(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년02월29일
(11) 등록번호 10-1113446
(24) 등록일자 2012년01월31일

(51) Int. Cl.
H04W 12/06 (2009.01) *G06F 21/20* (2006.01)
G06Q 20/00CO (2008.03)
(21) 출원번호 10-2010-0126795
(22) 출원일자 2010년12월13일
심사청구일자 2010년12월13일
(56) 선행기술조사문헌
JP2008134985 A
KR1020040076045 A
KR1020060118102 A
전체 청구항 수 : 총 24 항

(73) 특허권자
인하대학교 산학협력단
인천광역시 남구 인하로 100, 인하대학교 (용현동)
(72) 발명자
양대헌
인천광역시 남구 인하로 100, 인하대학교 하이테크센터 317호 (용현동)
(74) 대리인
특허법인무한

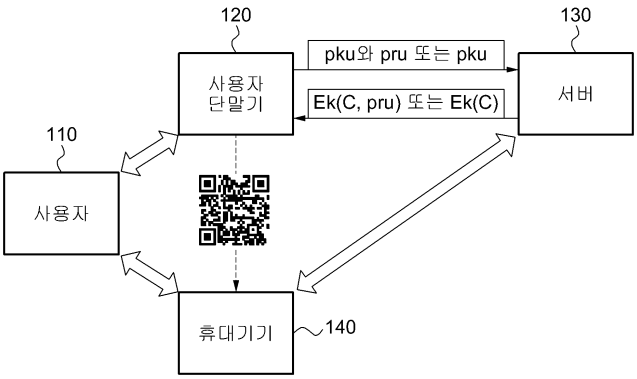
심사관 : 장상배

(54) 휴대기기에 공인인증서를 전송하는 시스템 및 방법 그리고 다차원 코드를 이용하여 데이터를 전송 및 인증하는 시스템 및 방법

(57) 요 약

휴대기기에 공인인증서를 전송하는 시스템 및 방법 그리고 다차원 코드를 이용하여 데이터를 전송 및 인증하는 시스템 및 방법이 개시된다. 휴대기기는 카메라를 통해 입력된 이미지에서 다차원 코드를 인식하는 다차원 코드 인식부, 인식된 다차원 코드에서 암호화된 공인인증서를 추출하는 추출부 및 공인인증기관의 서버와 미리 교환된 임시 비밀키 및 사용자의 예전 공개키 중 하나의 키를 이용하여 암호화된 공인인증서를 복호화하는 복호화부를 포함하고, 공인인증서는 서버로 전송된 사용자의 공개키를 이용하여 서버에서 생성되고, 하나의 키를 이용하여 암호화되어 사용자의 사용자 단말기로 전송되고, 다차원 코드는 사용자 단말기에서 공인인증서를 이용하여 생성되어 사용자 단말기의 디스플레이 장치를 통해 표시된다.

대 표 도 - 도1



특허청구의 범위

청구항 1

카메라를 통해 입력된 이미지에서 다차원 코드를 인식하는 다차원 코드 인식부;

인식된 다차원 코드에서 암호화된 공인인증서를 추출하는 추출부; 및

공인인증기관의 서버와 미리 교환된 임시 비밀키 및 사용자의 예전 공개키 중 하나의 키를 이용하여 암호화된 공인인증서를 복호화하는 복호화부

를 포함하고,

상기 공인인증서는 상기 서버로 전송된 상기 사용자의 공개키를 이용하여 상기 서버에서 생성되고, 상기 하나의 키를 이용하여 암호화되어 상기 사용자의 사용자 단말기로 전송되고,

상기 다차원 코드는 상기 사용자 단말기에서 상기 공인인증서를 이용하여 생성되어 상기 사용자 단말기의 디스플레이 장치를 통해 표시되는, 휴대기기.

청구항 2

제1항에 있어서,

상기 사용자의 공개키와 쌍을 이루도록 함께 생성된 상기 사용자의 비밀키는 상기 공개키와 함께 상기 서버로 전송되고, 상기 서버에서 상기 하나의 키로 암호화되어 상기 사용자 단말기로 전송되고,

상기 다차원 코드는 상기 사용자 단말기에서 상기 암호화된 비밀키를 더 이용하여 생성되는, 휴대기기.

청구항 3

제1항에 있어서,

상기 사용자의 공개키와 쌍을 이루도록 함께 생성된 상기 사용자의 비밀키는 상기 사용자 단말기에서 상기 하나의 키를 이용하여 암호화되고,

상기 다차원 코드는 상기 사용자 단말기에서 상기 암호화된 비밀키를 더 이용하여 생성되는, 휴대기기.

청구항 4

제2항 또는 제3항에 있어서,

상기 추출부는, 상기 다차원 코드에서 상기 암호화된 비밀키를 더 추출하고,

상기 복호화부는, 상기 하나의 키를 이용하여 상기 암호화된 비밀키를 더 복호화하는, 휴대기기.

청구항 5

제1항에 있어서,

상기 복호화된 공인인증서가 포함하는 소유주, 인증기관명 및 공개키 중 적어도 하나를 이용하여 상기 복호화된 공인인증서를 검증하는 검증부

를 더 포함하는, 휴대기기.

청구항 6

공인인증서를 생성 및 전송하는 공인인증기관의 서버에 있어서,

사용자 단말기로부터 사용자의 공개키를 수신하는 키 수신부;

상기 공개키를 이용하여 상기 공인인증서를 생성하는 공인인증서 생성부;

상기 공인인증서를 휴대기기와 미리 교환된 임시 비밀키 및 사용자의 예전 공개키 중 하나의 키를 이용하여 암

호화하는 암호화부; 및

상기 암호화된 공인인증서를 상기 사용자 단말기로 전송하는 전송부

를 포함하고,

상기 암호화된 공인인증서를 이용하여 상기 사용자 단말기에서 다차원 코드가 생성 및 표시되고,

상기 다차원 코드는 상기 휴대기기의 카메라를 통해 입력 및 인식되어, 상기 암호화된 공인인증서가 추출되고, 상기 하나의 키를 통해 상기 암호화된 공인인증서가 상기 휴대기기에서 복호화되는, 서버.

청구항 7

제6항에 있어서,

상기 키 수신부는, 상기 사용자의 공개키와 쌍을 이루도록 함께 생성된 상기 사용자의 비밀키를 더 수신하고,

상기 암호화부는, 상기 비밀키를 상기 하나의 키를 이용하여 더 암호화하고,

상기 전송부는, 상기 암호화된 비밀키를 상기 사용자 단말기로 더 전송하는, 서버.

청구항 8

제6항에 있어서,

상기 사용자의 공개키와 쌍을 이루도록 함께 생성된 상기 사용자의 비밀키가 상기 사용자 단말기에서 상기 하나의 키를 이용하여 더 암호화되는, 서버.

청구항 9

제7항 또는 제8항에 있어서,

상기 다차원 코드는 상기 사용자 단말기에서 상기 암호화된 비밀키를 더 이용하여 생성되는, 서버.

청구항 10

사용자의 공개키 및 비밀키를 생성하는 키 생성부;

상기 공개키를 공인인증기관의 서버로 전송하는 키 전송부;

상기 서버에서 상기 공개키를 통해 생성되고, 상기 서버와 휴대기기간에 미리 교환된 임시 비밀키 및 사용자의 예전 공개키 중 하나의 키를 이용하여 암호화된 공인인증서를 상기 서버로부터 수신하는 수신부;

상기 암호화된 공인인증서를 이용하여 다차원 코드를 생성하는 다차원 코드 생성부; 및

상기 다차원 코드를 표시하는 표시부

를 포함하고,

상기 다차원 코드는 상기 휴대기기의 카메라를 통해 입력 및 인식되어, 상기 암호화된 공인인증서가 추출되고, 상기 하나의 키를 통해 상기 암호화된 공인인증서가 상기 휴대기기에서 복호화되는, 사용자 단말기.

청구항 11

제10항에 있어서,

상기 키 전송부는, 상기 비밀키를 상기 서버로 더 전송하고,

상기 수신부는, 상기 서버에서 상기 하나의 키를 통해 암호화된 비밀키를 상기 서버로부터 더 수신하고,

상기 다차원 코드 생성부는, 상기 암호화된 비밀키를 더 이용하여 상기 다차원 코드를 생성하는, 사용자 단말기.

청구항 12

제10항에 있어서,

상기 비밀키를 상기 하나의 키를 이용하여 암호화하는 암호화부를 더 포함하고,

상기 다차원 코드 생성부는, 상기 암호화된 비밀키를 더 이용하여 상기 다차원 코드를 생성하는, 사용자 단말기.

청구항 13

카메라를 통해 입력된 이미지에서 다차원 코드를 인식하는 다차원 코드 인식부;

상기 다차원 코드에서 암호화된 데이터, 서명된 데이터, 메시지 인증 코드 중 적어도 하나를 추출하는 추출부; 및

상기 암호화된 데이터를 복호화하여 데이터를 획득하거나 상기 서명된 데이터 또는 상기 메시지 인증 코드를 검증하는 복호화부

를 포함하고,

상기 다차원 코드는 사용자의 공개키 또는 공인인증기관의 서버와 미리 공유된 암호용/인증용 대칭키 중 암호용 대칭키를 통해 암호화된 상기 암호화된 데이터, 상기 서버의 비밀키를 통해 서명된 상기 서명된 데이터 및 상기 암호용/인증용 대칭키 중 인증용 대칭키를 통해 생성된 상기 메시지 인증 코드 중 적어도 하나를 이용하여 사용자 단말기 또는 상기 서버에서 생성되고, 상기 사용자 단말기의 디스플레이 장치를 통해 표시되는, 휴대기기.

청구항 14

제13항에 있어서,

상기 복호화부는, 상기 사용자의 비밀키, 상기 서버의 공개키, 상기 암호용/인증용 대칭키 중 적어도 하나를 이용하여 상기 복호화 또는 검증을 수행하는, 휴대기기.

청구항 15

사용자의 공개키 또는 휴대기기와 미리 공유된 암호용/인증용 대칭키 중 암호용 대칭키로 데이터를 암호화하거나 서버의 비밀키로 상기 데이터를 서명하거나 또는 상기 암호용/인증용 대칭키 중 인증용 대칭키를 이용하여 상기 데이터에 대한 메시지 인증 코드를 생성하는 암호화부; 및

상기 암호화된 데이터, 상기 서명된 데이터 및 상기 메시지 인증 코드 중 적어도 하나의 데이터를 사용자 단말기로 전송하거나 또는 상기 적어도 하나의 데이터를 이용하여 생성된 다차원 코드를 상기 사용자 단말기로 전송하는 전송부

를 포함하고,

상기 적어도 하나의 데이터가 상기 사용자 단말기로 전송되는 경우, 상기 사용자 단말기에서 상기 적어도 하나의 데이터를 이용하여 상기 다차원 코드가 생성 및 표시되고,

상기 다차원 코드가 상기 사용자 단말기로 전송되는 경우, 상기 다차원 코드가 상기 사용자 단말기에서 표시되는, 서버.

청구항 16

제15항에 있어서,

상기 사용자 단말기에서 표시되는 다차원 코드는 상기 휴대기기의 카메라를 통해 입력 및 인식되어, 상기 적어도 하나의 데이터가 추출되고,

상기 휴대기기에서 상기 사용자의 비밀키 또는 상기 인증용 대칭키로 상기 적어도 하나의 데이터가 복호화되거나 또는 상기 암호용 대칭키 또는 상기 서버의 공개키로 상기 적어도 하나의 데이터가 검증되는, 서버.

청구항 17

암호화된 데이터, 서명된 데이터 및 메시지 인증 코드 중 적어도 하나의 데이터를 또는 상기 적어도 하나의 데이터를 이용하여 서버에서 생성된 다차원 코드를 상기 서버로부터 수신하는 수신부;

상기 수신부에서 상기 적어도 하나의 데이터를 수신하는 경우, 상기 적어도 하나의 데이터를 이용하여 상기 다

차원 코드를 생성하는 다차원 코드 생성부; 및

상기 수신된 다차원 코드 또는 상기 생성된 다차원 코드를 디스플레이 장치를 통해 표시하는 표시부

를 포함하고,

상기 암호화된 데이터는 사용자의 공개키 또는 상기 서버와 휴대기기간에 미리 공유된 암호용/인증용 대칭키 중 암호용 대칭키로 암호화고,

상기 서명된 데이터는 상기 서버의 비밀키로 서명되고,

상기 메시지 인증 코드는 상기 암호용/인증용 대칭키 중 인증용 대칭키를 이용하여 생성되는, 사용자 단말기.

청구항 18

제17항에 있어서,

상기 표시되는 다차원 코드는 상기 휴대기기의 카메라를 통해 입력 및 인식되어, 상기 적어도 하나의 데이터가 추출되고,

상기 휴대기기에서 상기 사용자의 비밀키 또는 상기 인증용 대칭키로 상기 적어도 하나의 데이터가 복호화되거나 또는 상기 암호용 대칭키 또는 상기 서버의 공개키로 상기 적어도 하나의 데이터가 검증되는, 사용자 단말기.

청구항 19

카메라를 통해 입력된 이미지에서 다차원 코드를 인식하는 단계;

인식된 다차원 코드에서 암호화된 공인인증서를 추출하는 단계; 및

공인인증기관의 서버와 미리 교환된 임시 비밀키 및 사용자의 예전 공개키 중 하나의 키를 이용하여 암호화된 공인인증서를 복호화하는 단계

를 포함하고,

상기 공인인증서는 상기 서버로 전송된 상기 사용자의 공개키를 이용하여 상기 서버에서 생성되고, 상기 하나의 키를 이용하여 암호화되어 상기 사용자의 사용자 단말기로 전송되고,

상기 다차원 코드는 상기 사용자 단말기에서 상기 공인인증서를 이용하여 생성되어 상기 사용자 단말기의 디스플레이 장치를 통해 표시되는, 공인인증서 전송 방법.

청구항 20

공인인증서를 생성 및 전송하는 공인인증서 전송 방법에 있어서,

사용자 단말기로부터 사용자의 공개키를 수신하는 단계;

상기 공개키를 이용하여 상기 공인인증서를 생성하는 단계;

상기 공인인증서를 휴대기기와 미리 교환된 임시 비밀키 및 사용자의 예전 공개키 중 하나의 키를 이용하여 암호화하는 단계; 및

상기 암호화된 공인인증서를 상기 사용자 단말기로 전송하는 단계

를 포함하고,

상기 암호화된 공인인증서를 이용하여 상기 사용자 단말기에서 다차원 코드가 생성 및 표시되고,

상기 다차원 코드는 상기 휴대기기의 카메라를 통해 입력 및 인식되어, 상기 암호화된 공인인증서가 추출되고, 상기 하나의 키를 통해 상기 암호화된 공인인증서가 상기 휴대기기에서 복호화되는, 공인인증서 전송 방법.

