(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0092448
(43) 공개일자 2024년06월24일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
H04L 9/3247 (2013.01)
H04L 9/0861 (2013.01)
(21) 출원번호 10-2022-0175214
(22) 출원일자 2022년12월14일
심사청구일자 2022년12월14일

(71) 출원인
건양대학교산학협력단
충청남도 논산시 대학로 121 (내동)
(72) 발명자
정승욱
대전광역시 서구 청사로 281 샘머리아파트2단지, 218동 204호
(74) 대리인
특허법인도담

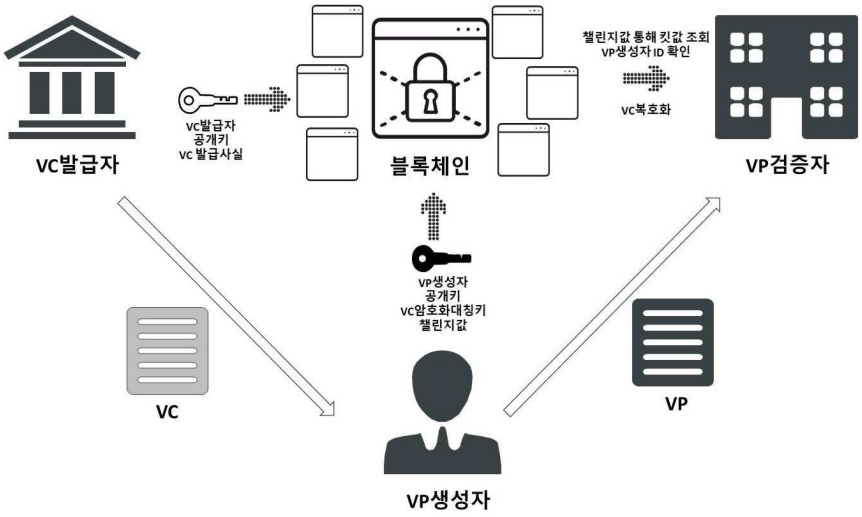
전체 청구항 수 : 총 5 항

(54) 발명의 명칭 **VP(Verifiable Credential) 유포 검증인 특정 방법**

(57) 요 약

본 발명은 DID 기술과 관련된 것으로, 신상정보를 암호화하여 넣은 VP의 신상정보를 복호화하고 검증하는 검증자를 특정하되 복호화된 신상정보를 무단 유출시 이를 포함하는 VP를 누가 유통했는지 특정할 수 있는 VP 유포 검증인 특정 방법에 관한 것이다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/3271 (2013.01)

명 세 서

청구범위

청구항 1

VC발급자와 VP생성자 및 VP검증자가 등록되고 상기 VC발급자가 발급한 VC를 통해 상기 VP생성자가 VP를 생성하여 상기 VP검증자에게 제출하는 DID 기반에서 VP 유포 검증인 특정 방법에 있어서,

상기 VC를 암호화할 제1대칭키와, VP생성자의 DID정보를 암호화할 제2대칭키를 생성하는 단계(S 110);

상기 VC에 포함된 신상정보를 상기 제1대칭키로 암호화하고, VP생성자의 DID정보를 상기 제2대칭키로 암호화하며, 상기 제2대칭키를 VP검증자의 공개키로 암호화한 킷값을 생성하고, 상기 VC에 문서의 타깃에 관한 챌린지값을 포함시켜 VP생성자의 서명을 통해 VP를 생성하는 단계(S 120);

상기 VP생성자가 상기 챌린지값과 VP검증자의 DID정보와 상기 킷값을 키스토리지에 기록하고, 상기 VP검증자에게 생성된 VP를 제출하는 단계(S 130);

상기 VP검증자가 제출받은 VP의 챌린지값을 통해 상기 킷값을 블록체인에서 조회하여 상기 VP생성자의 DID정보를 확인하고 VP생성자의 서명을 검증하는 단계(S 140);

상기 VP검증자가 상기 VP에 포함된 암호화된 신상정보를 복호화하는 단계(S 150); 를 포함하는 것을 특징으로 하는 VP 유포 검증인 특정 방법.

청구항 2

제1항에 있어서,

상기 VP를 생성하는 단계(S 120)에서,

상기 VP는 VP의 제3자유포를 금지하는 약관을 포함시키는 것을 특징으로 하는 VP 유포 검증인 특정 방법.

청구항 3

제1항에 있어서,

상기 키스토리지는 오프체인(offchain)서버 또는 블록체인 네트워크인 것을 특징으로 하는 VP 유포 검증인 특정 방법.

청구항 4

제1항에 있어서,

상기 VP를 생성하는 단계(S 120)에서,

VC의 내용은 JSON Web Encryption(jwe) 암호화되어 통신 및 저장중인 상태에서 지정된 검증자만 복호화가 가능하도록 구성되는 것을 특징으로 하는 VP 유포 검증인 특정 방법.

