(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2025-0100412
(43) 공개일자 2025년07월03일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
H04L 9/0825 (2013.01)
H04L 9/0897 (2013.01)
(21) 출원번호 10-2023-0191940
(22) 출원일자 2023년12월26일
심사청구일자 2023년12월26일

(71) 출원인
충남대학교산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
(72) 발명자
류재철
대전광역시 유성구 어은로 57, 132동 801호(어은동, 한빛아파트)
김근영
대전광역시 유성구 문화원로47번길 38, A동 403호(궁동, 스위트빌)
홍지나
대전광역시 유성구 온천로 26, 334호(봉명동, 리베라 아이누리2 도시형생활주택)
(74) 대리인
이은철, 김재문

전체 청구항 수 : 총 10 항

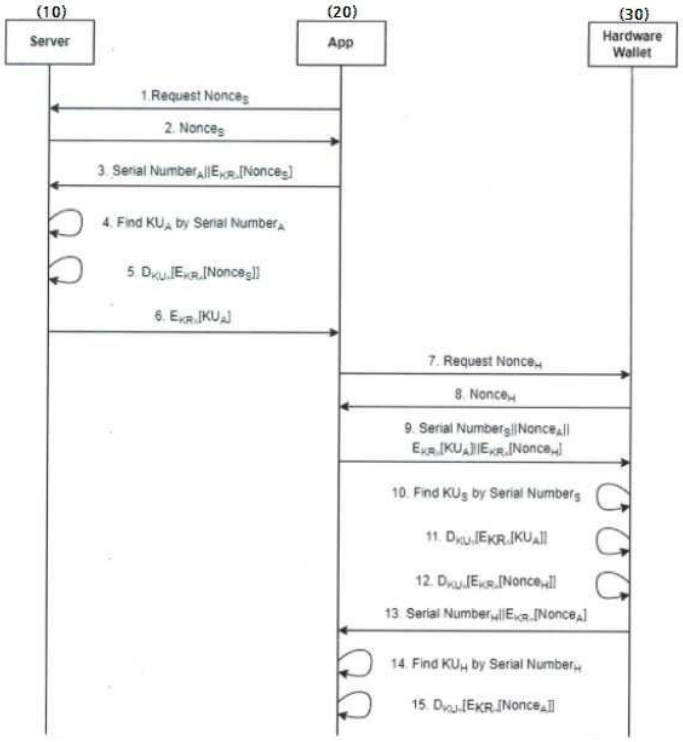
(54) 발명의 명칭 **하드웨어 지갑과 어플리케이션 간의 증명 방법**

(57) 요 약

본 발명은 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법에 관한 것으로서, 더욱 상세하게는 비대칭키 암호 알고리즘을 이용하여 서드 파티 어플리케이션과 하드웨어 지갑 간의 연동과정에서 사용할 수 있는 증명 방법을 제공할 수 있고, 사용자가 비공식 경로를 통해 어플리케이션을 설치한 경우 해당 어플리케이션이 변

(뒷면에 계속)

대 표 도 - 도2



조된 어플리케이션이라면 사용자가 변조된 사실을 알아차릴 수 없으므로 사용자가 확인하지 않더라도 하드웨어 지갑(Hardware Wallet) 자체에서 어플리케이션이 신뢰할 수 있는 어플리케이션임을 확인해주고, 반대로 어플리케이션도 하드웨어 지갑이 신뢰할 수 있는 하드웨어 지갑임도 확인할 수 있는 증명 방법을 제공할 수 있으며, 하드웨어 지갑과 연동하여 사용하는 어플리케이션(Application)의 경우 서드 파티 어플리케이션에서 하드웨어 지갑이 제공해주는 Software Development Kit(SDK)를 이용해 구현하는 것을 증명 과정을 이용해 적용시킬 수 있고, 하드웨어 지갑의 펌웨어 또는 어플리케이션 변조를 통한 암호화폐 해킹을 방어하는 기술로 사용할 수 있는 효과가 있다.

(52) CPC특허분류
H04L 9/32 (2022.08)
H04L 2209/08 (2013.01)
H04L 2209/56 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711193764
과제번호	2020-0-00321-004
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보보호핵심원천기술개발(R&D)
연구과제명	5G 서비스 환경에서 프라이버시가 보장되는 자기통제형 분산 디지털 신원 관리 및 보안 기술 개발
기 여 율	1/1
과제수행기관명	한국전자통신연구원
연구기간	2023.01.01 ~ 2023.12.31

명 세 서

청구범위

청구항 1

서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법에 있어서,

어플리케이션과 하드웨어 지갑이 연동되면, 어플리케이션(App)은 서버(Server)에 Nonce를 요청하는 단계(S1)와;

상기 어플리케이션이 서버로부터 Nonce를 받으면 어플리케이션의 개인키로 Nonce를 암호화하여 어플리케이션의 Serial Number와 함께 서버로 전송하는 단계(S2, S3)와;