청구항 21

사용자의 공개키 및 비밀키를 생성하는 단계;

상기 공개키를 공인인증기관의 서버로 전송하는 단계;

상기 서버에서 상기 공개키를 통해 생성되고, 상기 서버와 휴대기기간에 미리 교환된 임시 비밀키 및 사용자의 예전 공개키 중 하나의 키를 이용하여 암호화된 공인인증서를 상기 서버로부터 수신하는 단계;

상기 암호화된 공인인증서를 이용하여 다차원 코드를 생성하는 단계; 및

상기 다차원 코드를 표시하는 단계

를 포함하고,

상기 다차원 코드는 상기 휴대기기의 카메라를 통해 입력 및 인식되어, 상기 암호화된 공인인증서가 추출되고, 상기 하나의 키를 통해 상기 암호화된 공인인증서가 상기 휴대기기에서 복호화되는, 공인인증서 전송 방법.

청구항 22

카메라를 통해 입력된 이미지에서 다차원 코드를 인식하는 단계;

상기 다차원 코드에서 암호화된 데이터, 서명된 데이터, 메시지 인증 코드 중 적어도 하나를 추출하는 단계; 및

상기 암호화된 데이터를 복호화하여 데이터를 획득하거나 상기 서명된 데이터 또는 상기 메시지 인증 코드를 검증하는 단계

를 포함하고,

상기 다차원 코드는 사용자의 공개키 또는 공인인증기관의 서버와 미리 공유된 암호용/인증용 대칭키 중 암호용 대칭키를 통해 암호화된 상기 암호화된 데이터, 상기 서버의 비밀키를 통해 서명된 상기 서명된 데이터 및 상기 암호용/인증용 대칭키 중 인증용 대칭키를 통해 생성된 상기 메시지 인증 코드 중 적어도 하나를 이용하여 사용자 단말기 또는 상기 서버에서 생성되고, 상기 사용자 단말기의 디스플레이 장치를 통해 표시되는, 데이터 전송/인증 방법.

청구항 23

사용자의 공개키 또는 휴대기기와 미리 공유된 암호용/인증용 대칭키 중 암호용 대칭키로 데이터를 암호화하거나 서버의 비밀키로 상기 데이터를 서명하거나 또는 상기 암호용/인증용 대칭키 중 인증용 대칭키를 이용하여 상기 데이터에 대한 메시지 인증 코드를 생성하는 단계; 및

상기 암호화된 데이터, 상기 서명된 데이터 및 상기 메시지 인증 코드 중 적어도 하나의 데이터를 사용자 단말기로 전송하거나 또는 상기 적어도 하나의 데이터를 이용하여 생성된 다차원 코드를 상기 사용자 단말기로 전송하는 단계

를 포함하고,

상기 적어도 하나의 데이터가 상기 사용자 단말기로 전송되는 경우, 상기 사용자 단말기에서 상기 적어도 하나의 데이터를 이용하여 상기 다차원 코드가 생성 및 표시되고,

상기 다차원 코드가 상기 사용자 단말기로 전송되는 경우, 상기 다차원 코드가 상기 사용자 단말기에서 표시되는, 데이터 전송/인증 방법.

청구항 24

암호화된 데이터, 서명된 데이터 및 메시지 인증 코드 중 적어도 하나의 데이터를 또는 상기 적어도 하나의 데이터를 이용하여 서버에서 생성된 다차원 코드를 상기 서버로부터 수신하는 단계;

상기 수신부에서 상기 적어도 하나의 데이터를 수신하는 경우, 상기 적어도 하나의 데이터를 이용하여 상기 다차원 코드를 생성하는 단계; 및

상기 수신된 다차원 코드 또는 상기 생성된 다차원 코드를 디스플레이 장치를 통해 표시하는 단계

를 포함하고,

상기 암호화된 데이터는 사용자의 공개키 또는 상기 서버와 휴대기기간에 미리 공유된 암호용/인증용 대칭키 중 암호용 대칭키로 암호화고,

상기 서명된 데이터는 상기 서버의 비밀키로 서명되고,

상기 메시지 인증 코드는 상기 암호용/인증용 대칭키 중 인증용 대칭키를 이용하여 생성되는, 데이터 전송/인증 방법.

명 세 서

기 술 분 야

[0001] 본 발명의 실시예들은 휴대기기에 공인인증서를 전송하는 시스템 및 방법 그리고 다차원 코드를 이용하여 데이터를 전송 및 인증하는 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 공인인증서(certificate)는 전자상거래를 할 때 신원을 확인하고, 문서의 위조와 변조, 거래 사실의 부인 방지 등을 목적으로 공인인증기관(Certificate Authority, CA)이 발행하는 전자적 정보로서, 일종의 사이버 거래용 인감증명서이다. 이러한 공인인증서가 PC나 노트북과 같은 사용자 단말기에 존재하는 경우, 사용자 단말기에 저장된 공인인증서를 스마트폰과 같은 휴대기기에 설치하기 위한 마땅한 방법이 없는 실정이다. 즉, 휴대기기와 사용자 단말기를 연결한 후, 사용자 단말기를 통해 다시 공인인증기관을 거쳐 휴대기기로 공인인증서를 전송해야만 하는 불편함이 있다.

[0003] 본 명세서에서는 보다 효율적으로 휴대기기로 공인인증서를 전송하는 시스템 및 방법이 제공된다.

발명의 내용

해결하려는 과제

[0004] 사용자 단말기로 전송된 공인인증서를 QR 코드와 같은 다차원 코드를 이용하여 휴대기기로 전송할 수 있는 시스템 및 방법이 제공된다.

[0005] 사용자의 공개키를 이용하여 생성된 공인인증서를 휴대기기와 공인 인증기관 사이에 미리 교환된 임시 비밀키 또는 과거 사용되었으나 폐기되지 않은 사용자의 예전 공개키를 이용하여 암호화하고, 암호화된 공인인증서를 사용자 단말기로 전송하여 사용자 단말기에서 암호화된 공인인증서를 이용하여 다차원 코드를 생성 및 표시하여 휴대기기로 전송할 수 있는 시스템 및 방법이 제공된다.

[0006] 다차원 코드를 이용하여 데이터를 비밀 전송 및 인증할 수 있는 시스템 및 방법이 제공된다.

[0007] 공개키와 비밀키 그리고 다차원 코드를 이용하여 데이터를 비밀 전송 및 인증할 수 있는 시스템 및 방법이 제공된다.

[0008] 휴대기기와 공인인증기관의 서버간에 미리 공유된 암호용/인증용 대칭키와 다차원 코드를 이용하여 데이터를 비밀 전송 및 인증할 수 있는 시스템 및 방법이 제공된다.

과제의 해결 수단

[0009] 카메라를 통해 입력된 이미지에서 다차원 코드를 인식하는 다차원 코드 인식부, 인식된 다차원 코드에서 암호화된 공인인증서를 추출하는 추출부 및 공인인증기관의 서버와 미리 교환된 임시 비밀키 및 사용자의 예전 공개키 중 하나의 키를 이용하여 암호화된 공인인증서를 복호화하는 복호화부를 포함하고, 공인인증서는 서버로 전송된 사용자의 공개키를 이용하여 서버에서 생성되고, 하나의 키를 이용하여 암호화되어 사용자의 사용자 단말기로 전송되고, 다차원 코드는 사용자 단말기에서 공인인증서를 이용하여 생성되어 사용자 단말기의 디스플레이 장치를 통해 표시되는, 휴대기기가 제공된다.

[0010] 일측에 따르면, 사용자의 공개키와 쌍을 이루도록 함께 생성된 사용자의 비밀키는 공개키와 함께 서버로 전송되고, 서버에서 하나의 키로 암호화되어 사용자 단말기로 전송될 수 있고, 다차원 코드는 사용자 단말기에서 암호화된 비밀키를 더 이용하여 생성될 수 있다.

[0011] 다른 측면에 따르면, 사용자의 공개키와 쌍을 이루도록 함께 생성된 사용자의 비밀키는 사용자 단말기에서 하나의 키를 이용하여 암호화될 수 있고, 다차원 코드는 사용자 단말기에서 암호화된 비밀키를 더 이용하여 생성될 수 있다.

[0012] 또 다른 측면에 따르면, 추출부는, 다차원 코드에서 암호화된 비밀키를 더 추출할 수 있고, 복호화부는, 하나의

키를 이용하여 암호화된 비밀키를 더 복호화할 수 있다.

[0013] 또 다른 측면에 따르면, 휴대기기는 복호화된 공인인증서가 포함하는 소유주, 인증기관명 및 공개키 중 적어도 하나를 이용하여 복호화된 공인인증서를 검증하는 검증부를 더 포함할 수 있다.

[0014] 사용자 단말기로부터 사용자의 공개키를 수신하는 키 수신부, 공개키를 이용하여 공인인증서를 생성하는 공인인증서 생성부, 공인인증서를 휴대기기와 미리 교환된 임시 비밀키 및 사용자의 예전 공개키 중 하나의 키를 이용하여 암호화하는 암호화부 및 암호화된 공인인증서를 사용자 단말기로 전송하는 전송부를 포함하고, 암호화된 공인인증서를 이용하여 사용자 단말기에서 다차원 코드가 생성 및 표시되고, 다차원 코드는 휴대기기의 카메라를 통해 입력 및 인식되어, 암호화된 공인인증서가 추출되고, 하나의 키를 통해 암호화된 공인인증서가 휴대기기에서 복호화되는, 서버가 제공된다.

[0015] 사용자의 공개키 및 비밀키를 생성하는 키 생성부, 공개키를 공인인증기관의 서버로 전송하는 키 전송부, 서버에서 공개키를 통해 생성되고, 서버와 휴대기기간에 미리 교환된 임시 비밀키 및 사용자의 예전 공개키 중 하나의 키를 이용하여 암호화된 공인인증서를 서버로부터 수신하는 수신부, 암호화된 공인인증서를 이용하여 다차원 코드를 생성하는 다차원 코드 생성부 및 다차원 코드를 표시하는 표시부를 포함하고, 다차원 코드는 휴대기기의 카메라를 통해 입력 및 인식되어, 암호화된 공인인증서가 추출되고, 하나의 키를 통해 암호화된 공인인증서가 휴대기기에서 복호화되는, 사용자 단말기가 제공된다.

[0016] 카메라를 통해 입력된 이미지에서 다차원 코드를 인식하는 다차원 코드 인식부, 다차원 코드에서 암호화된 데이터, 서명된 데이터, 메시지 인증 코드 중 적어도 하나를 추출하는 추출부 및 암호화된 데이터를 복호화하여 데이터를 획득하거나 서명된 데이터 또는 메시지 인증 코드를 검증하는 복호화부를 포함하고, 다차원 코드는 사용자의 공개키 또는 공인인증기관의 서버와 미리 공유된 암호용/인증용 대칭키 중 암호용 대칭키를 통해 암호화된 암호화된 데이터, 서버의 비밀키를 통해 서명된 서명된 데이터 및 암호용/인증용 대칭키 중 인증용 대칭키를 통해 생성된 메시지 인증 코드 중 적어도 하나를 이용하여 사용자 단말기 또는 서버에서 생성되고, 사용자 단말기의 디스플레이 장치를 통해 표시되는, 휴대기기가 제공된다.

[0017] 사용자의 공개키 또는 휴대기기와 미리 공유된 암호용/인증용 대칭키 중 암호용 대칭키로 데이터를 암호화하거나 서버의 비밀키로 데이터를 서명하거나 또는 암호용/인증용 대칭키 중 인증용 대칭키를 이용하여 데이터에 대한 메시지 인증 코드를 생성하는 암호화부 및 암호화된 데이터, 서명된 데이터 및 메시지 인증 코드 중 적어도 하나의 데이터를 사용자 단말기로 전송하거나 또는 적어도 하나의 데이터를 이용하여 생성된 다차원 코드를 사용자 단말기로 전송하는 전송부를 포함하고, 적어도 하나의 데이터가 사용자 단말기로 전송되는 경우, 사용자 단말기에서 적어도 하나의 데이터를 이용하여 다차원 코드가 생성 및 표시되고, 다차원 코드가 사용자 단말기로 전송되는 경우, 다차원 코드가 사용자 단말기에서 표시되는, 서버가 제공된다.

[0018] 암호화된 데이터, 서명된 데이터 및 메시지 인증 코드 중 적어도 하나의 데이터를 또는 적어도 하나의 데이터를 이용하여 서버에서 생성된 다차원 코드를 서버로부터 수신하는 수신부, 수신부에서 적어도 하나의 데이터를 수신하는 경우, 적어도 하나의 데이터를 이용하여 다차원 코드를 생성하는 다차원 코드 생성부 및 수신된 다차원 코드 또는 생성된 다차원 코드를 디스플레이 장치를 통해 표시하는 표시부를 포함하고, 암호화된 데이터는 사용자의 공개키 또는 서버와 휴대기기간에 미리 공유된 암호용/인증용 대칭키 중 암호용 대칭키로 암호화고, 서명된 데이터는 서버의 비밀키로 서명되고, 메시지 인증 코드는 암호용/인증용 대칭키 중 인증용 대칭키를 이용하여 생성되는, 사용자 단말기가 제공된다.

[0019] 카메라를 통해 입력된 이미지에서 다차원 코드를 인식하는 단계, 인식된 다차원 코드에서 암호화된 공인인증서를 추출하는 단계 및 공인인증기관의 서버와 미리 교환된 임시 비밀키 및 사용자의 예전 공개키 중 하나의 키를 이용하여 암호화된 공인인증서를 복호화하는 단계를 포함하고, 공인인증서는 서버로 전송된 사용자의 공개키를 이용하여 서버에서 생성되고, 하나의 키를 이용하여 암호화되어 사용자의 사용자 단말기로 전송되고, 다차원 코드는 사용자 단말기에서 공인인증서를 이용하여 생성되어 사용자 단말기의 디스플레이 장치를 통해 표시되는, 공인인증서 전송 방법이 제공된다.

[0020] 공인인증서를 생성 및 전송하는 공인인증서 전송 방법에 있어서, 사용자 단말기로부터 사용자의 공개키를 수신하는 단계, 공개키를 이용하여 공인인증서를 생성하는 단계, 공인인증서를 휴대기기와 미리 교환된 임시 비밀키 및 사용자의 예전 공개키 중 하나의 키를 이용하여 암호화하는 단계 및 암호화된 공인인증서를 사용자 단말기로 전송하는 단계를 포함하고, 암호화된 공인인증서를 이용하여 사용자 단말기에서 다차원 코드가 생성 및 표시되고, 다차원 코드는 휴대기기의 카메라를 통해 입력 및 인식되어, 암호화된 공인인증서가 추출되고, 하나의 키를

통해 암호화된 공인인증서가 휴대기기에서 복호화되는, 공인인증서 전송 방법이 제공된다.

