(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0137093
(43) 공개일자 2012년12월20일

(51) 국제특허분류(Int. Cl.)
H04L 9/16 (2006.01) *H04L 9/32* (2006.01)
G06Q 20/42 (2012.01)
(21) 출원번호 10-2011-0056416
(22) 출원일자 2011년06월10일
심사청구일자 2011년06월10일

(71) 출원인
고려대학교 산학협력단
서울 성북구 안암동5가 1
(72) 발명자
이동훈
서울특별시 종로구 사직로8길 34, 경희궁의아침3단지 아파트 1404호 (내수동)
최민근
서울특별시 관악구 미성동 대우 푸르지오 아파트 107동 602호
(뒷면에 계속)
(74) 대리인
특허법인충현

전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **2차원바코드를 이용한 패스워드의 비밀키 생성 시스템 및 방법**

(57) 요 약

본 발명은 2차원바코드를 이용한 패스워드의 비밀키 생성 시스템 및 방법에 관한 것으로, 보다 구체적으로는 상기 사용자단말이 사용자로부터 공인인증서에 대한 패스워드 및 2차원바코드를 입력받아, 상기 패스워드와 2차원바코드로부터 획득한 난수열을 상호 조합하여 상기 패스워드에 대한 비밀키를 생성하는 것을 특징으로 한다.

이러한 구성에 의해, 본 발명의 2차원바코드를 이용한 패스워드의 비밀키 생성 시스템 및 방법은 사용자단말을 이용한 금융거래 시, 사용자 확인을 위해 사용되는 공인인증서의 패스워드를 사용자가 발급받은 고유의 2차원바코드와 상호 조합하여 상기 패스워드에 대한 비밀키를 생성함으로써, 공인인증서의 패스워드에 대한 복잡도를 향상시킬 수 있는 효과가 있다.

대 표 도 - 도1

(72) 발명자

김명환

전라남도 광양시 광양읍 인덕2길 24, 201호

양유현

서울특별시 성북구 보문로18길 41, 505호 (안암동3가)

조성아

인천광역시 남동구 논현로 235, 웰카운티 1008동 403호 (논현동)

장유철

서울특별시 동작구 신대방1가길 4, 401호 (신대방동, 둥지빌)

변정호

서울특별시 성북구 안암로9가길 40, 202호 (안암동5가)

백정하

서울특별시 송파구 송파대로32길 15, 105동 802호 (가락동, 가락금호아파트)

이 발명을 지원한 국가연구개발사업

과제고유번호	ITAC1090100100030001000100100
부처명	정보통신산업진흥원
연구사업명	대학IT연구센터육성지원사업
연구과제명	스마트 그리드 보안 연구센터(스마트 그리드 보안기술 개발)
주관기관	고려대학교 산학협력단
연구기간	2010.06.01 ~ 2010.12.31

특허청구의 범위

청구항 1

사용자단말과 금융서버간 금융거래 시, 사용자확인을 위해 사용되는 2차원바코드를 이용한 패스워드의 비밀키 생성 시스템에 있어서,

상기 사용자단말은

사용자로부터 공인인증서에 대한 패스워드 및 2차원바코드를 입력받아, 상기 패스워드와 2차원바코드로부터 획득한 난수열을 상호 조합하여 상기 패스워드에 대한 비밀키를 생성하는 것을 특징으로 하는 2차원바코드를 이용한 패스워드의 비밀키 생성 시스템.

청구항 2

제1항에 있어서,

상기 사용자단말은

공인인증서 발급, 사용 및 상기 패스워드 또는 2차원바코드의 변경 중 적어도 하나를 요청받은 경우에 상기 사용자로부터 패스워드 및 2차원바코드를 입력받는 것을 특징으로 하는 2차원바코드를 이용한 패스워드의 비밀키 생성 시스템.

청구항 3

제1항에 있어서,

상기 사용자단말은

상기 비밀키로부터 키추출함수에 기초하여 암호화된 추출키를 생성하는 것을 특징으로 하는 2차원바코드를 이용한 패스워드의 비밀키 생성 시스템.

청구항 4

제1항에 있어서,

상기 사용자단말은

내부에 포함된 카메라을 통해 2차원바코드를 촬영하여 입력받는 것을 특징으로 하는 2차원바코드를 이용한 패스워드의 비밀키 생성 시스템.

청구항 5

사용자단말과 금융서버간 금융거래 시, 사용자확인을 위해 사용되는 2차원바코드를 이용한 패스워드의 비밀키 생성 방법에 있어서,

상기 사용자단말이 사용자로부터 상기 공인인증서에 대한 패스워드 및 2차원바코드를 입력받는 입력단계;

상기 사용자단말이 상기 2차원바코드로부터 난수열을 획득하는 수열획득단계; 및

상기 사용자단말이 상기 패스워드 및 상기 난수열을 조합하여 상기 패스워드에 대한 비밀키를 생성하는 비밀키 생성단계;

를 포함하는 것을 특징으로 하는 2차원바코드를 이용한 패스워드의 비밀키 생성 방법.

청구항 6

제5항에 있어서,

상기 입력단계는

상기 사용자단말이 공인인증서의 발급, 사용 및 패스워드 또는 2차원바코드의 변경 중 적어도 하나를 요청받은 경우에, 상기 패스워드 및 2차원바코드를 입력받는 것을 특징으로 하는 2차원바코드를 이용한 패스워드의 비밀키 생성 방법.

청구항 7

제5항에 있어서,

상기 비밀키로부터 키추출함수에 기초하여 암호화된 추출키를 생성하는 암호화키추출단계;

를 더 포함하는 것을 특징으로 하는 2차원바코드를 이용한 패스워드의 비밀키 생성 방법.

청구항 8

제7항에 있어서,

상기 암호화키추출단계는

상기 암호화키가 상기 비밀키의 상위 16 Bytes인 것을 특징으로 하는 2차원바코드를 이용한 패스워드의 비밀키 생성 방법.

청구항 9

제6항에 있어서,

상기 사용자단말이 패스워드 또는 2차원바코드의 변경을 요청받은 경우에서, 상기 비밀키에 대한 복호화를 수행하는 비밀키보호단계:

를 더 포함하는 것을 특징으로 하는 2차원바코드를 이용한 패스워드의 비밀키 생성 방법.

