근거리 무선 통신을 통해 금융 카드(1a, 1b)에 기록된 정보를 독출하는 카드 리더부(12), 본인 인증 어플리케이션을 포함하는 응용 프로그램이 저장되는 메모리부(13), 본인 인증 어플리케이션의 프로세스 진행 상태를 포함한 사용자 인터페이스 정보를 디스플레이하고, 사용자로부터 정보를 입력받을 수 있는 터치 스크린 형태의 표시부(14) 및 설치된 본인 인증 어플리케이션을 실행하여 SAM 서버(20) 또는 카드사 서버(30)와의 무선 인터넷 통신을 통해 금융카드(1a, 1b)를 이용한 본인 인증 과정을 순차적으로 진행하는 제어부(15)를 구비한다.

[0034] 구체적으로 이동 통신 단말(10)의 사용자는 본인 인증 어플리케이션(13a)을 다운로드해서 제어부(15)에 설치 및 등록하고, 본인 인증 어플리케이션(13a)을 통해 SAM 서버(20) 및 카드사 서버(30)와 연동하여 본인 인증 과정을 수행한다. 즉, 이동 통신 단말(10)에 인증키가 수신되면, 인증키를 이용하여 금융 카드(1a, 1b)에 접근하여 본인 인증이 진행될 수 있으며, 이러한 본인 인증시에는 근거리 무선 통신 리더부(12)를 통해 암호화된 형태의 RF 카드 정보 즉, 카드 블록 정보를 먼저 독출한다. 카드 블록 정보는 해당 신용카드를 인식 또는 식별하기 위한 코드 정보로써 SAM 서버(20)로 전송된다. 이 후, SAM 서버(20)로부터 카드 블록 정보에 대응되는 카드 정보들이 제1 공캐키로 암호화된 상태로 수신되면 제어부(15)는 암호화된 해당 카드 정보와 사용자의 개인 식별 정보를 카드사 서버(30)로 송신 및 본인 인증 승인을 요청할 수 있다.

[0035] 또한, 본 발명의 다른 실시 예에 따라, 이동 통신 단말(10)은 제1 공개키로 암호화된 카드 정보를 추가적으로 비대칭키 방식으로 암호화하되, 제2 비밀키로 암호화하여 전자 서명되도록 할 수도 있다. 제2 비밀키는 암호화키 분배 서버(미도시)로부터 본인만 소유하도록 분배되는 것으로, 제2 비밀키는 이동 통신 단말(10)만이 소유하고, 제2 비밀키와 쌍을 이루는 공개키는 불특정 다수에게 분배 가능하다.

[0036] 여기서, SAM 서버(20)는 SAM(Secure Application Module)이 적어도 하나의 칩(chip) 형태로 구비되어 하드웨어

상태로 구성될 수 있다. 그리고, SAM 서버(20)는 SAM이 소프트웨어 상태로 서버에 프로그램화되도록 구성될 수도 있으며, 이때 SAM 서버(20)는 자체 구비된 PC나 무선 통신 수단을 통해 카드 블록 정보 및 해당 카드 정보와 본인 인증 정보 송수신 과정 등을 자동 처리하게 된다.

[0037] 또한, 상세하게는 SAM 서버(20)는 이동 통신 단말(10)에 설치된 본인 인증 어플리케이션을 통해 가맹점이나 사용자 정보 인증을 수행하고 카드 접근 권한으로 인증키 및 추후 카드 블록 정보의 복호화 유효성 검증을 위한 OTX를 생성하여 전송하는 인증 서버(20A), 이동 통신 단말(10)로부터 암호화된 카드 블록 정보가 수신되면 이를 복호화하고, 복호화된 카드 블록 정보에 대응되는 카드 정보를 공개키로 암호화하여 이동 통신 단말(10)로 제공하는 부호화 서버(20B)를 구비한다.

[0038] 인증 서버(20A)는 이동 통신 단말(10)에서 금융 카드(1a, 1b) 본인 인증 처리가 이루어질 수 있도록 본인 인증 어플리케이션을 통해 사용자 정보를 인증하고, 카드 접근 권한인 인증키를 이동 통신 단말(10)로 공급한다. 또한, SAM 서버(20)는 이동 통신 단말(10)로부터 인증키 요청이 오면 인증서버(20A)에서 요청 시간을 이용하여 고유(Unique)한 값의 16byte OTX를 생성하고, 인증서버 DB(미도시)에 저장한다. 그런 후, 인증서버(20A)는 인증키와 생성한 OTX를 이동 통신 단말(10)로 전송한다.

[0039] 암호화 서버(20B)는 이동 통신 단말(10)로부터 카드 블록 정보가 수신되면, 카드 블록 정보를 복호화하여 카드 번호 및 유효 기간 등을 포함하는 카드 정보를 추출하고, 추출된 카드 정보를 암호화하여 이를 이동 통신 단말(10)에 되돌려 준다. 이때, 암호화 서버(20B)는 카드번호 복호화 요청을 받으면 이동 통신 단말(10)에서 수신한 OTX를 인증서버(20A)로 보내고, 인증서버(20A)는 OTX로 카드번호 복호화 요청이 유효한지를 검증한 후 결과를 암호화 서버(20B)로 회신한다.

[0040] 암호화 서버(20B)는 카드사 서버(30)에서 배포한 제1 공개키를 이용하여 카드 정보를 암호화한다. 즉, 본 발명에서는 암호화하는 키와 복호화할 때 사용하는 키가 상이한 비대칭키 암호화 방식을 사용하는데, 즉, 이는 타인에게 절대 노출되지 않는 비밀키(개인키)와 비밀키를 토대로 만든 공개키가 쌍을 이룬 형태이다. 본 발명에서 비밀키는 카드사 서버(30)가 보관하고, 공개키는 카드사 서버(30)에 의해 배포되어 부호화 서버(20B)에 의해 사용된다.