[0021] 사용자의 공개키 및 비밀키를 생성하는 단계, 공개키를 공인인증기관의 서버로 전송하는 단계, 서버에서 공개키를 통해 생성되고, 서버와 휴대기기간에 미리 교환된 임시 비밀키 및 사용자의 예전 공개키 중 하나의 키를 이용하여 암호화된 공인인증서를 서버로부터 수신하는 단계, 암호화된 공인인증서를 이용하여 다차원 코드를 생성하는 단계 및 다차원 코드를 표시하는 단계를 포함하고, 다차원 코드는 휴대기기의 카메라를 통해 입력 및 인식되어, 암호화된 공인인증서가 추출되고, 하나의 키를 통해 암호화된 공인인증서가 휴대기기에서 복호화되는, 공인인증서 전송 방법이 제공된다.

[0022] 카메라를 통해 입력된 이미지에서 다차원 코드를 인식하는 단계, 다차원 코드에서 암호화된 데이터, 서명된 데이터, 메시지 인증 코드 중 적어도 하나를 추출하는 단계 및 암호화된 데이터를 복호화하여 데이터를 획득하거나 서명된 데이터 또는 메시지 인증 코드를 검증하는 단계를 포함하고, 다차원 코드는 사용자의 공개키 또는 공인인증기관의 서버와 미리 공유된 암호용/인증용 대칭키 중 암호용 대칭키를 통해 암호화된 암호화된 데이터, 서버의 비밀키를 통해 서명된 서명된 데이터 및 암호용/인증용 대칭키 중 인증용 대칭키를 통해 생성된 메시지 인증 코드 중 적어도 하나를 이용하여 사용자 단말기 또는 서버에서 생성되고, 사용자 단말기의 디스플레이 장치를 통해 표시되는, 데이터 전송/인증 방법이 제공된다.

[0023] 사용자의 공개키 또는 휴대기기와 미리 공유된 암호용/인증용 대칭키 중 암호용 대칭키로 데이터를 암호화하거나 서버의 비밀키로 데이터를 서명하거나 또는 암호용/인증용 대칭키 중 인증용 대칭키를 이용하여 데이터에 대한 메시지 인증 코드를 생성하는 단계 및 암호화된 데이터, 서명된 데이터 및 메시지 인증 코드 중 적어도 하나의 데이터를 사용자 단말기로 전송하거나 또는 적어도 하나의 데이터를 이용하여 생성된 다차원 코드를 사용자 단말기로 전송하는 단계를 포함하고, 적어도 하나의 데이터가 사용자 단말기로 전송되는 경우, 사용자 단말기에서 적어도 하나의 데이터를 이용하여 다차원 코드가 생성 및 표시되고, 다차원 코드가 사용자 단말기로 전송되는 경우, 다차원 코드가 사용자 단말기에서 표시되는, 데이터 전송/인증 방법이 제공된다.

[0024] 암호화된 데이터, 서명된 데이터 및 메시지 인증 코드 중 적어도 하나의 데이터를 또는 적어도 하나의 데이터를 이용하여 서버에서 생성된 다차원 코드를 서버로부터 수신하는 단계, 수신부에서 적어도 하나의 데이터를 수신하는 경우, 적어도 하나의 데이터를 이용하여 다차원 코드를 생성하는 단계 및 수신된 다차원 코드 또는 생성된 다차원 코드를 디스플레이 장치를 통해 표시하는 단계를 포함하고, 암호화된 데이터는 사용자의 공개키 또는 서버와 휴대기기간에 미리 공유된 암호용/인증용 대칭키 중 암호용 대칭키로 암호화고, 서명된 데이터는 서버의 비밀키로 서명되고, 메시지 인증 코드는 암호용/인증용 대칭키 중 인증용 대칭키를 이용하여 생성되는, 데이터 전송/인증 방법이 제공된다.

발명의 효과

[0025] 사용자 단말기로 전송된 공인인증서를 QR 코드와 같은 다차원 코드를 이용하여 휴대기기로 전송할 수 있다.

[0026] 사용자의 공개키를 이용하여 생성된 공인인증서를 휴대기기와 공인 인증기관 사이에 미리 교환된 임시 비밀키 또는 과거 사용되었으나 폐기되지 않은 사용자의 예전 공개키를 이용하여 암호화하고, 암호화된 공인인증서를 사용자 단말기로 전송하여 사용자 단말기에서 암호화된 공인인증서를 이용하여 다차원 코드를 생성 및 표시하여 휴대기기로 전송할 수 있다.

[0027] 다차원 코드를 이용하여 데이터를 비밀 전송 및 인증할 수 있다.

[0028] 공개키와 비밀키 그리고 다차원 코드를 이용하여 데이터를 비밀 전송 및 인증할 수 있다.

[0029] 휴대기기와 공인인증기관의 서버간에 미리 공유된 암호용/인증용 대칭키와 다차원 코드를 이용하여 데이터를 비밀 전송 및 인증할 수 있다.

도면의 간단한 설명

[0030] 도 1은 본 발명의 일실시예에 있어서, 휴대기기에 공인인증서를 설치하기 위한 전체적인 시스템 구조를 나타낸 도면이다.

도 2는 본 발명의 일실시예에 있어서, 휴대기기에 데이터를 안전하게 전달하거나 데이터 또는 서버를 인증하기 위한 전체적인 시스템 구조를 나타낸 도면이다.

도 3은 본 발명의 일실시예에 있어서, 공인인증서 전송을 위한 휴대기기의 내부 구성을 설명하기 위한 블록도이

다.

도 4는 본 발명의 일실시예에 있어서, 공인인증서 전송을 위한 서버의 내부 구성을 설명하기 위한 블록도이다.

도 5는 본 발명의 일실시예에 있어서, 공인인증서 전송을 위한 사용자 단말기의 내부 구성을 설명하기 위한 블록도이다.

도 6은 본 발명의 일실시예에 있어서, 공개키와 비밀키를 모두 전송하는 경우의 공인인증서 전송 방법을 도시한 흐름도이다.

도 7은 본 발명의 일실시예에 있어서, 공개키를 전송하는 경우의 공인인증서 전송 방법을 도시한 흐름도이다.

도 8은 본 발명의 일실시예에 있어서, 데이터의 전송 또는 인증을 위한 휴대기기의 내부 구성을 설명하기 위한 블록도이다.

도 9는 본 발명의 일실시예에 있어서, 데이터의 전송 또는 인증을 위한 서버의 내부 구성을 설명하기 위한 블록도이다.

도 10은 본 발명의 일실시예에 있어서, 데이터의 전송 또는 인증을 사용자 단말기의 내부 구성을 설명하기 위한 블록도이다.

도 11은 본 발명의 일실시예에 있어서, 공개키 및 비밀키를 이용하여 데이터를 전송하거나 또는 인증하는 방법을 도시한 흐름도이다.

도 12는 본 발명의 일실시예에 있어서, 암호용/인증용 대칭키를 이용하여 데이터를 전송하거나 또는 인증하는 방법을 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0031] 이하, 본 발명의 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0032] 도 1은 본 발명의 일실시예에 있어서, 휴대기기에 공인인증서를 설치하기 위한 전체적인 시스템 구조를 나타낸 도면이다. 도 1은 사용자(110), 사용자 단말기(120), 서버(130) 및 휴대기기(140)를 나타내고 있다. 여기서, 사용자 단말기(120)는 PC나 노트북과 같이 사용자(110)가 서버(130)로부터 공인인증서를 제공받기 위해 서버(130)에 접속하는 단말기를 의미할 수 있고, 서버(130)는 공인인증서를 제공하는 공인인증기관의 시스템을 의미할 수 있다. 또한, 휴대기기(140)는 카메라를 포함하는 휴대용 장치를 의미할 수 있다.

[0033] 이때, 사용자(110)에 의해 사용자 단말기(120)에서 생성된 공개키/비밀키 쌍을 <pku, pru>라 하자. 이때, 공개키는 다른 사람에게 알려지는 키이다. 하지만, 공개키 암호화 시스템의 특성상 일반적으로 공개키 'pku'는 랜덤한 값이고, 사용자(110)의 신원정보를 담고 있지 않기 때문에 공개키가 어떤 소유주의 것인지 확인할 수 없다. 이를 확인하기 위해 신뢰할 수 있는 기관(예를 들어, 상술한 공인인증기간)이 사용자(110)의 공개키의 정보에 전자서명을 한 공인인증서를 사용한다.

[0034] 이때, 휴대기기(140)에 공인인증서와 사용자 단말기(120)에서 생성된 비밀키 'pru'를 설치하기 위해 아래와 같은 방법이 이용될 수 있다.

[0035] 일실시예로, 공개키인 인증서와 비밀키를 모두 공인인증기관으로 전송하는 경우를 설명한다.

[0036] 사용자(110)에 의해 사용자 단말기(120)에서 공개키/비밀키 쌍인 <pku, pru>가 생성되면, 사용자 단말기(120)는 생성된 <pku, pru>를 공인인증기관의 서버(130)로 전송한다. 서버(130)는 사용자의 신원을 확인하고, 공개키 'pku'에 대한 공인인증서를 생성한다. 이때, 서버(130)는 생성된 공인인증서 'C'와 사용자(110)의 비밀키 쌍인 <C, pru>를 다른 키 'k'로 암호화하여 $E_k(C, pru)$를 생성할 수 있다. 즉, $E_k(C, pru)$는 다른 키 'k'로 암호화된 공인인증서 'C'와 비밀키 'pru'를 의미할 수 있다. 여기서, 다른 키 'k'는 서버(130)과 휴대기기(140)간에 미리 교환된 임시 비밀키이거나 기존에 생성되고 이용된 후 아직 폐기되지 않은 사용자(110)의 예전 공개키일 수 있다. 다시 말해, 다른 키 'k'는 서버(130)뿐만 아니라 휴대기가(140) 역시 알고 있다.

[0037] 이때, 서버(130)는 다른 키 'k'를 통해 암호화되어 생성된 $E_k(C, pru)$를 사용자 단말기(120)로 전송한다. 이 경우, 사용자 단말기(120)는 전송된 $E_k(C, pru)$를 이용하여 다차원 코드를 생성하고, 생성된 다차원 코드를 디스플레이 장치를 통해 화면에 표시한다. 여기서 다차원 코드는 일례로 QR 코드를 이용할 수 있고, 화면에 표시

된 다차원 코드는 $E_k(C, pru)$를 포함한다.

[0038] 휴대기기(140)는 카메라를 통해 입력되는 이미지를 통해 다차원 코드를 인식하여 $E_k(C, pru)$를 얻을 수 있고, 다른 키 'k'가 상술한 미리 교환된 임시 비밀키인 경우, 상기 다른 키 'k'를 이용하여 $E_k(C, pru)$로부터 공인인증서 'C'와 사용자(110)에 의해 사용자 단말기(120)에서 생성되었던 비밀키 'pru'를 얻을 수 있다. 또한, 휴대기기(140)는 다른 키 'k'가 상술한 예전 공개키인 경우, 상기 공개키에 대응하여 생성된 비밀키를 이용하여 $E_k(C, pru)$로부터 공인인증서 'C'와 사용자(110)에 의해 사용자 단말기(120)에서 생성되었던 비밀키 'pru'를 얻을 수 있다.

[0039] 얻어진 공인인증서 'C'와 비밀키 'pru'는 휴대기기(140)에서 공인인증서의 소유주가 사용자(110)가 맞는지, 인증기관명이 맞는지, 공인인증서에 포함된 공개키 'pku'가 사용자(110)에 의해 생성된 것이 맞는지, 그리고 공인인증서 검증결과가 유효한지 등을 확인함으로써, 인증될 수 있다.

[0040] 상술한 실시예에서는 공개키인 인증서와 비밀키를 모두 공인인증기관에 보내는 경우를 설명하였다. 그러나, 사용자의 비밀키는 사용자 단말기(120)나 휴대기기(140) 외에는 유출되지 않는 편이 바람직하다. 따라서, 다른 실시예에서는 공개키인 인증서만을 공인인증기관으로 전송하는 경우를 설명한다.

[0041] 사용자(110)에 의해 사용자 단말기(120)에서 공개키/비밀키 쌍인 <pku, pru>가 생성되면, 사용자 단말기(120)는 생성된 <pku, pru> 중 공개키 'pku'를 공인인증기관의 서버(130)로 전송한다. 서버(130)는 사용자의 신원을 확인하고, 공개키 'pku'에 대한 공인인증서를 생성한다. 이때, 서버(130)는 생성된 공인인증서 'C'를 다른 키 'k'로 암호화하여 $E_k(C)$를 생성할 수 있다. 즉, $E_k(C)$는 다른 키 'k'로 암호화된 공인인증서 'C'를 의미할 수 있다. 여기서, 다른 키 'k'는 서버(130)과 휴대기기(140)간에 미리 교환된 임시 비밀키이거나, 기존에 생성되고 이용된 후 아직 폐기되지 않은 사용자(110)의 예전 공개키일 수 있다. 다시 말해, 다른 키 'k'는 서버(130)뿐만 아니라 휴대기가(140) 역시 알고 있다.

[0042] 이때, 서버(130)는 다른 키 'k'를 통해 암호화되어 생성된 $E_k(C)$를 사용자 단말기(120)로 전송한다. 이 경우, 사용자 단말기(120)는 전송된 $E_k(C)$과 사용자(110)의 비밀키 'pru'를 다른 키 'k'로 암호화한 $E_k(pru)$를 이용하여 다차원 코드를 생성하고, 생성된 다차원 코드를 디스플레이 장치를 통해 화면에 표시한다. 즉, 화면에 표시된 다차원 코드는 $E_k(C)$과 $E_k(pru)$를 포함할 수 있다. 여기서, 사용자 단말기(120)는 상기 다른 키 'k'를 서버(130)나 휴대기기(140)를 통해 얻을 수 있다. 다른 실시예로, 사용자 단말기(120)는 휴대기기(140)와 사용자 단말기(120)간에 미리 교환된 또 다른 키를 이용하여 비밀키 'pru'를 암호화할 수 있고, 암호화된 비밀키를 휴대기기로 전송할 수도 있다

[0043] 휴대기기(140)는 카메라를 통해 입력되는 이미지를 통해 다차원 코드를 인식하여 $E_k(C)$과 $E_k(pru)$를 얻을 수 있고, 다른 키 'k'를 이용하여 $E_k(C)$과 $E_k(pru)$로부터 공인인증서 'C'와 사용자(110)에 의해 사용자 단말기(120)에서 생성되었던 비밀키 'pru'를 얻을 수 있다. 만약, 비밀키가 휴대기기(140)와 사용자 단말기(120)간에 미리 교환된 또 다른 키를 이용하여 암호화된 경우, 휴대기기(140)는 다른 키 'k'를 이용하여 공인인증서 'C'를 얻을 수 있고, 다른 키를 이용하여 비밀키 'pru'를 얻을 수 있다.