청구항 10

제5항 내지 제9항 중 어느 한 항에 따른 방법을 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독가능 기록매체.

명 세 서

기 술 분 야

[0001] 본 발명은 2차원바코드를 이용한 패스워드의 비밀키 생성 시스템 및 방법에 관한 것으로, 특히 공인인증서의 패스워드에 대한 보안성을 향상시키는 2차원바코드를 이용한 패스워드의 비밀키 생성 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] IT기술의 발전에 따라, 최근 들어 이동단말을 통한 금융거래가 대중에게 일반화되고 있다. 이러한 추세는 이동단말 사용자가 이동하는 중에도 이동단말을 사용하여 시간 또는 장소에 구애받지 않고, 금융거래를 이용할 수 있다는 장점으로 인해, 많은 사람들이 널리 이용하고 있다. 하지만 이와 같이, 이동단말을 이용한 금융거래는 사용자가 자신의 이동단말을 분실하는 경우, 사용자의 재산적 손실뿐만 아니라, 개인정보까지도 노출될 수 있어, 각종 범죄에 악용될 우려가 있다는 문제점이 발생했다.

[0003] 이러한 문제점을 해결하기 위해, 사용자는 각 개인별 공인인증서를 통해 금융거래를 수행하고 있으며, 상기 공인인증서에 대한 사용자 확인을 위해, OTP(One Time Password), HSM(Hardware Security Module)와 같은 부가적인 개인키 보호수단이 도입되고 있으나, 현실적으로 주로 사용자들은 패스워드만을 이용하여 공인인증서에 대한 사용자 확인을 수행하고 있다.

[0004] 하지만 이와 같이, 사용자의 확인을 위해 사용되는 공인인증서의 패스워드는 주로 동일한 사용자의 각종 이메일 패스워드 등과 같은 다른 사용자 확인을 사용되는 패스워드와 동일하거나, 유사하기 때문에 상기 사용자의 지인과 같은 가까운 사람이 상기 사용자의 개인 정보 등의 간단한 조합을 통해 용이하게 알 수 있어, 각종 범죄에 악용될 가능성이 높다는 문제점이 발생했다.

발명의 내용

해결하려는 과제

[0005] 상기와 같은 종래 기술의 문제점을 해결하기 위해, 본 발명은 전자상거래 또는 금융거래 시, 사용되는 공인인증서의 패스워드에 대하여, 상기 패스워드를 2차원바코드와 상호 조합하여 비밀키를 생성함으로써, 공인인증서의 패스워드를 보다 안전하게 사용할 수 있는 2차원바코드를 이용한 패스워드의 비밀키 생성 시스템 및 방법을 제공하고자 한다.

과제의 해결 수단

[0006] 위와 같은 과제를 해결하기 위한 본 발명의 한 실시 예에 따른 사용자단말과 금융서버간 금융거래 시, 사용자확인을 위해 사용되는 패스워드를 재생성하는 2차원바코드를 이용한 패스워드의 비밀키 생성 시스템은 사용자로부터 공인인증서에 대한 패스워드 및 2차원바코드를 입력받아, 상기 패스워드와 2차원바코드로부터 획득한 난수열을 상호 조합하여 상기 패스워드에 대한 비밀키를 생성하는 사용자단말을 포함할 수 있다.

[0007] 보다 바람직하게는 공인인증서 발급, 사용 및 상기 패스워드 또는 2차원바코드의 변경 중 적어도 하나를 요청받은 경우에 상기 사용자로부터 패스워드 및 2차원바코드를 입력받는 사용자단말을 포함할 수 있다.

[0008] 특히, 상기 비밀키로부터 키추출함수에 기초하여 암호화된 추출키를 생성하는 사용자단말을 포함할 수 있다.

[0009] 특히, 내부에 포함된 카메라을 통해 2차원바코드를 촬영하여 입력받는 사용자단말을 포함할 수 있다.

[0010] 위와 같은 과제를 해결하기 위한 본 발명의 다른 실시 예에 따른 사용자단말과 금융서버간 금융거래 시, 사용자확인을 위해 사용되는 패스워드를 재생성하는 2차원바코드를 이용한 패스워드의 비밀키 생성 방법은 사용자단말이 사용자로부터 상기 공인인증서에 대한 패스워드 및 2차원바코드를 입력받는 입력단계; 상기 사용자단말이 상기 2차원바코드로부터 난수열을 획득하는 수열획득단계; 및 상기 사용자단말이 상기 패스워드 및 상기 난수열을 조합하여 상기 패스워드에 대한 비밀키를 생성하는 비밀키생성단계;를 포함할 수 있다.

[0011] 보다 바람직하게는 상기 사용자단말이 공인인증서의 발급, 사용 및 패스워드 또는 2차원바코드의 변경 중 적어도 하나를 요청받은 경우에, 상기 패스워드 및 2차원바코드를 입력받는 입력단계를 포함할 수 있다.

[0012] 보다 바람직하게는 상기 비밀키로부터 키추출함수에 기초하여 암호화된 추출키를 생성하는 암호화키추출단계;를 더 포함할 수 있다.

[0013] 특히, 상기 암호화키는 상기 비밀키의 상위 16 Bytes인 암호화키추출단계를 포함할 수 있다.

[0014] 보다 바람직하게는 상기 사용자단말이 패스워드 또는 2차원바코드의 변경을 요청받은 경우에서, 상기 비밀키에

대한 복호화를 수행하는 비밀키보호단계:를 더 포함할 수 있다.

발명의 효과

[0015] 본 발명의 2차원바코드를 이용한 패스워드의 비밀키 생성 시스템 및 방법은 사용자단말을 이용한 금융거래 시, 사용자 확인을 위해 사용되는 공인인증서의 패스워드를 사용자가 발급받은 고유의 2차원바코드와 상호 조합하여 상기 패스워드에 대한 비밀키를 생성함으로써, 공인인증서의 패스워드에 대한 복잡도를 향상시킬 수 있는 효과가 있다.