청구항 5

제4항에 있어서,

상기 VP를 생성하는 단계(S 120)에서, 공개키암호알고리즘 및 대칭키암호알고리즘과 상기 킷값과 암호초기화벡터와 VC를 상기 제1대칭키로 암호화한 값을 포함하는 jwe1과, 공개키암호알고리즘 및 대칭키암호알고리즘과 암

호초기화벡터와 VP생성자의 DID정보를 상기 제2대칭키로 암호화한 값을 포함하는 jwe2를 각각 생성하고,

상기 서명을 검증하는 단계(S 140)에서, 상기 jwe2를 복호화하고,

상기 암호화된 신상정보를 복호화하는 단계(S 150)에서, 상기 jwe1을 복호화하는 것을 특징으로 하는 VP 유포 검증인 특정 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 DID 기술과 관련된 것으로, 자세하게는 신상정보를 암호화하여 넣은 VP(Verifiable Credential, 이하 'VP'라함)의 신상정보를 복호화하고 검증하는 검증자를 특정하되 복호화된 신상정보를 무단 유출시 이를 포함하는 VP를 누가 유통했는지 특정할 수 있는 VP 유포 검증인 특정 방법에 관한 것이다.

배 경 기 술

[0002] 분산 식별자(Decentralized Identifiers, 이하 'DID'라 함)는 분산원장기술 또는 그 밖의 다른 분산 네트워크 기술을 활용하여 분산된 저장소에 등록함으로써 중앙집중화된(centralized) 서버와 같은 등록기관이 필요하지 않은 전역 고유 식별자를 의미하며, 블록체인 기술을 기반으로 구축한 전자신분증 시스템 등에 사용된다.

[0003] 서비스제공 기관이 중앙에서 사용자의 디지털 신원을 관리하는 기존의 중앙화된 신원관리체계에서는, 사용자 ID와 이를 검증하기 위한 크리덴셜(credentials, 예. 패스워드)을 발행하고, 사용자 이름, 주소 등의 사용자 정보를 보유하며 관리하는 것이 일반적으로, 사용자 신원이 중앙 기관에 위임되어 관리됨에 따라 사용자는 중앙 기관이 관리하는 자신의 신원, 개인 데이터, 관련 속성 정보를 통제하기 어렵다.

[0004] 이에 반해 블록체인과 같은 분산 네트워크 기술을 사용하면 사용자 개인이 자신의 신원 정보를 관리할 수 있으며, 이를 분산 신원관리 시스템이라고 하고 이에 사용되는 식별자를 분산 DID라 한다.

[0005] 구체적으로 지갑에서 주민등록증을 꺼내 신원을 증명하는 것과 같이 필요한 상황에 블록체인 지갑에서 DID를 제출하여 신원을 증명하도록 할 수 있으며, 기존의 신원 인증방식과 비교하여 신원확인 과정에서 개개인이 자기 정보에 완전한 통제권을 행사하는 것이 특징이다.

[0006] 이러한 기존의 DID 기술에서는 VC(Verifiable Credential, 이하 'VC'라함)를 받아서 VP를 제출하고 VP를 검증하여 신원의 진위를 확인하는 과정을 거치며, 이때 VP에는 다수의 신상정보가 포함될 수 있어 복호화된 신상정보를 포함하는 VP 유통에 따른 신상정보유출의 위험성이 있다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) 대한민국 등록특허 제10-2439879호 (2022.08.30)

발명의 내용

해결하려는 과제

[0008] 본 발명은 상기와 같은 문제를 해결하기 위하여 창출된 것으로, 본 발명의 목적은 VP의 생성 과정에서 대칭키 암호화 및 챌린지값을 적용하여 신상정보를 암호화하여 넣은 VP의 신상정보를 복호화하고 검증하는 검증자를 특정하되 복호화된 신상정보를 무단 유출시 이를 포함하는 VP를 누가 유통했는지 특정할 수 있는 VP 유포 검증인 특정 방법을 제공하는 것이다.

과제의 해결 수단

[0009] 상기와 같은 목적을 위해 본 발명은 VC발급자와 VP생성자 및 VP검증자가 등록되고 상기 VC발급자가 발급한 VC를 통해 상기 VP생성자가 VP를 생성하여 상기 VP검증자에게 제출하는 DID 기반에서 VP 유포 검증인 특정 방법에 있어서, 상기 VC를 암호화할 제1대칭키와, VP생성자의 DID정보를 암호화할 제2대칭키를 생성하는 단계; 상기 VC에

포함된 신상정보를 상기 제1대칭키로 암호화하고, VP생성자의 DID정보를 상기 제2대칭키로 암호화하며, 상기 제2대칭키를 VP검증자의 공개키로 암호화한 킷값을 생성하고, 상기 VC에 문서의 타깃에 관한 챌린지값을 포함시켜 VP생성자의 서명을 통해 VP를 생성하는 단계; 상기 VP생성자가 상기 챌린지값과 VP검증자의 DID정보와 상기 킷값을 키스토리지에 기록하고, 상기 VP검증자에게 생성된 VP를 제출하는 단계; 상기 VP검증자가 제출받은 VP의 챌린지값을 통해 상기 킷값을 블록체인에서 조회하여 상기 VP생성자의 DID정보를 확인하고 VP생성자의 서명을 검증하는 단계; 상기 VP검증자가 상기 VP에 포함된 암호화된 신상정보를 복호화하는 단계; 를 포함하는 것을 특징으로 한다.

