(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년03월02일
(11) 등록번호 10-2220087
(24) 등록일자 2021년02월19일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *G06K 19/06* (2006.01)
(52) CPC특허분류
H04L 63/123 (2013.01)
G06K 19/06037 (2013.01)
(21) 출원번호 10-2019-7020063
(22) 출원일자(국제) 2017년12월04일
심사청구일자 2019년07월11일
(85) 번역문제출일자 2019년07월10일
(65) 공개번호 10-2019-0093640
(43) 공개일자 2019년08월09일
(86) 국제출원번호 PCT/CN2017/114382
(87) 국제공개번호 WO 2018/107988
국제공개일자 2018년06월21일
(30) 우선권주장
201611154671.9 2016년12월14일 중국(CN)
(56) 선행기술조사문헌
CN103854061 A
US20150288670 A1
US20160241405 A1

(73) 특허권자
어드밴스드 뉴 테크놀로지스 씨오., 엘티디.
케이만 군도, 그랜드 케이만 케이와이1-9008, 조지 타운, 27 하스피탈 로드, 케이만 코포레이트 센터
(72) 발명자
셴 링난
중국 저지앙 311121 항저우 유 항 디스트릭트 웨스트 웬 이 로드 넘버 969 빌딩 3 알리바바 그룹 리갈 디파트먼트 5층
첸 지
중국 저지앙 311121 항저우 유 항 디스트릭트 웨스트 웬 이 로드 넘버 969 빌딩 3 알리바바 그룹 리갈 디파트먼트 5층
(뒷면에 계속)
(74) 대리인
김태홍, 김진희

전체 청구항 수 : 총 14 항 심사관 : 오수정

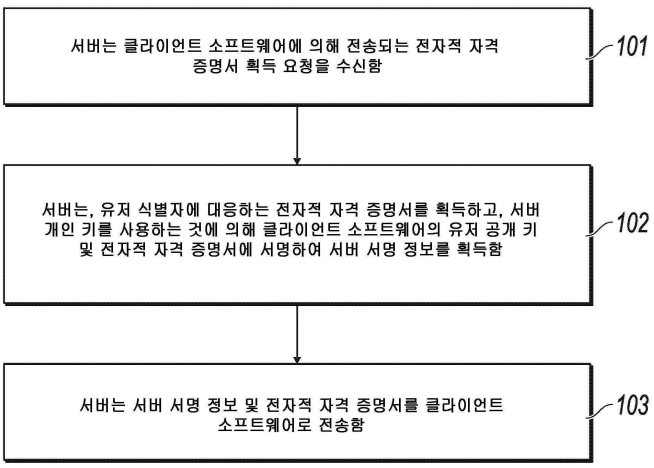
(54) 발명의 명칭 **이차원 바코드를 프로세싱하기 위한 방법, 장치, 및 시스템**

(57) 요 약

본 발명은, 이차원 바코드를 프로세싱하기 위한 방법, 장치, 및 시스템을 개시하고, 정보 프로세싱 기술의 분야에 관한 것이고, 전자적 자격 증명서가 정적 랜덤 코드에 기초하여 생성되고 일단 전자적 자격 증명서가 촬영을 통해 복사되거나 또는 도난당하면 전자적 자격 증명서의 보안성이 보장될 수 없는 현존하는 기술 문제점을 완화

(뒷면에 계속)

대 표 도 - 도2



하도록 주로 의도된다. 본 발명의 기술적 솔루션은 다음의 것을 포함한다: 서버에 의해, 클라이언트 소프트웨어에 의해 전송되는 전자적 자격 증명서 획득 요청 - 전자적 자격 증명서 획득 요청은 유저 식별자를 포함함 - 을 수신하는 것; 유저 식별자에 대응하는 전자적 자격 증명서를 획득하고, 서버 개인 키를 사용하는 것에 의해 클라이언트 소프트웨어의 유저 공개 키 및 전자적 자격 증명서에 서명하여 서버 서명 정보를 획득하는 것; 및 클라이언트 소프트웨어가 서버 서명 정보를 검증하고, 전자적 자격 증명서에 기초하여 이차원 바코드를 생성하여 자격 증명서 검증단 디바이스 - 자격 증명서 검증단 디바이스는 유저 식별자에 기초하여 전자적 자격 증명서를 생성하도록 구성됨 - 가 이차원 바코드에 포함되는 전자적 자격 증명서를 검증하도록, 서버 서명 정보 및 전자적 자격 증명서를 클라이언트 소프트웨어로 전송하는 것.

(52) CPC특허분류
H04L 63/126 (2013.01)
(72) 발명자
리우 양후이
중국 저지앙 311121 항저우 유 항 디스트릭트 웨스트 웬 이 로드 넘버 969 빌딩 3 알리바바 그룹 리갈 디파트먼트 5층
진 후이펭
중국 저지앙 311121 항저우 유 항 디스트릭트 웨스트 웬 이 로드 넘버 969 빌딩 3 알리바바 그룹 리갈 디파트먼트 5층

명 세 서

청구범위

청구항 1

서비스 요청을 프로세싱하기 위한 컴퓨터 구현(computer-implemented) 방법으로서,

하나 이상의 프로세서에 의해, 클라이언트로부터의 전자적 자격 증명서 요청(electronic credential request) - 상기 전자적 자격 증명서 요청은 유저 식별자를 포함함 - 을 수신하는 단계;

상기 하나 이상의 프로세서에 의해, 상기 유저 식별자에 대응하는 전자적 자격 증명서(electronic credential)를 리트리브하는(retrieving) 단계;

상기 하나 이상의 프로세서에 의해, 서버의 서버 서명 정보를 생성하는 단계 - 상기 서버 서명 정보는 상기 전자적 자격 증명서 및 상기 클라이언트의 유저 공개 키를 포함하고, 상기 전자적 자격 증명서 및 상기 유저 공개 키는 미리 결정된 기간 내에 서버 개인 키를 사용하여 서명됨 - ; 및

상기 하나 이상의 프로세서에 의해, 상기 서버 서명 정보를 상기 클라이언트로 송신하는 단계 - 상기 클라이언트는 상기 미리 결정된 기간 내에 상기 서버 서명 정보를 암호로(cryptographically) 검증하고 상기 전자적 자격 증명서에 기초하여 2차원 바코드를 생성하도록 구성되고, 상기 2차원 바코드에 포함된 상기 전자적 자격 증명서는 자격 증명서 검증 디바이스(credential verification device)에 의해 검증되도록 구성되고, 상기 자격 증명서 검증 디바이스는 상기 유저 식별자에 기초하여 상기 전자적 자격 증명서를 생성하도록 구성됨 -

를 포함하는, 서비스 요청을 프로세싱하기 위한 컴퓨터 구현 방법.

청구항 2

제1항에 있어서,

상기 서버 개인 키를 사용하여 상기 전자적 자격 증명서에 서명하는 것은,

상기 전자적 자격 증명서에 유저 서명 키를 할당하고 - 상기 유저 서명 키는 제1 유저 공개 키를 포함함 - , 상기 서버 개인 키를 사용하는 것에 의해 상기 전자적 자격 증명서 및 상기 제1 유저 공개 키에 서명하는 것; 또는

상기 클라이언트에 의해 전송되는 제2 유저 공개 키를 획득하고, 상기 서버 개인 키를 사용하는 것에 의해 상기 전자적 자격 증명서 및 상기 제2 유저 공개 키에 서명하는 것

을 포함하는 것인, 서비스 요청을 프로세싱하기 위한 컴퓨터 구현 방법.

청구항 3

제2항에 있어서,

상기 유저 서명 키는 비대칭 키인 것인, 서비스 요청을 프로세싱하기 위한 컴퓨터 구현 방법.

청구항 4

제2항에 있어서,

상기 제1 유저 공개 키는 상기 서버 개인 키를 사용하는 것에 의해 서명되고, 상기 서버 서명 정보 및 상기 전자적 자격 증명서를 상기 클라이언트로 송신하는 것은,

상기 할당된 유저 서명 키, 상기 서버 서명 정보, 및 상기 전자적 자격 증명서를 상기 클라이언트로 송신하는 것을 포함하는 것인, 서비스 요청을 프로세싱하기 위한 컴퓨터 구현 방법.

청구항 5

제1항에 있어서,

상기 유저 식별자에 대응하는 전자적 자격 증명서를 리트리브하기 이전에, 상기 방법은,

상기 전자적 자격 증명서 요청을 파싱(parsing)하는 단계;

상기 전자적 자격 증명서 요청에 포함되는 서비스 유효 시간(service validity time)을 획득하는 단계; 및

상기 서비스 유효 시간이 서비스 명세(service specification)를 따르는지의 여부를 검증하는 단계

를 더 포함하는, 서비스 요청을 프로세싱하기 위한 컴퓨터 구현 방법.

청구항 6

제5항에 있어서,

상기 유저 식별자에 대응하는 전자적 자격 증명서를 리트리브하는 것은,

상기 서비스 유효 시간이 상기 서비스 명세를 따르는지의 여부를 결정하는 것; 및

상기 서비스 유효 시간이 상기 서비스 명세를 따른다고 결정하는 것에 응답하여, 상기 유저 식별자에 대응하는 상기 전자적 자격 증명서를 리트리브하는 것

을 포함하는 것인, 서비스 요청을 프로세싱하기 위한 컴퓨터 구현 방법.

청구항 7

제6항에 있어서,

상기 유저 식별자에 대응하는 전자적 자격 증명서를 리트리브하는 것은,

상기 자격 증명서 검증 디바이스에 의해 동기화되는 상기 전자적 자격 증명서를 수신하는 것; 또는

전자적 자격 증명서를 리트리브하기 위해, 상기 전자적 자격 증명서를 리트리브하기 위한 요청 정보를 상기 유저 식별자에 기초하여 상기 자격 증명서 검증 디바이스로 송신하는 것

을 포함하는 것인, 서비스 요청을 프로세싱하기 위한 컴퓨터 구현 방법.

청구항 8

제6항에 있어서,

상기 방법은,

상기 서버 개인 키에 대응하는 서버 공개 키를 브로드캐스트하는 단계를 더 포함하되, 상기 클라이언트 및 상기 자격 증명서 검증 디바이스는 상기 서버 공개 키에 기초하여 상기 서명 정보를 검증하는 것인, 서비스 요청을 프로세싱하기 위한 컴퓨터 구현 방법.

청구항 9

제1항에 있어서,

상기 2차원 바코드는,

미리 결정된 보안 정보의 유효성 지속 기간(validity duration)을 설정하는 것; 및

상기 미리 결정된 보안 정보, 클라이언트 서명 정보, 상기 서버 서명 정보, 상기 전자적 자격 증명서, 상기 유저 공개 키, 상기 미리 결정된 보안 정보의 유효성 지속 기간, 및 상기 유저 식별자에 기초하여 상기 2차원 바코드를 생성하는 것

을 포함하는 동작들을 수행하는 것에 의해 생성되는 것인, 서비스 요청을 프로세싱하기 위한 컴퓨터 구현 방법.

청구항 10

제1항에 있어서,

상기 유저 식별자에 기초하여 상기 전자적 자격 증명서를 상기 서버에 동기화하는 단계를 더 포함하되, 상기 서버는 상기 전자적 자격 증명서를 상기 클라이언트로 전송하는 것인, 서비스 요청을 프로세싱하기 위한 컴퓨터

구현 방법.

청구항 11

제9항에 있어서,

상기 미리 결정된 보안 정보의 유효성 지속 기간은 상기 전자적 자격 증명서의 타입에 기초하는 것인, 서비스 요청을 프로세싱하기 위한 컴퓨터 구현 방법.

청구항 12

제1항에 있어서,

상기 전자적 자격 증명서는, 항공권(air ticket), 버스 티켓, 기차 티켓, 콘서트 티켓, 은행 카드, 액세스 제어 카드, 공원 입장 티켓, 신분증(identity card), 상인 쿠폰, 멤버십 카드, 운전 면허증, 운전 면허증 액세스 제어 카드(driving license access control card), 또는 버스 카드를 포함하는 것인, 서비스 요청을 프로세싱하기 위한 컴퓨터 구현 방법.

청구항 13

제1항에 있어서,

상기 유저 공개 키 및 상기 전자적 자격 증명서에 서명하는 것은,

해시 알고리즘(hash algorithm)을 사용하는 것에 의해 상기 유저 공개 키 및 상기 전자적 자격 증명서에 대해 해시 연산(hash operation)을 수행하여 해시 값(hash value)을 획득하는 것; 및

상기 서버 개인 키를 사용하는 것에 의해 상기 해시 값에 서명하여 상기 서버 서명 정보를 획득하는 것

을 포함하는 것인, 서비스 요청을 프로세싱하기 위한 컴퓨터 구현 방법.

청구항 14

제1항 내지 제13항 중 어느 한 항의 컴퓨터 구현 방법을 수행하도록 구성되는 복수의 모듈을 포함하는, 2차원 바코드를 프로세싱하기 위한 시스템.

청구항 15

삭제

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

청구항 32

삭제

청구항 33

삭제

청구항 34

삭제

청구항 35

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 정보 프로세싱 기술의 분야에 관한 것으로, 특히, 이차원 바코드를 프로세싱하기 위한 방법, 장치, 및 시스템에 관한 것이다.

배 경 기 술

[0002] 현재, 일상 업무 및 생활에서의 몇몇 자격 증명서 검증 적용 시나리오(credential verification application scenario), 예를 들면, 신분증(identity card), 은행 카드, 버스 티켓, 콘서트 티켓, 및 액세스 제어 카드가 존재한다. 몇몇 적용 시나리오에서, 자격 증명서 검증(credential verification)은, 특정한 엔티티, 예를 들면, 버스 티켓, 콘서트 티켓, 및 액세스 제어 카드를 사용하는 것에 의해서만 완료되는 것을 필요로 한다. 상대적으로 높은 보안 요건을 갖는 몇몇 자격 증명서 검증 시나리오의 경우, 검증을 완료하기 위해서는, 특정한 엔티티 및 개인 정보, 예를 들면, 은행 카드 및 집/회사 지문 액세스가 함께 사용되는 것을 필요로 한다.

[0003] 실제로, 특정한 엔티티를 사용하는 것에 의해서만 완료되는 것을 필요로 하는 자격 증명서 검증을 갖는 적용 시나리오에서, 자격 증명서 검증은 대응하는 특정한 엔티티를 획득하는 것에 의해 완료될 수 있다. 예를 들면, 유저는 티켓 창구에서 종이 버스 티켓 또는 종이 콘서트 티켓을 구입할 수 있고, 개찰구(ticket barrier)에서 검증이 완료된 이후 버스에 타거나 또는 콘서트에 입장할 수 있다. 이 검증 모드는 특정한 엔티티(버스 티켓 또는 콘서트 티켓)에 의존하며, 유저가 특정한 엔티티를 휴대할 것을 요구한다. 그러나 특정한 엔티티가 분실되거나 또는 손상된 경우, 특정한 엔티티를 등록 취소하는 또는 사후 등록하는 프로세스가 복잡하다.

[0004] 상대적으로 높은 보안 요건을 갖는 적용 시나리오의 경우, 보안은 추가적인 보안 인증 보조 디바이스, 예를 들면, 보안 키보드 또는 지문 인식 디바이스에 의해 보장될 수 있다. 그러한 만큼, 사용 비용이 증가된다. 비록 이 방법이 개인 정보 유출을 방지할 수 있지만, 개인 정보 유출의 위협은 여전히 존재한다.

[0005] 이전의 두 개의 적용 시나리오 둘 모두에서, 자격 증명서 검증이 상대적으로 낮은 보안성을 가지면서 덜 편리하고 자격 증명서 발행 당사자의 비용이 상대적으로 높다는 문제점이 있다. 이전의 문제점을 완화하기 위해, 현존하는 기술에서의 유저는 온라인에서 전자적 자격 증명서(electronic credential)를 구입할 수 있다. 전자적 자격 증명서에는 랜덤 코드의 문자열이 기록되며, 자격 증명서 검증 동안, 검증은 전자적 자격 증명서 내의 랜덤 코드를 검증하는 것에 의해 완료될 수 있고, 그에 의해, 자격 증명서 검증의 편의성 및 보안성을 향상시킬 수 있고, 자격 증명서 발행 당사자의 발행 비용을 감소시킬 수 있다. 그러나, 정적인 랜덤 코드가 전자적 자격 증명서에 사용되며, 만약 전자적 자격 증명서가 촬영을 통해 복사되거나 또는 도난당하면, 전자적 자격 증명서의 보안성이 보장될 수 없다.

발명의 내용

[0006] 이것을 고려하여, 본 발명은, 이차원 바코드를 프로세싱하기 위한 방법, 장치, 및 시스템을 제공하며, 전자적 자격 증명서가 정적인 랜덤 코드에 기초하여 생성되고, 일단 전자적 자격 증명서가 촬영을 통해 복사되거나 또는 도난당하면, 전자적 자격 증명서의 보안성이 보장될 수 없다는 현존하는 기술 문제점을 완화하도록 의도된다.

[0007] 본 발명의 제1 양태에 따르면, 본 발명은, 다음의 것을 포함하는, 이차원 바코드를 프로세싱하기 위한 방법을 제공한다: 서버에 의해, 클라이언트 소프트웨어에 의해 전송되는 전자적 자격 증명서 획득 요청 - 전자적 자격 증명서 획득 요청은 유저 식별자를 포함함 - 을 수신하는 것; 유저 식별자에 대응하는 전자적 자격 증명서를 획득하고, 서버 개인 키를 사용하는 것에 의해 클라이언트 소프트웨어의 유저 공개 키 및 전자적 자격 증명서에 서명하여 서버 서명 정보를 획득하는 것; 및 클라이언트 소프트웨어가 서버 서명 정보를 검증하고, 전자적 자격 증명서에 기초하여 이차원 바코드를 생성하여 자격 증명서 검증단 디바이스(credential verification end device) - 자격 증명서 검증단 디바이스는 유저 식별자에 기초하여 전자적 자격 증명서를 생성하도록 구성됨 - 가 이차원 바코드에 포함되는 전자적 자격 증명서를 검증하도록, 서버 서명 정보 및 전자적 자격 증명서를 클라이언트 소프트웨어로 전송하는 것.

[0008] 본 발명의 제2 양태에 따르면, 본 발명은, 다음의 것을 포함하는, 이차원 바코드를 프로세싱하기 위한 방법을 제공한다: 클라이언트 소프트웨어에 의해, 서버에 의해 전송되는 서버 서명 정보 및 전자적 자격 증명서 - 서버 서명 정보는, 서버 개인 키를 사용하는 것에 의해 클라이언트 소프트웨어의 유저 공개 키 및 전자적 자격 증명서에 서명하는 것에 의해 서버에 의해 획득됨 - 를 수신하는 것; 서버 서명 정보를 검증하여 전자적 자격 증명서를 획득하는 것; 유저 공개 키에 대응하는 유저 키를 획득하고, 유저 키를 사용하는 것에 의해 전자적 자격 증명서에 서명하여 클라이언트 소프트웨어 서명 정보를 획득하는 것; 및 자격 증명서 검증단 디바이스가 미리 결정된 보안 정보 - 미리 결정된 보안 정보는 유효성 지속 기간(validity duration)을 가지며, 자격 증명서 검증단 디바이스는 유저 식별자에 기초하여 전자적 자격 증명서를 생성하도록 구성됨 - 및 유저 공개 키에 기초하여 이차원 바코드에 포함되는 전자적 자격 증명서를 검증하도록, 미리 결정된 보안 정보, 클라이언트 소프트웨

어 서명 정보, 서버 서명 정보, 전자적 자격 증명서, 및 유저 공개 키에 기초하여 이차원 바코드를 생성하는 것.

[0009] 본 발명의 제3 양태에 따르면, 본 발명은, 다음의 것을 포함하는, 이차원 바코드를 프로세싱하기 위한 방법을 제공한다: 자격 증명서 검증단 디바이스에 의해, 클라이언트 소프트웨어에서 이차원 바코드 - 이차원 바코드는 미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 서버 서명 정보, 전자적 자격 증명서, 및 유저 공개 키에 기초하여 클라이언트 소프트웨어에 의해 생성되고, 클라이언트 소프트웨어 서명 정보는 전자적 자격 증명서에 서명하는 것에 의해 클라이언트 소프트웨어에 의해 획득되고, 서버 서명 정보는 전자적 자격 증명서 및 유저 공개 키에 서명하는 것에 의해 서버에 의해 획득됨 - 를 획득하는 것; 미리 결정된 보안 정보의 유효성 지속 기간을 검증하고, 클라이언트 소프트웨어 서명 정보 및 서버 서명 정보를 검증하는 것; 미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 및 서버 서명 정보의 각각에 대한 검증이 성공하면, 전자적 자격 증명서에 포함되는 서비스 유효 시간(service validity time)을, 검증을 위해, 획득하는 것; 및 전자적 자격 증명서에 포함되는 서비스 유효 시간에 대한 검증이 성공하면, 전자적 자격 증명서에 대한 검증이 성공한다는 것을 결정하는 것.