[0016] 또한, 본 발명의 2차원바코드를 이용한 패스워드의 비밀키 생성 시스템 및 방법은 사용자단말이 촬영하여 획득한 난수열을 통해 영대소문자와 숫자만으로 이루어지는 공인인증서의 패스워드에 대한 복잡도를 향상시킴에 따라, 사용자단말을 이용한 금융거래를 보다 안전하게 수행할 수 있도록 하는 효과가 있다.

[0017] 더불어, 본 발명의 2차원바코드를 이용한 패스워드의 비밀키 생성 시스템 및 방법은 사용자단말의 분실 시 공인인증서의 쉬운 패스워드로 인해 상기 사용자단말을 이용한 각종 금융범죄 및 개인정보 누출에 따른 피해발생을 방지할 수 있는 효과가 있다.

[0018] 이와 더불어, 본 발명의 2차원바코드를 이용한 패스워드의 비밀키 생성 시스템 및 방법은 사용자단말 내 보편적으로 구비되는 카메라를 이용하여 2차원바코드를 입력받음에 따라 추가되는 장치의 구성이 필요하지 않아 사용자가 용이하게 사용할 수 있는 효과가 있다.

도면의 간단한 설명

[0019] 도 1은 본 발명의 일 실시 예에 따른 2차원바코드를 이용한 패스워드의 비밀키 생성 시스템의 개략도이다.

도 2는 본 발명의 다른 실시 예에 따른 2차원바코드를 이용한 패스워드의 비밀키 생성 방법의 순서도이다.

도 3은 본 발명에 따른 패스워드에 대한 비밀키 생성과정의 예를 나타낸 도면이다.

도 4는 신규 공인인증서 발급요청에 따른 공인인증서의 패스워드에 대한 비밀키를 생성하는 과정에 대한 순서도이다.

도 5는 공인인증서 사용요청에 따른 공인인증서의 패스워드에 대한 비밀키를 생성하는 과정에 대한 순서도이다.

도 6은 공인인증서의 패스워드 또는 2차원바코드 변경요청에 따른 패스워드의 비밀키를 생성하는 과정에 대한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0020] 이하, 본 발명을 바람직한 실시 예와 첨부한 도면을 참고로 하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 여기에서 설명하는 실시 예에 한정되는 것은 아니다.

[0021] 본 발명은 전자상거래 또는 금융거래 시 사용되는 공인인증서에 대한 패스워드의 복잡도를 향상시키는 사용자단말에 관한 것으로, 사용자단말을 이용하여 금융서버와의 금융거래 시, 본인 인증을 위해 사용되는 공인인증서의 패스워드를 외부인이 알 수 없도록 상기 공인인증서의 패스워드에 대하여 복잡도를 향상시킨 비밀키를 생성하는 것이다.

[0022] 먼저, 본 발명에서 사용되는 공인인증서에 대하여 살펴보도록 한다. 공인인증서란, 전자상거래 또는 금융거래 시, 사용자의 신원을 확인하고, 문서의 위조 및 변조 또는 거래 사실의 부인을 방지하는 등의 목적으로 공인인증기관이 발생하는 전자적 정보로서, 일종의 사이버 거래용 인감증명서를 말한다. 이러한 공인인증서는 사용자의 본인 확인을 위해, 영대소문자와 숫자로 이루어지는 패스워드를 갖는다.

[0023] 이러한 사용자단말은 공인인증서의 패스워드에 대한 비밀키를 생성하기에 앞서, 먼저 금융서버 또는 개별적인 2차원바코드생성기를 이용하여 각 사용자마다 서로 다른 고유한 2차원바코드를 발급받는다.

[0024] 이러한 상기 2차원바코드는 2차원 형태 즉, X, Y 방향에 데이터를 배열시켜 평면화시킨 것으로, 그 예로는 QR코

드, 맥시코드(maxi-code), 슈퍼코드(super code), 인터코드(inter code), 아즈텍코드(aztec code), 세마코드(sema code) 등이 있으며, 본 발명에서는 상기 QR코드를 상기 2차원바코드의 예로 들어 설명하도록 한다. 상기 QR코드라 함은 Quick Response code의 약자로서, 종래에 사용되는 바코드보다 훨씬 많은 양의 정보를 담을 수 있는 사각형의 가로세로 격자무늬에 다양한 정보를 담고 있는 2차원 코드를 말한다. 종래의 1차원 코드는 20자 내외의 숫자정보만을 저장할 수 있는 반면, 상기 2차원바코드는 숫자로서 최대 7,089자, 아스키코드(ASCII)의 문자로서 최대 4,296자, 8비트 이진 데이터로서 최대 2,953 Byte, 한자로서 최대 1,817자를 저장할 수 있으며, 빠른 인식속도와 인식율 및 복원율을 갖는다.

[0025] 이하, 상기 2차원바코드를 발급받는 과정에 대하여 보다 자세히 살펴보도록 한다.

[0026] 상기 2차원바코드를 발급받는 과정은 크게 금융기관을 이용하는 과정과, 개별적인 2차원바코드생성기를 이용하는 과정으로 나누어진다.

[0027] 먼저, 금융기관을 통해 2차원바코드를 발급받는 과정에 대하여 살펴보면, 다음과 같다. 사용자단말을 사용하는 사용자가 금융기관으로 직접 방문하여 사용자 확인을 완료한 후, 난수열을 포함하는 2차원바코드의 발급을 신청한다.

[0028] 이때, 상기 금융기관은 2차원바코드의 발급을 신청한 상기 사용자에 대하여 신원확인을 수행한다. 상기 금융기관은 상기 사용자의 이름, 나이, 주소, 연락처 등의 개인정보를 참고로 하여, 상기 사용자에 대한 신원확인을 수행할 수 있다.

[0029] 이와 같이, 상기 사용자에 대한 신원확인을 완료한 상기 금융기관은 난수열을 포함하며, 각 사용자 마다 서로 다른 고유한 2차원바코드를 상기 사용자에게 발급한다.

[0030] 또는 금융기관을 통하지 않고, 별도의 2차원바코드생성기를 통해서도 상기 2차원바코드를 생성할 수 있다.

[0031] 먼저, 사용자가 2차원바코드생성기로 난수열을 포함하는 2차원바코드의 생성을 요청한다.