[0041] 카드사 서버(30)는 은행, 증권, 보험사 등의 다수의 서버들로 구성되는 서버 시스템이 될 수 있을 것이다. 카드사 서버(30)는 이동 통신 단말(10)로부터 본인인증 요청 정보를 수신하고, 본인인증 요청 신호에 포함된 카드정보와 사용자 식별정보에 대해 미리 등록되어 있는 카드정보를 비교하여 본인인증을 수행한 후, 본인인증 결과를 이동 통신 단말(10)로 제공한다.

[0042] 카드사 서버(30)는 도 3 내지 도 6을 참조하여 후술될 사용자가 소지한 금융 카드 기반 본인 인증 방법을 수행하는 본인 인증 어플리케이션이 소프트웨어 상태로 프로그램화되어 저장되는 메모리를 포함하거나, 하드웨어 상태로 사용자가 소지한 금융 카드 기반 본인 인증 방법을 수행하는 프로세스 정보가 저장된 칩으로 구성되어, 자체 구비된 프로세싱 PC의 CPU를 통해 메모리에 저장되거나 칩으로 구성될 수 있다.

[0043] 도 2는 본 발명의 일 실시 예에 따른 카드사 서버의 블록 구성도이다.

[0044] 도 2를 참조하면, 카드사 서버(30)는 복호화부(31), 고객 DB(32), 본인 인증 확인부(33) 및 메시지 발송 처리부(34)를 포함한다. 부가적으로, 인증 허용 시간 체크부(35) 및 인증 허용 시간 정보 DB(36)를 더 포함할 수 있다.

[0045] 복호화부(31)는 수신된 제1 공개키로 암호화된 카드 정보를 제1 비밀키로 복호화함과 아울러 개인 식별 정보를 대칭키로 복호화한다. 이때, 본 발명의 다른 실시 예에 따라, 카드 정보는 2차에 걸쳐 암호화되어 있을 수 있다. 즉, 카드 정보는 1차 암호화키인 제1 공개키로 암호화된 후, 2차 암호화키인 제2 비밀키로 암호화되어 있을 수 있다. 그러면, 복호화부(31)는 제2 비밀키와 쌍을 이루는 제2 공개키로 카드 정보를 1차 복호화한 후, 제1 비밀키로 2차 복호화하여 카드 정보를 획득한다. 즉, 제2 비밀키는 이동 통신 단말(10)만이 보유하는 것으로, 이와 같이 제2 비밀키로 카드 정보를 암호화하여 전송하고, 카드사 서버(30)가 이를 제2 공개키로 복호화하게 될 경우, 개인 인증 기능이 한층 강화될 수 있다. 왜냐하면, 제2 비밀키는 이동 통신 단말(10)만이 가지고 있기 때문이다.

[0046] 본인 인증 확인부(33)는 카드 정보 및 개인 식별 정보를 고객 DB(32)의 정보와 비교하여, 본인 인증을 수행한다. 고객 DB(32)에는 카드 발급 정보를 저장하는 것으로, 고객별 카드 정보 및 개인 식별 정보를 저장한다. 즉, 수신된 카드 정보 및 개인 식별 정보가 고객 DB(32)에 저장된 정보와 일치하는 경우, 본인 인증되는 것

으로 판단한다.

[0047] 메시지 발송 처리부(34)는 본인 인증 확인부(33)의 본인 인증 결과를 이동 통신 단말(10)에 통보한다.

[0048] 부가적으로, 인증 허용 시간 체크부(35)는 인증 허용 시간 정보 DB(36)을 검색하여, 복호화된 카드 정보 및 개인 식별 정보에 상응하는 고객이 설정한 인증 허용 시간 정보를 추출해낸다. 즉, 고객별로 사전에 본인 인증 시간을 설정해놓을 수 있다. 따라서, 설정해놓은 시간이 아닌 시간에 본인 인증이 요청되는 경우, 이는 부정한 본인 인증 요청으로 간주하여, 본인 인증 요청을 수행하지 않고, 대신에 메시지 발송부(34)를 통해 본인 인증 요청 불가 및 카드 정보 도용 경고 메시지가 전송되도록 한다. 이로써, 본인 인증의 보안성을 한층 강화시킬 수 있다.

[0049] 도 3은 본 발명의 일 실시 예에 따른 사용자가 소지한 금융 카드 기반 본인 인증 방법을 설명하기 위한 신호 흐름도이고, 도 4는 본 발명의 다른 실시 예에 따른 사용자가 소지한 금융 카드 기반 본인 인증 방법을 설명하기 위한 신호 흐름도이고, 도 5는 본 발명의 실시 예에 따라 SAM 서버에서 이동 통신 단말로 인증키 및 OTX가 제공되는 과정을 설명하기 위한 신호 흐름도이다.

[0050] 도 3 및 4를 참조하면, 우선 사용자가 요청한 임의의 서비스에 대한 본인 인증 이벤트가 발생에 따른 본인 인증 요청 신호가 수신됨(S101)에 따라, 이동 통신 단말(10)은 사용자에 의해 미리 다운로드되어 설치된 본인 인증 어플리케이션을 실행한다. 이러한 본인인증 요청은 사용자에게 임의의 서비스를 제공하기 위해 기관, 업체 및 매장 등에서 본인 인증 이벤트가 발생됨에 따라 이루어질 수 있다. 또한, 이러한 본인 인증 요청 신호는 이동 통신 단말(10)을 통해 기관, 업체 및 매장 등에서 실행되는 타 어플리케이션으로부터 발생되는 신호일 수 있다. 예컨대, 대학으로부터 성적 증명서 발급 서비스를 제공받을 경우, 증명서 발급 어플리케이션으로부터 본인 인증 요청 신호가 발생될 수 있고, 쇼핑 결제 서비스를 제공받을 경우, 해당 업체의 결제 어플리케이션으로부터 본인 인증 요청 신호가 발생될 수 있다.