[0044] 얻어진 공인인증서 'C'와 비밀키 'pru'는 휴대기기(140)에서 공인인증서의 소유주가 사용자(110)가 맞는지, 인증기관명이 맞는지, 공인인증서에 포함된 공개키 'pku'가 사용자(110)에 의해 생성된 것이 맞는지, 그리고 공인인증서 검증결과가 유효한지 등을 확인함으로써, 인증될 수 있다.

[0045] 도 2는 본 발명의 일실시예에 있어서, 휴대기기에 데이터를 안전하게 전달하거나 데이터 또는 서버를 인증하기 위한 전체적인 시스템 구조를 나타낸 도면이다. 도 2는 사용자(210), 사용자 단말기(220), 서버(230) 및 휴대기기(240)를 나타내고 있다. 여기서, 사용자 단말기(220)는 PC나 노트북과 같이 사용자(210)가 서버(230)과 통신하기 위해 서버(230)에 접속하는 단말기를 의미할 수 있고, 서버(230)는 데이터를 비밀 전송하거나 전송한 데이터에 대한 인증 데이터를 전송하기 위한 시스템을 의미할 수 있다. 또한, 휴대기기(240)는 카메라를 포함하는 휴대용 장치를 의미할 수 있다.

[0046] 일실시예에서는, 카메라가 부착된 휴대기기(240)과 다차원 코드를 이용하여 데이터 'M'을 사용자(210)에게 안전하게 전달하기 위해 사용자(210)의 공개키/비밀키 쌍인 <pku, pru>와 서버(220)의 공개키/비밀키 쌍인 <pks, prs>를 이용한다.

[0047] 우선, 서버(230)는 아래의 세 가지 방법 중 하나를 이용하여 휴대기기(240)로 데이터 'M'을 안전하게 전송하거나 전송된 데이터 또는 서버(230)가 휴대기기(240)에서 인증되도록 할 수 있다.

[0048] 첫 번째 방법으로, 서버(230)는 사용자(210)의 공개키 'pku'로 데이터 'M'을 암호화하여 $E_{pku}(M)$를 생성하고, 생성된 $E_{pku}(M)$를 이용하여 다차원 코드를 생성하고, 생성된 다차원 코드를 사용자 단말기(220)로 전송할 수 있다. 여기서, 생성된 다차원 코드는 $E_{pku}(M)$를 포함할 수 있다. 이 경우, 사용자 단말기(220)는 전송된 다차원 코드를 디스플레이 장치를 통해 표시하고, 휴대기기(240)는 카메라를 통해 다차원 코드가 포함된 이미지를 입력받아 인식할 수 있다. 이때, 휴대기기(240)는 다차원 코드에서 $E_{pku}(M)$를 추출하고, 사용자(210)의 비밀키 'pru'를 이용하여 $E_{pku}(M)$를 복호화함으로써, 데이터 'M'을 얻을 수 있다.

[0049] 두 번째 방법으로, 서버(230)는 서버(230)의 비밀키 'prs'로 데이터 'M'을 서명한 $Sign_{prs}(M)$를 생성하고, 생성된 $Sign_{prs}(M)$를 이용하여 다차원 코드를 생성하고, 생성된 다차원 코드를 사용자 단말기(220)로 전송할 수 있다. 여기서, 생성된 다차원 코드는 $Sign_{prs}(M)$를 포함할 수 있다. 이 경우, 사용자 단말기(220)는 전송된 다차원 코드를 디스플레이 장치를 통해 표시하고, 휴대기기(240)는 카메라를 통해 다차원 코드가 포함된 이미지를 입력받아 인식할 수 있다. 이때, 휴대기기(240)는 다차원 코드에서 $Sign_{prs}(M)$를 추출하고, 서버(230)의 공개키 'pks'를 이용하여 $Sign_{prs}(M)$를 서명검증함으로써, 데이터 'M'을 인증하거나 또는 서버(230)를 인증할 수 있다.

[0050] 세 번째 방법으로, 서버(230)는 서버(230)의 비밀키 'prs'로 데이터 'M'을 서명한 $Sign_{prs}(M)$를 생성하고, 생성된 $Sign_{prs}(M)$를 다시 사용자(210)의 공개키 'pku'로 암호화하여 $E_{pku}(M||S)$를 생성한다. 이때, 서버(230)는 생성된 $E_{pku}(M||S)$를 이용하여 다차원 코드를 생성하고, 생성된 다차원 코드를 사용자 단말기(220)로 전송할 수 있다. 여기서, 생성된 다차원 코드는 $E_{pku}(M||S)$를 포함할 수 있다. 이 경우, 사용자 단말기(220)는 전송된 다차원 코드를 디스플레이 장치를 통해 표시하고, 휴대기기(240)는 카메라를 통해 다차원 코드가 포함된 이미지를 입력받아 인식할 수 있다. 이때, 휴대기기(240)는 다차원 코드에서 $E_{pku}(M||S)$를 추출하고, 비밀키 'pru'로 $E_{pku}(M||S)$를 복호화하여 $Sign_{prs}(M)$를 얻을 수 있다. 또한, 휴대기기(240)는 서버(230)의 공개키 'pks'로 $Sign_{prs}(M)$를 서명검증함으로써, 데이터 'M'을 인증하거나 또는 서버(230)를 인증할 수 있다.

[0051] 또한, 첫 번째 방법에서, 전달하고자 하는 데이터 'M'의 크기가 기선정된 크기 이상인 경우, 서버(230)는 대칭키 'sk'를 임의로 선택하고, 데이터 'M'을 대칭키 'sk'로 암호화하여 $E_{sk}(M)$를 생성할 수 있다. 또한, 서버(230)는 사용자(210)의 공개키 'pku'를 이용하여 대칭키 'sk'를 암호화하여 $E_{pku}(sk)$를 생성할 수 있다. 이때, 서버(230)는 $E_{sk}(M)$과 $E_{pku}(sk)$를 이용하여 다차원 코드를 생성할 수 있고, 생성된 다차원 코드를 사용자 단말기(220)로 전송할 수 있다. 여기서, 다차원 코드는 $E_{sk}(M)$과 $E_{pku}(sk)$를 포함할 수 있다. 이 경우에도, 사용자 단말기(220)는 전송된 다차원 코드를 디스플레이 장치를 통해 표시하고, 휴대기기(240)는 카메라를 통해 다차원 코드가 포함된 이미지를 입력받아 인식할 수 있다. 이때, 휴대기기(240)는 다차원 코드에서 $E_{sk}(M)$과 $E_{pku}(sk)$를 추출할 수 있다. 휴대기기(240)는 사용자의 비밀키 'pru'로 $E_{pku}(sk)$를 복호화하여 대칭키 'sk'를 얻을 수 있고, 대칭키 'sk'로 $E_{sk}(M)$를 복호화하여 데이터 'M'을 얻을 수 있다.

[0052] 이에 더해, 세 번째 방법에서, 전달하고자 하는 'M||S' 즉, $Sign_{prs}(M)$의 크기가 기선정된 크기 이상인 경우, 서버(230)는 대칭키 'sk'를 임의로 선택하고, $Sign_{prs}(M)$를 대칭키 'sk'로 암호화하여 $E_{sk}(M||S)$를 생성할 수 있다. 또한, 서버(230)는 사용자의 공개키 'pku'를 이용하여 대칭키 'sk'를 암호화하여 $E_{pku}(sk)$를 생성할 수 있다. 이때, 서버(230)는 $E_{sk}(M||S)$과 $E_{pku}(sk)$를 이용하여 다차원 코드를 생성할 수 있고, 생성된 다차원 코드를 사용자 단말기(220)로 전송할 수 있다. 여기서, 다차원 코드는 $E_{sk}(M||S)$과 $E_{pku}(sk)$를 포함할 수 있다. 이 경우에도, 사용자 단말기(220)는 전송된 다차원 코드를 디스플레이 장치를 통해 표시하고, 휴대기기(240)는 카메라를 통해 다차원 코드가 포함된 이미지를 입력받아 인식할 수 있다. 이때, 휴대기기(240)는 다차원 코드에서 $E_{sk}(M||S)$과 $E_{pku}(sk)$를 추출할 수 있다. 휴대기기(240)는 사용자의 비밀키 'pru'로 $E_{pku}(sk)$를 복호화하여 대칭키 'sk'를 얻을 수 있고, 대칭키 'sk'로 $E_{sk}(M||S)$를 복호화하여 $Sign_{prs}(M)$를 얻을 수 있다. 이후, 휴대기

기(240)는 서버(230)의 공개키 'pks'를 이용하여 $Sign_{prs}(M)$를 서명검증함으로써, 데이터 'M'을 인증하거나 또는 서버(230)를 인증할 수 있다.

[0053] 각각의 경우에, 사용자 단말기(220)는 전송된 다차원 코드를 디스플레이 장치를 통해 표시하고, 휴대기기(240)는 카메라를 통해 다차원 코드가 포함된 이미지를 입력받아 인식하고, 다차원 코드를 통해 얻은 데이터를 복호화하여 데이터를 안전하게 수신하거나 또는 데이터를 서명검증하여 데이터나 서버(230)를 인증할 수 있다.

[0054] 다차원 코드를 생성하는 방법은 아래 수학식 1과 같이 표현될 수 있다.

수학식 1

[0055] $$QR\,code = encode(M_{QR})$$

[0056] 여기서, 'QR code'는 상술한 다차원 코드를, 'encode(x)'는 'x'를 이용하여 'x'를 포함하는 다차원 코드를 생성하기 위한 함수를 각각 의미할 수 있다. 또한, 'M_{QR}'는 상술한 첫 번째 방법에서는 $E_{pku}(M)$를, 두 번째 방법에서는 $Sign_{prs}(M)$를, 세 번째 방법에서는 $E_{pku}(M||S)$를 각각 포함할 수 있다. 또한 대칭키 'sk'를 이용한 방법에서는 $E_{sk}(M)$과 $E_{pku}(sk)$ 또는 $E_{sk}(M||S)$과 $E_{pku}(sk)$를 포함할 수 있다.

[0057] 다른 실시예에서는, 카메라가 부착된 휴대기기(240)과 다차원 코드를 이용하여 데이터 'M'을 사용자(210)에게 안전하게 전달하기 위해 휴대기기(240)과 서버(230)간에 미리 공유한 암호용/인증용 대칭키인 <ke, km>을 이용한다.

[0058] 우선, 서버(230)는 아래의 세 가지 방법 중 하나를 이용하여 휴대기기(240)로 데이터 'M'을 안전하게 전송하거나 전송된 데이터 또는 서버(230)가 휴대기기(240)에서 인증되도록 할 수 있다.

[0059] 첫 번째 방법으로, 서버(230)는 암호용 대칭키 'ke'로 데이터 'M'을 암호화하여 $E_{ke}(M)$를 생성하고, 생성된 $E_{ke}(M)$를 이용하여 다차원 코드를 생성하고, 생성된 다차원 코드를 사용자 단말기(220)로 전송할 수 있다. 여기서, 생성된 다차원 코드는 $E_{ke}(M)$를 포함할 수 있다. 사용자 단말기(220)는 전송된 다차원 코드를 디스플레이 장치를 통해 표시할 수 있고, 휴대기기(240)는 카메라를 통해 다차원 코드가 포함된 이미지를 입력받아 인식할 수 있다. 이때, 휴대기기(240)는 다차원 코드를 통해 얻어진 $E_{ke}(M)$를 인증용 대칭키 'km'을 이용하여 복호화함으로써, 데이터 'M'을 얻을 수 있다.

[0060] 두 번째 방법으로, 서버(230)는 인증용 대칭키 'km'을 이용하여 데이터 'M'에 대한 메시지 인증 코드 $MAC_{km}(M)$를 계산할 수 있다. 이때, 서버(230)는 메시지 인증 코드 $MAC_{km}(M)$를 이용하여 다차원 코드를 생성하고, 생성된 다차원 코드를 사용자 단말기(220)로 전송할 수 있다. 여기서, 생성된 다차원 코드는 메시지 인증 코드 $MAC_{km}(M)$를 포함할 수 있다. 또한, 사용자 단말기(220)는 전송된 다차원 코드를 디스플레이 장치를 통해 표시할 수 있고, 휴대기기(240)는 카메라를 통해 다차원 코드가 포함된 이미지를 입력받아 인식할 수 있다. 이때, 휴대기기(240)는 추가 전송된 데이터 'M'을 인증용 대칭키 'km'을 이용하여 메시지 인증 코드를 생성하고, 생성된 메시지 인증 코드와 다차원 코드를 이용하여 전송된 메시지 인증 코드 $MAC_{km}(M)$를 비교함으로써, 데이터 'M' 또는 서버(230)를 인증할 수 있다.

[0061] 세 번째 방법으로, 서버(230)는 인증용 대칭키 'km'을 이용하여 데이터 'M'에 대한 메시지 인증 코드 $MAC_{km}(M)$를 계산할 수 있다. 또한, 서버(230)는 암호용 대칭키 'ke'를 이용하여 'M||S' 즉, 메시지 인증 코드 $MAC_{km}(M)$를 암호화하여 $E_{ke}(M||S)$를 생성할 수 있다. 이때, 서버(230)는 $E_{ke}(M||S)$를 이용하여 다차원 코드를 생성하고, 생성된 다차원 코드를 사용자 단말기(220)로 전송할 수 있다. 여기서, 생성된 다차원 코드는 $E_{ke}(M||S)$를 포함할 수 있다. 또한, 사용자 단말기(220)는 전송된 다차원 코드를 디스플레이 장치를 통해 표시할 수 있고, 휴대기기(240)는 카메라를 통해 다차원 코드가 포함된 이미지를 입력받아 인식할 수 있다. 이때, 휴대기기(240)는 다차원 코드를 통해 전송된 $E_{ke}(M||S)$를 인증용 대칭키 'km'을 이용하여 복호화하여 $MAC_{km}(M)$를 얻을 수 있고, 추가 전송된 데이터 'M'을 인증용 대칭키 'km'을 이용하여 메시지 인증 코드를 생성할 수 있다. 즉, 휴대기기

(240)는 다차원 코드를 통해 얻어진 메시지 인증 코드 $MAC_{km}(M)$과 추가 전송된 데이터 'M'을 이용하여 생성한 메시지 인증 코드를 비교함으로써, 데이터 'M' 또는 서버(230)를 인증할 수 있다.

[0062] 즉, 두 번째 및 세 번째 방법에서는 별도로 전송된 데이터 'M'을 다차원 코드를 이용하여 인증하는 방법을 설명하고 있다. 이때, 두 번째 및 세 번째 방법에서도 필요에 따라서는 데이터 'M' 역시 다차원 코드에 포함되어 함께 전송될 수도 있다. 예를 들어, 데이터 'M'의 크기가 기선정된 크기 이하인 경우, 데이터 'M'이 다차원 코드에 함께 포함되어 전송될 수 있다.