상기 서버에서는 Serial Number를 이용해 해당 어플리케이션의 공개키를 찾아 공개키로 암호화된 Nonce를 복호화하는 단계(S4, S5)와;

상기 서버는 어플리케이션의 공개키를 서버의 개인키로 암호화하여 어플리케이션으로 전송하는 단계(S6)와;

상기 어플리케이션은 하드웨어 지갑에 Nonce를 요청하는 단계(S7)와;

상기 어플리케이션이 하드웨어 지갑으로부터 Nonce를 받으면, 상기 어플리케이션은 하드웨어 지갑으로 서버의 Serial Number와 어플리케이션의 Nonce, 서버로부터 받았던 서버의 개인키로 암호화된 어플리케이션의 공개키, 자신의 개인키로 암호화한 하드웨어 지갑의 Nonce를 전송하는 단계(S8, S9)와;

상기 하드웨어 지갑은 서버의 Serial Number를 이용해 매칭되는 서버의 공개키로 서버의 개인키로 암호화된 어플리케이션의 공개키를 복호화하여 어플리케이션의 공개키를 얻고 이를 이용해 어플리케이션의 개인키로 암호화된 Nonce를 복호화하는 단계(S10, S11, S12)와;

상기 하드웨어 지갑이 전송한 Nonce와 동일하면 어플리케이션이 변조되지 않은 신뢰할 수 있는 어플리케이션임을 알 수 있고, 하드웨어 지갑은 자신의 개인키로 어플리케이션의 Nonce를 암호화하여 하드웨어 지갑의 Serial Number와 함께 어플리케이션으로 전송하는 단계(S13)와;

상기 어플리케이션은 하드웨어 지갑의 Serial Number를 이용해 하드웨어 지갑의 공개키를 찾고, 공개키를 이용해 하드웨어 지갑의 개인키로 암호화된 어플리케이션의 Nonce를 복호화하여 자신이 전송한 Nonce와 동일하면 변조되지 않은 신뢰할 수 있는 하드웨어 지갑임을 아는 단계(S14, S15); 을 포함함을 특징으로 하는 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법.

청구항 2

제 1항에 있어서,

하드웨어 지갑과 어플리케이션 간의 증명 방법을 사용하기 위해서는 하드웨어 지갑 제조사의 서버, 하드웨어 지갑과 연동하려는 서드 파티인 어플리케이션, 하드웨어 지갑이 있어야 하는 것을 포함함을 특징으로 하는 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법.

청구항 3

제 1항에 있어서,

상기 단계(S1)에서, 상기 서버는 서버의 공개키, 개인키와 각 어플리케이션의 Serial Number에 매칭되는 어플리케이션 공개키를 가지고 있어야 하는 것을 포함함을 특징으로 하는 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법.

청구항 4

제 1항에 있어서,

상기 단계(S1)에서, 상기 어플리케이션은 어플리케이션의 공개키, 개인키와 각 하드웨어 지갑의 Serial Number에 매칭되는 하드웨어 지갑 공개키를 가지고 있어야 하는 것을 포함함을 특징으로 하는 서드 파티 환경에서 하

드웨어 지갑과 어플리케이션 간의 증명 방법.

청구항 5

제 1항에 있어서,

상기 단계(S1)에서, 상기 하드웨어 지갑은 하드웨어 지갑의 공개키, 개인키와 각 서버의 Serial Number에 매칭되는 서버 공개키를 가지고 있어야 하는 것을 포함함을 특징으로 하는 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법.

청구항 6

제 1항에 있어서,

상기 단계(S4, S5)에서, 상기 서버에서 어플리케이션으로 전송한 Nonce와 동일하면, 어플리케이션이 믿을 수 있는 어플리케이션인 것을 확인하는 것을 포함함을 특징으로 하는 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법.

청구항 7

제 1항에 있어서,

상기 단계(S4, S5)에서, 상기 서버가 어플리케이션의 공개키를 서버의 개인키로 암호화한 암호문을 어플리케이션이 신뢰할 수 있는 어플리케이션임의 증명 요소로 사용하는 것을 포함함을 특징으로 하는 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법.

청구항 8

제 1항에 있어서,

상기 단계(S6)에서, 상기 서버가 신뢰할 수 있는 서버임은 하드웨어 지갑이 서버의 공개키를 가지고 있고, 그 공개키로 서버가 개인키로 암호화한 암호문을 복호화하여 증명하는 것을 포함함을 특징으로 하는 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법.

청구항 9

제 1항에 있어서,

서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법에서, 서버와 어플리케이션 간과, 어플리케이션과 하드웨어 지갑 간의 신뢰 관계는 Nonce 값의 암호화, 복호화를 통해 형성하는 것을 포함함을 특징으로 하는 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법.