[0010] 본 발명의 제4 양태에 따르면, 본 발명은, 다음의 것을 포함하는 서버를 제공한다: 클라이언트 소프트웨어에 의해 전송되는 전자적 자격 증명서 획득 요청 - 전자적 자격 증명서 획득 요청은 유저 식별자를 포함함 - 을 수신하도록 구성되는 수신 유닛; 수신 유닛에 의해 수신되는 유저 식별자에 대응하는 전자적 자격 증명서를 획득하도록 구성되는 제1 획득 유닛; 서버 개인 키를 사용하는 것에 의해 클라이언트 소프트웨어의 유저 공개 키 및 전자적 자격 증명서에 서명하여 서버 서명 정보를 획득하도록 구성되는 서명 유닛(signing unit); 및 클라이언트 소프트웨어가 유저 키의 유효성 시간 내에 서버 서명 정보를 검증하고, 전자적 자격 증명서에 기초하여 이차원 바코드를 생성하여 자격 증명서 검증단 디바이스 - 자격 증명서 검증단 디바이스는 유저 식별자에 기초하여 전자적 자격 증명서를 생성하도록 구성됨 - 가 이차원 바코드에 포함되는 전자적 자격 증명서를 검증하도록, 서명 유닛에 의해 획득되는 서버 서명 정보 및 제1 획득 유닛에 의해 획득되는 전자적 자격 증명서를 클라이언트 소프트웨어로 전송하도록 구성되는 전송 유닛.

[0011] 본 발명의 제5 양태에 따르면, 본 발명은, 다음의 것을 포함하는 클라이언트 소프트웨어를 제공한다: 서버에 의해 전송되는 서버 서명 정보 및 전자적 자격 증명서 - 서버 서명 정보는, 서버 개인 키를 사용하는 것에 의해 클라이언트 소프트웨어의 유저 공개 키 및 전자적 자격 증명서에 서명하는 것에 의해 서버에 의해 획득됨 - 를 수신하도록 구성되는 제1 수신 유닛; 서버 서명 정보를 검증하여 전자적 자격 증명서를 획득하도록 구성되는 서명 검증 유닛; 유저 공개 키에 대응하는 유저 키를 획득하도록 구성되는 획득 유닛; 획득 유닛에 의해 획득되는 유저 키를 사용하는 것에 의해 전자적 자격 증명서에 서명하여 클라이언트 소프트웨어 서명 정보를 획득하도록 구성되는 서명 유닛; 및 자격 증명서 검증단 디바이스가 미리 결정된 보안 정보 - 미리 결정된 보안 정보는 유효성 지속 기간을 가지며, 자격 증명서 검증단 디바이스는 유저 식별자에 기초하여 전자적 자격 증명서를 생성하도록 구성됨 - 및 유저 공개 키에 기초하여 이차원 바코드에 포함되는 전자적 자격 증명서를 검증하도록, 미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 서버 서명 정보, 전자적 자격 증명서, 및 유저 공개 키에 기초하여 이차원 바코드를 생성하도록 구성되는 생성 유닛.

[0012] 본 발명의 제6 양태에 따르면, 본 발명은, 다음의 것을 포함하는 자격 증명서 검증단 디바이스를 제공한다: 클라이언트 소프트웨어에서 이차원 바코드 - 이차원 바코드는 미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 서버 서명 정보, 전자적 자격 증명서, 및 유저 공개 키에 기초하여 클라이언트 소프트웨어에 의해 생성되고, 클라이언트 소프트웨어 서명 정보는 전자적 자격 증명서에 서명하는 것에 의해 클라이언트 소프트웨어에 의해 획득되고, 서버 서명 정보는 전자적 자격 증명서 및 유저 공개 키에 서명하는 것에 의해 서버에 의해 획득됨 - 를 획득하도록 구성되는 제1 획득 유닛; 제1 획득 유닛에 의해 획득되는 미리 결정된 보안 정보의 유효성 지속 기간을 검증하도록 구성되는 제1 검증 유닛; 클라이언트 소프트웨어 서명 정보 및 서버 서명 정보를 검증하도록 구성되는 제2 검증 유닛; 미리 결정된 보안 정보에 대한 제1 검증 유닛의 검증이 성공하고, 클라이언트 소프트웨어 서명 정보 및 서버 서명 정보의 각각에 대한 제2 검증 유닛의 검증이 성공하는 경우, 전자적 자격 증명서에 포함되는 서비스 유효 시간을, 검증을 위해, 획득하도록 구성되는 제3 검증 유닛; 및 전자적 자격 증명서에 포함되는 서비스 유효 시간에 대한 제3 검증 유닛의 검증이 성공하는 경우, 전자적 자격 증명서에 대한 검증이 성공한다는 것을 결정하도록 구성되는 결정 유닛.

[0013] 본 발명의 제7 양태에 따르면, 본 발명은 이차원 바코드를 프로세싱하기 위한 시스템을 제공하는데, 시스템은 다음의 것: 전자적 자격 증명서 획득 요청 - 전자적 자격 증명서 획득 요청은 유저 식별자를 포함함 - 을 서버로 전송하도록 구성되는 클라이언트 소프트웨어; 클라이언트 소프트웨어에 의해 전송되는 전자적 자격 증명서

획득 요청을 수신하도록, 그리고 유저 식별자에 기초하여 자격 증명서 검증단 디바이스로부터 전자적 자격 증명서를 획득하도록 구성되는 서버; 및 서버에 의해 전송되는 전자적 자격 증명서를 획득하기 위한 요청 정보를 수신하도록 그리고 그에 응답하도록, 그리고 전자적 자격 증명서를 서버로 전송하도록 구성되는 자격 증명서 검증단 디바이스를 을 포함하되, 서버는 또한, 자격 증명서 검증단 디바이스에 의해 전송되는 전자적 자격 증명서를 수신하도록, 클라이언트 소프트웨어의 유저 공개 키 및 전자적 자격 증명서에 서명하여 서버 서명 정보를 획득하도록, 그리고 서버 서명 정보 및 전자적 자격 증명서를 클라이언트 소프트웨어로 전송하도록 구성되고; 클라이언트 소프트웨어는, 서버에 의해 전송되는 전자적 자격 증명서 및 서버 서명 정보를 수신하도록, 서버 서명 정보를 검증하여 전자적 자격 증명서를 획득하도록, 유저 공개 키에 대응하는 유저 키를 획득하도록, 유저 키를 사용하는 것에 의해 전자적 자격 증명서에 서명하여 클라이언트 소프트웨어 서명 정보를 획득하도록, 그리고 미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 서버 서명 정보, 전자적 자격 증명서, 및 유저 공개 키에 기초하여 이차원 바코드를 생성하도록 구성되고; 그리고 자격 증명서 검증단 디바이스는 클라이언트 소프트웨어에서 이차원 바코드를 획득하도록, 미리 결정된 보안 정보의 유효성 지속 기간을 검증하도록, 그리고 클라이언트 소프트웨어 서명 정보 및 서버 서명 정보를 검증하도록; 그리고 미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 및 서버 서명 정보의 각각에 대한 검증이 성공하는 경우, 전자적 자격 증명서에 포함되는 서비스 유효 시간을, 검증을 위해, 획득하도록, 그리고, 전자적 자격 증명서에 포함되는 서비스 유효 시간에 대한 검증이 성공하는 경우, 전자적 자격 증명서에 대한 검증이 성공한다는 것을 결정하도록 구성된다.

[0014] 이전의 기술적 솔루션에 따르면, 그리고 본 발명에서 제공되는 이차원 바코드를 프로세싱하기 위한 방법, 장치, 및 시스템에 따르면, 클라이언트 소프트웨어에 의해 전송되는 전자적 자격 증명서 획득 요청을 수신한 이후, 서버는 서버 개인 키를 사용하는 것에 의해 클라이언트 소프트웨어의 유저 공개 키 및 전자적 자격 증명서에 서명하여 서버 서명 정보를 획득하고, 서버 서명 정보 및 전자적 자격 증명서를 클라이언트 소프트웨어로 전송한다. 클라이언트 소프트웨어는, 서버에 의해 전송되는 서버 서명 정보 및 전자적 자격 증명서를 수신하고, 서버 서명 정보를 검증하고, 서명 정보에 대한 검증이 성공한 이후, 전자적 자격 증명서에 서명하고, 미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 서버 서명 정보, 전자적 자격 증명서, 및 유저 공개 키에 기초하여 이차원 바코드를 생성한다. 이차원 바코드를 획득한 이후, 자격 증명서 검증단 디바이스는, 서버 서명 정보, 클라이언트 소프트웨어 서명 정보, 및 미리 결정된 보안 정보를 이차원 바코드에서 검증하여, 전자적 자격 증명서가 송신 프로세스에서 변경되는지의 여부를 결정하여, 사용 프로세스에서 전자적 자격 증명서의 보안성을 보장할 수 있다.

[0015] 설명은 단지 본 발명의 기술적 솔루션의 개요에 불과하다. 본 명세서의 내용을 구현하기 위한 본 발명의 기술적 수단을 더욱 명확하게 이해하기 위해, 그리고 본 발명의 앞선 및 다른 목적, 피쳐, 및 이점을 더욱 이해 가능하게 만들기 위해, 이하에서는, 본 발명의 특정한 구현예를 열거한다.

도면의 간단한 설명

[0016] 이하의 바람직한 구현예에 대한 상세한 설명을 판독하는 것에 의해, 기술 분야에서 통상의 기술을 가진 자는 다양한 다른 이점 및 이익을 이해한다. 첨부의 도면은 단지 바람직한 구현예의 목적을 나타내기 위해 사용되는 것에 불과하며, 본 발명에 대한 제한으로 간주되지는 않는다. 또한, 모든 첨부의 도면에서 동일한 참조 번호는 동일한 부분을 나타내기 위해 사용된다. 첨부의 도면에서:

도 1은, 본 발명의 구현예에 따른, 클라이언트 소프트웨어, 서버, 및 자격 증명서 검증단 디바이스 사이의 상호작용을 예시하는 프레임워크 다이어그램이다;

도 2는, 본 발명의 구현예에 따른, 이차원 바코드를 프로세싱하기 위한 제1 방법을 예시하는 플로우차트이다;

도 3은, 본 발명의 구현예에 따른, 이차원 바코드를 프로세싱하기 위한 제2 방법을 예시하는 플로우차트이다;

도 4는, 본 발명의 구현예에 따른, 이차원 바코드를 프로세싱하기 위한 제3 방법을 예시하는 플로우차트이다;

도 5는, 본 발명의 구현예에 따른, 서명하기(signing) 및 서명에 대한 검증을 예시하는 개략도이다;

도 6은, 본 발명의 구현예에 따른, 이차원 바코드를 프로세싱하기 위한 제4 방법을 예시하는 플로우차트이다;

도 7은, 본 발명의 구현예에 따른, 이차원 바코드를 프로세싱하기 위한 제5 방법을 예시하는 플로우차트이다;

도 8은, 본 발명의 구현예에 따른, 서버를 예시하는 블록도이다;

도 9는, 본 발명의 구현예에 따른, 다른 서버를 예시하는 블록도이다;

도 10은, 본 발명의 구현예에 따른, 클라이언트 소프트웨어를 예시하는 블록도이다;

도 11은, 본 발명의 구현예에 따른, 다른 클라이언트 소프트웨어를 예시하는 블록도이다;

도 12는, 본 발명의 구현예에 따른, 자격 증명서 검증단 디바이스를 예시하는 블록도이다;

도 13은, 본 발명의 구현예에 따른, 다른 자격 증명서 검증단 디바이스를 예시하는 블록도이다; 그리고

도 14는, 본 발명의 구현예에 따른, 이차원 바코드를 프로세싱하기 위한 시스템을 예시하는 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0017] 이하, 첨부의 도면을 참조하여 본 개시의 예시적인 구현예를 더욱 상세하게 설명한다. 비록 첨부의 도면이 본 개시의 예시적인 구현예를 도시하지만, 본 개시는 다양한 형태로 구현될 수 있고, 본원에서 설명되는 구현예에 의해 제한되지 않아야 한다는 것이 이해되어야 한다. 대신, 이들 구현예는, 기술 분야의 숙련된 자가, 본 개시 및 본 개시의 범위를 더욱 완전하게 이해하게 만들기 위해 제공된다.

[0018] 이차원 바코드 내의 전자적 자격 증명서 정보가 쉽게 유출될 수 있다는 현존하는 기술 문제점을 완화하기 위해, 본 발명의 구현예는 이차원 바코드를 프로세싱하기 위한 방법을 제공한다. 방법은, 서버, 클라이언트 소프트웨어, 및 자격 증명서 검증단 디바이스의 협력을 통해 구현된다. 자격 증명서 검증단 디바이스는, 생성된 전자적 자격 증명서를 서버에 송신하도록, 적어도, 데이터를 생성 및 송신할 수 있고, 클라이언트 소프트웨어에서 이차원 바코드로부터 전자적 자격 증명서를 획득하고 전자적 자격 증명서가 정확한지의 여부를 검증하도록, 데이터를 획득하고 데이터를 검증할 수 있다. 서버는, 적어도, 자격 증명서 검증단 디바이스에 의해 전송되는 전자적 자격 증명서를 수신하도록, 그리고, 전자적 자격 증명서를 클라이언트 소프트웨어로 전송하여, 데이터 송신을 구현하도록, 데이터를 송신 및 수신할 수 있다. 클라이언트 소프트웨어는, 적어도, 서버에 의해 전송되는 전자적 자격 증명서를 수신하도록, 서버와 데이터를 교환할 수 있고, 전자적 자격 증명서 정보에 기초하여 이차원 바코드 등등을 생성하도록, 이미지를 생성할 수 있다.

[0019] 구현예의 방법이 설명되기 이전에, 이해의 용이성을 위해, 본 발명의 구현예에 따른, 클라이언트 소프트웨어, 서버, 및 자격 증명서 검증단 디바이스 사이의 상호 작용을 예시하는 프레임워크 다이어그램이, 도 1에서 도시되는 바와 같이, 먼저 제공된다. 본 발명의 구현예에서, 유저 식별자(예컨대 신분증 번호(identity card number), 이동 전화 번호(mobile number), 또는 전자 메일 주소)에 기초하여 전자적 자격 증명서를 생성한 이후, 자격 증명서 검증단 디바이스는 전자적 자격 증명서를 서버로 전송하고, 서버는 자격 증명서 검증단 디바이스에 의해 생성되는 전자적 자격 증명서에 대한 액세스 퍼미션을 갖는다. 클라이언트 소프트웨어로부터 전자적 자격 증명서 획득 요청을 수신한 이후, 자격 증명서 검증단 디바이스가 검증할 전자적 자격 증명서에 기초하여 클라이언트 소프트웨어가 이차원 바코드를 생성하도록, 서버는 전자적 자격 증명서를 클라이언트 소프트웨어로 전송한다.

[0020] 본 발명의 이 구현예에서, 전자적 자격 증명서가 이차원 바코드에서 운반되는 예를 사용하는 것에 의해 설명이 이루어진다는 것을 주목할 가치가 있다. 그러나, 이론적으로, 전자적 자격 증명서는, 다른 매체, 예를 들면, SE 성능 또는 HCE 성능과 같은 NFC 성능을 갖는 클라이언트 소프트웨어에 또한 의존할 수 있다. 본 발명의 구현예에서는, 전자적 자격 증명서 유저 및 자격 증명서 검증단 디바이스의 경우, 이차원 바코드가, 사용되는 하드웨어 디바이스에 대한 상대적으로 낮은 요건을 가지며 하드웨어 디바이스가 상대적으로 보편적이기 때문에, 전자적 자격 증명서가 이차원 바코드에서 운반되는 예를 사용하는 것에 의해 설명이 이루어진다. 그러나, 그러한 설명 방법은, 전자적 자격 증명서가 이차원 바코드를 사용하는 것에 의해서만 운반될 수 있다는 제한을 부과하도록 의도되는 것은 아니다는 것을 분명히 알고 있어야 한다.

[0021] 이하, 도 1에서 도시되는 개략도에 기초하여 서버 측 상에서 구현되는 이차원 바코드를 프로세싱하기 위한 방법을 먼저 제공한다. 도 2에서 도시되는 바와 같이, 방법은 다음의 단계를 포함한다.

[0022] 101. 서버는 클라이언트 소프트웨어에 의해 전송되는 전자적 자격 증명서 획득 요청을 수신한다.

[0023] 서버에 성공적으로 로그인한 이후, 클라이언트 소프트웨어는 전자적 자격 증명서 획득 요청을 서버로 전송하는데, 여기서, 전자적 자격 증명서 획득 요청은, 서버가 유저 식별자에 기초하여 대응하는 전자적 자격 증명서 정보를 검색하도록, 유저 식별자를 포함한다. 특정한 구현예 프로세스에서, 전자적 자격 증명서는 다음의 콘텐츠를 포함할 수 있지만 그러나 이들로 제한되지는 않는다: 항공권(air ticket), 버스 티켓, 기차 티켓, 콘서트 티켓, 은행 카드, 액세스 제어 카드, 공원 입장 티켓, 신분증, 상인 쿠폰, 멤버십 카드, 운전 면허증, 운전 면허

증 액세스 제어 카드(driving license access control card), 또는 버스 카드에 대응하는 전자적 자격 증명서.

[0024] 특정한 구현예 프로세스에서, 클라이언트 소프트웨어는 전자 디바이스 또는 웹사이트에 설치되는 애플리케이션(APP(앱))이다. 클라이언트 소프트웨어가 서버와 상호 작용하기 이전에, 클라이언트 소프트웨어는 유저 식별자에 기초하여 서버에 등록할 수 있고, 유저 식별자는, 유저 신분증, 신분증과 일치하는 실제 이름, 이동 전화 번호, 전자 메일 주소, 계정명, 등등을 포함할 수 있지만, 그러나 이들로 제한되지는 않는다. 등록 프로세스에서, 서버에 로그인하기 위한 로그인 패스워드를 설정할 수 있고, 등록 및 성공적인 로그인 이후, 클라이언트 소프트웨어는 서버에 연결되어 서버와 통신할 수 있다.

[0025] 102. 서버는, 유저 식별자에 대응하는 전자적 자격 증명서를 획득하고, 서버 개인 키를 사용하는 것에 의해 클라이언트 소프트웨어의 유저 공개 키 및 전자적 자격 증명서에 서명하여 서버 서명 정보를 획득한다.

[0026] 본 발명의 이 구현예에서 설명되는 서버는, 전자적 자격 증명서를 생성하지는 않는다. 클라이언트 소프트웨어에 의해 전송되는 전자적 자격 증명서 획득 요청을 수신한 이후, 서버는, 전자적 자격 증명서를 생성하는 자격 증명서 검증단 디바이스로부터 유저 식별자에 대응하는 전자적 자격 증명서를 획득한다. 서버는, 전자적 자격 증명서 사용 당사자(electronic credential using party)(클라이언트 소프트웨어)와 전자적 자격 증명서 검증단 디바이스(자격 증명서 검증단 디바이스) 사이의 다리(bridge)로서 역할을 하며, 자격 증명서 검증단 디바이스에 의해 생성되는 전자적 자격 증명서를 전자적 자격 증명서 사용 당사자로 포워딩하는 것을 담당한다. 본 발명의 이 구현예에서 설명되는 서버가 국가의 규제 요건을 충족한다는 전제하에서, 서버는 자격 증명서 검증단 디바이스에 액세스하기 위해 자격 증명서 검증단 디바이스에 의해 승인되는 것을 필요로 한다는 것을 주목할 가치가 있다.

[0027] 서버 및 클라이언트 소프트웨어의 송신 프로세스에서 전자적 자격 증명서가 변경되는 것을 방지하기 위해, 서버가 클라이언트 소프트웨어에 의해 전송되는 전자적 자격 증명서 획득 요청에 응답하기 이전에, 서버는 서버 개인 키를 사용하는 것에 의해 클라이언트 소프트웨어의 유저 공개 키에 서명하여 서버 서명 정보를 획득하는 것을 필요로 한다. 본 발명의 이 구현예에서, 클라이언트 소프트웨어의 유저 공개 키는, 클라이언트 소프트웨어 및 서버가 서로의 신원을 검증할 수 있도록, 신원 정보에 대한 보안 인증을 수행할 수 있도록, 그리고 데이터 송신 프로세스에서 정보가 변경되지 않는 것을 보장할 수 있도록, 서명된다. 서버는, 원래의 전자적 자격 증명서의 무결성이 결정될 수 있도록, 서버 개인 키를 사용하는 것에 의해 전자적 자격 증명서에 서명한다.

[0028] 또한, 서버는 유저 공개 키 및 전자적 자격 증명서에 서명하는 경우, 서버는 또한, 클라이언트 소프트웨어에 의해 송신되는 전자적 자격 증명서가 서버에 의해 전송되고, 클라이언트 소프트웨어에 의해 검증되고, 승인되고 신뢰 가능하다는 것을 보장하기 위해, 서버가 전자적 자격 증명서 및 유저 공개 키에 서명할 때 획득되는 서버 서명 정보를, 클라이언트 소프트웨어가 후속하여 이차원 바코드를 생성할 때 생성된 이차원 바코드의 속성 정보(attribute information)로서 사용할 수 있다. 그러한 만큼, 전자적 자격 증명서는 위조 또는 거부될 수 없다.

[0029] 103. 서버는 서버 서명 정보 및 전자적 자격 증명서를 클라이언트 소프트웨어로 전송한다.

[0030] 그러한 만큼, 클라이언트 소프트웨어는 서명된 전자적 자격 증명서를 검증하고, 전자적 자격 증명서에 기초하여 이차원 바코드를 생성하고, 그 결과, 자격 증명서 검증단 디바이스는 이차원 바코드에 포함되는 전자적 자격 증명서를 검증한다. 자격 증명서 검증단 디바이스는 유저 식별자에 기초하여 전자적 자격 증명서를 생성하도록 구성된다.