[0032] 이에 따라, 상기 2차원바코드생성기는 각 사용자마다 서로 다른 난수열을 포함하도록 고유의 2차원바코드를 생성하고, 이를 프린트하여 생성된 상기 2차원바코드를 출력한다.

[0033] 이후, 상기 사용자는 상기 2차원바코드생성기로부터 생성된 상기 2차원바코드를 수신하여, 고유한 2차원바코드를 발급받는다.

[0034] 이와 같이, 금융기관 또는 2차원바코드생성기를 통해 해당 사용자만의 2차원바코드를 이용하는 공인인증서의 패스워드에 따른 비밀키 생성에 대하여 자세히 살펴보도록 한다.

[0035] 도 1은 본 발명의 일 실시 예에 따른 2차원바코드를 이용한 패스워드의 비밀키 생성 시스템의 개략도이다.

[0036] 도 1에 도시된 바와 같이, 본 발명의 2차원바코드를 이용한 패스워드의 비밀키 생성 시스템은 사용자단말(120)이 사용자로부터 사용하고자 하는 공인인증서에 대해 기설정된 패스워드와, 앞서 금융기관 또는 2차원바코드생성기를 통해 발급받은 2차원바코드를 입력받고, 입력받은 2차원바코드로부터 난수열을 획득한 후, 상기 난수열과 상기 패스워드를 상호 조합하여 비밀키를 생성하고, 생성된 상기 비밀키를 통해 상기 공인인증서에 대한 사용 또는 인증을 수행한다.

[0037] 특히, 이러한 사용자단말(120)은 전자상거래 또는 금융거래 시, 사용자의 신원확인을 위해 사용되는 공인인증서를 신규로 발급받거나, 미리 발급받은 공인인증서를 이용하여 전자상거래 또는 금융거래를 수행하거나, 미리 발급받은 공인인증서의 패스워드를 변경하는 경우에 사용자로부터 상기 공인인증서에 대한 패스워드 및 2차원바코드를 입력받는다.

[0038] 이때, 상기 사용자단말(120)은 내부에 포함된 키패드를 통해 상기 공인인증서에 대한 패스워드를 입력받을 수 있고, 또한 내부에 포함된 카메라를 통해 앞서 금융기관 또는 2차원바코드생성기로부터 발급받은 2차원바코드를 촬영하여 입력받을 수 있다. 이러한 상기 사용자단말(120)은 입력받은 상기 2차원바코드로부터 난수열을 획득하고, 획득한 난수열을 입력받은 상기 패스워드와 상호 조합하여 상기 패스워드에 대한 비밀키를 생성한다.

[0039] 또한 상기 사용자단말(120)은 앞서 생성된 상기 공인인증서에 대한 패스워드의 비밀키로부터 PBKDF()함수와 같은 키추출함수를 이용하여 암호화된 추출키를 생성한다. 이 때, 상기 추출키는 상기 비밀키 중 상위 16 Byte에 해당하는 것이 바람직하다.

[0040] 이에 따라, 상기 사용자단말(120)은 공인인증서의 패스워드에 대한 비밀키를 생성하여, 상기 공인인증서를 통해

사용자의 본인확인을 수행한다.

[0041] 이하, 도 2를 참조하여 본 발명의 2차원바코드를 이용한 패스워드의 비밀키 생성 방법에 대하여 자세히 살펴보도록 한다.

[0042] 도 2는 본 발명의 다른 실시 예에 따른 2차원바코드를 이용한 패스워드의 비밀키 생성 방법의 순서도이다.

[0043] 도 2에 도시된 바와 같이, 본 발명의 2차원바코드를 이용한 패스워드의 비밀키 생성 방법은 먼저, 사용자단말이 사용자로부터 공인인증서를 새로 발급받거나, 이미 발급받은 공인인증서를 사용하거나 또는 이미 발급받은 공인인증서에 대하여 기설정된 패스워드를 변경하는 것 중 하나를 요청받으면, 상기 사용자로부터 상기 공인인증서에 대한 패스워드 및 금융기관 또는 2차원바코드생성기로부터 발급받은 2차원바코드를 입력받는다(S210).

[0044] 이때, 사용되는 상기 공인인증서란, 전자상거래 또는 금융거래 시, 사용자의 신원을 확인하고, 문서의 위조 및 변조 또는 거래사실의 부인을 방지하는 등의 목적으로 공인인증기관이 발생하는 전자적 정보로서, 일종의 사이버 거래용 인감증명서를 말한다.

[0045] 이러한 공인인증서는 사용자의 확인을 위해, 영대소문자와 숫자의 조합으로 이루어지는 패스워드를 포함한다. 따라서, 상기 사용자단말(120)은 상기 공인인증서에 기설정된 패스워드를 사용자로부터 입력받는다. 또한, 상기 사용자단말은 내부에 포함된 카메라를 통해 2차원바코드를 촬영하여 입력받는다.

[0046] 이때, 상기 사용자단말(120)이 입력받는 2차원바코드는 각 사용자 마다 서로 다른 것으로, 사용자가 금융기관에 직접 방문하여 신원확인을 완료 후 발급받거나, 개별적으로 2차원바코드생성기를 통해 상기 2차원바코드를 발급받을 수 있다.

[0047] 이때, 상기 사용자단말은 촬영을 통해 입력받은 상기 2차원바코드로부터 난수열을 획득한다(S220). 이러한 난수열은 이후 패스워드의 비밀키 생성을 위해 사용되는 것으로, 보다 복잡한 비밀키가 생성되도록 한다.

[0048] 이후, 상기 사용자단말은 앞서 S210과정에서 입력받은 상기 공인인증서에 대한 패스워드를 앞서 S220 과정에서 입력받은 2차원바코드로부터 획득한 난수열과 상호 조합하여 상기 패스워드에 대한 비밀키를 생성한다(S230).

[0049] 예를 들어, 도 3에 도시된 바와 같이, 상기 공인인증서에 대한 패스워드가 'gildong1234'이고, 난수열이 '0F 2D FF 57 98 5E E1 58 EF 46 FF 51 AA 65 C9 66 C8 18 A5 81 D5'를 획득한 경우, 상기 사용자단말이 상기 패스워드와 상기 난수열을 XOR연산하여 '68 44 93 33 F7 30 86 69 DD 75 CB 51 AA 65 C9 66 C8 18 A5 81 D5'라는 비밀키를 생성할 수 있다.