청구항 10

제 1항에 있어서,

서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법은 하드웨어 지갑의 펌웨어 또는 어플리케이션 변조를 통한 암호화폐 해킹을 방어하는 기술로 사용할 수 있는 것을 포함함을 특징으로 하는 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 비대칭키 암호 알고리즘을 이용하여 서드 파티 어플리케이션과 하드웨어 지갑 간의 연동과정에서 사용할 수 있는 증명 방법을 제공할 수 있고, 사용자가 비공식 경로를 통해 어플리케이션을 설치한 경우 해당 어플리케이션이 변조된 어플리케이션이라면 사용자가 변조된 사실을 알아차릴 수 없으므로 사용자가 확인하지 않더라도 하드웨어 지갑(Hardware Wallet) 자체에서 어플리케이션이 신뢰할 수 있는 어플리케이션임을 확인하여 주고, 반대로 어플리케이션도 하드웨어 지갑이 신뢰할 수 있는 하드웨어 지갑임도 확인할 수 있는 증명 방법을 제공할 수 있으며, 하드웨어 지갑과 연동하여 사용하는 어플리케이션(Application)의 경우 서드 파티 어플리케이션에서 하드웨어 지갑이 제공해주는 Software Development Kit(SDK)를 이용해 구현하는 것을 증명 과정을 이

용해 적용시킬 수 있고, 하드웨어 지갑의 펌웨어 또는 어플리케이션 변조를 통한 암호화폐 해킹을 방어하는 기술로 사용할 수 있는 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법에 관한 기술이다.

배 경 기 술

[0002] 현재 암호화폐의 해킹 사례가 점점 증가하고 있는 것이 현실이다. 하드웨어 지갑의 해킹 사례는 하드웨어 지갑의 펌웨어를 변조하거나 하드웨어 지갑 전용 어플리케이션을 변조하는 것이 있다.

[0003] 비공식적인 방법으로 조사해 본 결과에 의하면, 하드웨어 지갑을 구매하고 사용하였을 때 이를 정품임을 인증하는 증명 방법은 발명된 것이 있으나, 비공식적인 방법으로 어플리케이션을 설치하여 사용하였을 때 위조 어플리케이션(fake application)임을 증명하는 방법은 발명된 것이 없었다.

[0004] 특히, 위조 어플리케이션이 하드웨어 지갑에서 제공하는 특정 플랫폼 또는 서비스용 애플리케이션을 개발하는데 사용할 수 있는 도구인 Software Development Kit(SDK)를 이용해 구현을 한 경우라면 하드웨어 지갑은 어플리케이션이 위조(fake)임을 아는 것이 더욱 어려운 실정이다.

[0005] 한편, 하드웨어 지갑의 증명 과정을 구현한 사례는 있으나, 어플리케이션의 증명 과정을 구현한 사례는 없는 실정이다.

[0006] 그러므로 비대칭키 암호 알고리즘을 이용하여 서드 파티 어플리케이션과 하드웨어 지갑 간의 연동과정에서 사용할 수 있는 증명 방법을 제공할 수 있고, 사용자가 비공식 경로를 통해 어플리케이션을 설치한 경우 해당 어플리케이션이 변조된 어플리케이션이라면 사용자가 변조된 사실을 알아차릴 수 없으므로 사용자가 확인하지 않더라도 하드웨어 지갑(Hardware Wallet) 자체에서 어플리케이션이 신뢰할 수 있는 어플리케이션임을 확인하여 주고, 반대로 어플리케이션도 하드웨어 지갑이 신뢰할 수 있는 하드웨어 지갑임도 확인할 수 있는 증명 방법을 제공할 수 있으며, 하드웨어 지갑과 연동하여 사용하는 어플리케이션(Application)의 경우 서드 파티 어플리케이션에서 하드웨어 지갑이 제공해주는 Software Development Kit(SDK)를 이용해 구현하는 것을 증명 과정을 이용해 적용시킬 수 있는 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법의 개발이 절실히 요구되고 있는 실정이다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) KR 10-2017-0125132(2017. 11. 13)

발명의 내용

해결하려는 과제

[0008] 이에 본 발명은 상기 문제점들을 해결하기 위하여 착상된 것으로서, 비대칭키 암호 알고리즘을 이용하여 서드 파티 어플리케이션과 하드웨어 지갑 간의 연동과정에서 사용할 수 있는 증명 방법을 제공할 수 있는 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법을 제공하는 데 그 목적이 있다.

[0009] 또한 본 발명의 목적은 사용자가 비공식 경로를 통해 어플리케이션을 설치한 경우 해당 어플리케이션이 변조된 어플리케이션이라면 사용자가 변조된 사실을 알아차릴 수 없으므로 사용자가 확인하지 않더라도 하드웨어 지갑(Hardware Wallet) 자체에서 어플리케이션이 신뢰할 수 있는 어플리케이션임을 확인하여 주고, 반대로 어플리케이션도 하드웨어 지갑이 신뢰할 수 있는 하드웨어 지갑임도 확인할 수 있는 증명 방법을 제공할 수 있는 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법을 제공하는 데 있다.