[0031] 본 발명의 이 구현예에서 제공되는 이차원 바코드를 프로세싱하기 위한 방법에 따르면, 클라이언트 소프트웨어에 의해 전송되는 전자적 자격 증명서 획득 요청을 수신한 이후, 서버는 서버 개인 키를 사용하는 것에 의해 클라이언트 소프트웨어의 유저 공개 키 및 전자적 자격 증명서에 서명하여 서버 서명 정보를 획득하고, 서버 서명 정보 및 전자적 자격 증명서를 클라이언트 소프트웨어로 전송한다. 클라이언트 소프트웨어는, 서버에 의해 전송되는 서버 서명 정보 및 전자적 자격 증명서를 수신하고, 서버 서명 정보를 검증하고, 서명 정보에 대한 검증이 성공한 이후, 전자적 자격 증명서에 서명하고, 미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 서버 서명 정보, 전자적 자격 증명서, 및 유저 공개 키에 기초하여 이차원 바코드를 생성한다. 이차원 바코드를 획득한 이후, 자격 증명서 검증단 디바이스는, 서버 서명 정보, 클라이언트 소프트웨어 서명 정보, 및 미리 결정된 보안 정보를 이차원 바코드에서 검증하여, 전자적 자격 증명서가 송신 프로세스에서 변경되는지의 여부를 결정하여, 사용 프로세스에서 전자적 자격 증명서의 보안성을 보장할 수 있다.

[0032] 도 1에서 도시되는 방법의 추가적인 설명으로서, 클라이언트 소프트웨어의 유저 식별자의 유효성을 보장하기 위해 그리고 클라이언트 소프트웨어의 유저 식별자가 콘텐츠 송신 프로세스에서 변경되지 않는 것을 보장하기 위

해, 단계 102에서, 클라이언트 소프트웨어의 유저 공개 키 및 전자적 자격 증명서는, 다음의 방법, 등등에서 서버 개인 키를 사용하는 것에 의해 서명될 수 있다. 예를 들면:

[0033] 방법 1: 서버는 전자적 자격 증명서에 유저 서명 키를 할당하고, 서버 개인 키를 사용하는 것에 의해 전자적 자격 증명서 및 제1 유저 공개 키에 서명하는데, 여기서, 할당된 유저 서명 키는 제1 유저 공개 키를 포함한다.

[0034] 서버가 클라이언트 소프트웨어에 의해 전송되는 전자적 자격 증명서 획득 요청을 수신할 때, 클라이언트 소프트웨어의 어떠한 유저 공개 키도 전자적 자격 증명서 획득 요청으로부터 획득되지 않는 경우, 서버는 유저 서명 키의 쌍을 전자적 자격 증명서에 일시적으로 할당하여 클라이언트 소프트웨어의 유저 식별자를 인증하고, 따라서, 전자적 자격 증명서가 변경되지 않는 것을 보장하고 - 할당된 유저 서명 키는 하나의 제1 유저 공개 키 및 하나의 제1 유저 개인 키를 포함함 - ; 그리고, 서버 개인 키를 사용하는 것에 의해 제1 유저 개인 키에 서명하여, 서버 서명 정보가 수신된 이후 서버 서명 정보에 대한 보안 인증을 수행한다.

[0035] 유저 서명 키가 서버에 의해 전자적 자격 증명서에 일시적으로 할당되기 때문에, 클라이언트 소프트웨어에 의해 유저 서명 키가 획득되지 않으면, 서버 내의 서버 서명 정보는 검증될 수 없다. 이전 문제점을 완화하기 위해, 서버가 방법 1을 사용하는 것에 의해 클라이언트 소프트웨어의 제1 유저 공개 키 및 전자적 자격 증명서에 서명하는 경우, 서버가 서버 서명 정보와 전자적 자격 증명서를 클라이언트 소프트웨어로 전송할 때, 서버는, 클라이언트 소프트웨어가 유저 서명 키에 기초하여 서버 서명 정보를 검증할 수 있도록, 전자적 자격 증명서에 할당되는 유저 서명 키를 클라이언트 소프트웨어로 동시에 전송하는 것을 필요로 한다.

[0036] 특정한 구현예 프로세스에서, 서버에 의해 전자적 자격 증명서에게 일시적으로 할당되는 유저 서명 키를 수신하고, 유저 서명 키에 기초하여 서버 서명 정보를 검증한 이후, 클라이언트 소프트웨어는 유저 서명 키를 직접적으로 폐기할 수 있거나, 유저 서명 키를 클라이언트 소프트웨어의 유저 공개 키 및 공통 유저 키로서 사용할 수 있다. 구현예는 본 발명의 이 구현예에서 제한되지 않는다.

[0037] 방법 2: 서버는 클라이언트 소프트웨어에 의해 전송되는 제2 유저 공개 키를 획득하고, 서버 개인 키를 사용하는 것에 의해 제2 유저 공개 키 및 전자적 자격 증명서에 서명한다.

[0038] 이 구현예에서, 클라이언트 소프트웨어의 신원을 식별하기 위해, 서버에 전자적 자격 증명서 획득 요청을 전송할 때, 서버가 클라이언트 소프트웨어에 대한 신원 인증을 수행하고 서버가 서버 개인 키를 사용하는 것에 의해 클라이언트 소프트웨어의 전자적 자격 증명서 및 제2 유저 공개 키에 서명하도록, 클라이언트 소프트웨어는 클라이언트 소프트웨어의 제2 유저 공개 키를 서버에 동시에 전송한다. 서명된 제2 유저 공개 키 및 서명된 전자적 자격 증명서를 수신한 이후, 클라이언트 소프트웨어는, 전자적 자격 증명서가 변경되지 않는 것을 보장하기 위해, 성공적인 서명 검증 이후에만 전자적 자격 증명서 정보를 획득할 수 있다.

[0039] 본 발명의 이 구현예에서 설명되는 제1 유저 공개 키 및 제2 유저 공개 키는 클라이언트 소프트웨어의 상이한 유저 공개 키를 구별하기 위해 사용된다는 것을 주목할 가치가 있다. "제1" 및 "제2"는 어떠한 다른 의미도 없으며, 유저 공개 키의 수, 우선 순위, 등등을 제한하도록 의도되지는 않는다. 클라이언트 소프트웨어에서 유저 공개 키를 명명하기 위한 방법은, 본 발명의 이 구현예에서 제한되지 않는다.

[0040] 설명의 용이성을 위해, 본 발명의 구현예에서의 후속하는 설명에서, 설명은, 유저 공개 키 및 유저 개인 키가 비대칭 키인 예를 사용하는 것에 의해 이루어진다. 그러나, 유저 공개 키와 유저 개인 키는 비대칭 키로 제한되는 것이 아니며, 대칭 키일 수 있다는 것을 분명히 알고 있어야 한다. 구현예는 본 발명의 이 구현예에서 제한되지 않는다.

[0041] 서버의 서명 프로세스의 이해를 용이하게 하기 위해, 이하, 설명을 위해, 유저 공개 키 및 전자적 자격 증명서에 서버가 서명하는 예를 사용한다. 특정한 프로세스는 다음의 것을 포함한다: 유저 공개 키 및 전자적 자격 증명서를 획득한 이후, 서버는 해시 알고리즘(hash algorithm)을 사용하는 것에 의해 유저 공개 키 및 전자적 자격 증명서에 대해 해시 연산(hash operation)을 수행하여 해시 값을 획득할 수 있고, 그 다음, 서버 개인 키를 사용하는 것에 의해 해시 값에 서명하여 서버 서명 정보를 획득할 수 있다. 서명 프로세스에서 사용되는 알고리즘(예컨대 해시 연산)은 본 발명의 이 구현예에서 제한되지 않는다.

[0042] 전자적 자격 증명서 및 유저 공개 키에 서명한 이후, 클라이언트 소프트웨어가 서버 서명 정보를 검증하고 전자적 자격 증명서가 데이터 송신 프로세스에서 악의적인 유저에 의해 변경되지 않는 것을 보장하도록, 서버는 전자적 자격 증명서, 서명된 유저 공개 키, 및 서명된 전자적 자격 증명서를 클라이언트 소프트웨어로 전송한다. 게다가, 서버는 또한, 클라이언트 소프트웨어 및 자격 증명서 검증단 디바이스가 서버에 의해 브로드캐스트되는 공개 키를 수신하고 서버 공개 키를 사용하여 서명 정보를 검증하도록, 서버가 서명 정보를 획득할 때 사용되는

서버 개인 키에 대응하는 공개 키를 브로드캐스트하는 것을 필요로 한다.

[0043] 게다가, 본 발명의 이 구현예에서 설명되는 서버는, 자격 증명서 정보 검증 당사자 및 클라이언트 소프트웨어를 운반하는 다리로서 역할을 한다. 서버는 유저의 유효성을 인증하는 것을 담당하며, 게다가, 서버는 또한, 전자적 자격 증명서를 사용하는 것의 유효성을 검증할 수 있다. 특정한 사용 프로세스에서, 전자적 자격 증명서는 상이한 서비스 타입에 대응하며, 상이한 서비스 타입은 상이한 서비스 명세(service specification)를 사용하는 것에 의해 제한된다. 예를 들면, 전자적 자격 증명서가 항공권인 경우, 항공권 서비스는 비행기의 출발 시간을 포함한다(이 적용 시나리오는 비행기가 지연 없이 정각에만 이륙하는 시나리오일 수 있다). 대안적으로, 전자적 자격 증명서가 콘서트 티켓인 경우, 티켓 서비스는 또한 콘서트의 시작 시간, 입장 시간, 등등을 포함한다. 따라서, 본 발명의 이 구현예에서, 유저 식별자에 기초하여 대응하는 전자적 자격 증명서를 획득하기 이전에, 서버는 전자적 자격 증명서 획득 요청을 파싱하는 것, 전자적 자격 증명서 획득 요청에 포함되는 서비스 유효 시간을 획득하는 것, 및 서비스 유효 시간이 서비스 명세를 따르는지의 여부를 검증하는 것을 필요로 한다. 서비스 유효 시간이 서비스 명세를 따르는 경우, 서버는 유저 식별자에 대응하는 전자적 자격 증명서를 획득한다. 서비스 유효 시간이 서비스 명세를 따르지 않으면, 서버는, 어떠한 대응하는 전자적 자격 증명서도 이용 가능하지 않다는 것을 나타내는 프롬프트 정보(prompt information)를, 클라이언트 소프트웨어로 반환한다.

[0044] 더 나은 이해를 위해, 이하, 서비스 유효 시간 및 서비스 명세를, 예를 사용하여 설명한다. 예를 들면, 전자적 자격 증명서가 버스 티켓 서비스이고, 자격 증명서 검증단 디바이스가 버스 티켓을 예매하는 시간이 7일이며, 현재 날짜는 2016년 11월 1일이다는 것을 가정한다. 유저는 2016년 11월 1일에 클라이언트 소프트웨어를 사용하는 것에 의해 전자적 자격 증명서 획득 요청을 서버에게 전송하고, 요청에 포함되는 서비스 유효 시간은 2016년 11월 20일이고, 자격 증명서 검증단 디바이스에 의해 생성되는 전자적 자격 증명서의 최대 유효성 시간은 2016년 11월 8일까지이다. 따라서, 서버는 서비스 유효 시간이 서비스 명세를 준수하지 않는다는 것을 결정할 수 있다. 이전의 설명은 예에 불과하다. 본 발명의 이 구현예는, 전자적 자격 증명서의 서비스 타입, 서비스 유효 시간, 서비스 명세, 등등에 대해 어떠한 제한도 부과하지 않는다.

[0045] 게다가, 단계 102에서, 유저 식별자에 대응하는 전자적 자격 증명서는, 다음 방법에 제한되지는 않지만 다음 방법에서 획득될 수 있다. 예를 들면:

[0046] 방법 1: 자격 증명서 검증단 디바이스가 유저 식별자에 기초하여 전자적 자격 증명서를 생성한 이후, 자격 증명서 검증단 디바이스에 의해 동기화되는 전자적 자격 증명서가 수신된다.

[0047] 이 구현예에서, 전자적 자격 증명서를 생성한 이후, 자격 증명서 검증단 디바이스는 생성된 전자적 자격 증명서를 서버에 능동적으로 전송한다. 특정한 구현예 프로세스에서, 복수의 전자적 자격 증명서의 관리를 용이하게 하기 위해, 서버는 미리 결정된 목록을 로컬하게 생성할 수 있는데, 여기서 미리 결정된 목록은, 유저 식별자와 전자적 자격 증명서 사이의 매핑 관계를 기록하기 위해 사용된다. 자격 증명서 검증단 디바이스에 의해 동기화되는 전자적 자격 증명서를 수신한 이후, 서버는, 전자적 자격 증명서와 미리 결정된 목록 내의 유저 식별자 사이의 새롭게 수신된 매핑 관계를 기록한다. 전자적 자격 증명서를 클라이언트 소프트웨어로 전송한 이후, 서버는, 미리 결정된 목록으로부터 성공적으로 전송된 전자적 자격 증명서를 삭제하여, 서버에 의해 점유되는 리소스를 감소시킬 수 있다.

[0048] 방법 2: 전자적 자격 증명서를 획득하기 위해, 전자적 자격 증명서를 획득하기 위한 요청 정보가 유저 식별자에 기초하여 자격 증명서 검증단 디바이스로 전송된다.

[0049] 이 구현예에서, 서버는 포워딩을 위해 사용된다. 서버는, 클라이언트 소프트웨어에 의해 전송되는 전자적 자격 증명서 획득 요청을 수신하는 경우에만 전자적 자격 증명서 획득 요청에서의 유저 식별자에 기초하여 자격 증명서 검증단 디바이스에게 전자적 자격 증명서를 요청하고, 그 다음, 획득된 전자적 자격 증명서를 클라이언트 소프트웨어로 포워딩한다. 서버에 의해 전자적 자격 증명서를 획득하기 위한 방법은, 본 발명의 이 구현예에서 제한되지 않는다.

[0050] 게다가, 이전 방법의 추가 설명 및 확장으로서, 본 발명의 구현예는 또한, 이차원 바코드를 프로세싱하기 위한 방법을 제공한다. 방법에서, 설명의 용이성을 위해, 클라이언트 소프트웨어는 ALIPAY(알리페이)이고 전자적 자격 증명서는 전자적 콘서트 티켓(electronic concert ticket)인 예를 사용하는 것에 의해 설명이 이루어진다. 그러한 설명 방법은, 본 발명의 이 구현예에서 설명되는 클라이언트 소프트웨어가 오로지 ALIPAY일 수 있다는 제한을 부과하도록 의도되는 것은 아니다는 것을 분명히 알고 있어야 한다. 도 3에서 도시되는 바와 같이, 방법은 다음의 단계를 포함한다.

[0051] 201. 서버는 ALIPAY에 의해 전송되는 전자적 콘서트 티켓 획득 요청을 수신하는데, 여기서, 전자적 콘서트 티켓 획득 요청은 이동 전화 번호 및 서비스 유효 시간을 포함한다.

[0052] 실제로, 서비스 유효 시간은 전자적 콘서트 티켓의 예약 시간일 수 있거나, 또는 전자적 콘서트 티켓의 시작 시간일 수 있거나, 또는 전자적 콘서트 티켓에 관련되지 않는 임의의 시간일 수 있다. 서비스 유효 시간은 본 발명의 이 구현예에서 제한되지 않는다.

[0053] 202a. 서버는 전자적 콘서트 티켓 획득 요청을 파싱하고, 전자적 콘서트 티켓 획득 요청에 포함되는 서비스 유효 시간을 획득한다.

[0054] 예를 들면, 요청에서의 서비스 유효 시간은 콘서트의 시작 시간: 2016년 9월 20일 16:00이고, 현재 날짜는 2016년 9월 1일이다.

[0055] 203a. 서비스 유효 시간이 서비스 명세를 따르는지의 여부를 검증함.

[0056] 서비스 유효 시간이 서비스 명세를 따르는 경우, 단계 204가 수행된다. 서비스 유효 시간이 서비스 명세를 따르지 않으면, 단계 205가 수행된다.

[0057] 본 발명의 이 구현예에서, 전자적 콘서트 티켓은 다음 시나리오의 경우에 획득된다: 콘서트에 대한 종이 티켓이 분실되거나 또는 손상되는 경우, 종이 티켓을 사후 등록하지 않고도, 전자적 콘서트 티켓을 검증하는 것에 의해 콘서트에 입장할 수 있다. 그것은 티켓을 사후 등록하는 지루한 프로세스를 감소시킨다. 이 예에서, 서비스 명세는, 콘서트가 열리기 이전 30일 이내에 전자적 콘서트 티켓이 획득될 수 있거나, 또는 콘서트가 열린 이후 30분 이내에 전자적 콘서트 티켓이 획득될 수 있다는 것이다는 것이 명시될 수 있다. 단계 202b는, 서비스 유효 시간이 서비스 명세를 따르면 수행될 수 있다. 단계 201에서 설명되는 유효 시간은, 서비스 명세를 따르는 2016년 9월 20일의 콘서트의 시작 시간이고, 따라서 단계 202b가 수행된다.

[0058] 202b. 서버는 전자적 콘서트 티켓 획득 요청을 파싱하고, 전자적 콘서트 티켓 획득 요청에서 이동 전화 번호를 획득한다.

[0059] 203b. 이동 전화 번호의 유효성을 검증함.

[0060] 이동 전화 번호가 유효한 경우, 단계 204가 수행된다. 이동 전화 번호가 무효한 경우, 단계 205가 수행된다.

[0061] 현 단계에서, 요청에서의 이동 전화 번호가 서버 내의 이동 전화 번호와 일치하는지의 여부가 검증된다.

[0062] 단계 202a 및 단계 202b가 수행될 때, 두 단계 사이에서는 어떠한 시퀀스도 존재하지 않는다는 것을 주목할 가치가 있다. 또한, 서비스 유효 시간에 대한 검증 및 유저 식별자(이동 전화 번호)에 대한 검증이 성공한 이후에만, 후속 단계가 계속 수행된다.

[0063] 204. 서버는, 이동 전화 번호에 대응하는 전자적 콘서트 티켓을 획득하고, 서버 개인 키를 사용하는 것에 의해 ALIPAY의 유저 공개 키 및 전자적 자격 증명서에 서명하여 서버 서명 정보를 획득한다.

[0064] 상이한 서비스 타입에 기초하여, 전자적 자격 증명서는 대응하는 세부 사항을 갖는다. 예로서, 전자적 콘서트 티켓이 사용된다. 전자적 콘서트 티켓은, 콘서트 위치, 스탠드, 특정한 좌석 번호, 콘서트 이름, 가격, 등등을 포함한다. 구현예는 본 발명의 이 구현예에서 제한되지 않는다.

[0065] 205. 전자적 콘서트 티켓 획득 요청을 가로채고, 요청 실패 프롬프트(request failure prompt)를 ALIPAY에 전송함.

[0066] 206. 서버 서명 정보 및 전자적 콘서트 티켓을 ALIPAY로 전송함.

[0067] 207. ALIPAY가 서버 공개 키에 기초하여 서명 정보를 검증하도록, 서버 개인 키에 대응하는 공개 키를 브로드캐스트함.

[0068] 도 3에서 도시되는 방법의 확장으로서, 종이 자격 증명서가 분실된 이후, 등록 취소(mobile number), 사후 등록(post-registration), 등등을 방지하면서, ALIPAY가 설치된 전자 디바이스(예를 들면, 이동 전화)가 분실된 이후, 유저는 이동 전화를 바꿀 수 있고, ALIPAY에 성공적으로 로그인한 이후, 계속해서, 전자적 자격 증명서를 사용할 수 있다. 그러한 적용 시나리오는, ALIPAY가 유저 개인 키, 서버 공개 키, 및 전자적 자격 증명서를 사용하는 것에 의해 성공적인 서명 검증을 수행한 이후에만 적용될 수 있다. ALIPAY가 서버 서명 정보를 검증하지 않은 경우, ALIPAY는 서버 공개 키에 기초하여 서버 서명 정보를 검증하는 것 및 검증이 성공한 이후 전자적 자

격 증명서를 획득하는 것을 필요로 한다. 본 발명의 옵션 사항인 구현예에서, 전자적 자격 증명서가 유출되지 않은 것을 추가로 결정하기 위해, 서버가 서버 서명 정보 및 전자적 자격 증명서를 클라이언트 소프트웨어로 전송한 이후, 서버 공개 키에 대한 검증 유효성 지속 기간(verification validity duration)이 설정될 수 있다. 그러한 만큼, 클라이언트 소프트웨어는 명시된 제한 시간 내에 서버 서명 정보에 대한 검증을 완료해야 한다. 서버 공개 키에 대한 검증 유효성 지속 기간이 만료되면, 서버 서명 정보는 검증될 수 없다.

[0069] 게다가, 본 발명의 구현예는 또한, 이차원 바코드를 프로세싱하기 위한 방법을 제공한다. 방법은 도 1에 도시되는 클라이언트 소프트웨어 측에 적용된다. 도 4에서 도시되는 바와 같이, 방법은 다음의 단계를 포함한다.

[0070] 301. 클라이언트 소프트웨어는, 서버에 의해 전송되는 서버 서명 정보 및 전자적 자격 증명서를 수신한다.