[0010] 이때 상기 VP를 생성하는 단계에서, 상기 VP는 VP의 제3자유포를 금지하는 약관을 포함시킬 수 있다.

[0011] 또한, 상기 키스토리지는 오프체인(offchain)서버 또는 블록체인 네트워크가 될 수 있다.

[0012] 또한, 상기 VP를 생성하는 단계에서, VC의 내용은 JSON Web Encryption(jwe) 암호화되어 통신 및 저장중인 상태에서 지정된 검증자만 복호화가 가능하도록 구성될 수 있다.

[0013] 또한, 상기 VP를 생성하는 단계에서, 공개키암호알고리즘 및 대칭키암호알고리즘과 상기 킷값과 암호초기화벡터와 VC를 상기 제1대칭키로 암호화한 값을 포함하는 jwe1과, 공개키암호알고리즘 및 대칭키암호알고리즘과 암호초기화벡터와 VP생성자의 DID정보를 상기 제2대칭키로 암호화한 값을 포함하는 jwe2를 각각 생성하고, 상기 서명을 검증하는 단계에서, 상기 jwe2를 복호화하고, 상기 암호화된 신상정보를 복호화하는 단계에서, 상기 jwe1을 복호화할 수 있다..

발명의 효과

[0014] 본 발명을 통해 신상정보를 암호화하여 넣은 VP의 신상정보를 복호화하고 검증하는 검증자를 특정할 수 있으며, 해당 검증자가 복호화된 신상정보를 무단 유출시 이를 포함하는 VP를 누가 유통했는지 특정하여 VP생성자의 신상정보를 보호할 수 있다. 또한, VP검증자가 이러한 추적을 피하고자 VP의 정보를 임의 변경시 문서에 포함된 신상정보의 검증이 이루어질 수 없게 되므로 정보유출 시도를 무력화할 수 있다.

도면의 간단한 설명

[0015] 도 1은 본 발명의 개념도,

도 2는 본 발명의 실시예에 따른 플로어차트,

도 3은 본 발명의 실시예에 따른 프로토콜 설명도,

도 4는 본 발명의 실시예에 따른 구성 및 연결관계를 나타낸 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0016] 이하 첨부된 도면을 참조하여 본 발명 VP 유포 검증인 특정 방법을 구체적으로 설명한다.

[0017] 도 1은 본 발명의 개념도, 도 2는 본 발명의 실시예에 따른 플로어차트, 도 3은 본 발명의 실시예에 따른 프로토콜 설명도이다.

[0018] 기본적인 DID의 개념에서 VC는 VC 발급자(did:sov:ABC1)가 VC 요청자(=VP생성자, did:sov:123)에게 발행하는 하는 것으로, Claim에 요청자의 property를 넣고 proof에 발급자 개인키로 서명한 서명값을 넣어서 발급한 확인이 가능한 인증서이다. 예를 들어 did:sov:123이 자신이 다녔던 회사 did:sov:ABC1에서 발급해준 경력증명서가 VC가 된다.

[0019] VP는 did:sov:123이 자신의 경력증명서들(did:sov:ABC1, did:sov:ABC2...)로받은 VC들을 모아서 did:sov:123의 개인키로 서명하고 서명값을 proof에 넣은 인증서이다.

[0020] 본 발명에서는 VP생성자(did:sov:123)가 자신의 경력을 증명하기 위해서 구인회사(=VP검증자, did:sov:BCD)에 자신의 경력 증명서(VP)를 발급시 자신의 개인정보가 유출되지 않도록 하고 만약 개인정보가 유출되면 누가 유출했는지 추적 가능한 방안을 제시한다.

[0021] 이러한 DID는 블록체인을 기반으로 하며 3개의 주체인 VC발급자(A), VP생성자(B), VP검증자(C)의 각자 자신의 공개키를 등록하고 DID 주소를 부여받는 DID 생성과정을 전제로 한다.

[0022] 상기 VC발급자(A)는 Issuer(발행자)로서 이용자의 신원정보인 VC를 발행하는 주체이며, 정보주체인 이용자의 요

구에 의해 신원정보와 DID를 발급하는 기관이다. 발행자는 발급한 정보에 대해 신뢰할 수 있는 신원 정보를 전달한다.