[0010] 또한 본 발명의 목적은 하드웨어 지갑과 연동하여 사용하는 어플리케이션(Application)의 경우 서드 파티 어플리케이션에서 하드웨어 지갑이 제공해주는 Software Development Kit(SDK)를 이용해 구현하는 것을 증명 과정을 이용해 적용시킬 수 있는 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법을 제공하는 데 있다.

[0011] 또한 본 발명의 목적은 하드웨어 지갑의 펌웨어 또는 어플리케이션 변조를 통한 암호화폐 해킹을 방어하는 기술로 사용할 수 있는 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법을 제공하는 데 있다.

과제의 해결 수단

[0012] 상기 목적을 달성하기 위한 본 발명의 바람직한 실시예에 따른 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법은 어플리케이션과 하드웨어 지갑이 연동되면, 어플리케이션(App)은 서버(Server)에 Nonce를 요청하는 단계(S1)와; 상기 어플리케이션이 서버로부터 Nonce를 받으면 어플리케이션의 개인키로 Nonce를 암호화하여 어플리케이션의 Serial Number와 함께 서버로 전송하는 단계(S2, S3)와; 상기 서버에서는 Serial Number를 이용해 해당 어플리케이션의 공개키를 찾아 공개키로 암호화된 Nonce를 복호화하는 단계(S4, S5)와; 상기 서버는 어플리케이션의 공개키를 서버의 개인키로 암호화하여 어플리케이션으로 전송하는 단계(S6)와; 상기 어플리케이션은 하드웨어 지갑에 Nonce를 요청하는 단계(S7)와; 상기 어플리케이션이 하드웨어 지갑으로부터 Nonce를 받으면, 상기 어플리케이션은 하드웨어 지갑으로 서버의 Serial Number와 어플리케이션의 Nonce, 서버로부터 받았던 서버의 개인키로 암호화된 어플리케이션의 공개키, 자신의 개인키로 암호화한 하드웨어 지갑의 Nonce를 전송하는 단계(S8, S9)와; 상기 하드웨어 지갑은 서버의 Serial Number를 이용해 매칭되는 서버의 공개키로 서버의 개인키로 암호화된 어플리케이션의 공개키를 복호화하여 어플리케이션의 공개키를 얻고 이를 이용해 어플리케이션의 개인키로 암호화된 Nonce를 복호화하는 단계(S10, S11, S12)와; 상기 하드웨어 지갑이 전송한 Nonce와 동일하면 어플리케이션이 변조되지 않은 신뢰할 수 있는 어플리케이션임을 알 수 있고, 하드웨어 지갑은 자신의 개인키로 어플리케이션의 Nonce를 암호화하여 하드웨어 지갑의 Serial Number와 함께 어플리케이션으로 전송하는 단계(S13)와; 상기 어플리케이션은 하드웨어 지갑의 Serial Number를 이용해 하드웨어 지갑의 공개키를 찾고, 공개키를 이용해 하드웨어 지갑의 개인키로 암호화된 어플리케이션의 Nonce를 복호화하여 자신이 전송한 Nonce와 동일하면 변조되지 않은 신뢰할 수 있는 하드웨어 지갑임을 아는 단계(S14, S15); 을 포함함을 특징으로 한다.

[0013] 상기 본 발명에 있어서, 하드웨어 지갑과 어플리케이션 간의 증명 방법을 사용하기 위해서는 하드웨어 지갑 제조사의 서버, 하드웨어 지갑과 연동하려는 서드 파티인 어플리케이션, 하드웨어 지갑이 있어야 하는 것을 포함함을 특징으로 한다.

[0014] 상기 본 발명에 있어서, 상기 단계(S1)에서, 상기 서버는 서버의 공개키, 개인키와 각 어플리케이션의 Serial Number에 매칭되는 어플리케이션 공개키를 가지고 있어야 하는 것을 포함함을 특징으로 한다.

[0015] 상기 본 발명에 있어서, 상기 단계(S1)에서, 상기 어플리케이션은 어플리케이션의 공개키, 개인키와 각 하드웨어 지갑의 Serial Number에 매칭되는 하드웨어 지갑 공개키를 가지고 있어야 하는 것을 포함함을 특징으로 한다.

[0016] 상기 본 발명에 있어서, 상기 단계(S1)에서, 상기 하드웨어 지갑은 하드웨어 지갑의 공개키, 개인키와 각 서버의 Serial Number에 매칭되는 서버 공개키를 가지고 있어야 하는 것을 포함함을 특징으로 한다.

[0017] 상기 본 발명에 있어서, 상기 단계(S4, S5)에서, 상기 서버에서 어플리케이션으로 전송한 Nonce와 동일하면, 어플리케이션이 믿을 수 있는 어플리케이션인 것을 확인하는 것을 포함함을 특징으로 한다.