[0050] 이에 따라, 처음 사용자단말로 입력된 패스워드는 11글자 즉, 11 Byte를 가지며 오직 문자의 형태를 갖는 것에 비하여, 난수열과의 상호 조합을 통해 생성된 상기 패스워드에 대한 비밀키는 20 Byte로 그 길이가 확장되며, 문자 인코딩 방식에 있어서, 문자로 사용하지 않는 범위까지도 패스워드에 대한 비밀키의 경우의 수가 많아지는 것을 알 수 있다.

[0051] 이와 같이 생성된 상기 비밀키는 2차원바코드로부터 획득한 난수열과의 조합을 통해 생성됨에 따라, 일반적으로 영대소문자와 숫자의 조합으로 이루어지는 상기 공인인증서의 패스워드 보다 복잡도가 향상된 것을 알 수 있다.

[0052] 이처럼, 본 발명을 통해 공인인증서의 패스워드를 영대소문자와 숫자의 간단조합으로 이루어지는 것에서 완료되는 것이 아니라, 상기 패스워드를 난수열을 이용하여 다시 조합한 후 비밀키를 생성함으로써, 상기 패스워드를 용이하게 유추할 수 없도록 하여 상기 공인인증서의 보안성을 강화시킬 수 있다.

[0053] 이어서, 각 상황에 따른 본 발명의 2차원바코드를 이용한 패스워드의 비밀키 생성 방법에 대하여 도 4 내지 도 6을 참조하여 자세히 설명하도록 한다.

[0054] 도 4는 신규 공인인증서 발급요청에 따른 공인인증서의 패스워드에 대한 비밀키를 생성하는 과정에 대한 순서도이다.

[0055] 도 4에 도시된 바와 같이, 신규 공인인증서의 발급 요청에 따른 패스워드의 비밀키 생성과정은 살펴보면 먼저, 사용자단말(120)이 거래하고자 하는 금융서버(140)로 신규 공인인증서의 발급을 요청한다(S311).

[0056] 상기 사용자단말(120)로부터 신규 공인인증서에 대한 발급을 요청받은 상기 금융서버(140)는 전송받은 요청에 응답하여, 신규 공인인증서를 상기 사용자단말(120)로 전송한다(S312).

[0057] 상기 금융서버(140)로부터 신규 공인인증서를 전송받은 상기 사용자단말(120)은 패스워드 입력요청메시지를 출

력하여 사용자로부터 패스워드를 입력받는다(S313).

[0058] 또한, 상기 사용자단말(120)은 내부에 포함된 카메라를 통해 상기 사용자가 소지하고 있는 고유한 2차원바코드를 촬영하여 2차원바코드를 입력받는다(S314).

[0059] 상기 사용자단말(120)은 촬영한 상기 2차원바코드로부터 패스워드의 조합을 위해 사용되는 난수열을 획득한다(S315).

[0060] 이후, 상기 사용자단말(120)은 입력받은 상기 패스워드를 상기 난수열과 상호 조합하여 신규 발급받고자 하는 공인인증서의 패스워드에 대한 비밀키를 생성한다(S316).

[0061] 이어서, 상기 사용자단말(120)은 생성한 상기 비밀키로부터 PBKDF()함수와 같은 키추출함수를 이용하여 상기 비밀키 중 상위 16 Byte의 데이터를 암호화된 추출키로 생성한다(S317).

[0062] 이에 따라, 상기 사용자단말(120)과 상기 금융서버(140)간 신규 공인인증서의 발급요청에 따른 상기 신규 공인인증서의 패스워드에 대한 비밀키 생성이 완료된다.

[0063] 도 5는 공인인증서 사용요청에 따른 공인인증서의 패스워드에 대한 비밀키를 생성하는 과정에 대한 순서도이다.

[0064] 도 5에 도시된 바와 같이, 공인인증서의 사용 요청에 따른 패스워드의 비밀키 생성과정은 먼저, 사용자단말(120)이 금융서버(140)로 미리 발급받은 공인인증서에 대한 사용을 요청한다(S411).

[0065] 상기 사용자단말(120)로부터 공인인증서에 대한 사용을 요청받은 상기 금융서버(140)는 사용하고자 하는 공인인증서에 대한 패스워드의 전송을 상기 사용자단말(120)로 요청한다(S412).

[0066] 이에 따라, 상기 사용자단말(120)은 사용자로부터 사용하고자 하는 상기 공인인증서에 대한 패스워드를 입력받고(S413), 이어서, 사용자가 금융기관 또는 2차원바코드생성기를 통해 미리 발급받은 2차원바코드를 카메라를 통해 촬영하여 입력받는다(S414).

[0067] 이와 같이, 카메라를 통해 2차원바코드를 촬영한 상기 사용자단말(120)은 입력받은 상기 2차원바코드로부터 상기 패스워드의 비밀키 생성을 위한 난수열을 획득한다(S415).

[0068] 이후, 상기 사용자단말(120)은 입력받은 상기 패스워드와 상기 2차원바코드로부터 획득한 난수열을 상호 조합하여 상기 공인인증서의 패스워드에 대하여 복잡도가 향상된 비밀키를 생성한다(S416).

[0069] 상기 사용자단말(120)은 상기 비밀키의 생성을 완료한 후, 사용하고자 하는 상기 공인인증서에 대한 인증을 금융서버(140)로 요청한다(S417).

[0070] 이에 따라, 상기 금융서버(140)는 인증요청을 받은 공인인증서에 대하여 패스워드 및 비밀키 확인을 완료한 후, 인증을 수행한다(S418).

[0071] 이후, 인증이 완료된 공인인증서를 이용하여 상기 사용자단말(120)과 금융서버(140)간 금융거래를 수행한다.

[0072] 도 6은 공인인증서의 패스워드 또는 2차원바코드 변경요청에 따른 패스워드의 비밀키를 생성하는 과정에 대한 순서도이다.