[0023] 상기 VP생성자(B)는 이용자, Holder(소유자)로서 신원정보를 소유한 주체이며, 정보주체로 DID를 활용하여 본인의 신원을 증명하고자 하는 이용자이다. 시스템에서 DID를 발급 받고 제출한다.

[0024] 상기 VP검증자(Verifier)는 서비스제공자로, 신원정보를 검증하는 주체이다. 정보주체인 이용자로부터 VP를 받아 신원정보를 검증한다.

[0025] VP생성자(B)의 요청에 따라 VC발급자(A)가 VP생성자(B)의 신원정보가 포함된 자격증명인 VC를 VC발급자(A)의 개인키로 서명하여 발급하며, 이러한 서명 및 발급 내역이 블록체인에 저장된다.

[0026] VP생성자(B)는 VC발급자(A)가 발급한 VC를 개인 단말기에 저장하며, 이 중 필요한 정보를 VP생성자(B)의 개인키로 서명하여 VP를 생성하여, VP검증자(C)에게 제출한다.

[0027] VP검증자(C)는 제출받은 VP를 통해 VC발급자, VP생성자의 정보와, VC발급자의 VC 발행사실을 블록체인을 통해 검증하는 것이 일반적인 DID의 개념이다.

[0028] 이때 VC는 Credential metadata, Claims(s), Proof(s)로 구성되며, Credential metadata에는 VC 발행주체, 명시하고 있는 객체, 만료기간, 폐기방법 등이 포함되고, Claim(s)에는 Credential subject의 ID속성에 대한 정보가 ' Subject-Property-Value ' 방식으로 저장된다. Proof(s)에는 VC에 대한 진위 검증에 필요한 값이 포함되어, 검증하는 주체는 VC의 Proof를 검증함으로써 해당 VC가 VC에 명시된 발행인으로부터 발행된 것인지 검증 가능하다.

[0029] VP는 Presentation Metadata, Verifiable Credential(s), Proof(s)로 구성되며, Presentation Metadata에는 해당 데이터가 VP라는 것을 명시한 type, 이용약관, evidence 등 VP 검증에 필요한 데이터를 포함하고, Verifiable Credential(s)는 검증인이 요구하는 ID 속성을 가진 VC를 선택하여 넣는 영역으로, VP생성자는 VP검증인이 요구하는 ID 속성을 가진 Claim만 선택하여 넣어 프라이버시 보호가 이루어진다. Proof에는 VP생성자의 서명이 포함된다.

[0030] 이러한 종래의 DID 기반에서 본 발명은, VP를 생성함에 있어서 다음과 같은 절차를 통해 신상정보를 암호화하여 VP에 넣고 신상정보를 복호화하고 검증을 하는 자를 특정할 수 있도록 한다.

[0031] 먼저, VP생성자가 VC발행자로부터 발급된 VC 중 자신이 원하는 정보를 선택하여 VP를 생성함에 있어 상기 VC를 암호화할 제1대칭키와, VP생성자의 DID정보를 암호화할 제2대칭키를 생성하는 단계(S 110)가 진행된다. VP생성자가 VC 내용 및 VP생성자의 DID정보를 각각의 대칭키를 통해 암호화하여 VP검증자에게 제출하며 후술되는 일련의 인증 등의 과정을 거쳐 VP검증자는 상기 대칭키를 통해 암호화된 VP생성자의 DID정보를 비롯하여 VC 내용을 복호화할 수 있도록 한다.

[0032] 다음 VP를 생성하는 단계(S 120)에서 VP생성에 있어 상기 VC에 포함된 신상정보와 상기 VP생성자의 DID 정보를, 상기 대칭키를 생성하는 단계(S 110)에서 생성된 제1대칭키 및 제2대칭키로 각각 암호화한다. 이때 상기 제2대칭키를 VP검증자에게 전달하기 위해 상기 대칭키를 VP검증자의 공개키로 암호화한 킷값을 생성하며, 상기 VP에 문서의 타깃에 관한 챌린지값(challenge)을 포함시켜 VP생성자의 서명을 통해 VP를 생성한다.

[0033] 이때 상기 챌린지값이 VP에 포함되는 이유는 VP검증자와 키스토리지(keystorage)에 챌린지값이 같이 있어 VP가 누구를 타깃으로 하는 문서인지 확인할 수 있고 VP검증자가 신상정보를 유출할 경우 누가 유출했는지 확인하기 위한 용도이다.

[0034] 본 발명의 실시예에서 VP의 특징적인 형태는 다음과 같다.

[0035] {

[0036] Presentation Metadata: .... 생략

[0037] “verifiableCrednetial”:[{

[0038] jwe1: 내용

[0039] challenge: 내용

[0040] }]

[0041] “Proof”:{

[0042] .... 생략,

[0043] “id” : jwe2 내용,

[0044] “keystorage” : URL or blockchain A,

[0045] “verifier: did:sov:BCD,

[0046] “jws” : ... 내용

[0047] }

[0048] },

[0049] termOfUser:[{

[0050] ....생략

[0051] “action” : [“3rdPartyCorrelation”]

[0052] }]

[0053] 생략된 DID 관련 내용은 공지의 기술로서 본 발명의 취지가 흐려지는 것을 방지하고자 기존 DID와 동일한 내용은 생략한다.