[0063] 다차원 코드를 생성하는 방법은 상술한 수학식 1과 같이 표현될 수 있다. 다만, 이 경우, 'M_{QR}'는 상술한 첫 번째 방법에서는 $E_{ke}(M)$를, 두 번째 방법에서는 $MAC_{km}(M)$를, 세 번째 방법에서는 $E_{ke}(M||S)$를 각각 포함할 수 있다.

[0064] 도 2에서는 서버(230)에서 다차원 코드를 생성하여 사용자 단말기(220)로 전송하는 방법에 대해 설명하였으나, 필요에 따라 암호화된 또는 서명된 데이터를 사용자 단말기(220)로 전송하고, 사용자 단말기(220)에서 다차원 코드를 생성할 수도 있다.

[0065] 또한, 도 1 및 도 2에서 실선 화살표는 직접적인 데이터 전달을 의미할 수 있고, 점선 화살표는 간접적인 데이터 전달을 의미할 수 있다. 여기서 직접적인 데이터 전달이란, 유무선 네트워크를 통해 데이터를 직접 전송하는 것을 의미할 수 있고, 간접적인 데이터 전달은 상술한 바와 같이, 사용자 단말기(120 또는 220)에서 화면에 다차원 코드를 표시하고, 휴대기기(140 또는 240)의 카메라를 통해 다차원 코드를 입력받는 전달을 의미할 수 있다.

[0066] 도 3은 본 발명의 일실시예에 있어서, 공인인증서 전송을 위한 휴대기기의 내부 구성을 설명하기 위한 블록도이다. 본 실시예에 따른 휴대기기(300)는 도 1을 통해 설명한 휴대기기(140)에 대응될 수 있다. 휴대기기(300)는 도 3에 도시된 바와 같이 다차원 코드 인식부(310), 추출부(320), 복호화부(330) 및 검증부(340)를 포함할 수 있다. 또한, 필요에 따라 수신부(350)를 더 포함할 수 있다.

[0067] 다차원 코드 인식부(310)는 카메라를 통해 입력된 이미지에서 다차원 코드를 인식한다. 이때, 다차원 코드는 사용자 단말기의 디스플레이 장치를 통해 표시되고, 다차원 코드 인식부(310)는 다차원 코드가 표시된 화면을 카메라로 찍어 입력된 이미지에서 다차원 코드를 인식할 수 있다. 여기서, 일실시예로, 다차원 코드는 암호화된 공인인증서 및 암호화된 사용자의 비밀키를 포함한다. 즉, 사용자에 의해 사용자 단말기에서 생성된 공개키 및 비밀키는 공인인증기관의 서버로 전송될 수 있고, 서버는 공개키와 비밀키 중 공개키를 이용하여 공인인증서를 생성할 수 있다. 또한, 공인인증서 및 비밀키는 휴대기기(300)와 공인인증기관의 서버간에 미리 교환된 임시 비밀키와 과거에 사용자에 의해 사용자 단말기에서 생성되어 이용된 후 폐기되지 않은 사용자의 예전 공개키 중 하나의 키를 이용하여 암호화될 수 있다. 이때, 암호화된 공인인증서와 암호화된 비밀키는 서버에서 사용자 단말기로 전송될 수 있고, 사용자 단말기는 암호화된 공인인증서와 암호화된 비밀키를 이용하여 다차원 코드를 생성하여 디스플레이 장치를 통해 표시할 수 있다.

[0068] 추출부(320)는 인식된 다차원 코드에서 암호화된 공인인증서와 암호화된 비밀키를 추출한다.

[0069] 복호화부(330)는 임시 비밀키와 예전 공개키 중 하나의 키를 이용하여 암호화된 공인인증서와 암호화된 비밀키를 복호화한다.

[0070] 검증부(340)는 복호화된 공인인증서가 포함하는 소유주, 인증기관명 및 공개키 중 적어도 하나를 이용하여 복호화된 공인인증서를 검증한다.

[0071] 다른 실시예에서, 다차원 코드는 암호화된 공인인증서를 포함한다. 이때, 휴대기기(300)는 사용자 단말기로부터 암호화된 비밀키를 수신하는 비밀키 수신부(350)를 더 포함할 수 있다. 여기서, 비밀키는 임시 비밀키와 예전 공개키 중 하나의 키를 이용하여 암호화될 수 있다. 이 경우, 추출부(320)는 인식된 다차원 코드에서 암호화된 공인인증서를 추출한다.

[0072] 도 4는 본 발명의 일실시예에 있어서, 공인인증서 전송을 위한 서버의 내부 구성을 설명하기 위한 블록도이다. 본 실시예에 따른 서버(400)는 도 1을 통해 설명한 서버(130)에 대응될 수 있다. 서버(400)는 도 4에 도시된 바와 같이 키 수신부(410), 공인인증서 생성부(420), 암호화부(430) 및 전송부(440)를 포함할 수 있다.

[0073] 키 수신부(410)는 사용자 단말기로부터 사용자의 공개키 및 비밀키를 수신한다. 여기서, 사용자의 공개키 및 비밀키는 사용자에 의해 사용자 단말기에서 생성될 수 있다.

[0074] 공인인증서 생성부(420)는 공개키를 이용하여 공인인증서를 생성한다. 공인인증서를 생성하는 방법으로는 이미

알려진 다양한 방법들 중 하나가 이용될 수 있다.

[0075] 암호화부(430)는 생성된 공인인증서 및 비밀키를 휴대기기와 미리 교환한 임시 비밀키 및 과거에 사용자에 의해 사용자 단말기에서 생성되어 이용된 후 폐기되지 않은 사용자의 예전 공개키 중 하나의 키를 이용하여 암호화한다.

[0076] 전송부(440)는 암호화된 공인인증서를 사용자 단말기로 전송한다. 이때, 사용자 단말기는 암호화된 공인인증서를 이용하여 다차원 코드를 생성하고, 생성된 다차원 코드는 사용자 단말기의 디스플레이 장치를 통해 표시된다. 이 경우, 표시된 다차원 코드는 휴대기기의 카메라를 통해 촬영되어 휴대기기로 입력된다. 휴대기기는 촬영된 이미지에서 다차원 코드를 인식하고, 다차원 코드에서 암호화된 공인인증서 및 암호화된 비밀키를 추출하고 복호화하여 공인인증서와 비밀키를 얻을 수 있다.

[0077] 다른 실시예에서, 키 수신부(410)는 사용자 단말기로부터 사용자의 공개키를 수신한다. 이때, 암호화부(430)는 생성된 공인인증서를 암호화할 수 있다. 사용자 단말기는 암호화된 공인인증서를 수신할 수 있고, 사용자의 비밀키를 임시 비밀키와 예전 공개키 중 하나의 키를 이용하여 암호화할 수 있다. 이 경우, 사용자 단말기는 암호화된 공인인증서와 암호화된 비밀키를 이용하여 다차원 코드를 생성할 수 있고, 생성된 다차원 코드를 디스플레이 장치를 통해 화면에 표시할 수 있다. 휴대기기는 카메라를 통해 입력된 이미지에서 다차원 코드를 인식하고, 다차원 코드에서 암호화된 공인인증서와 암호화된 비밀키를 얻을 수 있게 된다. 이 경우, 휴대기기는 임시 비밀키와 예전 공개키 중 하나의 키를 이용하여 공인인증서와 비밀키를 복호화함으로써, 공인인증서와 비밀키를 얻게 된다.

[0078] 도 5는 본 발명의 일실시예에 있어서, 공인인증서 전송을 위한 사용자 단말기의 내부 구성을 설명하기 위한 블록도이다. 본 실시예에 따른 사용자 단말기(500)는 도 1을 통해 설명한 사용자 단말기(120)에 대응될 수 있다. 사용자 단말기(500)는 도 5에 도시된 바와 같이 키 생성부(510), 키 전송부(520), 수신부(530), 다차원 코드 생성부(540) 및 표시부(550)를 포함할 수 있다.

[0079] 키 생성부(510)는 사용자의 공개키 및 비밀키를 생성한다.

[0080] 키 전송부(520)는 공개키 및 비밀키를 공인인증기관의 서버로 전송한다.

[0081] 수신부(530)는 서버로부터 암호화된 공인인증서 및 암호화된 비밀키를 수신한다. 이때, 서버는 수신한 공개키를 이용하여 공인인증서를 생성하고, 휴대기기와 미리 교환한 임시 비밀키 및 과거에 사용자에 의해 사용자 단말기에서 생성되어 이용된 후 폐기되지 않은 사용자의 예전 공개키 중 하나의 키를 이용하여 생성된 공인인증서와 비밀키를 암호화할 수 있다. 이 경우, 서버는 암호화된 공인인증서와 암호화된 비밀키를 사용자 단말기(500)로 전송할 수 있고, 수신부(530)는 암호화된 공인인증서와 암호화된 비밀키를 수신할 수 있게 된다.

[0082] 다차원 코드 생성부(540)는 암호화된 공인인증서와 암호화된 비밀키를 이용하여 다차원 코드를 생성한다.

[0083] 표시부(550)는 다차원 코드를 디스플레이 장치를 통해 표시한다.

[0084] 이후, 휴대기기는 휴대기기의 카메라를 통해 다차원 코드를 포함하는 이미지를 촬영하고, 이미지에서 다차원 코드를 인식할 수 있다. 또한, 휴대기기는 다차원 코드로부터 암호화된 공인인증서와 암호화된 비밀키를 추출하여 복호화함으로써, 공인인증서와 비밀키를 얻을 수 있다.

[0085] 도 6은 본 발명의 일실시예에 있어서, 공개키와 비밀키를 모두 전송하는 경우의 공인인증서 전송 방법을 도시한 흐름도이다. 도 6은 도 3 내지 도 5 각각의 첫 번째 실시예에서 설명한 휴대기기(300), 사용자 단말기(500) 및 서버(400)를 나타내고 있다.

[0086] 우선, 사용자 단말기(500)는 사용자의 공개키 및 비밀키를 생성(601)한다. 이때, 제1 실선(602)은 사용자의 공개키 및 비밀키가 사용자 단말기(500)에서 서버(400)로 전송됨을 의미할 수 있다. 서버(400)는 공개키로 공인인증서를 생성(603)하고, 공인인증서 및 비밀키를 암호화(604)한다. 이때, 암호화(604)는 서버(400)와 휴대기기(300)간에 미리 교환한 임시 비밀키 및 과거에 사용자에 의해 사용자 단말기(500)에서 생성되어 이용된 후 폐기되지 않은 사용자의 예전 공개키 중 하나의 키를 이용하여 수행될 수 있다. 제2 실선(605)은 암호화된 공인인증서와 암호화된 비밀키가 서버(400)에서 사용자 단말기(500)로 전송됨을 의미할 수 있다. 이때, 사용자 단말기(500)는 다차원 코드를 생성(606)한다. 이 경우, 사용자 단말기(500)는 암호화된 공인인증서와 암호화된 비밀키를 이용하여 암호화된 공인인증서와 암호화된 비밀키가 포함되도록 다차원 코드를 생성할 수 있다.

[0087] 점선(607)은 사용자 단말기(500)의 디스플레이 장치를 통해 표시된 다차원 코드가 휴대기기(300)의 카메라를 통

해 촬영됨으로써, 휴대기기(300)로 제공될 수 있음을 나타낸다. 이때, 휴대기기(300)는 촬영된 이미지에서 다차원 코드를 인식할 수 있다. 또한, 휴대기기(300)는 다차원 코드에서 암호화된 공인인증서 및 암호화된 비밀키를 추출(608)하고, 암호화된 공인인증서 및 암호화된 비밀키를 복호화(609)함으로써, 공인인증서와 비밀키를 얻을 수 있다. 이때, 복호화(609)는 임시 비밀키 및 예전 공개키 중 하나의 키를 이용하여 수행될 수 있다.

[0088] 도 7은 본 발명의 일실시예에 있어서, 공개키를 전송하는 경우의 공인인증서 전송 방법을 도시한 흐름도이다. 도 7은 도 3 내지 도 5 각각의 두 번째 실시예에서 설명한 휴대기기(300), 사용자 단말기(500) 및 서버(400)를 나타내고 있다.

[0089] 우선, 사용자 단말기(500)는 사용자의 공개키 및 비밀키를 생성(701)한다. 이때, 제1 실선(702)은 사용자의 공개키가 사용자 단말기(500)에서 서버(400)로 전송됨을 의미할 수 있다. 서버(400)는 공개키로 공인인증서를 생성(703)하고, 공인인증서를 암호화(704)한다. 이때, 암호화(704)는 서버(400)와 휴대기기(300)간에 미리 교환한 임시 비밀키 및 과거에 사용자에 의해 사용자 단말기(500)에서 생성되어 이용된 후 폐기되지 않은 사용자의 예전 공개키 중 하나의 키를 이용하여 수행될 수 있다. 제2 실선(705)은 암호화된 공인인증서가 서버(400)에서 사용자 단말기(500)로 전송됨을 의미할 수 있다. 이때, 사용자 단말기(500)는 비밀키를 암호화(706)하고, 다차원 코드를 생성(707)한다. 이 경우, 사용자 단말기(500)는 상술한 임시 비밀키 및 예전 공개키 중 하나의 키를 이용하여 비밀키를 암호화할 수 있고, 암호화된 공인인증서와 암호화된 비밀키를 이용하여 암호화된 공인인증서와 암호화된 비밀키가 포함되도록 다차원 코드를 생성할 수 있다.

[0090] 점선(708)은 사용자 단말기(500)의 디스플레이 장치를 통해 표시된 다차원 코드가 휴대기기(300)의 카메라를 통해 촬영됨으로써, 휴대기기(300)로 제공될 수 있음을 나타낸다. 이때, 휴대기기(300)는 촬영된 이미지에서 다차원 코드를 인식할 수 있다. 또한, 휴대기기(300)는 다차원 코드에서 암호화된 공인인증서 및 암호화된 비밀키를 추출(709)하고, 암호화된 공인인증서 및 암호화된 비밀키를 복호화(710)함으로써, 공인인증서와 비밀키를 얻을 수 있다. 이때, 복호화(710)는 임시 비밀키 및 예전 공개키 중 하나의 키를 이용하여 수행될 수 있다.

[0091] 도 8은 본 발명의 일실시예에 있어서, 데이터의 전송 또는 인증을 위한 휴대기기의 내부 구성을 설명하기 위한 블록도이다. 본 실시예에 따른 휴대기기(800)는 도 2를 통해 설명한 휴대기기(240)에 대응될 수 있다. 휴대기기(800)는 도 8에 도시된 바와 같이, 다차원 코드 인식부(810), 추출부(820) 및 복호화부(830)를 포함할 수 있고, 필요에 따라 검증부(840)를 더 포함할 수 있다.