[0071] 클라이언트 소프트웨어가 유저 계정명 및 로그인 패스워드를 사용하는 것에 의해 서버에 성공적으로 로그인한 이후, 클라이언트 소프트웨어는 전자적 자격 증명서 획득 요청을 서버로 전송한다. 서버는 전자적 자격 증명서 획득 요청에 응답한다. 송신 프로세스에서 전자적 자격 증명서가 변경되는 것을 방지하기 위해, 서버는 서버 서명 정보 및 전자적 자격 증명서를 클라이언트 소프트웨어로 전송하여, 클라이언트 소프트웨어의 신원의 유효성을 검증한다. 서버 서명 정보는, 서버 개인 키를 사용하는 것에 의해 클라이언트 소프트웨어의 전자적 자격 증명서 및 유저 공개 키에 서명하는 것에 의해 서버에 의해 획득된다. 서버 서명 정보를 획득하는 것에 관한 관련된 설명에 대해서는, 이전 구현예에서의 상세한 설명에 대한 참조가 이루어질 수 있다. 본 발명의 이 구현예에서는 간략화를 위해 세부 사항이 생략된다.

[0072] 302. 클라이언트 소프트웨어는 전자적 자격 증명서를 획득하기 위해 서버 서명 정보를 검증한다.

[0073] 예를 들면, 서버에 의해 유저 공개 키 및 전자적 자격 증명서에 서명하는 것에 의해 획득되는 서버 서명 정보, 및 클라이언트 소프트웨어에 의해 수행되는 서버 서명 정보에 대한 검증은, 상세한 설명에 대한 예로서 사용된다. 도 5는, 본 발명의 구현에 따른, 서명 및 서명에 대한 검증을 예시하는 개략도이다. 유저 공개 키 및 전자적 자격 증명서를 획득한 이후, 서버는 해시 알고리즘을 사용하는 것에 의해 유저 공개 키 및 전자적 자격 증명서에 대해 해시 연산을 수행하여 제1 해시 값을 획득하고, 서버 개인 키를 사용하는 것에 의해 제1 해시 값을 암호화하여 서버 서명 정보를 획득한다. 서버는 서버 서명 정보 및 전자적 자격 증명서를 클라이언트 소프트웨어로 전송한다. 서버 서명 정보 및 전자적 자격 증명서를 수신한 이후, 클라이언트 소프트웨어는 전자적 자격 증명서를 추출하고, 전자적 자격 증명서에 대해 해시 연산을 수행하여 제2 해시 값을 획득한다. 또한, 클라이언트 소프트웨어는 서버 공개 키를 사용하여 서버 서명 정보를 암호 해제하여 제1 해시 값을 획득하고, 암호 해제를 통해 획득되는 제1 해시 값을, 계산을 통해 획득되는 제2 해시 값과 비교한다. 제1 해시 값이 제2 해시 값과 동일한 경우, 그것은, 송신 프로세스에서 전자적 자격 증명서가 변경되지 않았다는 것을 나타내고, 전자적 자격 증명서가 획득된 이후 전자적 자격 증명서는 직접적으로 사용될 수 있다. 제1 해시 값과 제2 해시 값이 상이한 경우, 그것은 데이터 송신 프로세스에서 전자적 자격 증명서가 변경되었다는 것을 나타내고, 정보 유출의 위험이 있을 수 있다. 도 5는 단지 예일 뿐이며, 서버 서명 정보의 특정한 콘텐츠는 제한되지 않는다는 것을 주목할 가치가 있다.

[0074] 303. 클라이언트 소프트웨어는, 유저 공개 키에 대응하는 유저 키를 획득하고, 유저 키를 사용하는 것에 의해 전자적 자격 증명서에 서명하여 클라이언트 소프트웨어 서명 정보를 획득한다.

[0075] 클라이언트 소프트웨어는 이차원 바코드에서 운반되는 전자적 자격 증명서를 생성한다. 전자적 자격 증명서가 불법적으로 변경되는 것을 방지하기 위해 그리고 전자적 자격 증명서 정보가 유출되는 것을 방지하기 위해, 클라이언트 소프트웨어는 유저 개인 키를 사용하는 것에 의해 전자적 자격 증명서에 서명하여, 클라이언트 소프트웨어 서명 정보를 획득하는 것을 필요로 한다. 클라이언트 소프트웨어가 생성된 이차원 바코드의 속성 정보로서 클라이언트 소프트웨어 서명 정보를 사용하는 경우, 자격 증명서 검증단 디바이스는 클라이언트 소프트웨어 서명 정보를 검증할 수 있고, 또한, 클라이언트 소프트웨어의 유효성을 인증할 수 있다.

[0076] 특정한 서명 구현예 방법에 대해서는, 도 5의 상세한 설명에 대한 참조가 이루어질 수 있다. 본 발명의 이 구현예에서는 간략화를 위해 세부 사항이 생략된다.

[0077] 304. 클라이언트 소프트웨어는, 미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 서버 서명 정보, 전자적 자격 증명서, 및 유저 공개 키에 기초하여 이차원 바코드를 생성한다.

[0078] 클라이언트 소프트웨어 및 자격 증명서 검증 당사자가 근거리 데이터(전자적 자격 증명서) 송신을 행하는 경우, 전자적 자격 증명서를 송신하는 것의 보안성을 보장하기 위해, 인증 정보가 생성된 이차원 바코드에 추가될 수 있고, 인증 정보는, 클라이언트 소프트웨어 서명 정보, 서버 서명 정보, 및 미리 결정된 보안 정보를 포함할 수

있지만 그러나 이들로 제한되지는 않는다. 자격 증명서 검증단 디바이스는 클라이언트 소프트웨어 서명 정보를 검증하여, 검증되는 것을 필요로 하는 전자적 자격 증명서가 클라이언트 소프트웨어에 의해 전송된다는 것을 결정할 수 있다. 또한, 자격 증명서 검증단 디바이스는, 이차원 바코드 내의 전자적 자격 증명서가 서버에 의해 전송된다는 것을 결정하기 위해 서버 서명 정보를 검증하여, 전자적 자격 증명서가 변경되지 않는 것을 보장할 수 있다.

[0079] 본 발명의 이 구현예에서, 미리 결정된 보안 정보는 이차원 바코드의 동적 구현예로서 사용되며, 클라이언트 소프트웨어와 자격 증명서 검증단 디바이스 사이의 "신뢰 가능한" 데이터 송신을 확립하기 위한 자격 증명서로서 사용된다. 클라이언트 소프트웨어에 의해 전송되는 이차원 바코드를 수신하기 이전에, 자격 증명서 검증단 디바이스는 클라이언트 소프트웨어에 의해 전송되는 전자적 자격 증명서의 보안을 보장하기 위해 미리 결정된 보안 정보의 유효성 및 보안성을 검증한다. 미리 결정된 보안 정보는 다음의 콘텐츠를 포함할 수 있지만 그러나 이들로 제한되지는 않는다: 동적 패스워드 정보, 시간 정보, 랜덤 코드 정보, 등등. 구현예는 본 발명의 이 구현예에서 제한되지 않는다.

[0080] 예를 들면, 본원에서 설명되는 바와 같이, 현재의 시스템 시간이 미리 결정된 보안 정보에 대해 사용된다. 클라이언트 소프트웨어가 08:00에 이차원 바코드를 생성하는 경우, 미리 결정된 보안 정보가 08/00이다는 것이 결정될 수 있다. 클라이언트 소프트웨어가 10:21에 이차원 바코드를 생성하는 경우, 미리 결정된 보안 정보가 10/21이다는 것이 결정될 수 있다. 앞선 예는, 미리 결정된 보안 정보를 현재의 시스템 시간으로서 사용하는 것에 의해 설명된다. 그러나, 그러한 설명 방법은, 본 발명의 이 구현예에서 설명되는 미리 결정된 보안 정보가 오로지 클라이언트 소프트웨어의 현재의 시스템 시간일 수 있다는 제한을 부과하도록 의도되지 않는다는 것을 분명히 알고 있어야 한다.

[0081] 이차원 바코드가 생성될 때, 클라이언트 소프트웨어의 유저 공개 키는 브로드캐스트되지 않고, 대신, 유저 공개 키는, 생성된 이차원 바코드의 속성 정보로서 직접적으로 사용된다는 것을 주목할 가치가 있다. 그것은 클라이언트 소프트웨어의 추가적인 오버헤드 및 비용을 효과적으로 감소시킬 수 있다.

[0082] 본 발명의 이 구현예에서 제공되는 이차원 바코드를 프로세싱하기 위한 방법에 따르면, 클라이언트 소프트웨어에 의해 전송되는 전자적 자격 증명서 획득 요청을 수신한 이후, 서버는 서버 개인 키를 사용하는 것에 의해 클라이언트 소프트웨어의 유저 공개 키 및 전자적 자격 증명서에 서명하여 서버 서명 정보를 획득하고, 서버 서명 정보 및 전자적 자격 증명서를 클라이언트 소프트웨어로 전송한다. 클라이언트 소프트웨어는, 서버에 의해 전송되는 서버 서명 정보 및 전자적 자격 증명서를 수신하고, 서버 서명 정보를 검증하고, 서명 정보에 대한 검증이 성공한 이후, 전자적 자격 증명서에 서명하고, 미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 서버 서명 정보, 전자적 자격 증명서, 및 유저 공개 키에 기초하여 이차원 바코드를 생성한다. 이차원 바코드를 획득한 이후, 자격 증명서 검증단 디바이스는, 서버 서명 정보, 클라이언트 소프트웨어 서명 정보, 및 미리 결정된 보안 정보를 이차원 바코드에서 검증하여, 전자적 자격 증명서가 송신 프로세스에서 변경되는지의 여부를 결정하여, 사용 프로세스에서 전자적 자격 증명서의 보안성을 보장할 수 있다.

[0083] 본 발명의 한 구현예에서, 유저 공개 키에 대응하는 유저 키를 획득할 때, 클라이언트 소프트웨어는, 서버에 의해 전송되며 전자적 자격 증명서에 할당되는 유저 서명 키를 수신하는데, 여기서, 유저 서명 키는 제1 유저 공개 키 및 제1 유저 키를 포함하고, 유저 키 및 유저 공개 키는 비대칭 키이고, 클라이언트 소프트웨어는, 서버에 의해 전자적 자격 증명서에 할당되는 유저 서명 키에서 제1 유저 키를 획득한다. 본 발명의 다른 구현예에서, 유저 공개 키에 대응하는 유저 키를 획득할 때, 클라이언트 소프트웨어는, 클라이언트 소프트웨어에 의해 생성되며 유저 공개 키에 대응하는 제2 유저 키를 획득할 수 있다. 클라이언트 소프트웨어가 유저 키를 획득하는 방법은 본 발명의 이 구현예에서 제한되지 않는다.

[0084] 게다가, 상기 서버 서명 정보를 검증할 때, 방법은 다음의 것을 포함한다: 서버에 의해 브로드캐스트되는 서버 공개 키를 수신 및 저장하는 것, 및 서버 공개 키 및 전자적 자격 증명서에 기초하여 서버 서명 정보를 검증하는 것.

[0085] 서버가 클라이언트 소프트웨어에 의해 생성되는 제2 유저 공개 키에 서명한다는 것을 결정하는 경우, 클라이언트 소프트웨어는 서버 공개 키, 전자적 자격 증명서, 및 제1 유저 공개 키에 기초하여 서버 서명 정보를 검증한다.

[0086] 서버가 서버에 의해 전자적 자격 증명서에 할당되는 제1 유저 공개 키에 서명한다는 것을 결정하는 경우, 클라이언트 소프트웨어는 서버 공개 키, 전자적 자격 증명서, 및 제2 유저 공개 키에 기초하여 서버 서명 정보를 검

증한다. 클라이언트 소프트웨어가 서버 서명 정보를 검증하는 프로세스의 경우, 도 5의 상세한 설명에 대한 참조가 이루어질 수 있다. 구현예는 본 발명의 이 구현예에서 제한되지 않는다.

[0087] 전자적 자격 증명서를 클라이언트 소프트웨어로 전송하는 경우, 클라이언트 소프트웨어가 후속하여 이차원 바코드를 생성할 때, 서버 서명 정보가 생성된 이차원 바코드의 속성 정보로서 사용될 수 있도록, 서버는 전자적 자격 증명서 및 유저 공개 키에 서명하여 서버 서명 정보를 획득하는 것을 필요로 한다는 것을 주목할 가치가 있다. 유저는 유저 개인 키를 사용하여 서버에 의해 전송되는 정보에 서명하여, 전자적 자격 증명서의 원래의 정보의 정확도를 보장하고, 검증될 때 유저 공개 키가 유효하고 신뢰 가능하며 위조 또는 거부될 수 없다는 것을 보장한다.

[0088] 게다가, 클라이언트 소프트웨어에는 복수의 유저 서명 키(클라이언트 소프트웨어에 의해 생성되는 제1 유저 키, 및 서버에 의해 전자적 자격 증명서에 할당되는 제2 유저 키를 포함함)가 존재할 수 있다. 따라서, 클라이언트 소프트웨어는, 클라이언트 소프트웨어와 매치하는 임의의 유저 개인 키를 사용하는 것에 의해 전자적 자격 증명서에 서명할 수 있다. 예를 들면, 클라이언트 소프트웨어는 제1 유저 키를 사용하는 것에 의해 전자적 자격 증명서에 서명할 수 있거나, 또는 제2 유저 키를 사용하는 것에 의해 전자적 자격 증명서에 서명할 수 있다. 구현예는 본 발명의 이 구현예에서 제한되지 않는다.

[0089] 전자적 자격 증명서의 보안성을 추가로 보장하기 위해, 클라이언트 소프트웨어가 이차원 바코드를 생성할 때, 클라이언트 소프트웨어는 또한 프로세스에서 클라이언트 소프트웨어 서명 정보를 사용한다. 그러한 만큼, 자격 증명서 검증단 디바이스는 클라이언트 소프트웨어 서명 정보를 검증하여, 전자적 자격 증명서가 클라이언트 소프트웨어에 의해 생성되고 클라이언트 소프트웨어가 전자적 자격 증명서를 사용하도록 승인되고 신뢰 가능하며, 전자적 자격 증명서가 위조 또는 거부될 수 없다는 것을 보장한다. 이차원 바코드는, 다음의 방법에서 미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 서버 서명 정보, 전자적 자격 증명서, 및 유저 공개 키에 기초하여 생성될 수 있다: 미리 결정된 보안 정보의 유효 지속 기간을 설정하는 것, 및 미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 서버 서명 정보, 전자적 자격 증명서, 유저 공개 키, 미리 결정된 보안 정보의 유효성 지속 기간, 및 유저 식별자에 기초하여 이차원 바코드를 생성하는 것.

[0090] 본 발명의 이 구현예에서, 이차원 바코드를 생성할 때, 클라이언트 소프트웨어는 생성된 이차원 바코드의 속성 정보로서 유저 식별자를 사용하는 것을 필요로 한다는 것을 주목할 가치가 있다. 이것은 유저 실명 시스템을 필요로 하는 자격 증명서 검증단 디바이스를 갖는 적용 시나리오에 적용될 수 있다. 예를 들면, 전자적 자격 증명서가 항공권, 버스 티켓, 기차표, 은행 카드, 등등에 대응하는 자격 증명서인 경우, 자격 증명서 검증단 디바이스가 그러한 전자적 자격 증명서를 검증할 때, 실명 시스템 조건을 체크하기 위해, 검증을 완료함에 있어서 지원하기 위해, 실명 시스템을 필요로 하는 몇몇 적용 시나리오에서 요건을 충족하기 위해, 유저 신분증 엔티티가 사용될 수 있다.

[0091] 본 발명의 이 구현예에서의 옵션 사항인 솔루션에서, 몇몇 높은 보안성 시나리오에서는, 이차원 바코드가 생성될 때, 이동 전화 또는 태블릿 컴퓨터가 분실되는 경우 또는 이차원 바코드가 크랙되는 시간의 짧은 기간 내에 이차원 바코드가 악의적인 유저에 의해 사용되는 것을 방지하기 위해, 전자적 자격 증명서를 사용하는 사람의 생체 인식 피쳐(biometric feature)가 이차원 바코드에 추가될 수 있다. 예를 들면, 전자적 자격 증명서를 사용하는 사람의 지문과 같은 생체 인식 피쳐가 이차원 바코드에 포함된다. 자격 증명서 검증단 디바이스가 이차원 바코드를 검증할 때, 전자적 자격 증명서의 보안성을 추가로 보장하기 위해서는, 사람의 생체 인식 피쳐에 대한 검증이 필요로 된다.

[0092] 게다가, 이전 구현예에서, 이차원 바코드를 프로세싱하기 위한 서버 및 클라이언트 소프트웨어의 특정한 기능 및 특정한 구현예가 상세하게 설명된다. 도 1에서 도시되는 자격 증명서 검증단 디바이스는, 이차원 바코드에 의존하는 생성된 전자적 자격 증명서에 대한 검증을 수행하는 것을 필요로 한다. 다음은 이차원 바코드를 프로세싱하기 위한 방법을 제공한다. 방법은 자격 증명서 검증단 디바이스에 적용된다. 도 6에서 도시되는 바와 같이, 방법은 다음의 단계를 포함한다.

[0093] 401. 자격 증명서 검증단 디바이스는 클라이언트 소프트웨어에서 이차원 바코드를 획득한다.

[0094] 이차원 바코드는 미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 서버 서명 정보, 전자적 자격 증명서, 및 유저 공개 키에 기초하여 클라이언트 소프트웨어에 의해 생성되고, 클라이언트 소프트웨어 서명 정보는 전자적 자격 증명서에 서명하는 것에 의해 클라이언트 소프트웨어에 의해 획득되고, 서버 서명 정보는 전자적 자격 증명서 및 유저 공개 키에 서명하는 것에 의해 서버에 의해 획득된다.

[0095] 자격 증명서 검증단 디바이스는, 다음의 방법의 등등에서 클라이언트 소프트웨어에서 이차원 바코드를 획득할 수 있다. 예를 들면, 이차원 바코드는, 미리 결정된 데이터 획득 지시(predetermined data acquisition instruction)를 사용하는 것에 의해 획득된다. 미리 결정된 데이터 획득 지시에 관한 방법은, 스캐닝 방법, 데이터 송신단 셰이킹 방법(data transmit end shaking method), 키 트리거링 방법(key triggering method), 음성 트리거 방법, 및 트랙을 따라 슬라이딩하는 방법을 포함한다.

[0096] 본 발명의 이 구현예에서의 미리 결정된 데이터 획득 지시 방법에서, 주사 방법 이외의 미리 결정된 데이터 획득 지시 방법은 데이터 송신 이전에 설정되는 것을 필요로 한다. 예를 들면, 데이터 송신단 셰이킹 방법은 다음과 같이 설정된다: 동일한 단일의 방향으로 두 번 흔드는 것, 좌측 및 우측으로 두 번 흔드는 것, 위아래로 세 번 흔드는 것. 키 트리거링 방법은 다음의 것을 포함한다: 자격 증명서 검증단 디바이스는 미리 결정된 키의 트리거링 상태를 모니터링하고, 미리 결정된 키는 물리적 키일 수 있거나, 또는 가상 키일 수 있다. 클라이언트 소프트웨어가 미리 결정된 키를 트리거하는 경우, 자격 증명서 검증단 디바이스는 클라이언트 소프트웨어에서 디스플레이되는 이차원 바코드를 획득할 수 있다. 클라이언트 소프트웨어가 터치스크린 클라이언트 소프트웨어인 경우, 자격 증명서 검증단 디바이스가 트랙을 따라 슬라이딩하는 방법을 미리 결정한 이후, 자격 증명서 검증단 디바이스는 클라이언트 소프트웨어에서 터치스크린의 슬라이딩 상태를 모니터링하고, 클라이언트 소프트웨어 유저가 스크린 상에서 슬라이딩 동작을 트리거하는 경우, 이차원 바코드를 획득한다. 미리 결정된 데이터 획득 지시는 상기에서 설명되고, 미리 결정된 데이터 획득 지시의 타입은 실제로 본 발명의 이 구현예에서 제한되지 않는다.

[0097] 402. 자격 증명서 검증단 디바이스는 미리 결정된 보안 정보의 유효성 지속 기간을 검증하고, 클라이언트 소프트웨어 서명 정보 및 서버 서명 정보를 검증한다.

[0098] 자격 증명서 검증단 디바이스는 획득된 이차원 바코드를 파싱하고, 이차원 바코드에 포함되는 미리 결정된 보안 정보 및 전자적 자격 증명서를 획득하고, 미리 결정된 보안 정보의 유효성 지속 기간 및 전자적 자격 증명서 내의 서비스 유효 시간의 유효성을 검증한다. 예를 들면, 미리 결정된 보안 정보가 클라이언트 소프트웨어의 현재 시스템 시간이고, 미리 결정된 보안 정보가 10/21이고, 미리 결정된 보안 정보의 유효성 지속 기간이 60 초라고 가정한다. 자격 증명서 검증단 디바이스는 현재 시스템 시간과 미리 결정된 보안 정보 사이의 시간 차이를 획득하고, 유효성 지속 기간이 60 초보다 더 큰지의 여부를 결정한다. 유효성 지속 기간이 60 초보다 더 크다는 것이 결정되면, 자격 증명서 검증단 디바이스는 이차원 바코드가 무효하다는 것을 결정한다. 앞선 설명은 예이다. 대안적으로, 미리 결정된 보안 정보의 유효성 지속 기간은 2 분, 등등으로 설정될 수 있다. 미리 결정된 보안 정보의 유효성 지속 기간은 본 발명의 이 구현예에서 제한되지 않는다.