[0054] 본 발명의 실시예에서 VP를 생성하는 단계(S 120)에서, VC 및 Proof의 내용은 JSON Web Encryption(jwe) 암호화되어 통신 및 저장중인 상태에서 지정된 검증자만 복호화가 가능하도록 구성되며, 바람직한 형태로 jwe1과, jwe2를 생성하게 된다.

[0055] 구체적으로 공개키암호알고리즘 및 대칭키암호알고리즘과 상기 킷값과 암호초기화벡터와 VC를 제1대칭키로 암호화한 값을 포함하는 jwe1과, 공개키암호알고리즘 및 대칭키암호알고리즘과 암호초기화벡터와 VP생성자의 DID정보를 제2대칭키로 암호화한 값을 포함하는 jwe2를 각각 생성할 수 있다.

[0056] 본 발명의 실시예에서 jwe1의 내용은 다음과 같이 구성할 수 있다.

[0057] “header” : { “alg”:공개키암호알고리즘, “enc” : 대칭키 암호 알고리즘 “ },

[0058] “encrypted_key” : VC들을 암호화하는데 사용한 대칭키 암호키를 did:sov:BCD의 공개키 암호알고리즘으로 암호화한 킷값

[0059] “iv” : Initial Vector (공개키로 암호화한 값)

[0060] “chipertext” : “VC들을 암호화한 값

[0061] 또한, 본 발명의 실시예에서 jwe2의 내용은 다음과 같이 구성할 수 있다.

[0062] “header” : { “alg”:공개키암호알고리즘, “enc” : 대칭키 암호 알고리즘 “ },

[0063] “iv” : Initial Vector (공개키로 암호화한 값)

[0064] “chipertext” : “did:sov:123”을 제2대칭키로 암호화한 값

[0065] VP에는 VC를 제1대칭키로 암호화하고, VP생성자의 DID정보(ID 등)을 제2대칭키를 통해 암호화하고, IV(Initialization Vecter, 초기화 벡터)를 공개키로 암호화한 값이 모두 포함된다.

[0066] 또한, 상기 VP를 생성하는 단계(S 120)에서 상기 VP는 VP의 제3자유포(“3rdPartyCorrelation”)를 금지하는 약관(termOfUser)을 포함하여, VP검증자가 약관을 위반하고 개인정보를 유출하는 것에 대한 1차적인 조치가 이루어지도록 한다.

[0067] 다음으로, 상기 VP생성자가 상기 챌린지값과 VP검증자의 DID정보와 상기 jwe2에 빠져있는 제2대칭키를 VP검증자의 공개키로 암호화한 킷갑을 키스토리지에 기록하고, 상기 VP검증자에게 생성된 VP를 제출하는 단계(S 130)가 진행된다.

[0068] 상기 키스토리지는 오프체인(offchain)서버 또는 블록체인 네트워크가 될 수 있다. 블록체인 네트워크는 온(O

n)체인(Chain)으로, 온체인 상의 모든 거래 정보가 블록에 포함되며 기록된 거래는 영구적으로 제거할 수 없다. 자체 네트워크를 구성하고 블록체인내 모든 내역이 기록되고 모든 사용자에게 공개가 되기 때문에 높은 안정성을 지니고 있다.

[0069] 오프체인은 온체인과 반대로 블록체인에 직접 기록하는 방식이 아닌 특정한 거래 내역을 블록체인이 아닌 독립된 외부에 기록한다. 합의과정이나 검증이 필요 없어서 온체인과는 다르게 빠른 처리가 가능하다. 핵심 데이터만을 블록체인에 기록하고 빠른 속도가 필요한 데이터는 블록체인이 아니라 DAPP 중앙 서버에 기록되며, 속도도 빠르고 비용이 저렴하다.

[0070] 이러한 키스토리지에 저장되는 값은 챌린지값/VP검증자 DID/jwe2에 빠진 상기 제2대칭키를 VP검증자의 공개키 암호 알고리즘으로 암호화한 킷값(encrypted_key)이다.

[0071] 이후 상기 VP검증자가 제출받은 VP의 챌린지값을 통해 상기 킷값을 블록체인에서 조회하고 개인키로 킷값을 복호화하여 제2대칭키를 얻고 상기 제2대칭키로 상기 VP생성자의 DID정보를 복호화하고 확인하여 VP생성자의 서명을 검증하는 단계(S 140)가 진행된다.