[0051] 이동 통신 단말(10)은 SAM 서버(20)와의 무선 통신으로 본인 인증 어플리케이션을 인증 요청하여 사용자 정보가 인증되도록 한다. 이때, SAM 서버(20)는 이동 통신 단말(10)에 설치된 본인 인증 어플리케이션(13a)을 통해 사용자 정보를 인증하고, 카드 블록 정보를 리딩할 수 있는 인증키를 공급한다(S102). 인증키는 금융 카드(1a, 1b)에서 사용자 인증정보가 저장된 저장공간으로의 접속을 가능하게 보안 접속키일 수 있다. 이때, SAM 서버(20)는 OTX를 생성하여 이동 통신 단말(10)에 인증키와 함께 전달한다. 여기서, OTX는 인증서버(20A)에서 생성하며, 카드번호 복호화 요청건에 대한 유효성 검증을 위해 사용된다. 즉, OTX는 복호화 요청건의 유효성, 카드 블록 정보의 재사용 및 저장 후 사용하는 것을 방지하기 위한 용도로 사용된다. 본 발명에 따른 인증키 및 OTX 제공의 실시 예에 대해 도 5를 참조하여 설명하기로 한다.

[0052] 도 5를 참조하면, 이동 통신 단말(10)은 근거리 무선 통신 리더부(12)를 구동하여, 금융카드(1a, 1b)의 고유 식별정보(Unique ID: UID) 또는 칩 시리얼 번호(Chip Serial Number : CSN)를 획득하여 카드정보를 읽을 준비를 한다(S210). 상세하게는, 본인 인증 어플리케이션의 실행에 의해 구동되어 근거리 무선 통신 리더부(12)를 활성화시킨 후, 표시부(14)를 통해 금융카드(1a, 1b)를 접촉시킬 것을 요청하는 메시지를 표시하고, 이에 응답하여 금융카드(1a, 1b)가 근거리 무선 통신 리더부(12)에 접촉되면 근거리 무선 통신 리더부(12)를 통해 고유 식별정보(Unique ID: UID) 또는 칩 시리얼 번호(Chip Serial Number : CSN)를 획득할 수 있다. 여기서, 고유 식별정보(Unique ID: UID) 또는 칩 시리얼 번호(Chip Serial Number : CSN)는 별도의 인증키 없이 이동 통신 단말(10)이 RF 방식으로 읽어들일 수 있는 정보로, 4 byte의 정보일 수 있다.

[0053] 이동 통신 단말(10)은 UID 또는 CSN을 SAM 서버(20)에 전송하여 1차 인증키를 요청한다(S220). 그러면, SAM 서버(20)는 UID 또는 CSN를 가지는 금융카드(1a, 1b)를 통해 위조 여부 등을 검증하여 1차 인증키를 이동 통신 단말(10)에 제공한다(S230). 여기서, 1차 인증키는 6 byte의 정보일 수 있다. 그러면, 이동 통신 단말(10)은 근거리 무선 통신 리더부(12)를 구동하여 SAM 서버(20)로부터 제공된 1차 인증키를 이용하여 금융 카드(1a, 1b)로부터 카드 정보 중 제1 섹터(1st sector) 정보를 독출한다(S240). 즉, 금융카드(1a, 1b)는 이동 통신 단말(10)로부터 1차 인증키가 RF 방식으로 수신됨에 따라, 해당 1차 인증키가 정당할 경우 저장 공간에 저장된 제1 섹터 정보를 이동 통신 단말(10)로 전달하여 준다.

[0054] 그런 후, 이동 통신 단말(10)은 금융 카드(1a, 1b)의 제1 섹터(1st sector) 정보를 SAM 서버(20)에 전송하여 2차 인증키를 요청한다(S250). 그러면, SAM 서버(20)는 제1 섹터(1st sector) 정보를 인증하고, 암호화된 카드 블록 정보에 접근 권한을 갖는 2차 인증키를 이동 통신 단말(10)에 전송한다(S260). 이때, SAM 서버(20)의 인증서버(20A)는 인증키 요청 시간을 이용하여 고유(Unique)한 값인 16byte OTX를 생성하고, 인증서버 DB(미도시)에

저장한다. 그런후, 인증 서버(20A)는 생성한 OTX를 2차 인증키를 이동 통신 단말(10)에 전송한다(S260).

[0055] 다시 도 3 및 4를 참조하면, 이동 통신 단말(10)의 사용자의 인증 처리가 수행된 후에는 SAM 서버(20)로부터 카드 접근 권한인 인증키를 이용해 사용자가 직접 금융 카드(1a, 1b)를 이동 통신 단말(10)에 태깅하면, 이동 통신 단말(10)은 근거리 무선 통신 리더부(12)를 카드 블록 정보를 독출한다(S110). 여기서, 인증키는 도 5에서 획득된 2차 인증키일 수 있다. 여기서, 카드 블록 정보는 암호화된 정보이다. 이동 통신 단말(10)은 무선 통신부(11)를 통해 카드 블록 정보를 SAM 서버(20)로 전송한다(S120). 이때, 이동 통신 단말(10)은 S102 단계에서 수신한 OTX를 함께 전송한다.