[0099] 자격 증명서 검증단 디바이스가 클라이언트 소프트웨어 서명 정보 및 서버 서명 정보를 검증하는 구현예에 대해서는, 도 5에서 도시되는 방법에 대한 참조가 이루어질 수 있다. 본 발명의 이 구현예에서는 간략화를 위해 세부 사항이 생략된다.

[0100] 403. 미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 및 서버 서명 정보의 각각에 대한 검증이 성공하는 경우, 전자적 자격 증명서에 포함되는 서비스 유효 시간을, 검증을 위해, 획득함.

[0101] 서비스 유효 시간에 대한 검증의 경우, 이전 구현예에서의 관련된 설명에 대한 참조가 이루어질 수 있다. 본 발명의 이 구현예에서는 간략화를 위해 세부 사항이 생략된다.

[0102] 404. 전자적 자격 증명서에 포함되는 서비스 유효 시간에 대한 검증이 성공하는 경우, 전자적 자격 증명서에 대한 검증이 성공한다는 것을 결정함.

[0103] 본 발명의 이 구현예에서 제공되는 이차원 바코드를 프로세싱하기 위한 방법에 따르면, 클라이언트 소프트웨어에 의해 전송되는 전자적 자격 증명서 획득 요청을 수신한 이후, 서버는 서버 개인 키를 사용하는 것에 의해 클라이언트 소프트웨어의 유저 공개 키 및 전자적 자격 증명서에 서명하여 서버 서명 정보를 획득하고, 서버 서명 정보 및 전자적 자격 증명서를 클라이언트 소프트웨어로 전송한다. 클라이언트 소프트웨어는, 서버에 의해 전송되는 서버 서명 정보 및 전자적 자격 증명서를 수신하고, 서버 서명 정보를 검증하고, 서명 정보에 대한 검증이 성공한 이후, 전자적 자격 증명서에 서명하고, 미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 서버 서명 정보, 전자적 자격 증명서, 및 유저 공개 키에 기초하여 이차원 바코드를 생성한다. 이차원 바코드를 획득한 이후, 자격 증명서 검증단 디바이스는, 서버 서명 정보, 클라이언트 소프트웨어 서명 정보, 및 미리 결정된 보안 정보를 이차원 바코드에서 검증하여, 전자적 자격 증명서가 송신 프로세스에서 변경되는지의 여부를 결정하여, 사용 프로세스에서 전자적 자격 증명서의 보안성을 보장할 수 있다.

[0104] 게다가, 도 6에서 도시되는 방법에 대한 확장으로서, 본 발명의 이 구현예에서, 방법의 단계 모두는, 자격 증명서 검증단 디바이스에 의해 생성되는 전자적 자격 증명서에 기초하여 수행된다. 따라서, 본 발명의 이 구현예에서, 클라이언트 소프트웨어에서 이차원 바코드가 획득되기 이전에, 자격 증명서 검증단 디바이스는 유저 식별자에 기초하여 전자적 자격 증명서를 생성하고, 전자적 자격 증명서를 생성하는 기회는 다음 콘텐츠를 포함할 수 있지만 그러나 이들로 제한되지는 않는다. 예를 들면, 유저가 티켓 창구에서 티켓을 구매한 이후, 티켓 시스템은, 종이 자격 증명서 정보를 생성하는 것 외에, 전자적 자격 증명서 정보를 생성하고, 전자적 자격 증명서 정보를 서버로 피드백한다. 그러한 만큼, 서버는 전자적 자격 증명서를 클라이언트 소프트웨어로 전송할 수 있다. 대안적으로, 유저가 티켓 웹사이트 상에서 전자 티켓을 구매한 이후, 전자 티켓에 대응하는 전자적 자격 증명서가 생성되고, 그 다음, 서버로 전송된다. 본 발명의 이 구현예에서, 자격 증명서 검증단 디바이스가 전자적 자격 증명서를 생성한 이후 종이 티켓을 제공하는지의 여부에 대해서는 어떠한 제한도 없다. 본 발명의 이 구현예에서, 전자적 자격 증명서는, 종이 자격 증명서가 분실되거나 또는 손상된 이후, 종이 자격 증명서에 대한 복잡한 사후 등록 동작을 방지하도록 의도된다. 또한, 자격 증명서 검증단 디바이스가, 동적인 이차원 바코드에서 운반되는 전자적 자격 증명서를 획득하는 경우, 전자적 자격 증명서의 보안성이 보장될 수 있다.

[0105] 자격 증명서 검증단 디바이스가 전자적 자격 증명서를 생성한 이후, 클라이언트 소프트웨어가 서버로부터 전자적 자격 증명서를 획득할 수 있도록, 대응하는 전자적 자격 증명서는 유저 식별 정보에 기초하여 서버에 동기화될 수 있다. 본 발명의 다른 구현예에서, 서버에 의해 전송되는 전자적 자격 증명서를 획득하기 위한 요청 정보를 수신한 이후, 자격 증명서 검증단 디바이스는 전자적 자격 증명서를 서버로 전송하는데, 여기서, 전자적 자격 증명서를 획득하기 위한 요청 정보는 유저 식별자를 포함한다.

[0106] 게다가, 자격 증명서 검증단 디바이스는 다음의 방법, 등등에서 클라이언트 소프트웨어 서명 정보 및 서버 서명 정보를 검증할 수 있다. 예를 들면, 자격 증명서 검증단 디바이스는 이차원 바코드에 포함되는 유저 공개 키를 획득하고, 유저 공개 키 및 전자적 자격 증명서에 기초하여 클라이언트 소프트웨어 서명 정보를 검증한다. 자격 증명서 검증단 디바이스는 서버 개인 키에 대응하며 서버에 의해 브로드캐스트되는 서버 공개 키를 수신 및 저장하고; 서버 공개 키 및 전자적 자격 증명서에 기초하여 서버 서명 정보를 검증한다.

[0107] 게다가, 상대적으로 높은 보안 요건을 갖는 몇몇 적용 시나리오에서, 자격 증명서 검증단 디바이스가 유저 신원 정보를 인증하도록, 클라이언트 소프트웨어는 생성된 이차원 바코드의 속성 정보로서 유저 식별자 정보를 사용한다. 예를 들면, 클라이언트 소프트웨어는 생성된 이차원 바코드의 속성 정보로서 유저 신분증을 사용한다. 자격 증명서 검증단 디바이스는 이차원 바코드를 파싱하고, 자격 증명서 검증단 디바이스에 포함되는 유저 식별자를 획득하고, 유저 식별자를 검증한다. 자격 증명서 검증단 디바이스가 유저 식별자에 대한 검증이 성공한다는 것을 결정하는 경우, 자격 증명서 검증단 디바이스는 전자적 자격 증명서에 대한 검증이 성공한다는 것을 결정한다. 예를 들면, 이차원 바코드 내의 전자적 자격 증명서가 기차 티켓인 경우, 유저가 전자적 기차 티켓을 사용하여 역 개찰구를 통과할 때, 유저의 신분증이 동시에 검증되어, 전자적 자격 증명서에 대한 검증을 완료할 수 있다.

[0108] 게다가, 자격 증명서 검증단 디바이스가 이차원 바코드에 포함되는 콘텐츠를 검증하는 경우, 이차원 바코드에 포함되는 콘텐츠의 양에 관계없이, 이차원 바코드에 포함되는 콘텐츠가 자격 증명서 검증단 디바이스에 의해 성공적으로 검증되는 한, 그것은, 전자적 자격 증명서 검증이 성공한다는 것을 나타낸다. 이차원 바코드에 포함되는 하나의 항목 또는 몇몇 항목이 검증에 실패하는 경우, 그것은 전자적 자격 증명서 검증이 실패한다는 것을 나타낸다. 예를 들면, 이차원 바코드가 미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 서버 서명 정보, 및 유저 식별자를 포함하는 경우, 미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 서버 서명 정보, 및 유저 식별자의 각각에 대한 검증이 성공한 이후에만 전자적 자격 증명서가 성공적으로 검증된다는 것이 결정될 수 있다는 것을 가정한다.

[0109] 상기에서 설명되는 바와 같이, 자격 증명서 검증단 디바이스는 이차원 바코드에서 운반되는 전자적 자격 증명서를 검증하고, 프로세스로부터 일상의 업무 및 생활에서의 전자적 자격 증명서의 편리성 및 보안성이 확인될 수 있다. 앞선 설명은, 클라이언트 소프트웨어가 하나의 타입의 전자적 자격 증명서를 포함하는 예를 사용하는 것에 의해 설명된다. 실제로, 클라이언트 소프트웨어는 복수의 타입의 전자적 자격 증명서를 포함할 수 있다. 전자적 자격 증명서는, 상이한 동적 이차원 바코드에 별개로 기록될 수 있거나, 또는 동일한 이차원 바코드에 기록될 수 있다. 구현예는 본 발명의 이 구현예에서 제한되지 않는다. 전자적 자격 증명서는 현존하는 기술의 엔티티 자격 증명서 정보를 대체하여, 엔티티 자격 증명서에서의 정보 유출을 방지할 수 있고, 엔티티 자격 증명서가 분실되는 경우 성가신 등록 취소 또는 사후 등록 단계를 완화할 수 있다. 본 발명의 이 구현예에서의 방법에 따르면, 유저는, 외출할 때, 클라이언트 소프트웨어가 설치된 하나의 단말 디바이스(이동 전화)를 휴대하는

것만을 필요로 하며, 어떠한 엔티티 자격 증명서도 운반하는 것을 필요로 하지 않는다.

[0110] 예를 들면, 유저 A는 클라이언트 소프트웨어가 설치된 하나의 이동 전화만을 휴대하고, 아침 8:00에 집에서 버스를 타고 회사로 간다. 유저는 클라이언트 소프트웨어 내의 버스 전자적 자격 증명서의 이차원 바코드를 사용하여 원활하게 이동할 수 있다. 도착한 이후, 유저는 액세스 제어 전자적 자격 증명서를 사용하여 회사에 들어갈 수 있고, 전자적 자격 증명서를 사용하는 것에 의해 출근 시간을 기록할(punch in) 수 있다. 오전 11:00에, 유저 A는 은행 서비스를 처리하기 위해 은행에 갈 필요가 있고, 전자 신분증 및 전자적 은행 카드가 사용되어 서비스를 처리할 수 있다. 17:00에, 유저 A는 출장(business trip)을 위해 기차역으로 이동하는 것을 필요로 한다. 유저 A가 개찰기를 통과하고 있을 때, 전자적 신분증 및 전자적 기차 티켓을 사용하는 것에 의해 실명 검증이 수행될 수 있다. 검증이 성공하는 경우, 유저는 기차를 탈 수 있다. 일단 전자적 자격 증명서가 검증되면, 이차원 바코드를 프로세싱하기 위한 이전의 보안 방법이 사용된다. 앞선 예는 일상 및 업무에 대해 전자적 자격 증명서가 가져오는 편리성 및 보안성을 예시하도록 의도되며, 전자적 자격 증명서의 특정한 적용 시나리오를 제한하도록 의도되는 것은 아니다.

[0111] 이전의 구현예에서, 서버, 클라이언트 소프트웨어, 및 자격 증명서 검증단 디바이스가 이차원 바코드를 프로세싱하는 프로세스는 개별적으로 상세히 설명된다. 그러나, 실제로는, 서버, 클라이언트 소프트웨어, 및 자격 증명서 검증단 디바이스는 이차원 바코드를 검증함에 있어서 절대 필요하다. 다음의 구현예에서, 서버, 클라이언트 소프트웨어, 및 자격 증명서 검증단 디바이스는 요약되어 설명된다. 도 7에서 도시되는 바와 같이, 방법은 다음의 단계를 포함한다.

[0112] 501. 자격 증명서 검증단 디바이스는 유저 식별자에 기초하여 전자적 자격 증명서를 생성하고, 서버가 전자적 자격 증명서를 클라이언트 소프트웨어로 전송하도록, 유저 식별자에 기초하여 대응하는 전자적 자격 증명서를 서버에 동기화시킨다.

[0113] 502. 클라이언트 소프트웨어는 전자적 자격 증명서 획득 요청을 서버로 전송하는데, 여기서, 전자적 자격 증명서 획득 요청은 유저 식별자 및 서비스 유효 시간을 포함한다.

[0114] 503. 서버는 클라이언트 소프트웨어에 의해 전송되는 전자적 자격 증명서 획득 요청을 수신하고, 전자적 자격 증명서 획득 요청을 파싱하고, 전자적 자격 증명서 획득 요청에 포함되는 서비스 유효 시간을 획득한다.

[0115] 504. 서버는 서비스 유효 시간이 서비스 명세를 따르는지의 여부를 검증한다.

[0116] 서비스 유효 시간이 서비스 명세를 따르는 경우, 단계 505가 수행된다. 서비스 유효 시간이 서비스 명세를 따르지 않는 경우, 전자적 자격 증명서 획득 요청이 무시된다.

[0117] 505. 유저 식별자에 대응하는 전자적 자격 증명서를 획득하고, 전자적 자격 증명서를 암호화한다.

[0118] 전자적 자격 증명서를 획득하기 위한 요청 정보는 또한, 전자적 자격 증명서를 획득하기 위해, 유저 식별자에 기초하여 자격 증명서 검증단 디바이스로 전송될 수 있다.

[0119] 506. 서버는 서버 개인 키를 사용하는 것에 의해 전자적 자격 증명서 및 클라이언트 소프트웨어의 유저 공개 키에 서명하여 서버 서명 정보를 획득하고, 서버 서명 정보 및 전자적 자격 증명서를 클라이언트 소프트웨어로 전송한다.

[0120] 507. 클라이언트 소프트웨어 및 자격 증명서 검증단 디바이스가 서버 공개 키에 기초하여 서명 정보를 검증하도록, 서버는 서버 개인 키에 대응하는 공개 키를 브로드캐스트한다.

[0121] 508. 클라이언트 소프트웨어는 서버에 의해 브로드캐스트되는 공개 키를 수신 및 저장한다.

[0122] 509. 클라이언트 소프트웨어는, 서버에 의해 전송되는 서버 서명 정보 및 전자적 자격 증명서를 수신한다.

[0123] 510. 클라이언트 소프트웨어는 서버에 의해 브로드캐스트되는 공개 키에 기초하여 서버 서명 정보를 검증하여, 전자적 자격 증명서를 획득한다.

[0124] 서버 서명 정보에 대한 검증이 성공하는 경우, 단계 511이 수행된다. 서버 서명 정보에 대한 검증이 실패하는 경우, 서버에 의해 제공되는 전자적 자격 증명서는 획득될 수 없다.

[0125] 511. 클라이언트 소프트웨어는 유저 키를 사용하는 것에 의해 전자적 자격 증명서에 서명하여 클라이언트 소프트웨어 서명 정보를 획득하고, 미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 서버 서명 정보, 전자적 자격 증명서, 및 유저 공개 키에 기초하여 이차원 바코드를 생성한다.

[0126] 512. 자격 증명서 검증단 디바이스는 클라이언트 소프트웨어에서 이차원 바코드를 획득하고, 미리 결정된 보안 정보의 유효성 지속 기간을 검증하고, 클라이언트 소프트웨어 서명 정보 및 서버 서명 정보를 검증한다.

[0127] 513. 미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 및 서버 서명 정보의 각각에 대한 검증이 성공하는 경우, 전자적 자격 증명서에 포함되는 서비스 유효 시간을, 검증을 위해, 획득하고; 전자적 자격 증명서에 포함되는 서비스 유효 시간에 대한 검증이 성공하는 경우, 전자적 자격 증명서에 대한 검증이 성공한다는 것을 결정한다.

[0128] 단계 501 내지 단계 513의 상세한 설명의 경우, 앞선 관련 설명에 대한 참조가 이루어질 수 있다는 것을 주목할 가치가 있다. 본 발명의 이 구현예에서는 간략화를 위해 세부 사항이 생략된다.

[0129] 게다가, 도 1에서 도시되는 방법의 구현예로서, 본 발명의 다른 구현예는 또한 서버를 제공한다. 이 장치 구현예는 앞선 방법 구현예에 대응한다. 판독의 용이성을 위해, 앞선 방법 구현예에서의 세부 사항은 이 장치 구현예에서 생략된다. 그러나, 이 구현예에서의 장치는 앞선 방법 구현예에서의 모든 콘텐츠를 상응하게 구현할 수 있다는 것을 분명히 알고 있어야 한다.

[0130] 게다가, 본 발명의 구현예는 서버를 제공한다. 도 8에서 도시되는 바와 같이, 장치는 다음을 더 포함한다: 클라이언트 소프트웨어에 의해 전송되는 전자적 자격 증명서 획득 요청 - 전자적 자격 증명서 획득 요청은 유저 식별자를 포함함 - 을 수신하도록 구성되는 수신 유닛(61); 수신 유닛에 의해 수신되는 유저 식별자에 대응하는 전자적 자격 증명서를 획득하도록 구성되는 제1 획득 유닛(62); 서버 개인 키를 사용하는 것에 의해 클라이언트 소프트웨어의 유저 공개 키 및 전자적 자격 증명서에 서명하여 서버 서명 정보를 획득하도록 구성되는 서명 유닛(63); 및 클라이언트 소프트웨어가 유저 키의 유효성 시간 내에 서버 서명 정보를 검증하고, 전자적 자격 증명서에 기초하여 이차원 바코드를 생성하여 자격 증명서 검증단 디바이스 - 자격 증명서 검증단 디바이스는 유저 식별자에 기초하여 전자적 자격 증명서를 생성하도록 구성됨 - 가 이차원 바코드에 포함되는 전자적 자격 증명서를 검증하도록, 서명 유닛(63)에 의해 획득되는 서버 서명 정보 및 제1 획득 유닛에 의해 획득되는 전자적 자격 증명서를 클라이언트 소프트웨어로 전송하도록 구성되는 전송 유닛(64).

[0131] 도 9에서 도시되는 바와 같이, 서명 유닛(63)은 다음의 것을 포함한다: 유저 서명 키를 전자적 자격 증명서에 할당하도록 구성되는 할당 모듈(631); 서버 개인 키를 사용하는 것에 의해, 할당 모듈에 의해 할당되는 제1 유저 공개 키 및 전자적 자격 증명서에 서명하도록 구성되는 제1 서명 모듈(first signing module)(632) - 할당된 유저 서명 키는 제1 유저 공개 키를 포함함 - ; 클라이언트 소프트웨어에 의해 전송되는 제2 유저 공개 키를 획득하도록 구성되는 획득 모듈(633); 및 서버 개인 키를 사용하는 것에 의해, 획득 모듈에 의해 획득되는 제2 유저 공개 키 및 전자적 자격 증명서에 서명하도록 구성되는 제2 서명 모듈(634).

[0132] 게다가, 제1 유저 공개 키가 서버 개인 키를 사용하는 것에 의해 서명되는 경우, 전송 유닛(64)은 또한, 할당된 유저 서명 키, 서버 서명 정보, 및 전자적 자격 증명서를 클라이언트 소프트웨어로 전송하도록 구성된다.

[0133] 게다가, 도 9에서 도시되는 바와 같이, 서버는 다음의 것: 제1 획득 유닛(62)이 유저 식별자에 대응하는 전자적 자격 증명서를 획득하기 이전에, 전자적 자격 증명서 획득 요청을 파싱하도록 구성되는 파싱 유닛(65); 파싱 유닛(65)이 전자적 자격 증명서 획득 요청을 파싱한 이후, 전자적 자격 증명서 획득 요청에 포함되는 서비스 유효 시간을 획득하도록 구성되는 제2 획득 유닛(66); 및 제2 획득 유닛(66)에 의해 획득되는 서비스 유효 시간이 서비스 명세를 따르는지의 여부를 검증하도록 구성되는 검증 유닛(67)을 더 포함하되, 제1 획득 유닛(62)은 또한: 서비스 유효 시간이 서비스 명세를 따른다는 것을 검증 유닛(67)이 검증하는 경우, 유저 식별자에 대응하는 전자적 자격 증명서를 획득하도록 구성된다.

[0134] 게다가, 도 9에서 도시되는 바와 같이, 제1 획득 유닛(62)은 다음의 것을 포함한다: 자격 증명서 검증단 디바이스가 유저 식별자에 기초하여 전자적 자격 증명서를 생성한 이후, 자격 증명서 검증단 디바이스에 의해 동기화되는 전자적 자격 증명서를 수신하도록 구성되는 수신 모듈(621); 및 전자적 자격 증명서를 획득하기 위한 요청 정보를 유저 식별자에 기초하여 자격 증명서 검증단 디바이스로 전송하여, 전자적 자격 증명서를 획득하도록 구성되는 프로세싱 모듈(622).

[0135] 게다가, 유저 서명 키는 비대칭 키이다.

[0136] 게다가, 도 9에 나타낸 바와 같이, 서버는 다음의 것을 더 포함한다: 클라이언트 소프트웨어 및 자격 증명서 검증단 디바이스가 서버 공개 키에 기초하여 서명 정보를 검증하도록, 서버 개인 키에 대응하는 공개 키를 브로드캐스트하도록 구성되는 브로드캐스팅 유닛(68).