[0092] 일실시예에서, 다차원 코드 인식부(810)는 카메라를 통해 입력된 이미지에서 다차원 코드를 인식한다. 이때, 다차원 코드는 사용자 단말기의 디스플레이 장치를 통해 표시되고, 다차원 코드 인식부(810)는 다차원 코드가 표시된 화면을 카메라로 찍어 입력된 이미지에서 다차원 코드를 인식할 수 있다. 여기서, 다차원 코드는 암호화된 데이터 또는 서명된 데이터를 포함한다. 즉, 서버는 사용자의 공개키로 전송하기 위한 데이터를 암호화하거나 또는 서버의 비밀키로 데이터를 서명할 수 있고, 암호화된 데이터 또는 서명된 데이터를 이용하여 다차원 코드를 생성한 후 사용자 단말기로 전송할 수 있다. 사용자의 공개키로 데이터를 암호화하거나 서버의 비밀키로 서명하는 방법에 대해서는 도 2를 참조할 수 있다. 이때, 사용자 단말기는 다차원 코드를 수신하여 디스플레이 장치를 통해 표시할 수 있다. 휴대기기(800)는 표시된 다차원 코드를 카메라를 이용하여 촬영할 수 있고, 다차원 코드 인식부(810)는 촬영된 이미지에서 다차원 코드를 인식할 수 있다.

[0093] 추출부(820)는 인식된 다차원 코드에서 암호화된 데이터 또는 서명된 데이터를 추출한다.

[0094] 복호화부(830)는 암호화된 데이터를 복호화하여 데이터를 획득하거나 또는 서명된 데이터를 검증하여 서버로부터 전송된 데이터 또는 서버를 인증한다. 암호화된 데이터를 복호화하여 데이터를 획득하는 방법과, 데이터 또는 서버를 인증하는 방법에 대해서는 도 2를 참조할 수 있다.

[0095] 또한, 필요에 따라 다차원 코드의 생성은 사용자 단말기에서 수행될 수도 있다. 즉, 서버는 암호화된 데이터 또는 서명된 데이터를 사용자 단말기로 전송하고, 사용자 단말기는 암호화된 데이터 또는 서명된 데이터를 이용하여 다차원 코드를 생성할 수도 있다.

[0096] 다른 실시예에서, 다차원 코드 인식부(810)는 카메라를 통해 입력된 이미지에서 다차원 코드를 인식한다. 이때, 다차원 코드는 사용자 단말기의 디스플레이 장치를 통해 표시되고, 다차원 코드 인식부(810)는 다차원 코드가 표시된 화면을 카메라로 찍어 입력된 이미지에서 다차원 코드를 인식할 수 있다. 여기서, 다차원 코드는 암호화된 데이터 또는 메시지 인증 코드를 포함한다. 이때, 서버는 휴대기기(800)와 사전에 공유한 암호용/인증용 대칭키를 이용하여 암호용 대칭키로 전송하기 위한 데이터를 암호화하거나 또는 인증용 대칭키로 전송하기 위한 데이터의 메시지 인증 코드를 생성할 수 있다. 또한, 서버는 암호화된 데이터 또는 메시지 인증 코드를

이용하여 다차원 코드를 생성한 후 사용자 단말기로 전송할 수 있다. 암호용 대칭키로 데이터를 암호화하거나 메시지 인증 코드를 생성하는 방법에 대해서는 도 2를 참조할 수 있다. 이때, 사용자 단말기는 다차원 코드를 수신하여 디스플레이 장치를 통해 표시할 수 있다. 휴대기기(800)는 표시된 다차원 코드를 카메라를 이용하여 촬영할 수 있고, 다차원 코드 인식부(810)는 촬영된 이미지에서 다차원 코드를 인식할 수 있다.

[0097] 추출부(820)는 인식된 다차원 코드에서 암호화된 데이터 또는 메시지 인증 코드를 추출한다.

[0098] 복호화부(830)는 암호화된 데이터를 복호화하여 데이터를 획득하거나 또는 메시지 인증 코드를 이용하여 서버로부터 전송된 데이터 또는 서버를 인증한다. 암호화된 데이터를 복호화하여 데이터를 획득하는 방법과, 메시지 인증 코드를 이용하여 데이터 또는 서버를 인증하는 방법에 대해서는 도 2를 참조할 수 있다.

[0099] 다른 실시예에서도 다차원 코드는 서버가 아닌 사용자 단말기에서 생성될 수 있다.

[0100] 도 9는 본 발명의 일실시예에 있어서, 데이터의 전송 또는 인증을 위한 서버의 내부 구성을 설명하기 위한 블록도이다. 본 실시예에 따른 서버(900)는 도 2를 통해 설명한 서버(230)에 대응될 수 있다. 서버(900)는 도 9에 도시된 바와 같이, 암호화부(910), 다차원 코드 생성부(920) 및 전송부(930)를 포함할 수 있다.

[0101] 일실시예에서, 암호화부(910)는 사용자의 공개키로 데이터를 암호화하거나 또는 서버의 비밀키로 데이터를 서명한다. 이때, 암호화부(910)는 서명된 데이터를 사용자의 공개키로 다시 암호화할 수도 있다. 데이터를 암호화하거나 서명하는 방법에 대해서는 도 2를 참조할 수 있다.

[0102] 다차원 코드 생성부(920)는 암호화된 데이터 또는 서명된 데이터를 이용하여 다차원 코드를 생성한다.

[0103] 전송부(930)는 생성된 다차원 코드를 사용자 단말기로 전송한다.

[0104] 이때, 사용자 단말기에서 다차원 코드를 생성하는 경우에는, 서버(900)에서 다차원 코드 생성부(920)는 생략될 수도 있다. 즉, 서버(900)는 암호화부(910)와 전송부(930)만을 포함할 수도 있다. 이 경우, 전송부(930)는 암호화부(910)를 통해 암호화된 데이터 또는 서명된 데이터를 사용자 단말기로 전송할 수 있다. 이때, 사용자 단말기는 암호화된 데이터 또는 서명된 데이터를 이용하여 다차원 코드를 생성할 수 있다.

[0105] 사용자 단말기는 전송된 또는 생성된 다차원 코드를 디스플레이 장치를 통해 표시하고, 휴대기기는 표시된 다차원 코드를 카메라로 촬영하고, 촬영된 이미지에서 다차원 코드를 인식할 수 있다. 또한, 휴대기기는 인식된 다차원 코드에서 암호화된 데이터 또는 서명된 데이터를 추출하고, 추출된 데이터를 복호화하여 서버(900)에서 전송하고자 하는 데이터를 획득하거나 서명된 데이터를 서명검증하여 서버(900)로부터 전송된 데이터나 서버(900)를 인증할 수 있다.

[0106] 다른 실시예에서, 암호화부(910)는 휴대기기와 사전에 공유한 암호용/인증용 대칭키를 이용하여 암호용 대칭키로 전송하기 위한 데이터를 암호화하거나 또는 인증용 대칭키로 전송하기 위한 데이터의 메시지 인증 코드를 생성한다. 이때, 암호화부(910)는 생성된 메시지 인증 코드를 암호용 대칭키로 다시 암호화할 수도 있다. 암호용 대칭키로 데이터를 암호화하거나 메시지 인증 코드를 생성하는 방법에 대해서는 도 2를 참조할 수 있다.

[0107] 다차원 코드 생성부(920)는 암호화된 데이터 또는 메시지 인증 코드를 이용하여 다차원 코드를 생성한다.

[0108] 전송부(930)는 생성된 다차원 코드를 사용자 단말기로 전송한다.

[0109] 이때, 사용자 단말기에서 다차원 코드를 생성하는 경우에는, 다른 실시예에서도, 서버(900)에서 다차원 코드 생성부(920)가 생략될 수도 있다. 즉, 서버(900)는 암호화부(910)와 전송부(930)만을 포함할 수도 있다. 이 경우, 전송부(930)는 암호화부(910)를 통해 암호화된 데이터 또는 메시지 인증 코드를 사용자 단말기로 전송할 수 있다. 이때, 사용자 단말기는 암호화된 데이터 또는 서명된 데이터를 이용하여 다차원 코드를 생성할 수 있다.

[0110] 사용자 단말기는 전송된 또는 생성된 다차원 코드를 디스플레이 장치를 통해 표시하고, 휴대기기는 표시된 다차원 코드를 카메라로 촬영하고, 촬영된 이미지에서 다차원 코드를 인식할 수 있다. 또한, 휴대기기는 인식된 다차원 코드에서 암호화된 데이터 또는 서명된 데이터를 추출하고, 추출된 데이터를 복호화하여 서버(900)에서 전송하고자 하는 데이터를 획득하거나 서명된 데이터를 서명검증하여 서버(900)로부터 전송된 데이터나 서버(900)를 인증할 수 있다.

[0111] 도 10은 본 발명의 일실시예에 있어서, 데이터의 전송 또는 인증을 사용자 단말기의 내부 구성을 설명하기 위한 블록도이다. 본 실시예에 따른 사용자 단말기(1000)는 도 2를 통해 설명한 사용자 단말기(220)에 대응될 수 있다. 사용자 단말기(1000)는 수신부(1010) 및 표시부(1030)를 포함할 수 있고, 사용자 단말기(1000)에서 다차원

코드를 생성하는 경우, 다차원 코드 생성부(1020)를 더 포함할 수 있다.

[0112] 우선, 일실시예에서 수신부(1010)는 서버로부터 다차원 코드를 수신할 수 있다. 여기서, 다차원 코드는 서버에서 사용자의 공개키로 암호화된 데이터 또는 서버의 비밀키로 서명된 데이터를 포함할 수 있다.

[0113] 표시부(1030)는 다차원 코드를 디스플레이 장치를 통해 표시한다. 이때, 디스플레이 장치를 통해 표시된 다차원 코드는 휴대기기의 카메라를 통해 휴대기기에 입력되어 인식될 수 있다.

[0114] 이때, 상술한 바와 같이 사용자 단말기(1000)는 다차원 코드 생성부(1020)를 더 포함할 수 있다. 이 경우, 수신부(1010)는 서버에서 암호화된 데이터 또는 서버에서 서명된 데이터를 수신할 수 있고, 다차원 코드 생성부(1020)는 암호화된 데이터 또는 서명된 데이터를 이용하여 다차원 코드를 생성할 수 있다. 이 경우, 표시부(1030)는 다차원 코드 생성부(1020)에서 생성된 다차원 코드를 디스플레이 장치를 통해 표시할 수 있다.

[0115] 다른 실시예에서, 수신부(1010)는 서버로부터 다차원 코드를 수신할 수 있다. 여기서, 다차원 코드는 서버에서 휴대기기와 사전에 공유한 암호용/인증용 대칭키 중 암호용 대칭키로 암호화된 데이터 또는 인증용 대칭키를 이용하여 생성된 메시지 인증 코드를 포함할 수 있다.

[0116] 표시부(1030)는 다차원 코드를 디스플레이 장치를 통해 표시한다. 이때, 디스플레이 장치를 통해 표시된 다차원 코드는 휴대기기의 카메라를 통해 휴대기기에 입력되어 인식될 수 있다.

[0117] 이때, 상술한 바와 같이 사용자 단말기(1000)는 다차원 코드 생성부(1020)를 더 포함할 수 있다. 이 경우, 수신부(1010)는 서버에서 암호화된 데이터 또는 메시지 인증 코드를 수신할 수 있고, 다차원 코드 생성부(1020)는 암호화된 데이터 또는 메시지 인증 코드를 이용하여 다차원 코드를 생성할 수 있다. 이 경우, 표시부(1030)는 다차원 코드 생성부(1020)에서 생성된 다차원 코드를 디스플레이 장치를 통해 표시할 수 있다.

[0118] 도 11은 본 발명의 일실시예에 있어서, 공개키 및 비밀키를 이용하여 데이터를 전송하거나 또는 인증하는 방법을 도시한 흐름도이다. 도 11은 서버(900)에서 다차원 코드를 생성하는 경우를 나타내고 있다.

[0119] 우선, 서버(900)는 데이터를 암호화하거나 또는 데이터를 서명(1101)한다. 이때, 서버(900)는 사용자의 공개키를 이용하여 데이터를 암호화하거나 서버(900)의 비밀키를 이용하여 데이터를 서명할 수 있다. 또한, 서버(900)는 암호화된 데이터 또는 서명된 데이터를 이용하여 다차원 코드를 생성(1102)할 수 있다.

[0120] 실선 화살표(1103)는 생성된 다차원 코드가 서버(900)에서 사용자 단말기(1000)로 전송됨을 의미할 수 있다. 또한, 점선 화살표(1104)는 사용자 단말기(1000)가 전송된 다차원 코드를 디스플레이 장치를 통해 표시하고, 휴대기기(800)가 카메라를 통해 표시된 다차원 코드를 촬영하여 촬영된 이미지에서 다차원 코드를 인식하는 과정을 의미할 수 있다.

[0121] 휴대기기(800)는 다차원 코드에서 암호화된 데이터 또는 서명된 데이터를 추출(1105)하고, 암호화된 데이터를 복호화하거나 또는 서명된 데이터를 서명검증하여 데이터 또는 서버(900)를 인증할 수 있다.

[0122] 이 경우에도, 도 11과는 다르게 서버(900)가 아닌 사용자 단말기(1000)에서 다차원 코드가 생성될 수 있다.

[0123] 도 12는 본 발명의 일실시예에 있어서, 암호용/인증용 대칭키를 이용하여 데이터를 전송하거나 또는 인증하는 방법을 도시한 흐름도이다. 도 12은 서버(900)에서 다차원 코드를 생성하는 경우를 나타내고 있다.

[0124] 우선, 서버(900)는 데이터를 암호화하거나 또는 메시지 인증 코드를 생성(1101)한다. 이때, 서버(900)는 휴대기기(800)와 사전에 공유된 암호용/인증용 대칭키 중 암호용 대칭키를 이용하여 데이터를 암호화하거나 인증용 대칭키를 이용하여 데이터에 대한 메시지 인증 코드를 생성할 수 있다. 또한, 서버(900)는 암호화된 데이터 또는 메시지 인증 코드를 이용하여 다차원 코드를 생성(1102)할 수 있다.

[0125] 실선 화살표(1103)는 생성된 다차원 코드가 서버(900)에서 사용자 단말기(1000)로 전송됨을 의미할 수 있다. 또한, 점선 화살표(1104)는 사용자 단말기(1000)가 전송된 다차원 코드를 디스플레이 장치를 통해 표시하고, 휴대기기(800)가 카메라를 통해 표시된 다차원 코드를 촬영하여 촬영된 이미지에서 다차원 코드를 인식하는 과정을 의미할 수 있다.