[0056] 그러면, SAM 서버(20)의 암호화 서버(20B)는 카드 블록 정보를 복호화하기 전에, 이동 통신 단말(10)로부터 전송된 OTX로 카드 블록 정보 복호화 요청건에 대한 유효성 검증을 수행한다(S121~S125).즉, 암호화 서버(20B)는 인증 서버(20A)에 OTX 검증 요청한다(S121). 그러면, 인증 서버(20A)는 OTX로 카드번호 복호화 요청이 유효한지를 검증 (S122)한 후, OTX 검증 결과를 회신한다(S123). 즉, 인증 서버(20A)는 이동 통신 단말(10)에서 검증 요청한 OTX가 인증서버(20A)에서 발급한 OTX인지 검증한다. 이때, OTX 검증이 완료되면 인증서버 DB에 저장된 OTX는 삭제되기 때문에 한 번 사용한 OTX는 재사용이 되지 않는다. 또한, OTX에 있는 생성시간을 체크하여 일정시간(예컨대, 3분)이 지난 복호화 요청은 거절하도록 검증 실패 결과를 회신할 수 있다.

[0057] S123에서 전송된 OTX 검증 결과가 실패일 경우, 암호화 서버(20B)는 본인 인증 불가 메시지를 이동 통신 단말(10)에 전송한다(S125). 그러면, 이동 통신 단말(10)는 본인 인증 불가 메시지를 본인 인증을 요청한 타 어플리케이션에 전송함(S126)하고, 본인 인증 과정을 종료된다.

[0058] 반면, S123에서 전송된 OTX 검증 결과가 성공일 경우, 암호화 서버(20B)는 카드 블록 정보를 복호화한다(S130). 그런 후, SAM 서버(20)는 복호화된 카드 블록 정보 중에서 본인 인증을 위한 카드 정보를 추출(S135)하여, 금융 카드(1a, 1b)를 발급한 카드사 서버(30)에 의해 배포된 제1 공개키를 이용하여 추출된 카드 정보를 암호화한다(S140). 여기서, 카드 정보는 카드 번호 및 유효 기간을 포함할 수 있다. 그런 후, SAM 서버(20)는 카드 정보를 제1 공개키로 암호화된 상태로 이동 통신 단말(10)에 전송한다(S150).

[0059] 도 3에 도시된 본 발명의 일 실시 예에 따라, 이동 통신 단말(10)은 암호화된 상태로 수신된 카드 정보를 수신함에 따라, 암호화된 카드 정보와 함께 개인 식별 번호(Personal Identification Number: PIN)를 카드사 서버(30)에 전송하여 본인 인증을 요청한다(S160, S170).

[0060] 즉, 이동 통신 단말(10)은 개인 식별 번호를 입력할 것을 요청하는 메시지를 표시하고, 입력 수단을 통해 입력되는 PIN을 획득하여 암호화한다(S160). 여기서, 사용자 식별정보는 사용자 이름, 생년월일, 주민등록번호, 이동 통신 단말 전화번호 등 중 하나 이상이 될 수 있으나, 생년월일 또는 이동 통신 단말 전화번호인 것이 바람직할 것이다. 여기서, 이동 통신 단말(10)과 사용자가 소지한 휴대 단말은 동일할 수도 있고, 이동 통신 단말(10)이 가맹점에 설치된 단말기일 경우 사용자가 소지한 휴대 단말은 이동 통신 단말(10)과 상이할 수도 있다.

[0061] 한편, 도 4에 도시된 본 발명의 다른 실시 예에 따라, 이동 통신 단말(10)은 제1 공개키로 암호화된 카드 정보를 추가적으로 제2 비밀키로 암호화할 수 있다(S155). 이를 위해, 이동 통신 단말(10)은 사전에 암호화키 분배 서버(미도시)로부터 이동 통신 단말만이 보유할 암호화키인 제2 비밀키를 미리 분배받아 둘 수 있다. 제2 비밀키는 암호화키 분배 서버(미도시)로부터 본인만 소유하도록 분배되는 것으로, 제2 비밀키는 이동 통신 단말(10)만이 소유하고, 제2 비밀키와 쌍을 이루는 제2 공개키는 불특정 다수에게 분배 가능하다. 즉, 현재의 신용카드 등은 실물 카드 자체를 불법적으로 취득한 경우, 취득자가 신용카드를 사용하여 불법적으로 결제하는 것이 가능하므로, 카드 분실시 그의 불법적인 사용을 막을 방법이 존재하지 않는다. 따라서, 이를 통해 카드 소지자의 본인 인증을 강화시킬 수 있다.

[0062] 또한, 도 3에 도시된 본 발명의 일 실시 예에 따라, 본인인증 요청 신호를 수신한 카드사 서버(30)는 본인인증 요청 신호에 포함된 카드 정보를 제1 비밀키로 복호화한다(S180). 상세하게는, 제1 공개키로 복호화된 카드 정보를 제1 공개키와 쌍을 이루는 제2 비밀키로 복호화한다. 한편, 도 4에 도시된 본 발명의 다른 실시 예에 따라, 카드 정보는 2차에 걸쳐 암호화되어 있을 수 있다. 즉, 카드 정보는 1차 암호화키인 제1 공개키로 암호화된 후, 2차 암호화키인 제2 비밀키로 암호화되어 있을 수 있다. 그러면, 복호화부(31)는 제2 비밀키와 쌍을 이루는 제2 공개키로 카드 정보를 1차 복호화(S175)한 후, 제1 비밀키로 2차 복호화하여 카드 정보를 획득한다(S185). 즉, 제2 비밀키는 이동 통신 단말(10)만이 보유하는 것으로, 이와 같이 제2 비밀키로 카드 정보를 암호화하여 전송하고, 카드사 서버(30)가 이를 제2 공개키로 복호화하게 될 경우, 개인 식별 기능이 한층 강화될 수 있다. 왜냐하면, 제2 비밀키는 이동 통신 단말(10)만이 가지고 있기 때문이다. 이러한 제2 공개키는 암호화키

분배 서버(미도시)로부터 실시간으로 요청하거나, 고객 DB(32)에 카드 사용자의 개인 식별 정보와 함께 매칭되어 저장되어 있을 수 있다.