[0018] 상기 본 발명에 있어서, 상기 단계(S4, S5)에서, 상기 서버가 어플리케이션의 공개키를 서버의 개인키로 암호화한 암호문을 어플리케이션이 신뢰할 수 있는 어플리케이션임의 증명 요소로 사용하는 것을 포함함을 특징으로 한다.

[0019] 상기 본 발명에 있어서, 상기 단계(S6)에서, 상기 서버가 신뢰할 수 있는 서버임은 하드웨어 지갑이 서버의 공개키를 가지고 있고, 그 공개키로 서버가 개인키로 암호화한 암호문을 복호화하여 증명하는 것을 포함함을 특징으로 한다.

[0020] 상기 본 발명에 있어서, 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법에서, 서버와 어플리케이션 간과, 어플리케이션과 하드웨어 지갑 간의 신뢰 관계는 Nonce 값의 암호화, 복호화를 통해 형성하는 것을 포함함을 특징으로 한다.

[0021] 상기 본 발명에 있어서, 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법은 하드웨어 지갑의 펌웨어 또는 어플리케이션 변조를 통한 암호화폐 해킹을 방어하는 기술로 사용할 수 있는 것을 포함함을 특징으로 한다.

발명의 효과

[0022] 본 발명에 따른 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법은 다음과 같은 효과를 나타

낸다.

[0023] 첫째, 본 발명은 비대칭키 암호 알고리즘을 이용하여 서드 파티 어플리케이션과 하드웨어 지갑 간의 연동과정에서 사용할 수 있는 증명 방법을 제공할 수 있다.

[0024] 둘째, 본 발명은 사용자가 비공식 경로를 통해 어플리케이션을 설치한 경우 해당 어플리케이션이 변조된 어플리케이션이라면 사용자가 변조된 사실을 알아차릴 수 없으므로 사용자가 확인하지 않더라도 하드웨어 지갑(Hardware Wallet) 자체에서 어플리케이션이 신뢰할 수 있는 어플리케이션임을 확인해주고, 반대로 어플리케이션도 하드웨어 지갑이 신뢰할 수 있는 하드웨어 지갑임도 확인할 수 있는 증명 방법을 제공할 수 있다.

[0025] 셋째, 본 발명은 하드웨어 지갑과 연동하여 사용하는 어플리케이션(Application)의 경우 서드 파티 어플리케이션에서 하드웨어 지갑이 제공해주는 Software Development Kit(SDK)를 이용해 구현하는 것을 증명 과정을 이용해 적용시킬 수 있다.

[0026] 넷째, 본 발명은 하드웨어 지갑의 펌웨어 또는 어플리케이션 변조를 통한 암호화폐 해킹을 방어하는 기술로 사용할 수 있다.

도면의 간단한 설명

[0027] 도 1은 본 발명의 일실시예에 따른 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법을 구현하기 위한 구성을 설명하기 위해 나타낸 도면.

도 2는 본 발명의 일실시예에 따른 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법을 설명하기 위해 나타낸 도면.

발명을 실시하기 위한 구체적인 내용

[0028] 이하, 첨부된 도면과 함께 본 발명의 바람직한 실시 예를 살펴보면 다음과 같은데, 본 발명을 설명함에 있어서 관련된 공지기술 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략할 것이며, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있으므로, 그 정의는 본 발명인 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법을 설명하는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0029] 이하, 본 발명의 바람직한 일실시예에 따른 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명하는 흐름을 상세히 설명한다.

[0030] 도 1은 본 발명의 일실시예에 따른 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법을 구현하기 위한 구성을 설명하기 위해 나타낸 도면이고, 도 2는 본 발명의 일실시예에 따른 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법을 설명하기 위해 나타낸 도면이다.

[0031] 도 1 내지 도 2에 도시한 바와 같이, 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법은 어플리케이션과 하드웨어 지갑이 연동되면, 어플리케이션(App)(20)은 서버(Server)(10)에 Nonce를 요청하는 단계(S1)와; 상기 어플리케이션(20)이 서버(10)로부터 Nonce를 받으면 어플리케이션(20)의 개인키로 Nonce를 암호화하여 어플리케이션(20)의 Serial Number와 함께 서버(10)로 전송하는 단계(S2, S3)와; 상기 서버(10)에서는 Serial Number를 이용해 해당 어플리케이션(20)의 공개키를 찾아 공개키로 암호화된 Nonce를 복호화하는 단계(S4, S5)와; 상기 서버(10)는 어플리케이션(20)의 공개키를 서버(10)의 개인키로 암호화하여 어플리케이션(20)으로 전송하는 단계(S6)와; 상기 어플리케이션(20)은 하드웨어 지갑(30)에 Nonce를 요청하는 단계(S7)와; 상기 어플리케이션(20)이 하드웨어 지갑(30)으로부터 Nonce를 받으면, 상기 어플리케이션(20)은 하드웨어 지갑(30)으로 서버(10)의 Serial Number와 어플리케이션(20)의 Nonce, 서버(10)로부터 받았던 서버(10)의 개인키로 암호화된 어플리케이션(20)의 공개키, 자신의 개인키로 암호화한 하드웨어 지갑(30)의 Nonce를 전송하는 단계(S8, S9)와; 상기 하드웨어 지갑(30)은 서버(10)의 Serial Number를 이용해 매칭되는 서버(10)의 공개키로 서버(10)의 개인키로 암호화된 어플리케이션(20)의 공개키를 복호화하여 어플리케이션(20)의 공개키를 얻고 이를 이용해 어플리케이션(20)의 개인키로 암호화된 Nonce를 복호화하는 단계(S10, S11, S12)와; 상기 하드웨어 지갑(30)이 전송한 Nonce와 동일하면 어플리케이션(20)이 변조되지 않은 신뢰할 수 있는 어플리케이션(20)임을 알 수 있고, 하드웨어 지갑(30)은 자신의 개인키로 어플리케이션(20)의 Nonce를 암호화하여 하드웨어 지갑(30)의 Serial Number와 함께 어플리케이션(20)으로 전송하는 단계(S13)와; 상기 어플리케이션(20)은 하드웨어 지갑(30)의