[0126] 휴대기기(800)는 다차원 코드에서 암호화된 데이터 또는 서명된 데이터를 추출(1105)하고, 암호화된 데이터를 복호화하거나 또는 서명된 데이터를 서명검증하여 데이터 또는 서버(900)를 인증할 수 있다.

[0127] 이 경우에도, 도 12와는 다르게 서버(900)가 아닌 사용자 단말기(1000)에서 다차원 코드가 생성될 수 있다.

[0128] 도 2 그리고 도 8내지 도 12에서는 서버에서 사용자의 공개키를 이용한 데이터 또는 서명된 데이터의 암호화,

서버의 비밀키를 이용한 데이터의 서명, 그리고 암호용 대칭키를 이용한 데이터의 암호화 및 인증용 대칭키를 이용한 메시지 인증 코드의 생성 등을 각각의 실시예로 설명하였으나, 필요에 따라 서버는 하나의 데이터를 사용자의 공개키로 암호화하고 서버의 비밀키로 서명하여 암호화된 데이터와 서명된 데이터를 모두 사용자 단말기로 전송하거나 또는 다차원 코드를 생성할 수 있다. 이는 암호용/인증용 대칭키 역시 동일하게 적용될 수 있다. 휴대기기 역시 하나의 휴대기기에서 사용자의 비밀키, 상기 서버의 공개키, 상기 암호용/인증용 대칭키를 모두 또는 일부 포함하여 암호화된 데이터, 서명된 데이터 및 메시지 인증 코드의 복호화 및 검증이 모두 수행될 수 있다. 예를 들어, 서버는 하나의 데이터를 사용자의 공개키로 암호화하고, 서버의 비밀키로 해당 데이터를 서명하여, 암호화된 데이터와 서명된 데이터를 통해 다차원 코드를 생성함으로써, 하나의 다차원 코드를 통해 데이터의 비밀 전송과 인증이 동시에 이루어지도록 할 수도 있다.

[0129] 이와 같이, 본 발명의 실시예들에 따른 시스템 및 방법을 이용하면, 사용자 단말기로 전송된 공인인증서를 QR 코드와 같은 다차원 코드를 이용하여 휴대기기로 전송할 수 있고, 사용자의 공개키를 이용하여 생성된 공인인증서를 휴대기기와 공인 인증기관 사이에 미리 교환된 임시 비밀키 또는 과거 사용되었으나 폐기되지 않은 사용자의 예전 공개키를 이용하여 암호화하고, 암호화된 공인인증서를 사용자 단말기로 전송하여 사용자 단말기에서 암호화된 공인인증서를 이용하여 다차원 코드를 생성 및 표시하여 휴대기기로 전송할 수 있다.

[0130] 다차원 코드를 이용하여 데이터를 비밀 전송 및 인증할 수 있고, 공개키와 비밀키 그리고 다차원 코드를 이용하여 데이터를 비밀 전송 및 인증할 수 있다. 또한, 휴대기기와 공인인증기관의 서버간에 미리 공유된 암호용/인증용 대칭키와 다차원 코드를 이용하여 데이터를 비밀 전송 및 인증할 수 있다.

[0131] 본 발명의 실시예에 따른 방법들은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 또한, 상술한 파일 시스템은 컴퓨터 판독이 가능한 기록 매체에 기록될 수 있다.

[0132] 이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[0133] 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