[0063] 카드사 서버(30)는 복호화된 카드 정보와 개인 식별 정보로 고객 DB(32)를 검색하여 본인 인증을 수행한다(S185). 이때, 카드사 서버(30)는 본인 인증을 수행함에 있어 미리 설정된 허용 타임 슬롯(time slot) 기반으로 본인 인증을 수행할 수 있는데, 이는 카드 정보 도용을 막기 위한 일종의 사이렌 서비스로, 이에 대한 상세한 설명은 도 5를 참조하여 후술하기로 한다.

[0064] 그런 후, 카드사 서버(30)는 이동 통신 단말(10)로 본인 인증 결과를 통보한다(S190). 이때, 본인인증 결과는 이동통신 메시지로 전송될 수 있을 것이다. 이때, 본인 인증 결과는 단문메시지서비스(Short Message Service: SMS), 장문메시지서비스(Long Message Service: LMS), 멀티미디어메시지서비스(Multimedia Message Service: MMS) 등과 같은 이동통신메시지, 푸시메시지 및 특정 어플 실행 요청 신호일 수 있을 것이다.

[0065] 그런 후, 이동 통신 단말(10)은 카드사 서버(30)로부터 수신한 본인 인증 결과를 타 어플리케이션에 회신(S195)하여, 본인 인증 프로세스 수행을 완료한다.

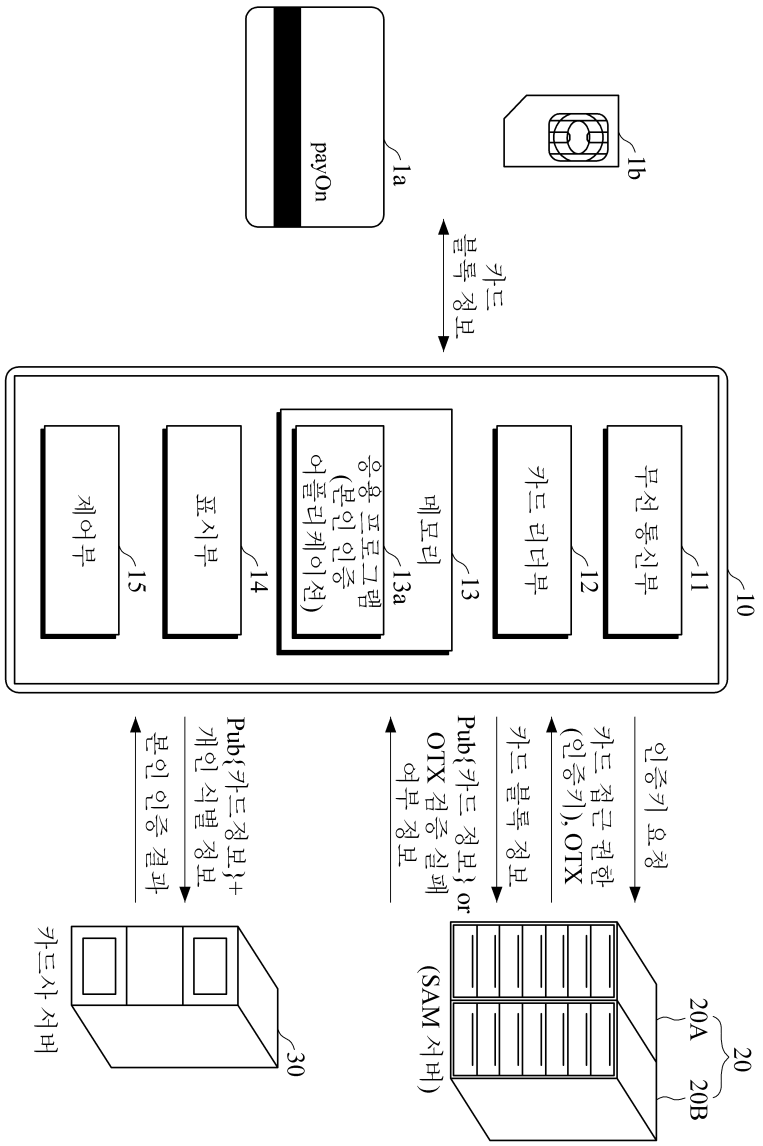
[0066] 도 6은 본 발명의 일 실시 예에 따른 카드사 서버에서의 고객 인증 방법을 설명하기 위한 순서도이다.

[0067] 도 6을 참조하면, 카드사 서버(30)의 인증 허용 시간 체크부(35)는 인증 허용 시간 정보 DB(36)을 검색하여, 복호화된 카드 정보 및 개인 식별 정보에 상응하는 고객이 설정한 인증 허용 시간 정보를 검색한다(S310). 이를 위해 카드사 서버(30)는 사용자로부터 입력받은 본인 인증 허용 시간을 카드사 서버에 전송하여 미리 등록받아 둘 수 있다. 즉, 고객별로 사전에 본인 인증 허용 시간을 설정해놓을 수 있다. 따라서, 카드사 서버(30)의 인증 허용 시간 체크부(35)는 설정해놓은 시간이 아닌 시간에 본인 인증이 요청되는 경우, 이는 부정한 본인 인증 요청으로 간주하여, 본인 인증 요청을 수행하지 않고, 대신에 메시지 발송부(34)를 통해 본인 인증 요청 불가 및 개인 정보 도용 경고 메시지가 전송되도록 한다(S340). 이로써, 본인 인증의 보안성을 한층 강화시킬 수 있다.