Serial Number를 이용해 하드웨어 지갑(30)의 공개키를 찾고, 공개키를 이용해 하드웨어 지갑(30)의 개인키로 암호화된 어플리케이션(20)의 Nonce를 복호화하여 자신이 전송한 Nonce와 동일하면 변조되지 않은 신뢰할 수 있는 하드웨어 지갑(30)임을 아는 단계(S14, S15); 을 구비한다.

[0032] 상기 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명하는 방법을 구성하는 기술적 단계들의 기능을 살펴보면 다음과 같다.

[0033] 첫 번째로는, 어플리케이션(App)은 서버(Server)에 Nonce를 요청하는 단계(S1)로서, 어플리케이션과 하드웨어 지갑이 연동되면, 어플리케이션(App)(20)은 서버(Server)(10)에 Nonce를 요청하는 것이다.

[0034] 여기서, 상기 서버(10)는 서버(10)의 공개키, 개인키와 각 어플리케이션(20)의 Serial Number에 매칭되는 어플리케이션 공개키를 가지고 있어야 하는 것이다.

[0035] 또한, 상기 어플리케이션(20)은 어플리케이션(20)의 공개키, 개인키와 각 하드웨어 지갑(30)의 Serial Number에 매칭되는 하드웨어 지갑 공개키를 가지고 있어야 하는 것이다.

[0036] 또한, 상기 하드웨어 지갑(30)은 하드웨어 지갑(30)의 공개키, 개인키와 각 서버(10)의 Serial Number에 매칭되는 서버 공개키를 가지고 있어야 하는 것이다.

[0037] 두 번째로는, 어플리케이션이 서버로부터 Nonce를 받으면 어플리케이션의 Serial Number를 서버로 전송하는 단계(S2, S3)로서, 상기 어플리케이션(20)이 서버(10)로부터 Nonce를 받으면 어플리케이션(20)의 개인키로 Nonce를 암호화하여 어플리케이션(20)의 Serial Number와 함께 서버(10)로 전송하는 것이다.

[0038] 세 번째로는, 서버에서 Serial Number를 이용해 공개키로 암호화된 Nonce를 복호화하는 단계(S4, S5)로서, 상기 서버(10)에서는 Serial Number를 이용해 해당 어플리케이션(20)의 공개키를 찾아 공개키로 암호화된 Nonce를 복호화하는 것이다.

[0039] 여기서, 상기 서버(10)에서 어플리케이션(20)으로 전송한 Nonce와 동일하면, 어플리케이션(20)이 믿을 수 있는 어플리케이션인 것을 확인하는 것이다.

[0040] 또한, 상기 서버(10)가 어플리케이션(20)의 공개키를 서버(10)의 개인키로 암호화한 암호문을 어플리케이션(20)이 신뢰할 수 있는 어플리케이션임의 증명 요소로 사용하는 것이다.

[0041] 네 번째로는, 서버의 개인키로 암호화하여 어플리케이션으로 전송하는 단계(S6)로서, 상기 서버(10)는 어플리케이션(20)의 공개키를 서버(10)의 개인키로 암호화하여 어플리케이션(20)으로 전송하는 것이다.

[0042] 여기서, 상기 서버(10)가 신뢰할 수 있는 서버임은 하드웨어 지갑(30)이 서버(10)의 공개키를 가지고 있고, 그 공개키로 서버(10)가 개인키로 암호화한 암호문을 복호화하여 증명하는 것이다.

[0043] 다섯 번째로는, 어플리케이션에서 하드웨어 지갑으로 Nonce를 요청하는 단계(S7)로서, 상기 어플리케이션(20)은 하드웨어 지갑(30)에 Nonce를 요청하는 것이다.