[0137] 본 발명의 구현예는 또한 클라이언트 소프트웨어를 제공한다. 도 10에서 도시되는 바와 같이, 클라이언트 소프트웨어는 다음의 것을 포함한다: 서버에 의해 전송되는 서버 서명 정보 및 전자적 자격 증명서 - 서버 서명 정보는, 서버 개인 키를 사용하는 것에 의해 클라이언트 소프트웨어의 유저 공개 키 및 전자적 자격 증명서에 서명하는 것에 의해 서버에 의해 획득됨 - 를 수신하도록 구성되는 제1 수신 유닛(71); 서버 서명 정보를 검증하여 전자적 자격 증명서를 획득하도록 구성되는 서명 검증 유닛(72); 유저 공개 키에 대응하는 유저 키를 획득하도록 구성되는 획득 유닛(73); 획득 유닛(73)에 의해 획득되는 유저 키를 사용하는 것에 의해 전자적 자격 증명서에 서명하여 클라이언트 소프트웨어 서명 정보를 획득하도록 구성되는 서명 유닛(74); 및 자격 증명서 검증단 디바이스가 미리 결정된 보안 정보 - 미리 결정된 보안 정보는 유효성 지속 기간을 가지며, 자격 증명서 검증단 디바이스는 유저 식별자에 기초하여 전자적 자격 증명서를 생성하도록 구성됨 - 및 유저 공개 키에 기초하여 이차원 바코드에 포함되는 전자적 자격 증명서를 검증하도록, 미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 서버 서명 정보, 전자적 자격 증명서, 및 유저 공개 키에 기초하여 이차원 바코드를 생성하도록 구성되는 생성 유닛(75).

[0138] 게다가, 도 11에서 도시되는 바와 같이, 클라이언트 소프트웨어는 다음의 것을 더 포함한다: 유저 공개 키에 대응하는 유저 키를 획득하기 이전에, 전자적 자격 증명서에 할당되며 서버에 의해 전송되는 유저 서명 키를 수신하도록 구성되는 제2 수신 유닛(76).

[0139] 획득 유닛(73)은 또한, 서버에 의해 전자적 자격 증명서에 할당되며 제2 수신 유닛에 의해 수신되는 유저 서명 키에 포함되는 제1 유저 키를 획득하도록 구성된다.

[0140] 획득 유닛(73)은 또한, 클라이언트 소프트웨어에 의해 생성되며 유저 공개 키에 대응하는 제2 유저 키를 획득하도록 구성된다.

[0141] 게다가, 도 11에서 도시되는 바와 같이, 서명 유닛(74)은 다음의 것을 포함한다: 제1 유저 키를 사용하는 것에 의해 전자적 자격 증명서에 서명하도록 구성되는 제1 서명 모듈(741); 및 제2 유저 키를 사용하는 것에 의해 전자적 자격 증명서에 서명하도록 구성되는 제2 서명 모듈(742).

[0142] 게다가, 도 11에서 도시되는 바와 같이, 서명 검증 유닛(72)은 다음의 것을 포함한다: 서버에 의해 브로드캐스트되는 서버 공개 키를 수신하도록 구성되는 수신 모듈(721); 수신 모듈에 의해 수신되는 서버 공개 키를 저장하도록 구성되는 저장 모듈(722); 및 저장 모듈에 의해 저장되는 서버 공개 키, 클라이언트 소프트웨어 공개 키, 및 전자적 자격 증명서에 기초하여 서버 서명 정보를 검증하도록 구성되는 제1 서명 검증 모듈(723).

[0143] 게다가, 유저 공개 키 및 유저 키는 비대칭 키이다.

[0144] 게다가, 도 11에서 도시되는 바와 같이, 생성 유닛(75)은 다음의 것을 포함한다: 미리 결정된 보안 정보의 유효성 지속 기간을 설정하도록 구성되는 설정 모듈(751); 및 미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 서버 서명 정보, 전자적 자격 증명서, 유저 공개 키, 미리 결정된 보안 정보의 유효성 지속 기간, 및 유저 식별자에 기초하여 이차원 바코드를 생성하도록 구성되는 생성 모듈(752).

[0145] 본 발명의 구현예는 또한 자격 증명서 검증단 디바이스를 제공한다. 도 12에서 도시되는 바와 같이, 자격 증명서 검증단 디바이스는 다음의 것을 포함한다: 클라이언트 소프트웨어에서 이차원 바코드 - 이차원 바코드는 미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 서버 서명 정보, 전자적 자격 증명서, 및 유저 공개 키에 기초하여 클라이언트 소프트웨어에 의해 생성되고, 클라이언트 소프트웨어 서명 정보는 전자적 자격 증명서에 서명하는 것에 의해 클라이언트 소프트웨어에 의해 획득되고, 서버 서명 정보는 전자적 자격 증명서 및 유저 공개 키에 서명하는 것에 의해 서버에 의해 획득됨 - 를 획득하도록 구성되는 제1 획득 유닛(81); 제1 획득 유닛에 의해 획득되는 미리 결정된 보안 정보의 유효성 지속 기간을 검증하도록 구성되는 제1 검증 유닛(82); 클라이언트 소프트웨어 서명 정보 및 서버 서명 정보를 검증하도록 구성되는 제2 검증 유닛(83); 미리 결정된 보안 정보에 대한 제1 검증 유닛의 검증이 성공하고, 클라이언트 소프트웨어 서명 정보 및 서버 서명 정보의 각각에 대한 제2 검증 유닛의 검증이 성공하는 경우, 전자적 자격 증명서에 포함되는 서비스 유효 시간을, 검증을 위해, 획득하도록 구성되는 제3 검증 유닛(84); 및 전자적 자격 증명서에 포함되는 서비스 유효 시간에 대한 제3 검증 유닛의 검증이 성공하는 경우, 전자적 자격 증명서에 대한 검증이 성공한다는 것을 결정하도록 구성되는 결정 유닛(85).

[0146] 도 13에서 도시되는 바와 같이, 자격 증명서 검증단 디바이스는 다음의 것: 제1 획득 유닛(81)이 클라이언트 소프트웨어에서 이차원 바코드를 획득하기 이전에, 유저 식별자에 기초하여 전자적 자격 증명서를 생성하도록 구성되는 생성 유닛(86); 서버가 전자적 자격 증명서를 클라이언트 소프트웨어로 전송하도록, 유저 식별자에 기초

하여 대응하는 전자적 자격 증명서를 서버에 동기화하도록 구성되는 동기화 유닛(87); 서버에 의해 전송되는 전자적 자격 증명서를 획득하기 위한 요청 정보를 수신하도록 구성되는 수신 유닛(88); 및 전자적 자격 증명서를 서버로 전송하도록 구성되는 전송 유닛(89)을 더 포함하되, 전자적 자격 증명서를 획득하기 위한 요청 정보는 유저 식별자를 포함한다.

[0147] 게다가, 도 13에서 도시되는 바와 같이, 제2 검증 유닛(83)은 다음의 것을 포함한다: 이차원 바코드에 포함되는 유저 공개 키를 획득하도록 구성되는 획득 모듈(831); 전자적 자격 증명서 및 획득 모듈에 의해 획득되는 유저 공개 키에 기초하여 클라이언트 소프트웨어 서명 정보를 검증하도록 구성되는 제1 서명 검증 모듈(832); 서버 개인 키에 대응하며 서버에 의해 브로드캐스트되는 서버 공개 키를 수신하도록 구성되는 수신 모듈(833); 수신 모듈에 의해 수신되는 서버 공개 키를 저장하도록 구성되는 저장 모듈(834); 및 저장 모듈에 의해 저장되는 서버 공개 키, 클라이언트 소프트웨어 공개 키, 및 전자적 자격 증명서에 기초하여 서버 서명 정보를 검증하도록 구성되는 제2 서명 검증 모듈(835).

[0148] 도 13에서 도시되는 바와 같이, 자격 증명서 검증단 디바이스는 다음의 것을 더 포함한다: 전자적 자격 증명서에 대한 검증이 성공한다는 것을 결정 유닛(85)이 결정하기 이전에, 이차원 바코드에 포함되는 유저 식별자를 획득하도록 구성되는 제2 획득 유닛(810); 및 제2 획득 유닛(810)에 의해 획득되는 유저 식별자를 검증하도록 구성되는 제4 검증 유닛(811).

[0149] 결정 유닛(85)은 또한: 유저 식별자에 대한 검증이 성공한다는 것을 제4 검증 유닛(811)이 결정하는 경우, 전자적 자격 증명서에 대한 검증이 성공한다는 것을 결정하도록 구성된다.

[0150] 게다가, 도 14에서 도시되는 바와 같이, 본 발명의 구현예는 또한, 이차원 바코드를 프로세싱하기 위한 시스템을 제공하는데, 시스템은 다음의 것을 포함한다: 전자적 자격 증명서 획득 요청 - 전자적 자격 증명서 획득 요청은 유저 식별자를 포함함 - 을 서버(92)로 전송하도록 구성되는 클라이언트 소프트웨어(91); 클라이언트 소프트웨어(91)에 의해 전송되는 전자적 자격 증명서 획득 요청을 수신하도록, 그리고 유저 식별자에 기초하여 자격 증명서 검증단 디바이스(93)로부터 전자적 자격 증명서를 획득하도록 구성되는 서버(92); 및 서버(92)에 의해 전송되는 전자적 자격 증명서를 획득하기 위한 요청 정보를 수신하도록 그리고 그에 응답하도록, 그리고 전자적 자격 증명서를 서버(92)로 전송하도록 구성되는 자격 증명서 검증단 디바이스(93).

[0151] 서버(92)는 또한, 자격 증명서 검증단 디바이스(93)에 의해 전송되는 전자적 자격 증명서를 수신하도록, 전자적 자격 증명서 및 클라이언트 소프트웨어(91)의 유저 공개 키에 서명하여 서버(92) 서명 정보를 획득하도록, 그리고 서버(92) 서명 정보 및 전자적 자격 증명서를 클라이언트 소프트웨어(91)로 전송하도록 구성된다.

[0152] 클라이언트 소프트웨어(91)는, 서버(92)에 의해 전송되는 전자적 자격 증명서 및 서버(92) 서명 정보를 수신하도록, 서버(92) 서명 정보를 검증하여 전자적 자격 증명서를 획득하도록, 유저 공개 키에 대응하는 유저 키를 획득하도록, 유저 키를 사용하는 것에 의해 전자적 자격 증명서에 서명하여 클라이언트 소프트웨어(91) 서명 정보를 획득하도록, 그리고 미리 결정된 보안 정보, 클라이언트 소프트웨어(91) 서명 정보, 서버(92) 서명 정보, 전자적 자격 증명서, 및 유저 공개 키에 기초하여 이차원 바코드를 생성하도록 구성된다.

[0153] 자격 증명서 검증단 디바이스(93)는 클라이언트 소프트웨어(91)에서 이차원 바코드를 획득하도록, 미리 결정된 보안 정보의 유효성 지속 기간을 검증하도록, 그리고 클라이언트 소프트웨어(91) 서명 정보 및 서버(92) 서명 정보를 검증하도록; 그리고 미리 결정된 보안 정보, 클라이언트 소프트웨어(91) 서명 정보, 및 서버(92) 서명 정보의 각각에 대한 검증이 성공하는 경우, 전자적 자격 증명서에 포함되는 서비스 유효 시간을, 검증을 위해, 획득하도록, 그리고, 전자적 자격 증명서에 포함되는 서비스 유효 시간에 대한 검증이 성공하는 경우, 전자적 자격 증명서에 대한 검증이 성공한다는 것을 결정하도록 구성된다.

[0154] 본 발명에서 제공되는 서버, 클라이언트 소프트웨어, 자격 증명서 검증단 디바이스, 이차원 바코드를 프로세싱하기 위한 시스템에 따르면, 클라이언트 소프트웨어에 의해 전송되는 전자적 자격 증명서 획득 요청을 수신한 이후, 서버는 서버 개인 키를 사용하는 것에 의해 클라이언트 소프트웨어의 유저 공개 키 및 전자적 자격 증명서에 서명하여 서버 서명 정보를 획득하고, 서버 서명 정보 및 전자적 자격 증명서를 클라이언트 소프트웨어로 전송한다. 클라이언트 소프트웨어는, 서버에 의해 전송되는 서버 서명 정보 및 전자적 자격 증명서를 수신하고, 서버 서명 정보를 검증하고, 서명 정보에 대한 검증이 성공한 이후, 전자적 자격 증명서에 서명하고, 미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 서버 서명 정보, 전자적 자격 증명서, 및 유저 공개 키에 기초하여 이차원 바코드를 생성한다. 이차원 바코드를 획득한 이후, 자격 증명서 검증단 디바이스는, 서버 서명 정보, 클라이언트 소프트웨어 서명 정보, 및 미리 결정된 보안 정보를 이차원 바코드에서 검증하여, 전자적 자

격 증명서가 송신 프로세스에서 변경되는지의 여부를 결정하여, 사용 프로세스에서 전자적 자격 증명서의 보안성을 보장할 수 있다.

[0155] 앞선 구현예에서, 각각의 구현예의 설명은 각각의 초점을 갖는다. 구현예에서 상세히 설명되지 않은 부분의 경우, 다른 구현예에서의 관련된 설명에 대해 참조가 이루어질 수 있다.

[0156] 앞선 방법 및 장치에서의 관련된 피쳐는 상호 참조될 수 있다는 것이 이해될 수 있다. 또한, 앞선 구현예에서의 "제1", "제2", 등등은, 구현예 사이의 구별을 위해 사용되며, 각각의 구현예의 이점 및 단점을 표현하는 것은 아니다.

[0157] 기술 분야의 숙련된 자는, 설명의 편의성 및 간략화를 위해, 상기에서 설명되는 시스템, 장치, 및 유닛의 특정한 작업 프로세스의 경우, 앞선 방법 구현예에서의 대응하는 프로세스에 대한 참조가 이루어질 수 있고, 본 발명의 구현예에서의 간략화를 위해 세부 사항은 생략된다는 것을 명확히 이해할 수 있다.

[0158] 본원에서 제공되는 알고리즘 및 디스플레이는 본질적으로 임의의 특정한 컴퓨터, 가상 시스템, 또는 다른 디바이스에 관련되지 않는다. 본원에 기반한 지침과 함께 다양한 범용 시스템이 또한 함께 사용될 수 있다. 상기의 설명에 기초하여, 그러한 시스템을 구축하는 데 필요한 구조는 명백하다. 더구나, 본 발명은 임의의 특정한 프로그래밍 언어에 적용되는 것은 아니다. 본원에서 설명되는 본 발명의 내용은, 다양한 프로그래밍 언어를 사용하는 것에 의해 구현될 수 있고, 상세한 언어의 앞선 설명은 본 발명의 최상의 구현예를 개시하기 위해 사용된다는 것이 이해되어야 한다.

[0159] 본 명세서에서는 많은 수의 세부 사항이 제공된다. 그러나, 본 발명의 구현예는 이들 세부 사항 없이도 실시될 수 있다는 것이 이해될 수 있다. 몇몇 경우에는, 널리 공지된 방법, 구조, 및 기술은, 본 명세서의 이해를 불명확하게 하지 않도록, 상세히 도시되지 않는다.

[0160] 마찬가지로, 본 개시를 능률화하고 다양한 발명적 양태 중 하나 이상을 이해하는 것을 돕기 위해, 본 발명의 피쳐는 때때로 본 발명의 단일의 구현예, 도면, 또는 설명으로 함께 그룹화된다는 것이 이해되어야 한다. 그러나, 개시된 방법은 다음의 의도를 반영하는 것으로 해석되지 않아야 한다: 즉, 청구된 개시는 각각의 청구항에서 명시되는 피쳐보다 더 많은 피쳐를 필요로 한다. 더 정확하게는, 아래의 청구범위에서 반영되는 바와 같이, 발명적 양태는 앞서 개시된 단일의 구현예의 모든 피쳐보다 더 적다. 따라서, 상세한 구현예를 따르는 청구항은 상세한 구현예를 명확하게 통합한다. 각각의 청구항은 본 발명의 별개의 구현예로서 역할을 한다.

[0161] 기술 분야의 숙련된 자는, 구현예에서의 디바이스 내의 모듈이, 구현예와는 상이한 하나 이상의 디바이스에서 적응적으로 변경 및 배치될 수 있다는 것을 이해할 수 있다. 구현에서의 모듈 또는 유닛 또는 컴포넌트는, 하나의 모듈 또는 유닛 또는 컴포넌트로 결합될 수 있고, 복수의 서브 모듈 또는 서브유닛 또는 서브컴포넌트로 추가적으로 분할될 수 있다. 이들 피쳐 및/또는 프로세스 또는 유닛의 적어도 일부가 상호 배타적이다는 사실을 제외하면, 명세서(첨부된 청구범위, 요약서, 및 첨부의 도면을 포함함)에서 그러한 방법으로 개시되는 임의의 방법 및 디바이스의 모든 개시된 피쳐 및 모든 프로세스 또는 유닛은 임의의 조합 모드에서 결합될 수 있다. 달리 명시적으로 언급되지 않는 한, 명세서(첨부된 청구범위, 요약서, 및 첨부의 도면을 포함함)에서 개시되는 각각의 피쳐는, 동일한, 등가적인, 또는 유사한 목적에 맞는 대안적 피쳐에 의해 대체될 수 있다.

[0162] 또한, 기술 분야의 숙련된 자는, 본원에서 설명되는 몇몇 구현예가, 다른 피쳐를 포함하는 대신, 다른 구현예에 포함되는 몇몇 피쳐를 포함하지만, 상이한 구현예의 피쳐의 조합이 본 발명의 범위 내에 속하고 상이한 구현예를 형성하는 것을 의미한다는 것을 이해할 수 있다. 예를 들면, 다음의 청구항에서, 고려된 구현예 중 임의의 하나는 임의의 조합 모드에서 사용될 수 있다.

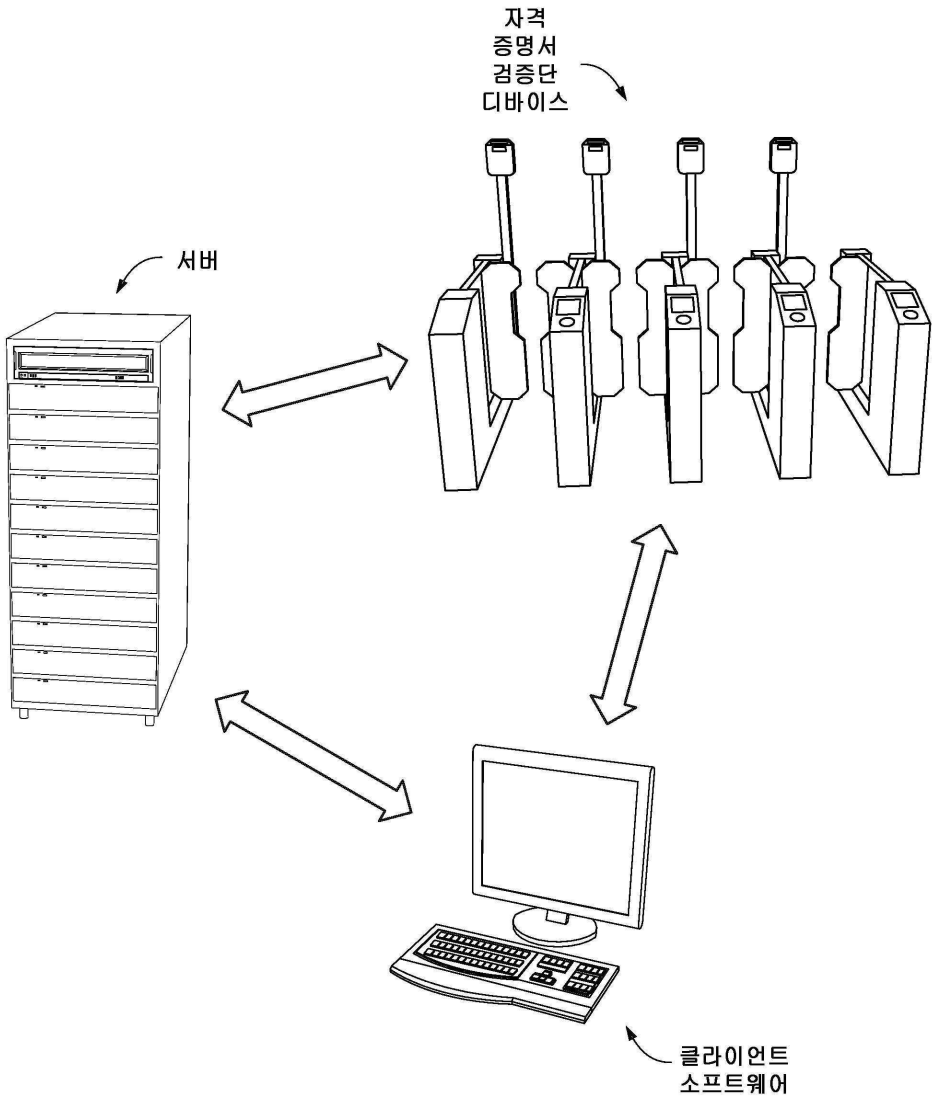
[0163] 본 발명에서의 다양한 부분의 구현예는, 하드웨어, 또는 하나 이상의 프로세서 상에서 실행되는 소프트웨어 모듈, 또는 이들의 조합에 의해 구현될 수 있다. 기술 분야의 숙련된 자는, 본 발명의 구현예에 기초하여 개시 명칭(예를 들면, 이차원 바코드를 프로세싱하기 위한 장치)의 컴포넌트 중 몇몇 또는 전체의 기능 중 몇몇 또는 전체를 구현하기 위해, 마이크로프로세서 또는 디지털 신호 프로세서(digital signal processor; DSP)가 실제 사용될 수 있다는 것을 이해할 수 있다. 본 발명은 또한, 본원에서 설명되는 방법 중 일부 또는 전체를 실행하기 위한 디바이스 또는 장치 프로그램(예를 들면, 컴퓨터 프로그램 및 컴퓨터 프로그램 제품)으로서 구현될 수 있다. 본 발명을 구현하기 위한 그러한 프로그램은, 컴퓨터 판독 가능 매체에 저장될 수 있거나, 또는 하나 이상의 신호의 형태를 가질 수 있다. 그러한 신호는, 인터넷 웹사이트로부터 다운로드 가능하거나, 캐리어 신호 상에서 제공될 수 있거나, 또는 임의의 다른 형태로 제공될 수 있다.