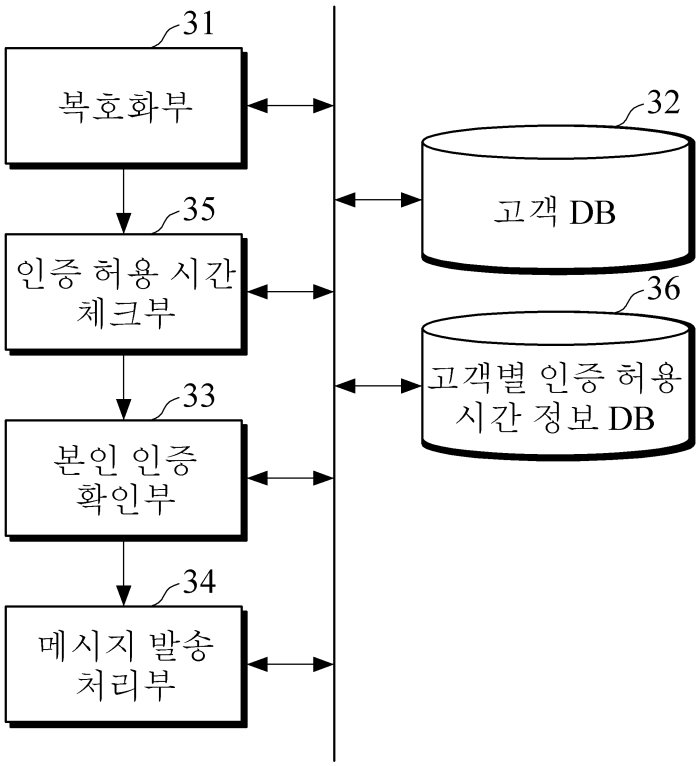
[0068] 반면, 고객이 설정해놓은 시간에 본인 인증이 요청된 경우, 카드사 서버(30)의 본인 인증 수행부(35)는 고객 DB(32)의 정보와 비교하여, 본인 인증을 수행한다(S350). S350의 판단 결과, 수신된 카드 정보 및 개인 식별 정보가 고객 DB(32)에 저장된 정보와 일치하는 경우, 본인 인증 확인된 것으로 판단하여, 카드사 서버(30)의 메시지 발송 처리부(34)는 본인 인증 확인 메시지를 발송한다(S380). 반면, S350의 판단 결과, 수신된 카드 정보 및 개인 식별 정보가 고객 DB(32)에 저장된 정보와 일치하지 않는 경우, 본인 인증 실패한 것으로 판단하여, 카드사 서버(30)의 메시지 발송 처리부(34)는 본인 인증 오류 메시지를 발송한다(S380).

도면

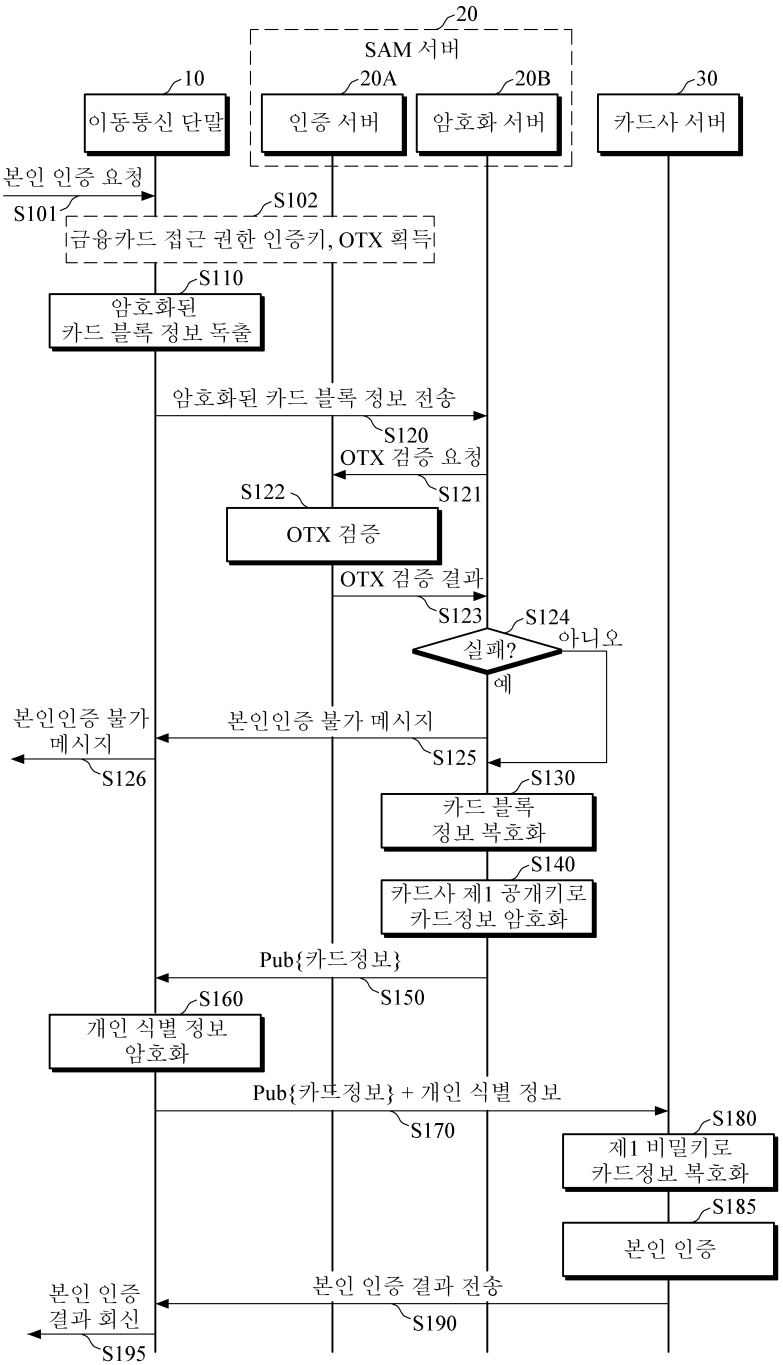
도면1


payOn
1a
1b
카드 블록 정보
10
무선 통신부
11
카드 리더부
12
메모리
13
응용 프로그램 (본인 인증 어플리케이션)
13a
표시부
14
제어부
15
인증키 요청
카드 접근 권한 (인증키), OTX
카드 블록 정보
Pub{카드 정보} or OTX 검증 실패 여부 정보
Pub{카드정보}+ 개인 식별 정보
본인 인증 결과
20
20A
20B
(SAM 서버)
카드사 서버
30