[0072] 앞서 설명한 jwe2는 VP를 구성하는 Proof에 있는 id를 암호화한 것으로 이를 복호화하기 위해서 VP검증자가 챌린지값과 자신의 id(did:sov:BCD)를 통해 키스토리지로 요청해서 제2킷값(encrypted_key)을 받아 사용자, 즉 VP생성자의 ID를 확인할 수 있고 이를 통해 VP생성자의 ID를 기반으로 VP의 proof를 검증할 수 있다.

[0073] 마지막으로 상기 VP검증자가 상기 VP에 포함된 암호화된 신상정보를 복호화하는 단계(S 150)를 통해 VP생성자 공개키로 서명검증 후 jwe1 복호화가 진행되어 VP검증자가 VP의 신상정보를 확인할 수 있게 된다.

[0074] 즉 상기 서명을 검증하는 단계(S 140)에서, 상기 jwe2를 복호화하고, 상기 암호화된 신상정보를 복호화하는 단계(S 150)에서, 상기 jwe1을 복호화한다.

[0075] 이러한 절차를 통해 만약 VP검증자가 VP를 유출시 VP 문서에 저장된 챌린지값을 통해 누가 유출하였는지 확인할 수 있으며, 이러한 추적을 피하기 위해 챌린지값을 바꾸면 VP가 검증될 수 없어, VC에 있는 신상정보가 사실과 맞느냐 검증이 될 수 없다.

[0076] 또한, VP검증자는 약관을 위반하고 신상정보를 유출하는 행위로 VP의 jwe1과 jwe2를 복호화하여 VP를 유통할 수도 있다. 이때 유출된 신상정보를 검증하기 위해서 VP검증자의 공개키로 jwe1을 암호화하여 만들고 jwe2의 공개키로 VP를 검증할 수 있다. 하지만, 일단 검증이 되면 챌린지값이 바뀌지 않을 것이므로 여전히 누가 유출했는지 특정할 수 있으며, 검증이 되지 않도록 챌린지값과, verifier를 바꿔 누가 유출했는지 알 수 없도록 하더라도 문서에 포함된 신상정보의 검증이 불가능하므로 이러한 시도를 무력화할 수 있다.

[0077] 도 4는 본 발명의 실시예에 따른 구성 및 연결관계를 나타낸 블록도로서, 본 발명에 따른 방법이 수행되는 각 주체가 소유한 단말기와 동작하는 네트워크 환경을 간략히 나타내고 있다.

[0078] 기본적으로 상기 서버(140)는 네트워크를 통해 VC발급자 단말기(110)와, VP생성자 단말기(120) 및 VP검증자 단말기(130)와 유무선으로 통신 가능하도록 구성되며, 오프체인 서버 내지는 블록체인이 될 수 있다.

[0079] 상기 VC발급자 단말기(110)는 VC를 발급하는 주체에 의해 사용되는 단말기로 신원 인증이 완료된 사용자에 대해 자격 인증에 대한 데이터인 VC를 발급하며, 예를 들어, 공공기관을 비롯하여 사용자가 요구하는 각종 증빙서류를 발급하는 기업이나 기관일 수 있다.

[0080] 상기 VP생성자 단말기(120)는 VP를 생성하는 주체에 의해 사용되는 단말기로 정보의 주체가 되는 사용자가 소유한 단말기이다. 상기 VC발급자 단말기(110)로 VC의 발급요청을 비롯하여 발급된 VC를 통해 VP를 만들고 이에 따른 정보를 상기 서버(140)로 등록과 함께 VP를 상기 VP검증자 단말기(130)로 제출하는 역할을 한다.

[0081] 상기 VP검증자 단말기(130)는 VP를 검증하는 주체에 의해 사용되는 단말기로, 사용자의 신원 확인 데이터를 받고, 받은 신원 확인 데이터에 기반을 두어 신원 인증을 수행할 수 있는 기관의 단말이 될 수 있다. 블록체인 네트워크에 등록된 복호화 정보를 활용하여 사용자에 대한 검증을 수행할 수 있다.

[0082] 상기 VC발급자 단말기(110)와, VP생성자 단말기(120) 및 VP검증자 단말기(130)는 네트워크를 통하여 원격지의 서버나 단말에 접속할 수 있는 컴퓨터로 구현될 수 있다. 예를 들어, 컴퓨터는 웹 브라우저(WEB Browser)가 탑재된 노트북, 데스크톱(Desktop), 랩톱(Laptop) 등을 포함할 수 있다. 또한, VP생성자 단말기(120)는 네트워크를 통하여 원격지의 서버나 다른 단말기에 접속할 수 있는 단말로 스마트폰(smartphone), 스마트 패드(smartpad), 태블릿 PC(Table PC) 등과 같은 모든 종류의 휴대용 개인 단말 장치를 포함할 수 있다.

[0083] 본 발명의 권리는 위에서 설명된 실시예에 한정되지 않고 청구범위에 기재된 바에 의해 정의되며, 본 발명의 분야에서 통상의 지식을 가진 자가 청구범위에 기재된 권리범위 내에서 다양한 변형과 개작을 할 수 있다는 것은 자명하다.