[0073] 도 6에 도시된 바와 같이, 공인인증서의 패스워드 또는 2차원바코드 변경요청에 따른 비밀키 생성과정은 사용자단말(120)이 금융서버(140)로 현재 사용하고 있는 공인인증서에 대한 패스워드 또는 2차원바코드의 변경을 요청한다(S511).

[0074] 이후, 상기 사용자단말(120)은 변경 전 패스워드를 사용자로부터 입력받거나, 변경 전 2차원바코드를 내부에 포함된 카메라를 통해 촬영하여 입력받는다(S512). 이때, 상기 사용자단말(120)은 입력받은 변경 전 2차원바코드로부터 패스워드의 비밀키 암호화에 사용되는 난수열을 획득한다.

[0075] 상기 사용자단말(120)은 변경 전 패스워드와, 변경 전 2차원바코드로부터 획득한 난수열의 상호 조합을 통해 비밀키를 생성하고, 상기 비밀키에 대한 복호화를 수행한다(S513).

[0076] 이후, 상기 사용자단말(120)은 변경하고자 하는 신규 패스워드를 사용자로부터 입력받고, 변경하고자 하는 2차원바코드를 내부에 포함된 카메라를 통해 다시 촬영하여 입력받는다(S514).

[0077] 이때, 상기 사용자단말(120)은 촬영한 상기 2차원바코드로부터 난수열을 획득한다(S515).

[0078] 이후, 상기 사용자단말(120)은 입력받은 상기 신규 패스워드와, 앞서 획득한 상기 2차원바코드의 난수열을 상호

조합하여 비밀키를 생성한다(S516).

[0079] 이어서, 상기 사용자단말(120)은 PBKDF()함수와 같은 키추출함수를 이용하여 생성한 상기 비밀키 중 상위 16 Byte의 데이터를 암호화된 추출키로 생성한다(S517).

[0080] 이에 따라, 동일한 공인인증서에 대한 신규 패스워드 또는 2차원바코드로의 변경이 완료된다(S518).

[0081] 본 발명의 2차원바코드를 이용한 패스워드의 비밀키 생성 시스템 및 방법은 사용자단말을 이용한 금융거래 시, 사용자 확인을 위해 사용되는 공인인증서의 패스워드를 사용자가 발급받은 고유의 2차원바코드와 상호 조합하여 상기 패스워드에 대한 비밀키를 생성함으로써, 공인인증서의 패스워드에 대한 복잡도를 향상시킬 수 있는 효과가 있다.

[0082] 또한, 본 발명의 2차원바코드를 이용한 패스워드의 비밀키 생성 시스템 및 방법은 사용자단말이 촬영하여 획득한 난수열을 통해 영대소문자와 숫자만으로 이루어지는 공인인증서의 패스워드에 대한 복잡도를 향상시킴에 따라, 사용자단말을 이용한 금융거래를 보다 안전하게 수행할 수 있도록 하는 효과가 있다.

[0083] 더불어, 본 발명의 2차원바코드를 이용한 패스워드의 비밀키 생성 시스템 및 방법은 사용자단말의 분실 시 공인인증서의 쉬운 패스워드로 인해 상기 사용자단말을 이용한 각종 금융범죄 및 개인정보 누출에 따른 피해발생을 방지할 수 있는 효과가 있다.

[0084] 이와 더불어, 본 발명의 2차원바코드를 이용한 패스워드의 비밀키 생성 시스템 및 방법은 사용자단말 내 보편적으로 구비되는 카메라를 이용하여 2차원바코드를 입력받음에 따라 추가되는 장치의 구성이 필요하지 않아 사용자가 용이하게 사용할 수 있는 효과가 있다.

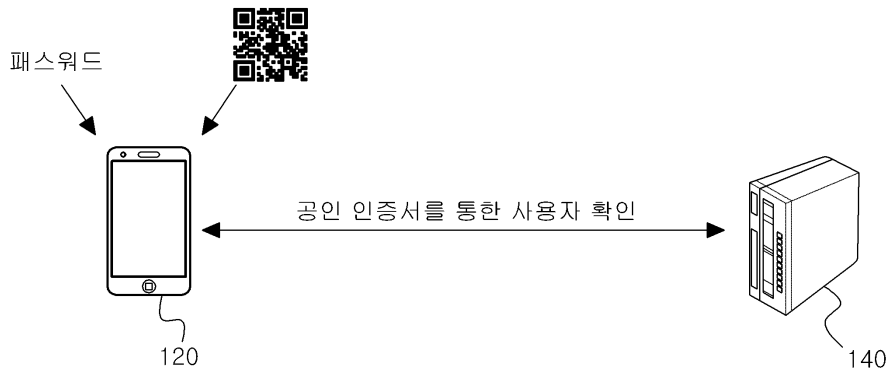
[0085] 상기에서는 본 발명의 바람직한 실시 예에 대하여 설명하였지만, 본 발명은 이에 한정되는 것이 아니고 본 발명의 기술 사상 범위 내에서 여러 가지로 변형하여 실시하는 것이 가능하고 이 또한 첨부된 특허청구범위에 속하는 것은 당연하다.