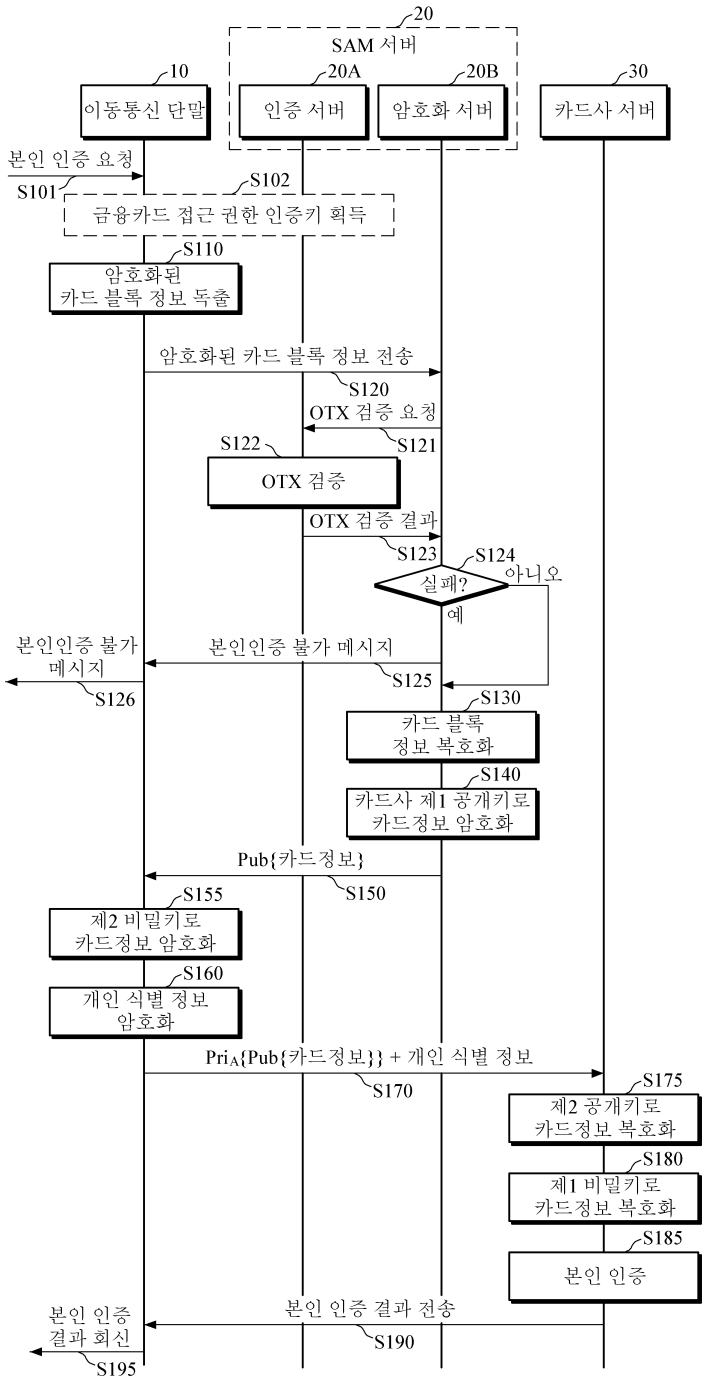
도면2


31
복호화부
32
고객 DB
35
인증 허용 시간 체크부
36
고객별 인증 허용 시간 정보 DB
33
본인 인증 확인부
34
메시지 발송 처리부