[0044] 여섯 번째로는, 어플리케이션이 하드웨어 지갑으로부터 Nonce를 받고, 하드웨어 지갑으로 서버의 Serial Number와 어플리케이션의 Nonce, 서버로부터 받았던 서버의 개인키로 암호화된 어플리케이션의 공개키, 자신의 개인키로 암호화한 하드웨어 지갑의 Nonce를 전송하는 단계(S8, S9)로서, 상기 어플리케이션(20)이 하드웨어 지갑(30)으로부터 Nonce를 받으면, 상기 어플리케이션(20)은 하드웨어 지갑(30)으로 서버(10)의 Serial Number와 어플리케이션(20)의 Nonce, 서버(10)로부터 받았던 서버(10)의 개인키로 암호화된 어플리케이션(20)의 공개키, 자신의 개인키로 암호화한 하드웨어 지갑(30)의 Nonce를 전송하는 것이다.

[0045] 일곱 번째로는, 하드웨어 지갑은 서버의 공개키로 서버의 개인키로 암호화된 어플리케이션의 공개키를 복호화하여 어플리케이션의 공개키를 얻고 이를 이용해 어플리케이션의 개인키로 암호화된 Nonce를 복호화하는 단계(S10, S11, S12)로서,

[0046] 상기 하드웨어 지갑(30)은 서버(10)의 Serial Number를 이용해 매칭되는 서버(10)의 공개키로 서버(10)의 개인키로 암호화된 어플리케이션(20)의 공개키를 복호화하여 어플리케이션(20)의 공개키를 얻고 이를 이용해 어플리케이션(20)의 개인키로 암호화된 Nonce를 복호화하는 것이다.

[0047] 여덟 번째로는, 하드웨어 지갑에서 자신의 개인키로 어플리케이션(20)의 Nonce를 암호화하여 하드웨어 지갑의 Serial Number와 함께 어플리케이션으로 전송하는 단계(S13)로서, 상기 하드웨어 지갑(30)이 전송한 Nonce와 동일하면 어플리케이션(20)이 변조되지 않은 신뢰할 수 있는 어플리케이션(20)임을 알 수 있고, 하드웨어 지갑

(30)은 자신의 개인키로 어플리케이션(20)의 Nonce를 암호화하여 하드웨어 지갑(30)의 Serial Number와 함께 어플리케이션(20)으로 전송하는 것이다.

[0048] 아홉 번째로는, 어플리케이션에서 하드웨어 지갑의 공개키를 찾고, 공개키를 이용해 하드웨어 지갑(30)의 개인키로 암호화된 어플리케이션(20)의 Nonce를 복호화하는 단계(S14, S15)로서, 상기 어플리케이션(20)은 하드웨어 지갑(30)의 Serial Number를 이용해 하드웨어 지갑(30)의 공개키를 찾고, 공개키를 이용해 하드웨어 지갑(30)의 개인키로 암호화된 어플리케이션(20)의 Nonce를 복호화하여 자신이 전송한 Nonce와 동일하면 변조되지 않은 신뢰할 수 있는 하드웨어 지갑(30)임을 아는 것이다.

[0049] 상술한 바와 같은, 하드웨어 지갑과 어플리케이션 간의 증명 방법을 사용하기 위해서는 하드웨어 지갑 제조사의 서버, 하드웨어 지갑과 연동하려는 서드 파티인 어플리케이션, 하드웨어 지갑이 있어야 하는 것이다.

[0050] 또한, 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법에서, 서버와 어플리케이션 간과, 어플리케이션과 하드웨어 지갑 간의 신뢰 관계는 Nonce 값의 암호화, 복호화를 통해 형성하는 것이다.

[0051] 상술한 바와 같은, 서드 파티 환경에서 하드웨어 지갑과 어플리케이션 간의 증명 방법은 하드웨어 지갑의 펌웨어 또는 어플리케이션 변조를 통한 암호화폐 해킹을 방어하는 기술로 사용할 수 있는 것이다.

[0052] 도면과 명세서에서 최적의 실시예가 개시되었으며, 여기서 사용된 용어들은 단지 본 발명을 설명하기 위한 목적에서 사용된 것이며, 의미한정이나 특허청구범위에 기재된 본 발명의 범위를 제한하기 위하여 사용된 것은 아니다. 그러므로 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능할 것이며, 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