[0164] 앞선 구현예는, 본 발명을 제한하는 대신, 본 발명을 설명하도록 의도되며, 기술 분야의 숙련된 자는, 첨부된

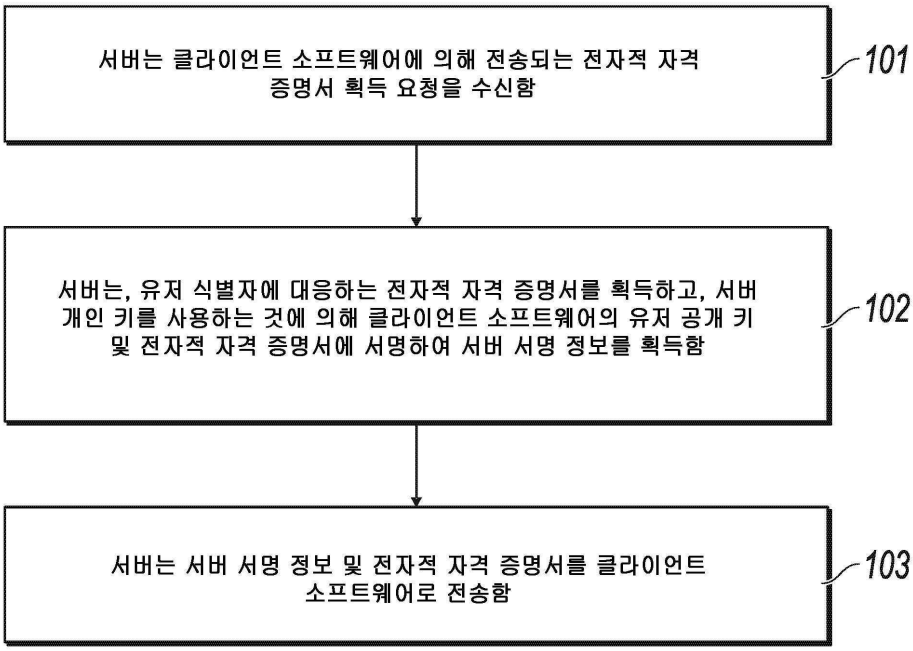
청구범위의 범위를 벗어나지 않으면서 대안적인 구현예를 설계할 수 있다는 것을 주목할 가치가 있다. 청구범위에서, 괄호 사이에 위치되는 임의의 참조 부호는 클레임에 대한 제한으로 구성되지 않아야 한다. 단어 "포함한다(include)"는, 청구범위에서 열거되지 않는 엘리먼트 또는 단계의 존재를 배제하지 않는다. 엘리먼트 앞의 단어 "하나" 또는 "한/한(a/an)"은, 복수의 그러한 엘리먼트의 존재를 배제하지 않는다. 본 발명은, 여러 가지 상이한 엘리먼트를 포함하는 하드웨어 및 적절하게 프로그래밍되는 컴퓨터에 의해 구현될 수 있다. 여러 가지 장치를 열거하는 단위 청구항에서, 이들 장치 중 몇몇은 동일한 하드웨어 항목을 사용하는 것에 의해 구체화될 수 있다. 단어 "제1", "제2", 및 "제3"의 사용은, 어떠한 순서도 나타내지 않는다. 이들 단어는 이름으로서 해석될 수 있다.

도면

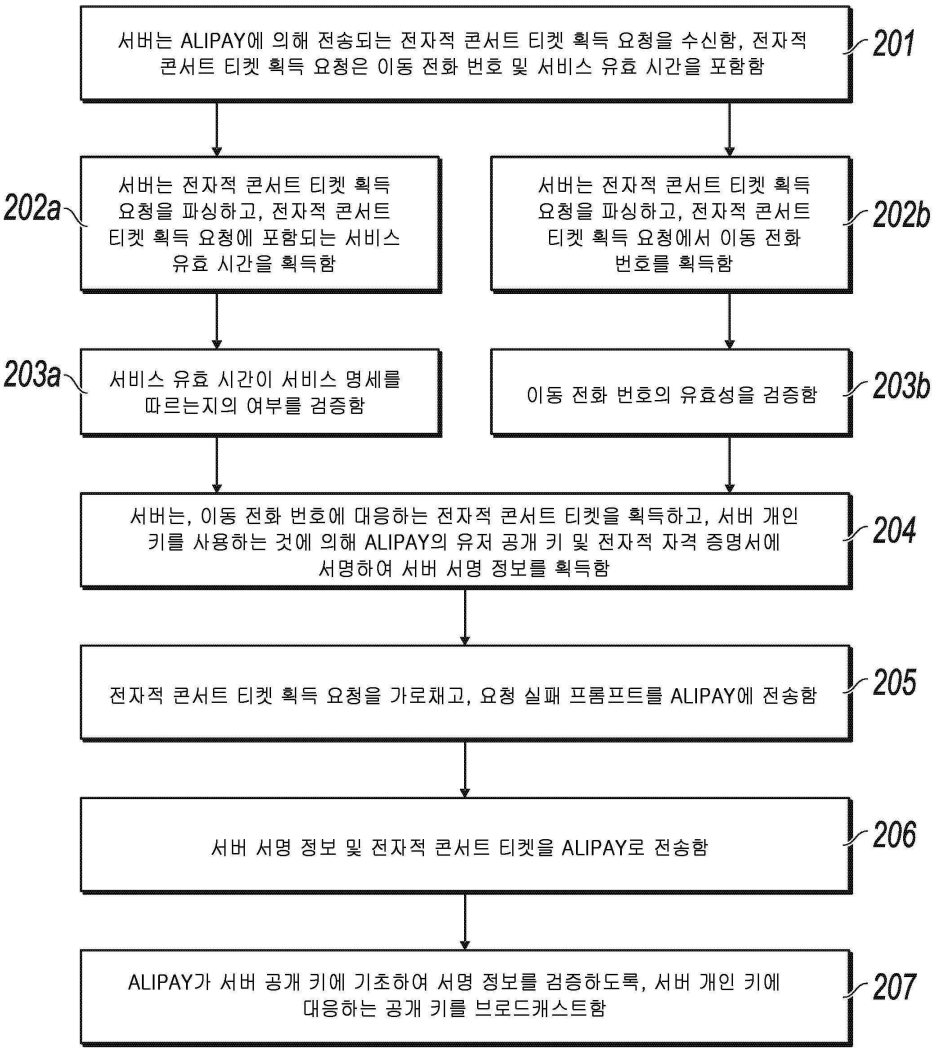
도면1



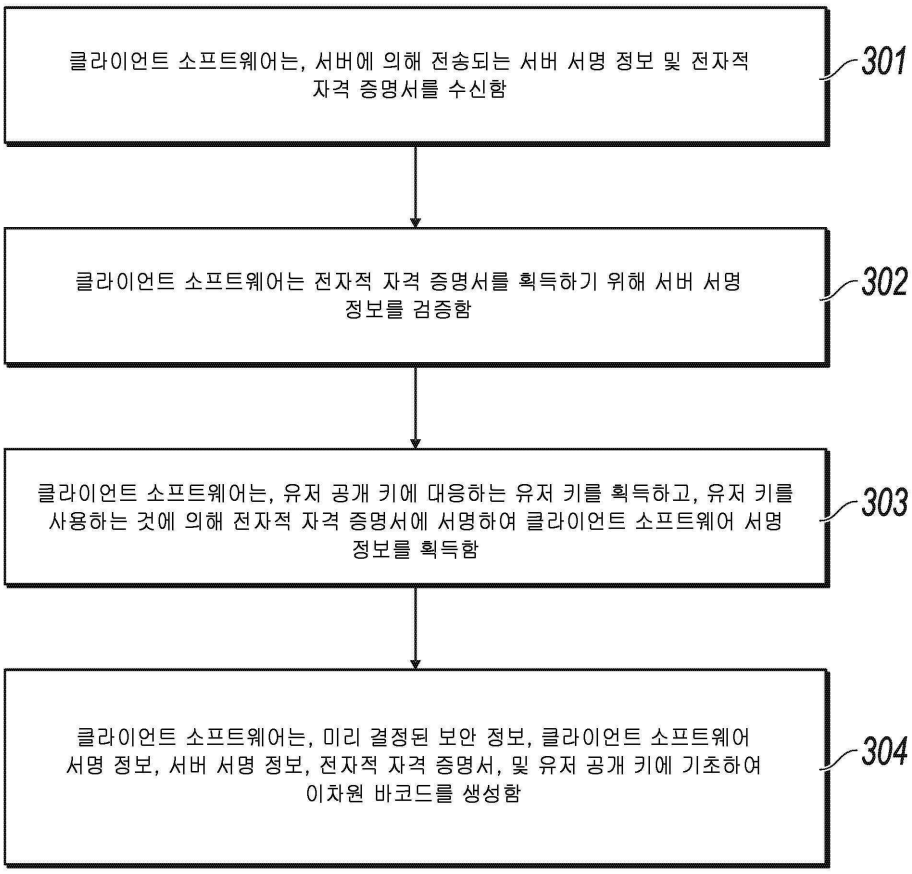
도면2


서버는 클라이언트 소프트웨어에 의해 전송되는 전자적 자격 증명서 획득 요청을 수신함
101
서버는, 유저 식별자에 대응하는 전자적 자격 증명서를 획득하고, 서버 개인 키를 사용하는 것에 의해 클라이언트 소프트웨어의 유저 공개 키 및 전자적 자격 증명서에 서명하여 서버 서명 정보를 획득함
102
서버는 서버 서명 정보 및 전자적 자격 증명서를 클라이언트 소프트웨어로 전송함
103

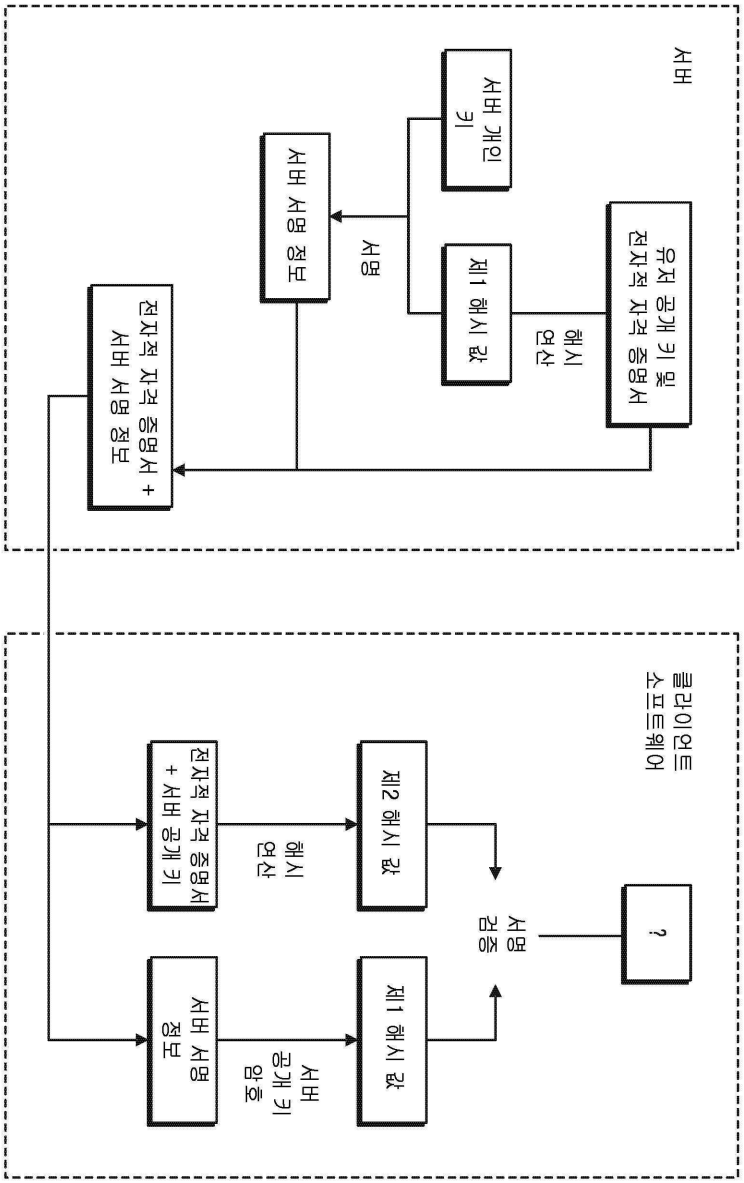
도면3


서버는 ALIPAY에 의해 전송되는 전자적 콘서트 티켓 획득 요청을 수신함, 전자적 콘서트 티켓 획득 요청은 이동 전화 번호 및 서비스 유효 시간을 포함함
201
서버는 전자적 콘서트 티켓 획득 요청을 파싱하고, 전자적 콘서트 티켓 획득 요청에 포함되는 서비스 유효 시간을 획득함
202a
서버는 전자적 콘서트 티켓 획득 요청을 파싱하고, 전자적 콘서트 티켓 획득 요청에서 이동 전화 번호를 획득함
202b
서비스 유효 시간이 서비스 명세를 따르는지의 여부를 검증함
203a
이동 전화 번호의 유효성을 검증함
203b
서버는, 이동 전화 번호에 대응하는 전자적 콘서트 티켓을 획득하고, 서버 개인 키를 사용하는 것에 의해 ALIPAY의 유저 공개 키 및 전자적 자격 증명서에 서명하여 서버 서명 정보를 획득함
204
전자적 콘서트 티켓 획득 요청을 가로채고, 요청 실패 프롬프트를 ALIPAY에 전송함
205
서버 서명 정보 및 전자적 콘서트 티켓을 ALIPAY로 전송함
206
ALIPAY가 서버 공개 키에 기초하여 서명 정보를 검증하도록, 서버 개인 키에 대응하는 공개 키를 브로드캐스트함
207

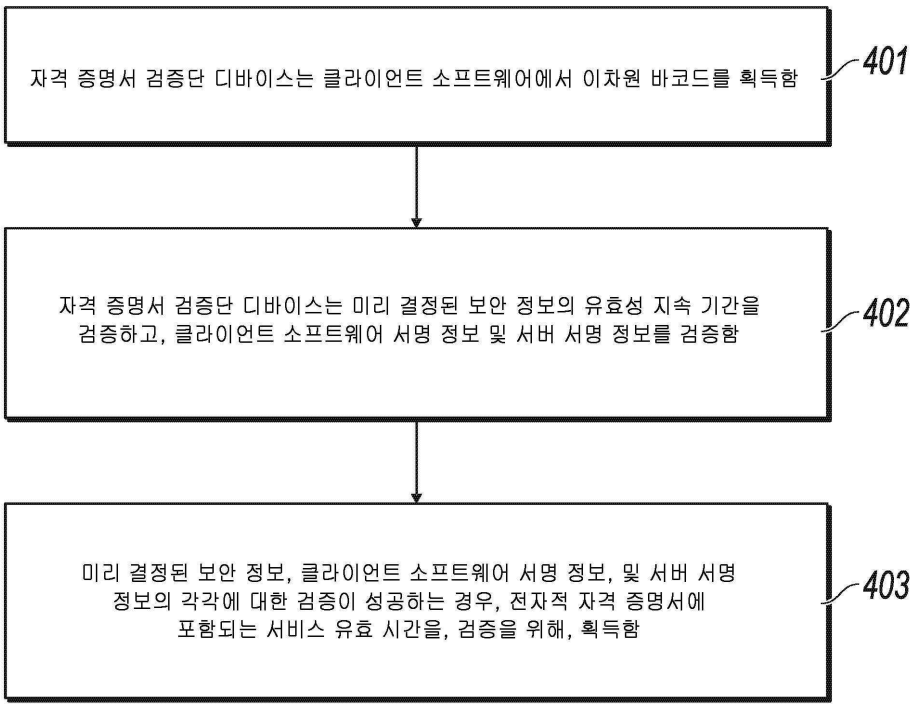
도면4


클라이언트 소프트웨어는, 서버에 의해 전송되는 서버 서명 정보 및 전자적 자격 증명서를 수신함
301
클라이언트 소프트웨어는 전자적 자격 증명서를 획득하기 위해 서버 서명 정보를 검증함
302
클라이언트 소프트웨어는, 유저 공개 키에 대응하는 유저 키를 획득하고, 유저 키를 사용하는 것에 의해 전자적 자격 증명서에 서명하여 클라이언트 소프트웨어 서명 정보를 획득함
303
클라이언트 소프트웨어는, 미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 서버 서명 정보, 전자적 자격 증명서, 및 유저 공개 키에 기초하여 이차원 바코드를 생성함
304

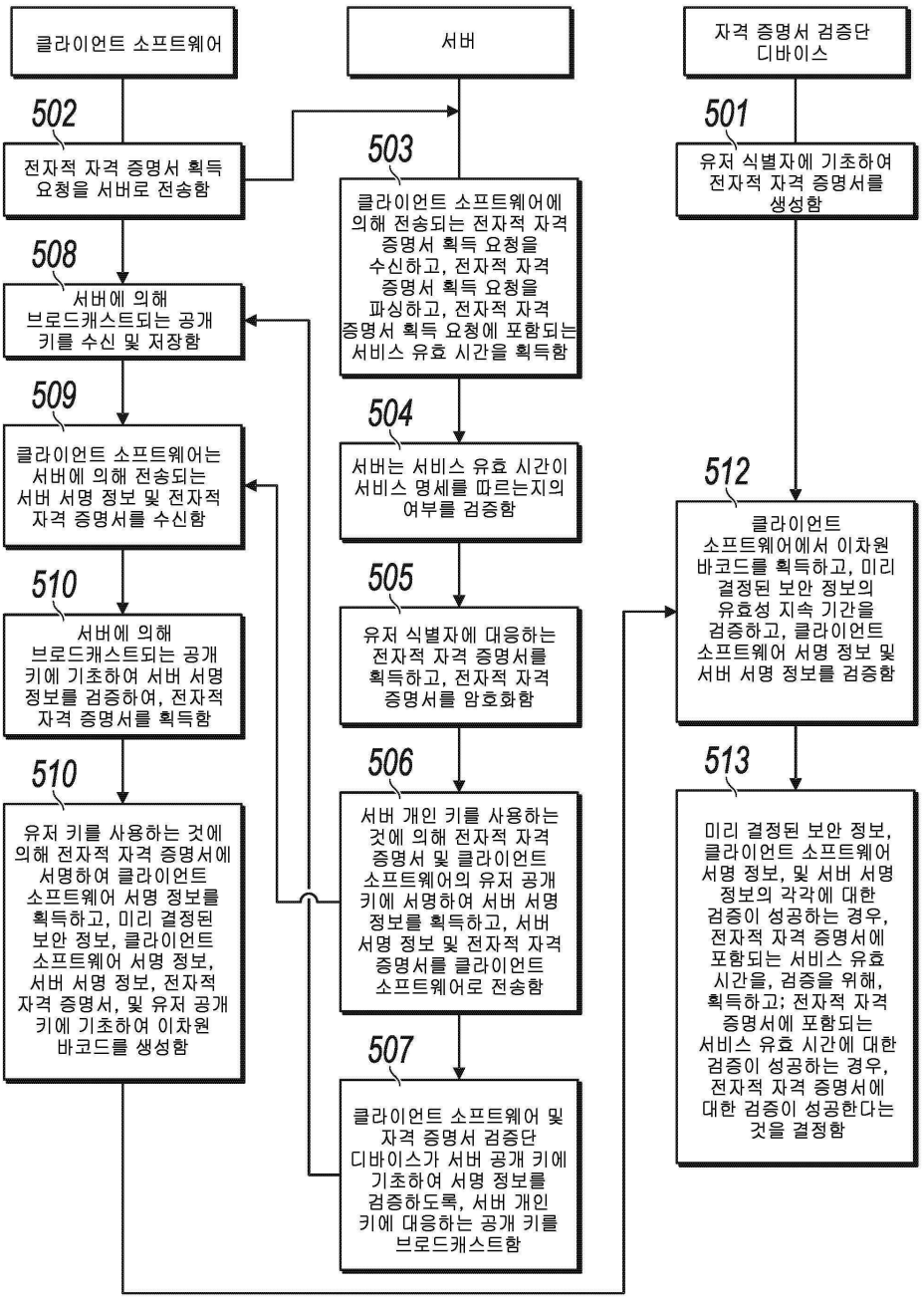
도면5


서버
서버 개인 키
서버 서명 정보
서명
제1 해시 값
해시 연산
유저 공개 키 및 전자적 자격 증명서
전자적 자격 증명서 + 서버 서명 정보
클라이언트 소프트웨어
전자적 자격 증명서 + 서버 공개 키
해시 연산
제2 해시 값
서명 검증
?
서버 서명 정보
서버 공개 키 암호
제1 해시 값