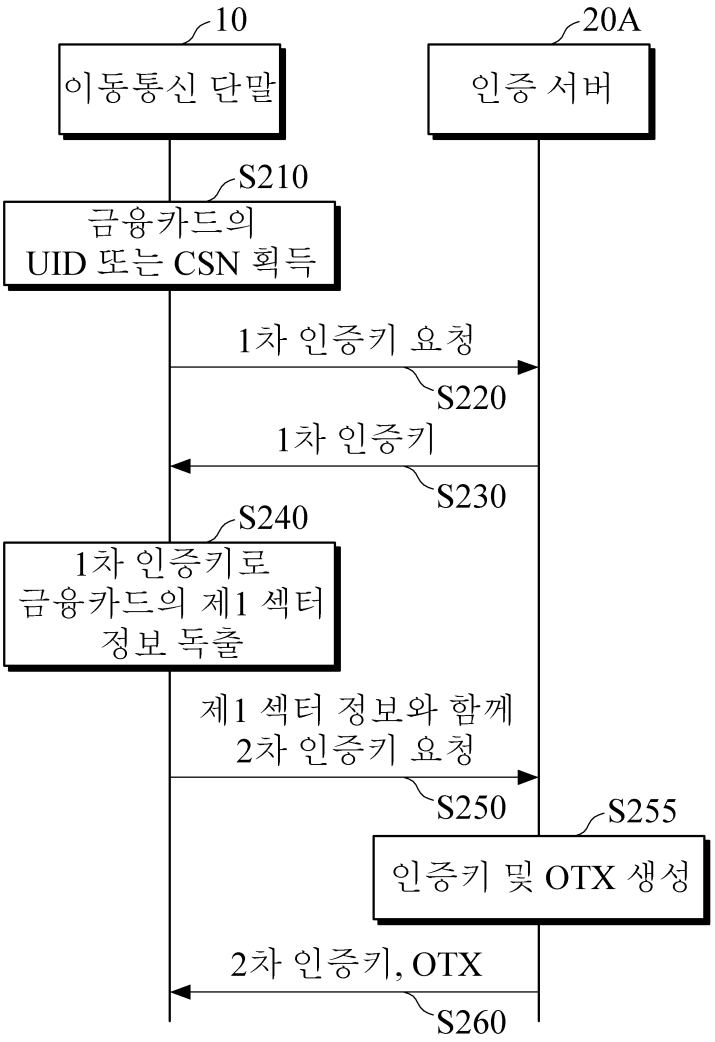
도면3


20
SAM 서버
10
이동통신 단말
20A
인증 서버
20B
암호화 서버
30
카드사 서버
본인 인증 요청
S101
S102
금융카드 접근 권한 인증키, OTX 획득
S110
암호화된
카드 블록 정보 독출
암호화된 카드 블록 정보 전송
S120
OTX 검증 요청
S121
S122
OTX 검증
OTX 검증 결과
S123
S124
실패?
아니오
예
본인인증 불가
메시지
본인인증 불가 메시지
S125
S126
S130
카드 블록
정보 복호화
S140
카드사 제1 공개키로
카드정보 암호화
Pub{카드정보}
S150
S160
개인 식별 정보
암호화
Pub{카드정보} + 개인 식별 정보
S170
S180
제1 비밀키로
카드정보 복호화
S185
본인 인증
본인 인증
결과 회신
본인 인증 결과 전송
S190
S195

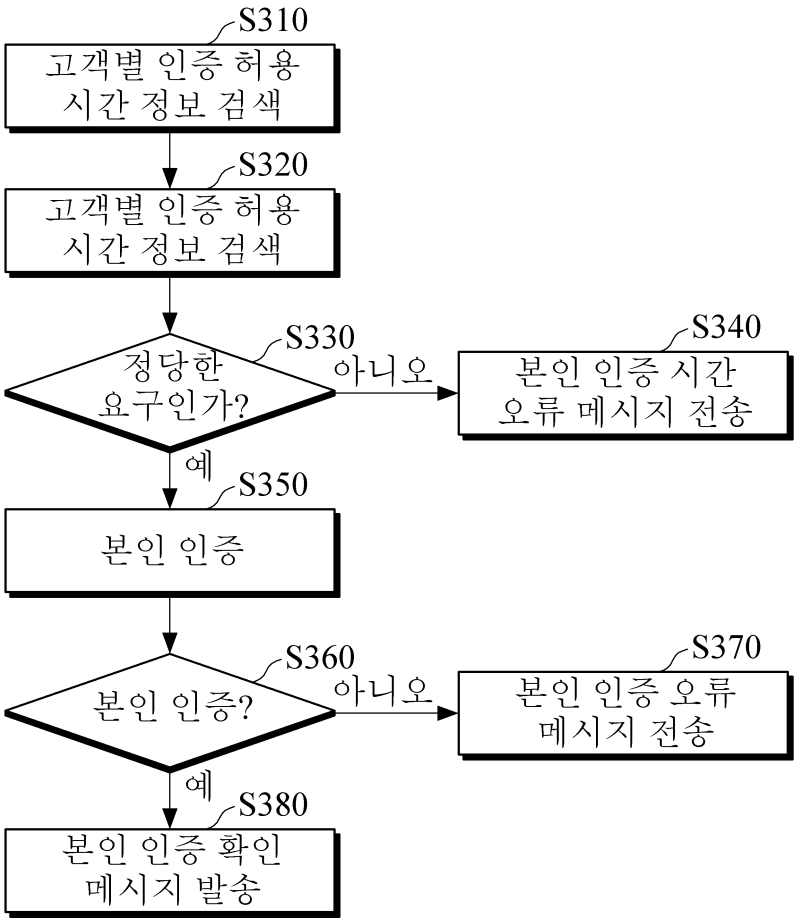
도면4


20
SAM 서버
10
이동통신 단말
20A
인증 서버
20B
암호화 서버
30
카드사 서버
본인 인증 요청
S101
S102
금융카드 접근 권한 인증키 획득
S110
암호화된
카드 블록 정보 독출
암호화된 카드 블록 정보 전송
S120
OTX 검증 요청
S121
S122
OTX 검증
OTX 검증 결과
S123
S124
실패?
아니오
예
본인인증 불가
메시지
본인인증 불가 메시지
S125
S126
S130
카드 블록
정보 복호화
S140
카드사 제1 공개키로
카드정보 암호화
Pub{카드정보}
S150
S155
제2 비밀키로
카드정보 암호화
S160
개인 식별 정보
암호화
Pri$_A${Pub{카드정보}} + 개인 식별 정보
S170
S175
제2 공개키로
카드정보 복호화
S180
제1 비밀키로
카드정보 복호화
S185
본인 인증
본인 인증 결과 전송
S190
본인 인증
결과 회신
S195

도면5


10
이동통신 단말
20A
인증 서버
S210
금융카드의
UID 또는 CSN 획득
1차 인증키 요청
S220
1차 인증키
S230
S240
1차 인증키로
금융카드의 제1 섹터
정보 독출
제1 섹터 정보와 함께
2차 인증키 요청
S250
S255
인증키 및 OTX 생성
2차 인증키, OTX
S260

도면6


S310
고객별 인증 허용 시간 정보 검색
S320
고객별 인증 허용 시간 정보 검색
S330
정당한 요구인가?
아니오
S340
본인 인증 시간 오류 메시지 전송
예
S350
본인 인증
S360
본인 인증?
아니오
S370
본인 인증 오류 메시지 전송
예
S380
본인 인증 확인 메시지 발송