부호의 설명

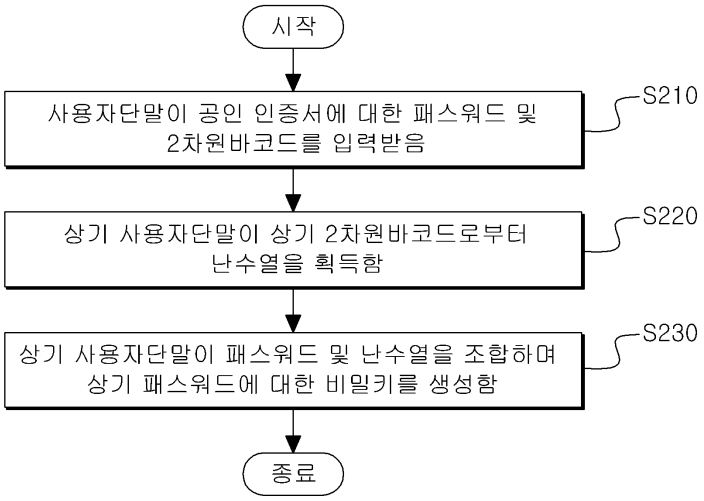
[0086] 120: 사용자단말 140: 금융서버

도면

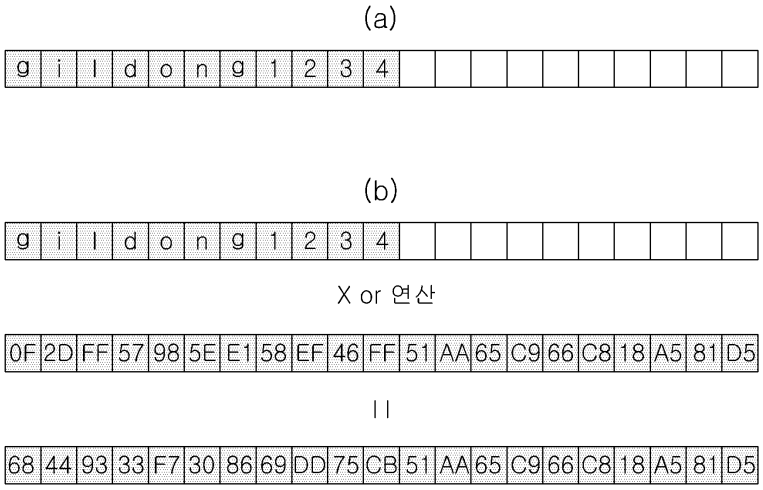
도면1



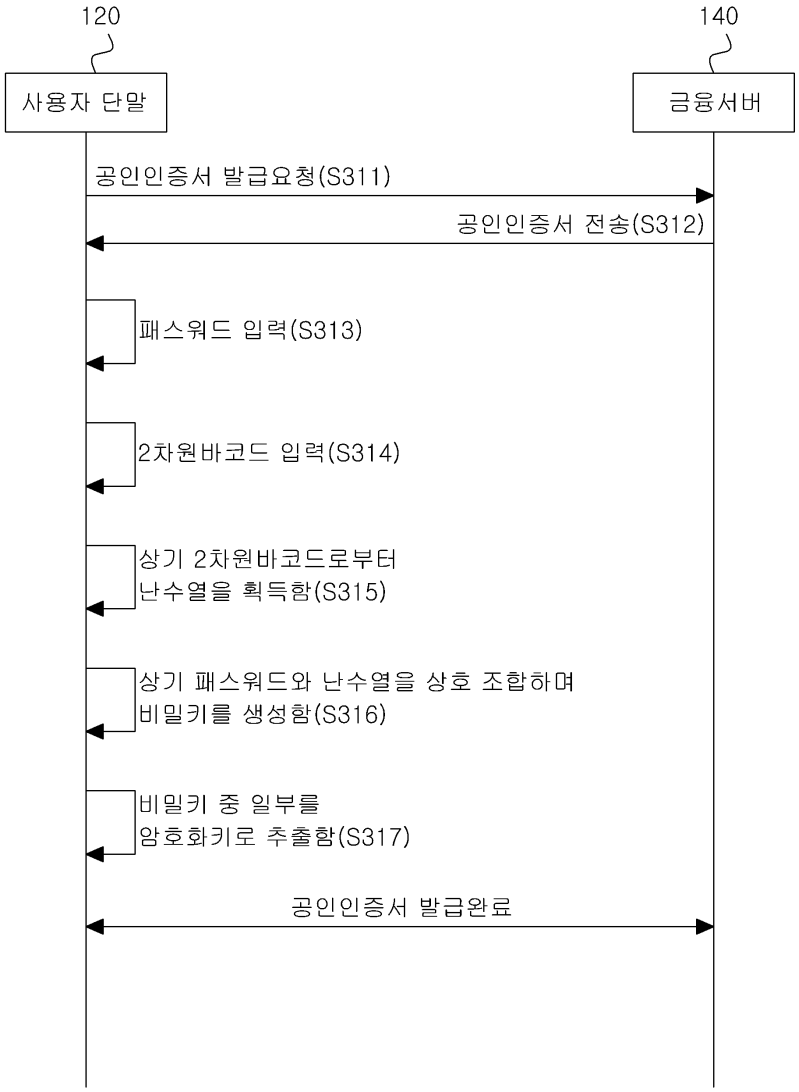
도면2


시작
사용자단말이 공인 인증서에 대한 패스워드 및 2차원바코드를 입력받음
S210
상기 사용자단말이 상기 2차원바코드로부터 난수열을 획득함
S220
상기 사용자단말이 패스워드 및 난수열을 조합하며 상기 패스워드에 대한 비밀키를 생성함
S230
종료