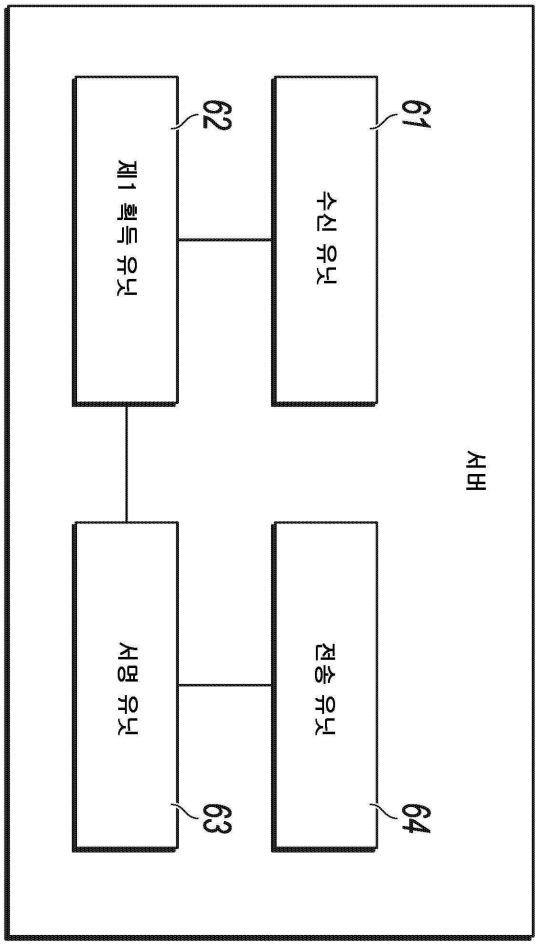
도면6


자격 증명서 검증단 디바이스는 클라이언트 소프트웨어에서 이차원 바코드를 획득함
401
자격 증명서 검증단 디바이스는 미리 결정된 보안 정보의 유효성 지속 기간을 검증하고, 클라이언트 소프트웨어 서명 정보 및 서버 서명 정보를 검증함
402
미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 및 서버 서명 정보의 각각에 대한 검증이 성공하는 경우, 전자적 자격 증명서에 포함되는 서비스 유효 시간을, 검증을 위해, 획득함
403

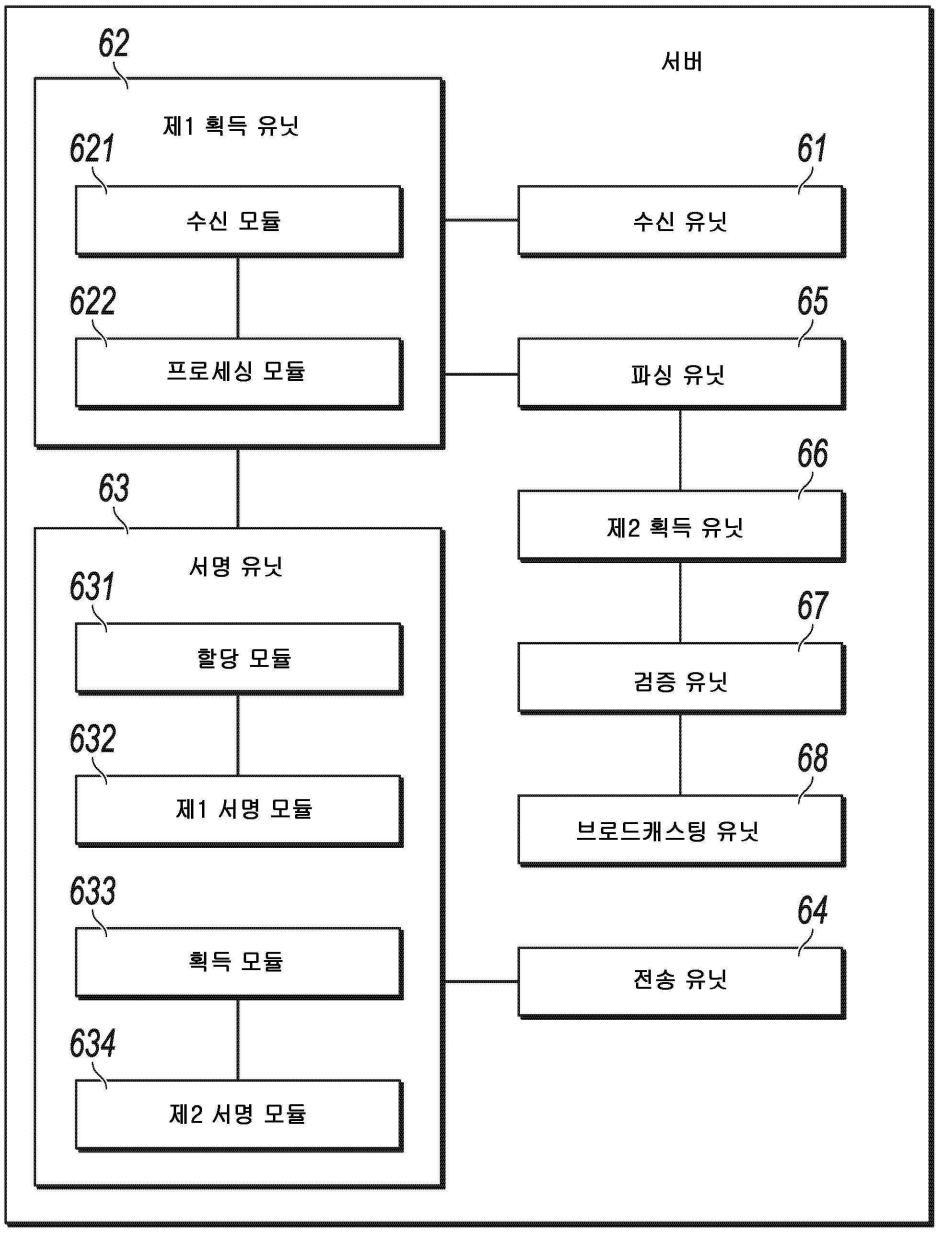
도면7


클라이언트 소프트웨어
서버
자격 증명서 검증단 디바이스
502
전자적 자격 증명서 획득 요청을 서버로 전송함
503
클라이언트 소프트웨어에 의해 전송되는 전자적 자격 증명서 획득 요청을 수신하고, 전자적 자격 증명서 획득 요청을 파싱하고, 전자적 자격 증명서 획득 요청에 포함되는 서비스 유효 시간을 획득함
501
유저 식별자에 기초하여 전자적 자격 증명서를 생성함
508
서버에 의해 브로드캐스트되는 공개 키를 수신 및 저장함
509
클라이언트 소프트웨어는 서버에 의해 전송되는 서버 서명 정보 및 전자적 자격 증명서를 수신함
504
서버는 서비스 유효 시간이 서비스 명세를 따르는지의 여부를 검증함
512
클라이언트 소프트웨어에서 이차원 바코드를 획득하고, 미리 결정된 보안 정보의 유효성 지속 기간을 검증하고, 클라이언트 소프트웨어 서명 정보 및 서버 서명 정보를 검증함
505
유저 식별자에 대응하는 전자적 자격 증명서를 획득하고, 전자적 자격 증명서를 암호화함
510
서버에 의해 브로드캐스트되는 공개 키에 기초하여 서버 서명 정보를 검증하여, 전자적 자격 증명서를 획득함
506
서버 개인 키를 사용하는 것에 의해 전자적 자격 증명서 및 클라이언트 소프트웨어의 유저 공개 키에 서명하여 서버 서명 정보를 획득하고, 서버 서명 정보 및 전자적 자격 증명서를 클라이언트 소프트웨어로 전송함
513
미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 및 서버 서명 정보의 각각에 대한 검증이 성공하는 경우, 전자적 자격 증명서에 포함되는 서비스 유효 시간을, 검증을 위해, 획득하고; 전자적 자격 증명서에 포함되는 서비스 유효 시간에 대한 검증이 성공하는 경우, 전자적 자격 증명서에 대한 검증이 성공한다는 것을 결정함
510
유저 키를 사용하는 것에 의해 전자적 자격 증명서에 서명하여 클라이언트 소프트웨어 서명 정보를 획득하고, 미리 결정된 보안 정보, 클라이언트 소프트웨어 서명 정보, 서버 서명 정보, 전자적 자격 증명서, 및 유저 공개 키에 기초하여 이차원 바코드를 생성함
507
클라이언트 소프트웨어 및 자격 증명서 검증단 디바이스가 서버 공개 키에 기초하여 서명 정보를 검증하도록, 서버 개인 키에 대응하는 공개 키를 브로드캐스트함

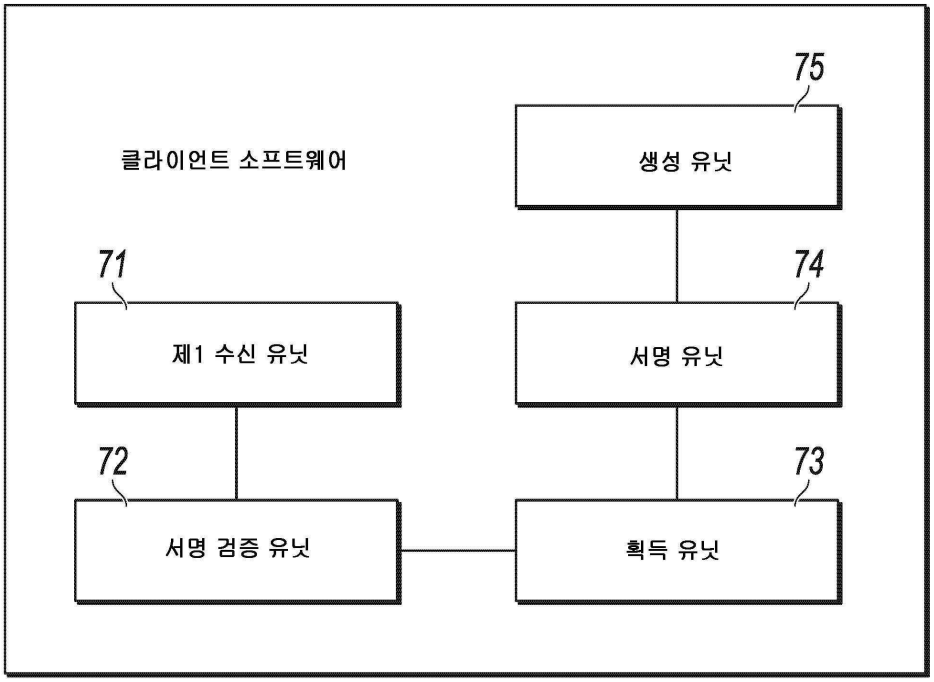
도면8



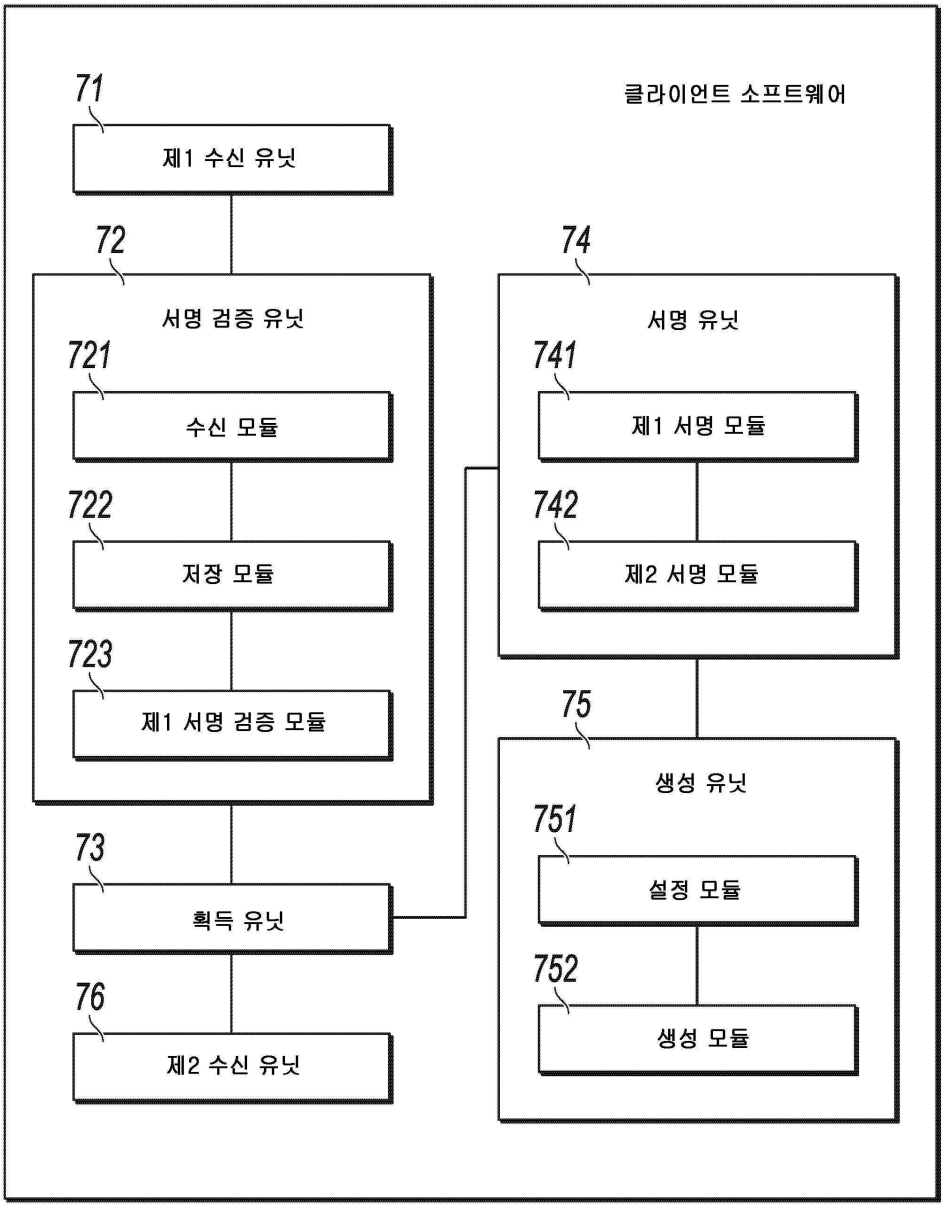
도면9


서버
62
제1 획득 유닛
621
수신 모듈
622
프로세싱 모듈
63
서명 유닛
631
할당 모듈
632
제1 서명 모듈
633
획득 모듈
634
제2 서명 모듈
61
수신 유닛
65
파싱 유닛
66
제2 획득 유닛
67
검증 유닛
68
브로드캐스팅 유닛
64
전송 유닛

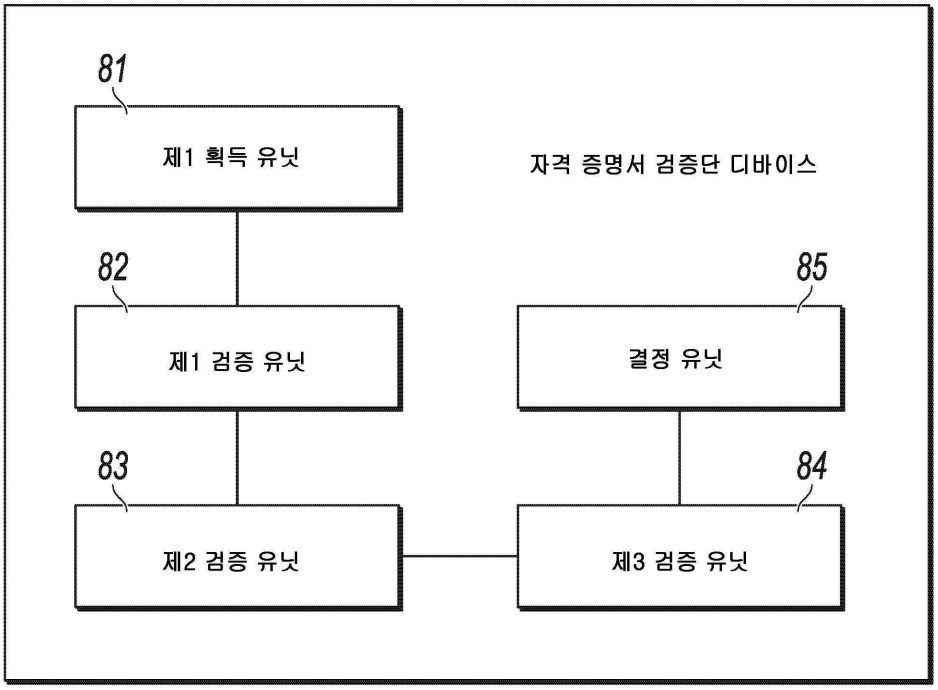
도면10



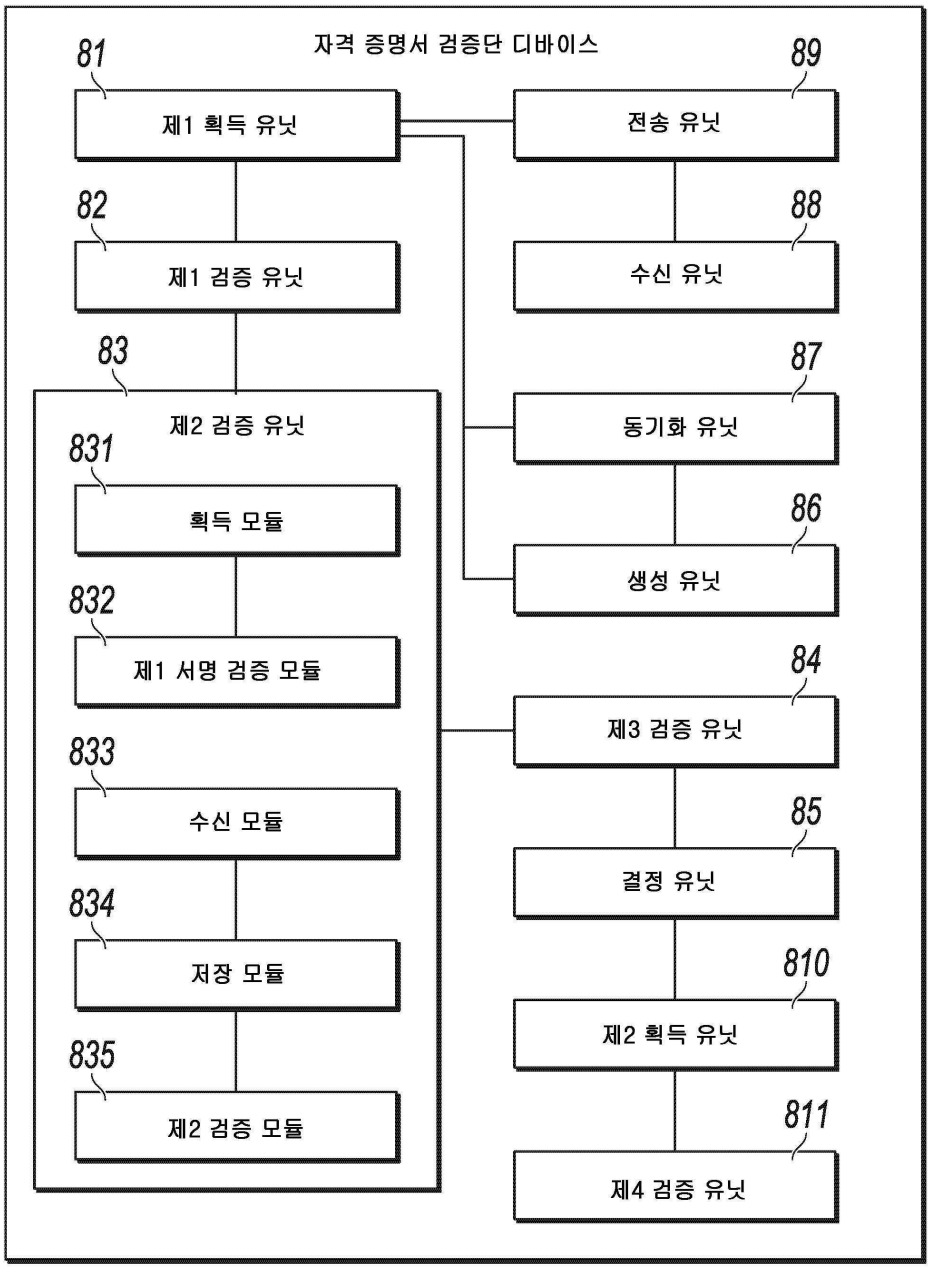
도면11


클라이언트 소프트웨어
71
제1 수신 유닛
72
서명 검증 유닛
721
수신 모듈
722
저장 모듈
723
제1 서명 검증 모듈
73
획득 유닛
76
제2 수신 유닛
74
서명 유닛
741
제1 서명 모듈
742
제2 서명 모듈
75
생성 유닛
751
설정 모듈
752
생성 모듈

도면12


81
제1 획득 유닛
자격 증명서 검증단 디바이스
82
85
제1 검증 유닛
결정 유닛
83
84
제2 검증 유닛
제3 검증 유닛

도면13


자격 증명서 검증단 디바이스
81
제1 획득 유닛
89
전송 유닛
82
제1 검증 유닛
88
수신 유닛
83
제2 검증 유닛
87
동기화 유닛
831
획득 모듈
86
생성 유닛
832
제1 서명 검증 모듈
84
제3 검증 유닛
833
수신 모듈
85
결정 유닛
834
저장 모듈
810
제2 획득 유닛
835
제2 검증 모듈
811
제4 검증 유닛

도면14