[0134] 110: 사용자

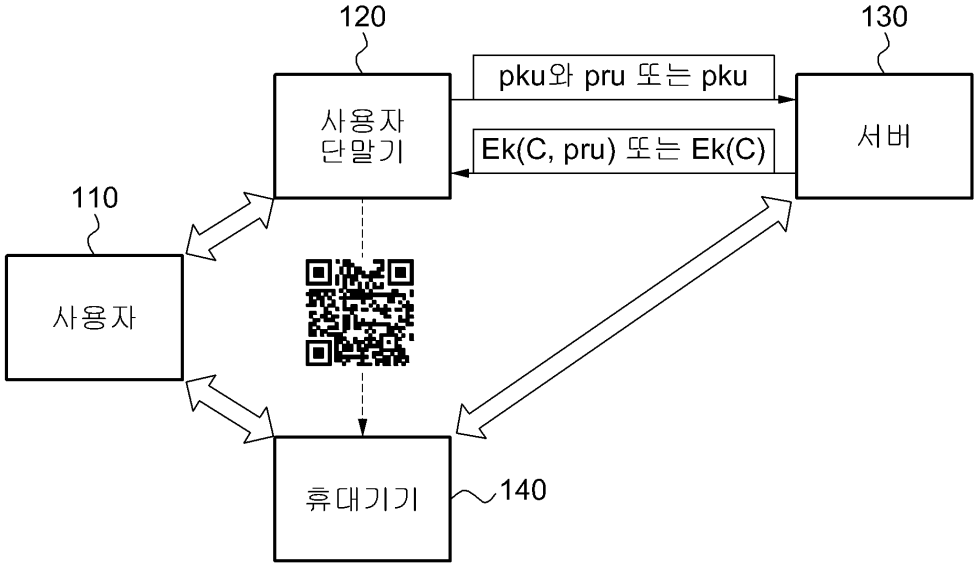
120: 사용자 단말기

130: 서버

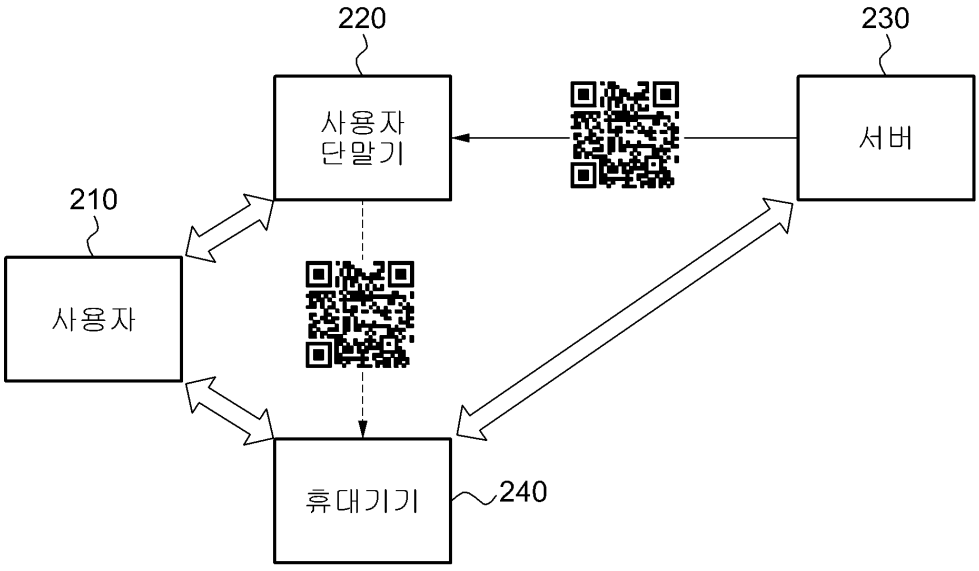
140: 휴대기기

도면

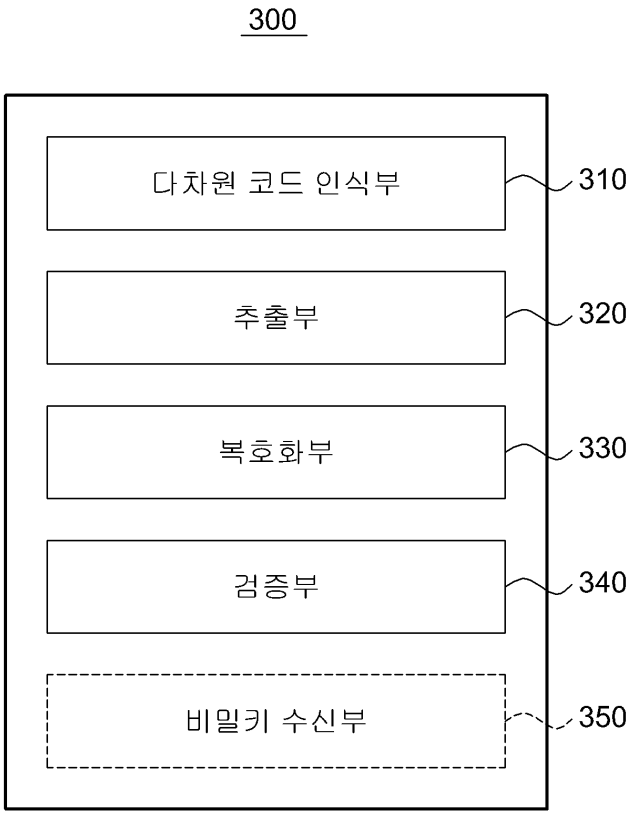
도면1


120
130
pku와 pru 또는 pku
사용자
단말기
Ek(C, pru) 또는 Ek(C)
서버
110
사용자
휴대기기
140

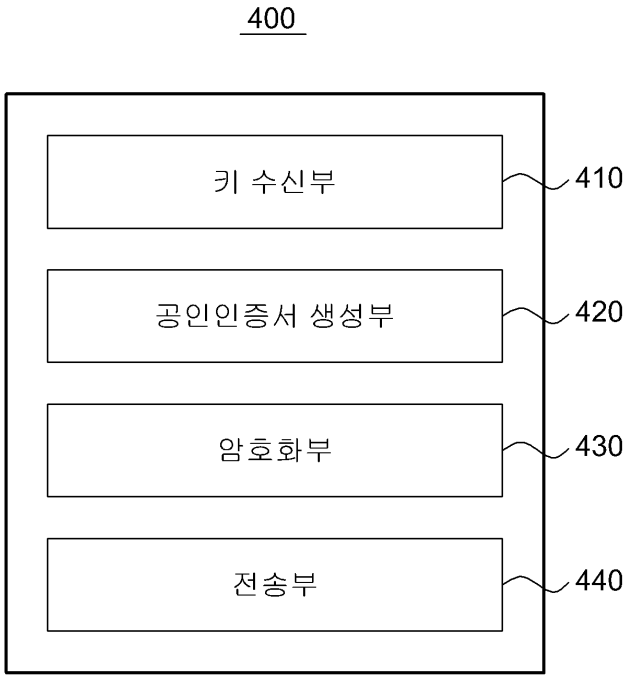
도면2


220
230
사용자
단말기
서버
210
사용자
휴대기기
240

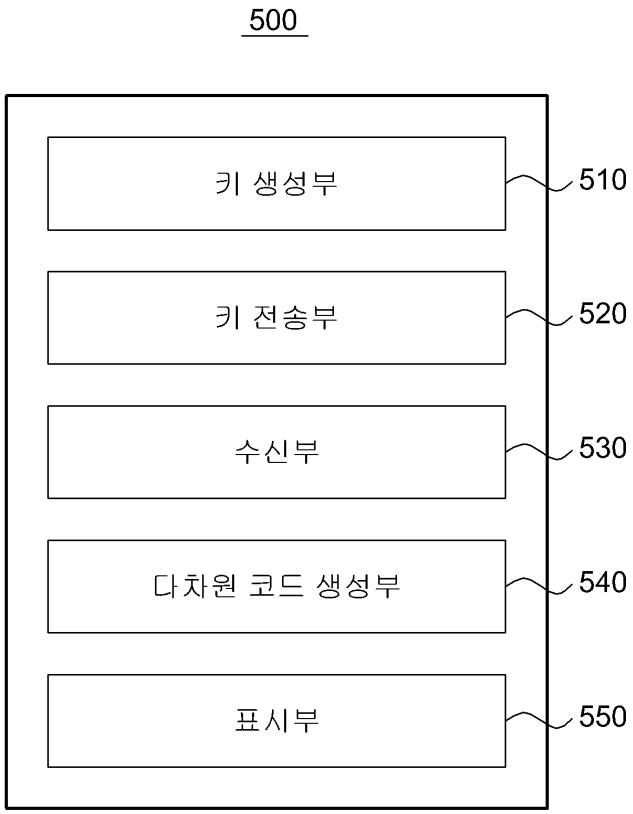
도면3


300
다차원 코드 인식부
310
추출부
320
복호화부
330
검증부
340
비밀키 수신부
350

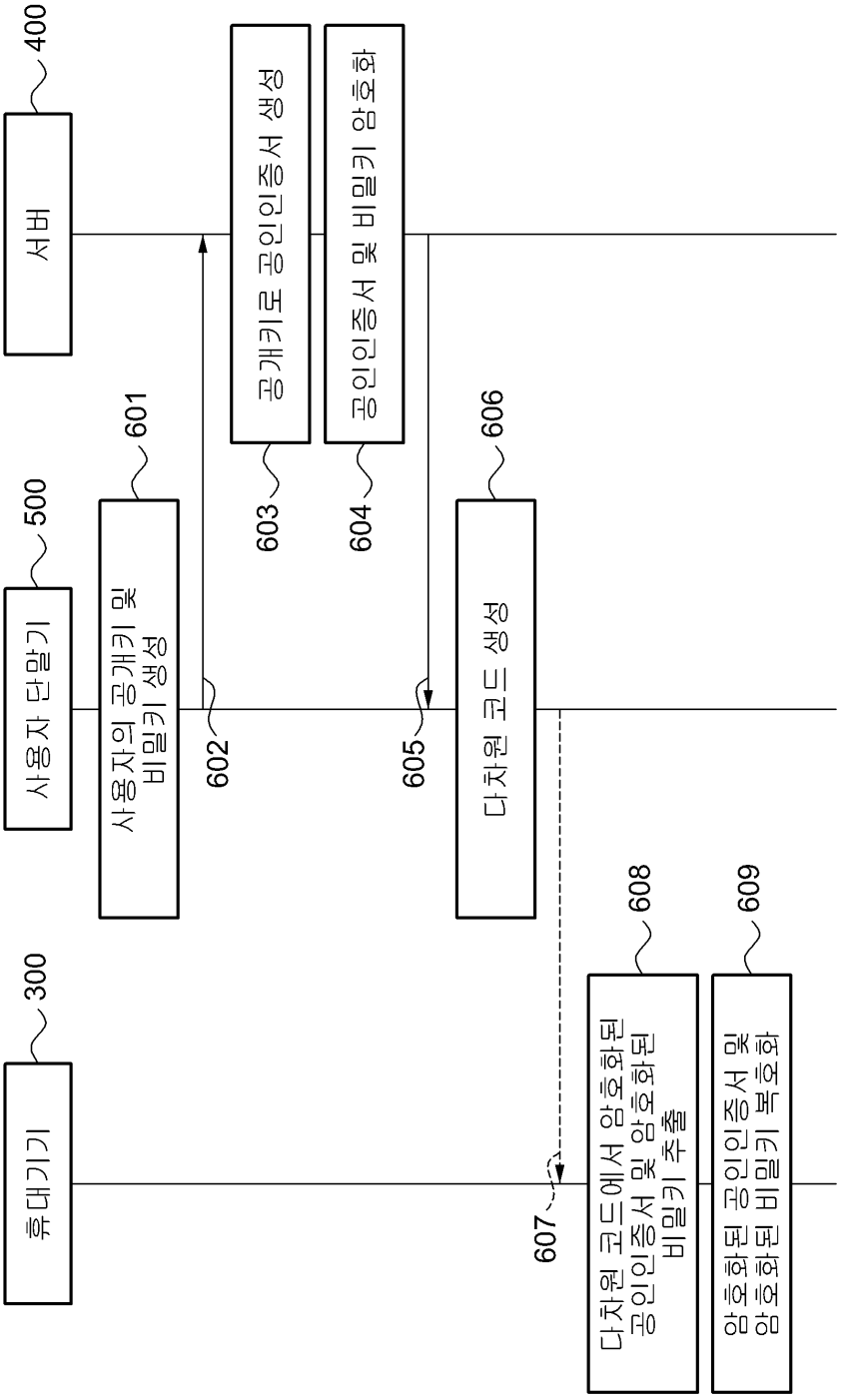
도면4


400
키 수신부
410
공인인증서 생성부
420
암호화부
430
전송부
440

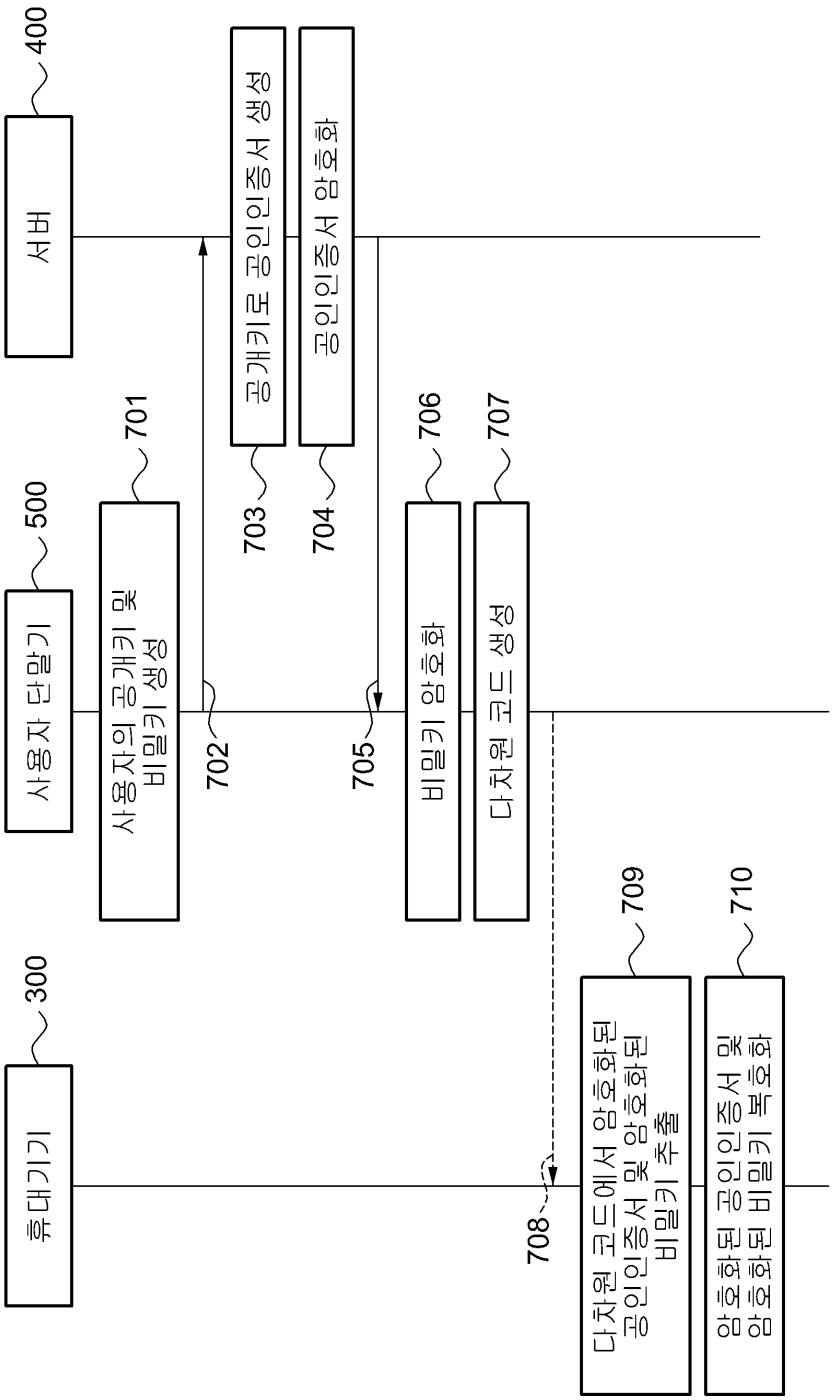
도면5



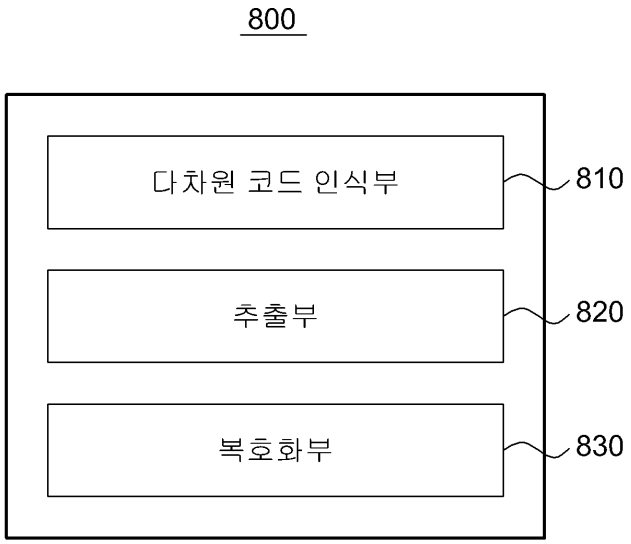
도면6


400
서버
601
500
사용자 단말기
사용자의 공개키 및
비밀키 생성
603
공개키로 공인인증서 생성
604
공인인증서 및 비밀키 암호화
606
602
605
다차원 코드 생성
300
휴대기기
608
609
다차원 코드에서 암호화된
공인인증서 및 암호화된
비밀키 추출
암호화된 공인인증서 및
암호화된 비밀키 복호화
607

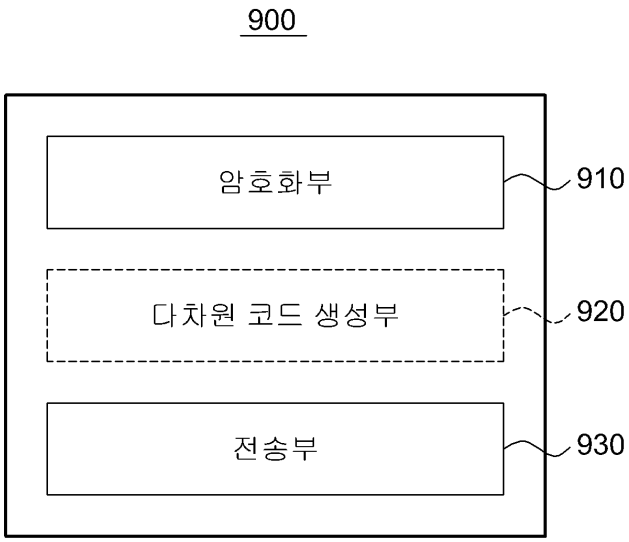
도면7


400
서버
500
사용자 단말기
701
사용자의 공개키 및
비밀키 생성
702
703
공개키로 공인인증서 생성
704
공인인증서 암호화
705
706
비밀키 암호화
707
다차원 코드 생성
300
휴대기기
708
709
다차원 코드에서 암호화된
공인인증서 및 암호화된
비밀키 추출
710
암호화된 공인인증서 및
암호화된 비밀키 복호화

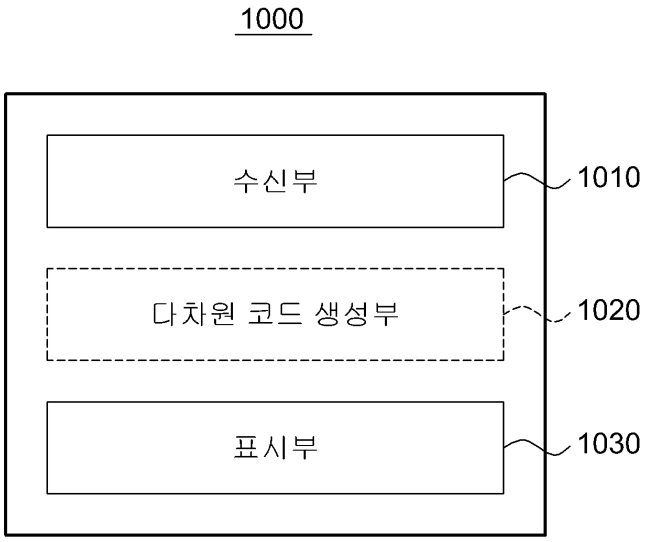
도면8


800
다차원 코드 인식부
810
추출부
820
복호화부
830

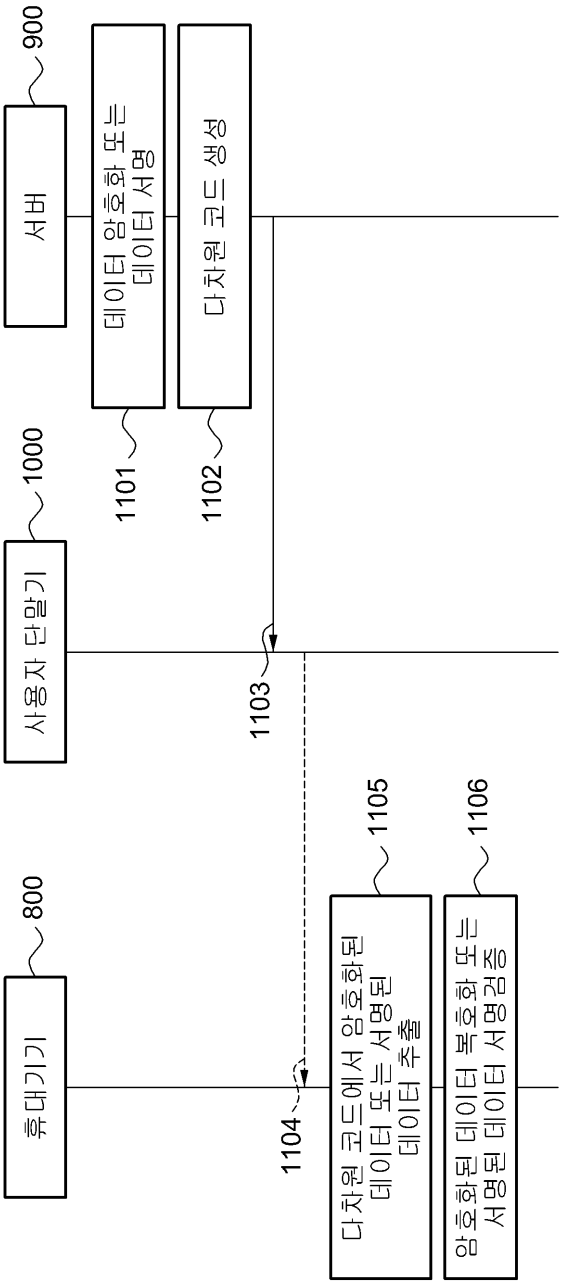
도면9


900
암호화부
910
다차원 코드 생성부
920
전송부
930

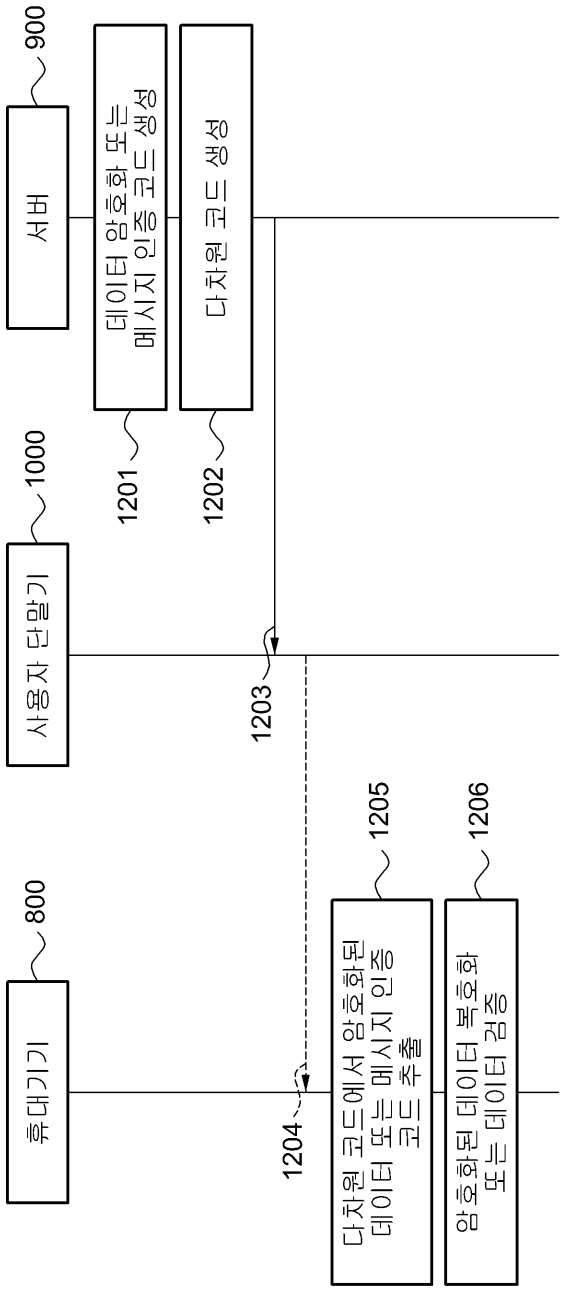
도면10



도면11


900
서버
데이터 암호화 또는
데이터 서명
다차원 코드 생성
1101
1102
1000
사용자 단말기
1103
800
휴대기기
1104
다차원 코드에서 암호화된
데이터 또는 서명된
데이터 추출
1105
암호화된 데이터 복호화 또는
서명된 데이터 서명검증
1106

도면12


서버
900
데이터 암호화 또는
메시지 인증 코드 생성
다차원 코드 생성
1201
1202
사용자 단말기
1000
1203
휴대기기
800
1204
다차원 코드에서 암호화된
데이터 또는 메시지 인증
코드 추출
1205
암호화된 데이터 복호화
또는 데이터 검증
1206