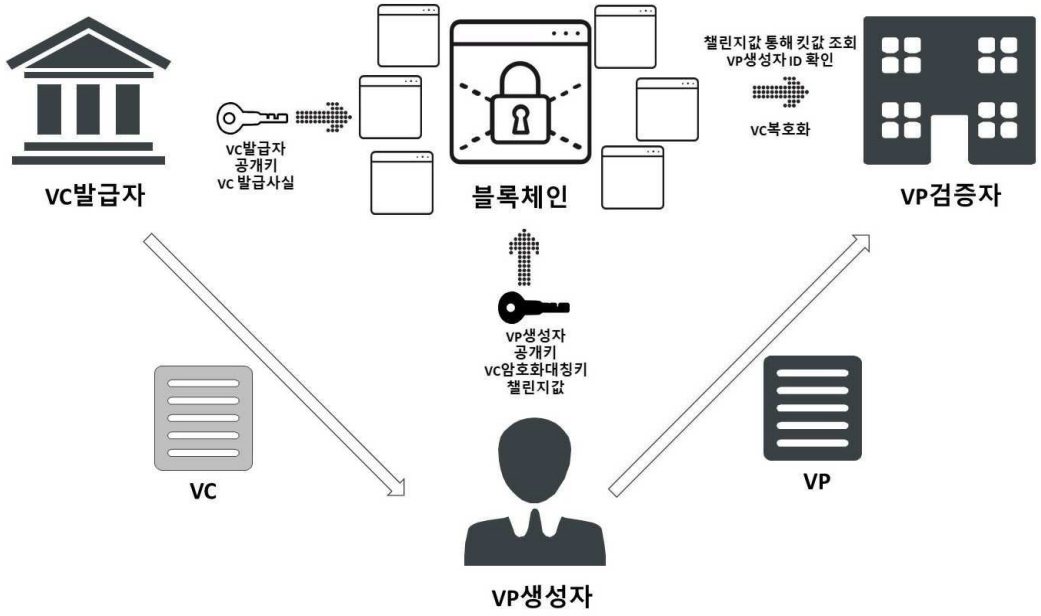
부호의 설명

[0084] 110: VC발급자 단말기 120: VP생성자 단말기

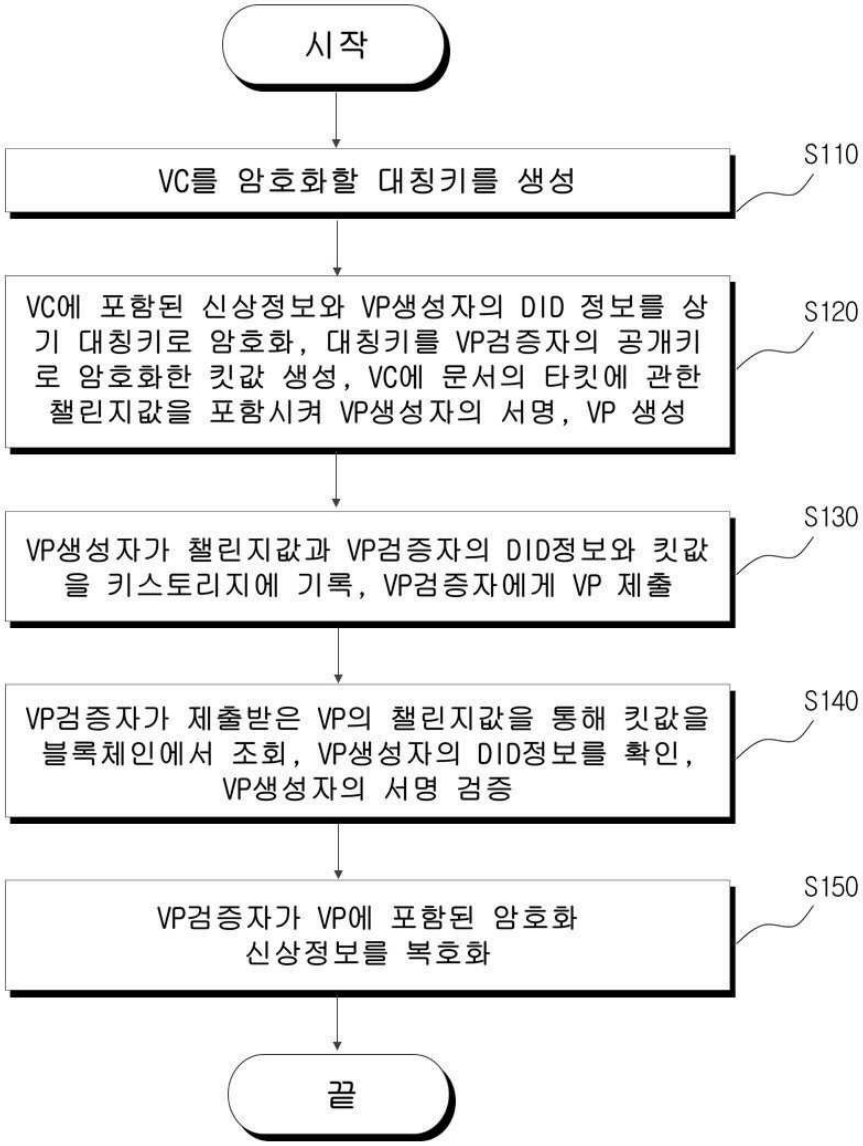
130: VP검증자 단말기 140: 서버

도면

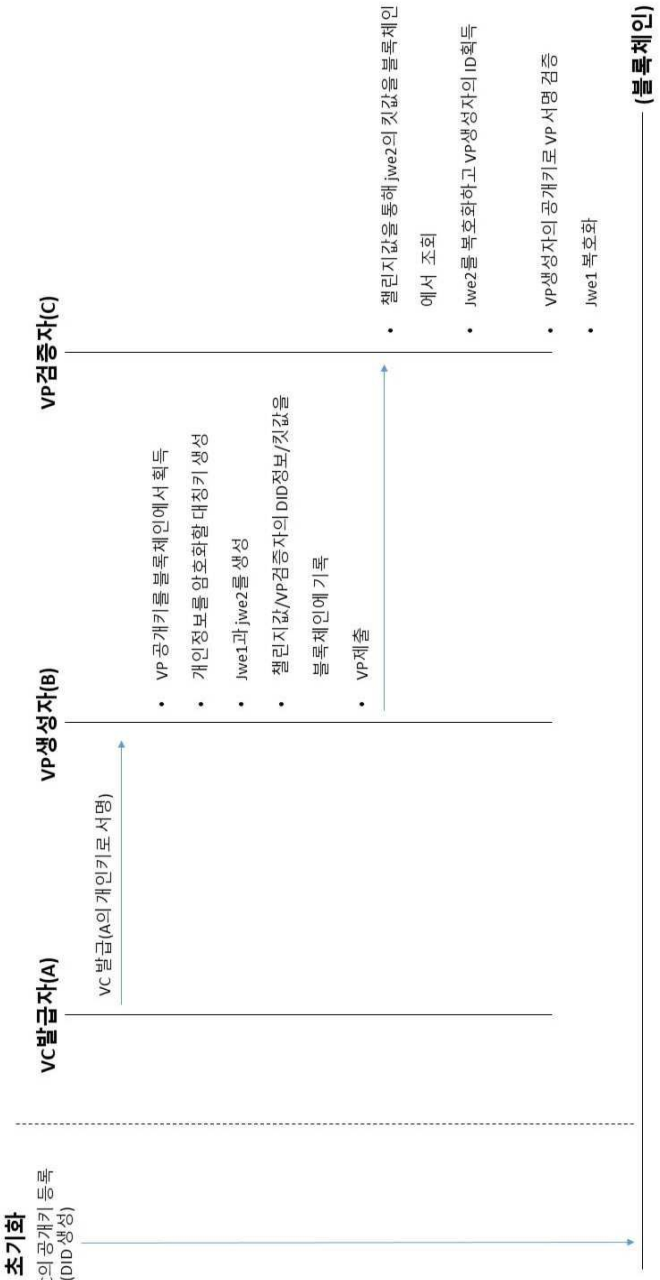
도면1



도면2


시작
VC를 암호화할 대칭키를 생성
S110
VC에 포함된 신상정보와 VP생성자의 DID 정보를 상기 대칭키로 암호화, 대칭키를 VP검증자의 공개키로 암호화한 킷값 생성, VC에 문서의 타킷에 관한 챌린지값을 포함시켜 VP생성자의 서명, VP 생성
S120
VP생성자가 챌린지값과 VP검증자의 DID정보와 킷값을 키스토리지에 기록, VP검증자에게 VP 제출
S130
VP검증자가 제출받은 VP의 챌린지값을 통해 킷값을 블록체인에서 조회, VP생성자의 DID정보를 확인, VP생성자의 서명 검증
S140
VP검증자가 VP에 포함된 암호화 신상정보를 복호화
S150
끝

도면3


초기화
A, B, C의 공개키 등록
(DID 생성)
VC발급자(A)
VP생성자(B)
VP검증자(C)
VC 발급(A의 개인키로 서명)
• VP 공개키를 블록체인에서 획득
• 개인정보를 암호화할 대칭키 생성
• Jwe1과 jwe2를 생성
• 챌린지값/VP검증자의 DID정보/키값을 블록체인에 기록
• VP제출
• 챌린지값을 통해 jwe2의 키값을 블록체인에서 조회
• Jwe2를 복호화하고 VP생성자의 ID획득
• VP생성자의 공개키로 VP 서명 검증
• Jwe1 복호화
(블록체인)

도면4