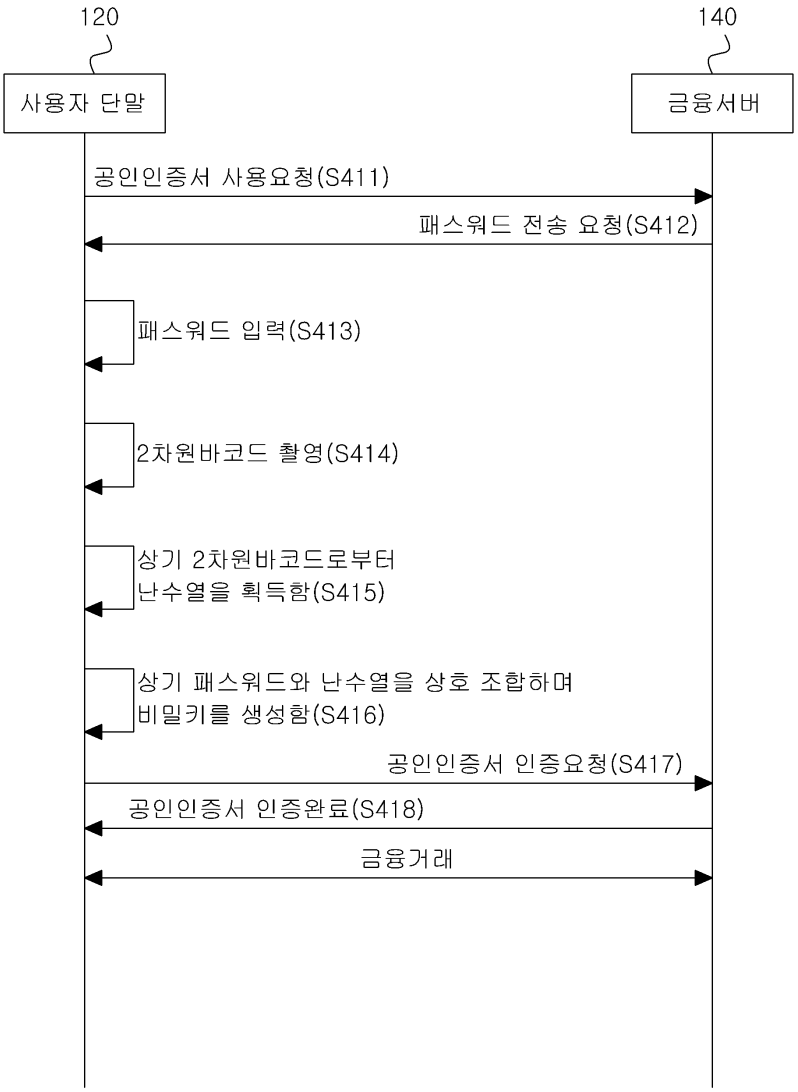
도면3


(a)
g i l d o n g 1 2 3 4
(b)
g i l d o n g 1 2 3 4
X or 연산
0F 2D FF 57 98 5E E1 58 EF 46 FF 51 AA 65 C9 66 C8 18 A5 81 D5
| |
68 44 93 33 F7 30 86 69 DD 75 CB 51 AA 65 C9 66 C8 18 A5 81 D5

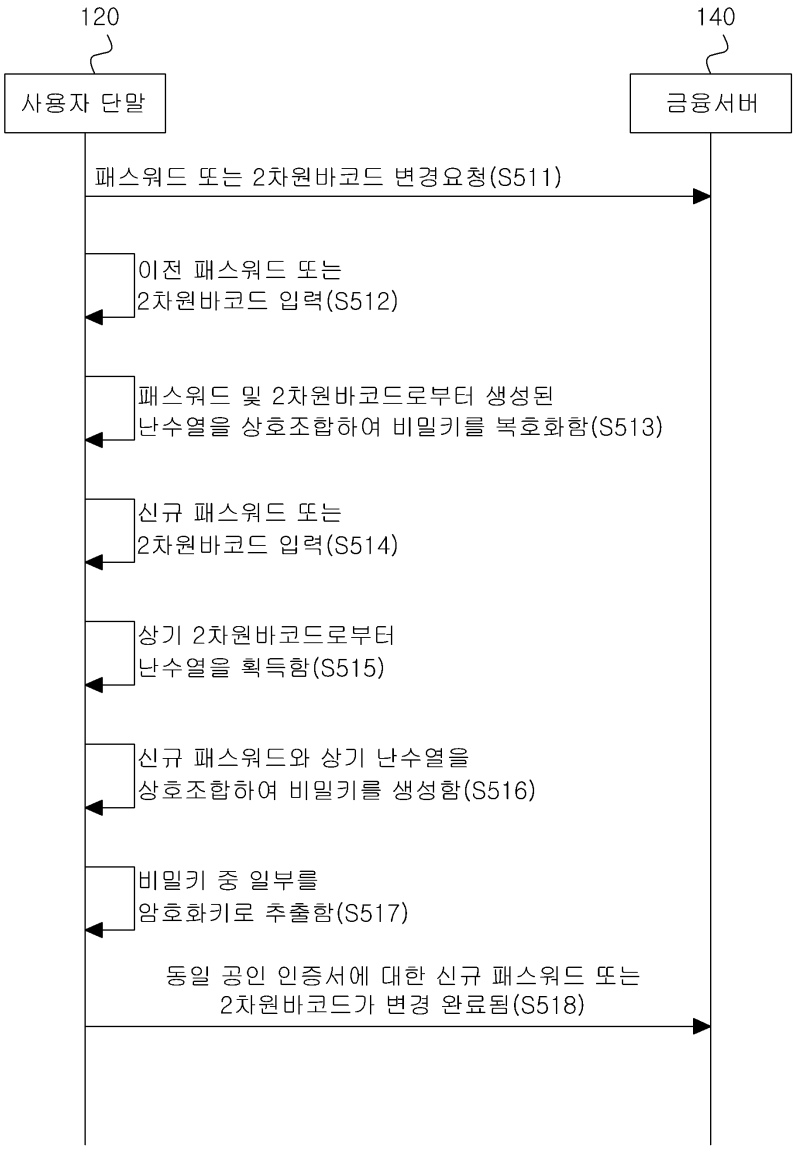
도면4


120
140
사용자 단말
금융서버
공인인증서 발급요청(S311)
공인인증서 전송(S312)
패스워드 입력(S313)
2차원바코드 입력(S314)
상기 2차원바코드로부터
난수열을 획득함(S315)
상기 패스워드와 난수열을 상호 조합하며
비밀키를 생성함(S316)
비밀키 중 일부를
암호화키로 추출함(S317)
공인인증서 발급완료

도면5


120
140
사용자 단말
금융서버
공인인증서 사용요청(S411)
패스워드 전송 요청(S412)
패스워드 입력(S413)
2차원바코드 촬영(S414)
상기 2차원바코드로부터
난수열을 획득함(S415)
상기 패스워드와 난수열을 상호 조합하며
비밀키를 생성함(S416)
공인인증서 인증요청(S417)
공인인증서 인증완료(S418)
금융거래

도면6


120
140
사용자 단말
금융서버
패스워드 또는 2차원바코드 변경요청(S511)
이전 패스워드 또는
2차원바코드 입력(S512)
패스워드 및 2차원바코드로부터 생성된
난수열을 상호조합하여 비밀키를 복호화함(S513)
신규 패스워드 또는
2차원바코드 입력(S514)
상기 2차원바코드로부터
난수열을 획득함(S515)
신규 패스워드와 상기 난수열을
상호조합하여 비밀키를 생성함(S516)
비밀키 중 일부를
암호화키로 추출함(S517)
동일 공인 인증서에 대한 신규 패스워드 또는
2차원바코드가 변경 완료됨(S518)