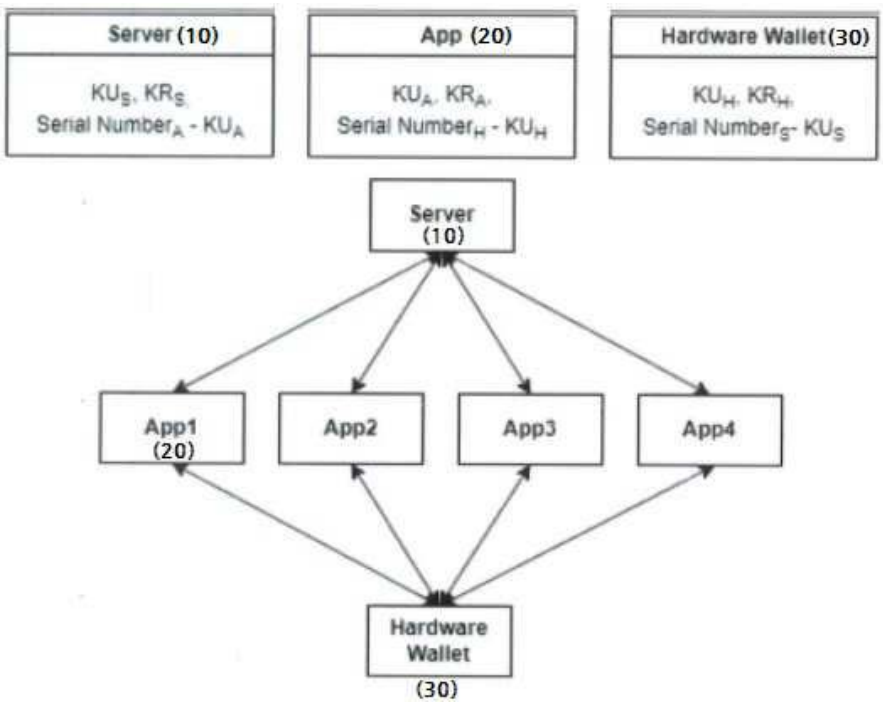
부호의 설명

[0053] 10 : 서버(Server) 20 : 어플리케이션(App)

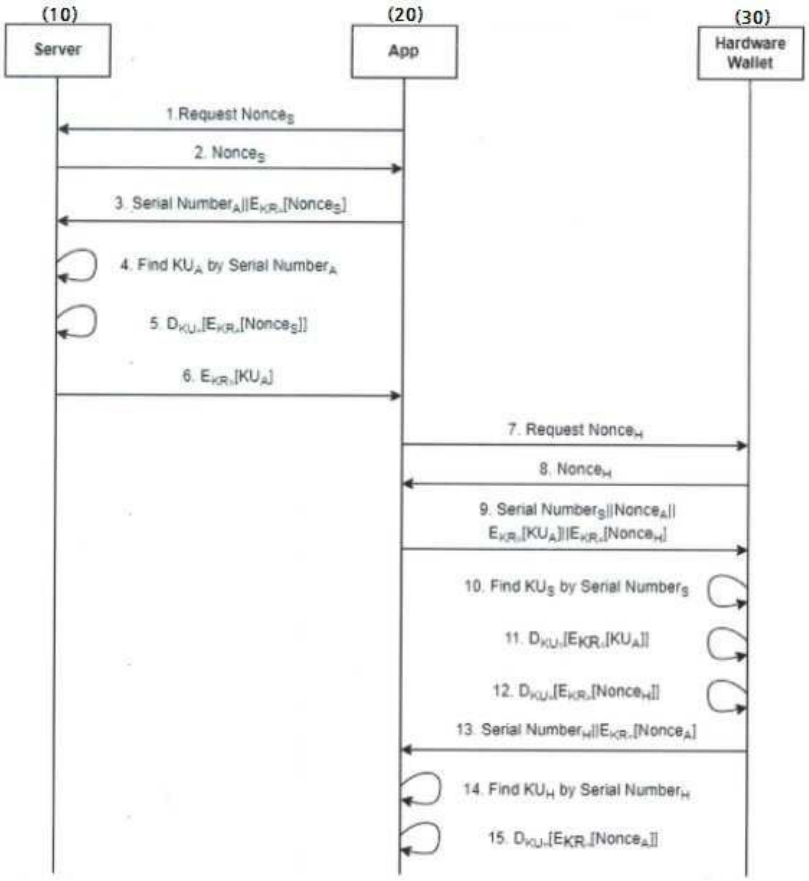
30 : 하드웨어 지갑(Hardware Wallet)

도면

도면1



도면2


(10)
Server
(20)
App
(30)
Hardware Wallet
1.Request Nonce$_S$
2. Nonce$_S$
3. Serial Number$_A$||E$_{KR_A}$[Nonce$_S$]
4. Find KU$_A$ by Serial Number$_A$
5. D$_{KU_A}$[E$_{KR_A}$[Nonce$_S$]]
6. E$_{KR_S}$[KU$_A$]
7. Request Nonce$_H$
8. Nonce$_H$
9. Serial Number$_S$||Nonce$_A$||
E$_{KR_S}$[KU$_A$]||E$_{KR_A}$[Nonce$_H$]
10. Find KU$_S$ by Serial Number$_S$
11. D$_{KU_S}$[E$_{KR_S}$[KU$_A$]]
12. D$_{KU_A}$[E$_{KR_A}$[Nonce$_H$]]
13. Serial Number$_H$||E$_{KR_A}$[Nonce$_A$]
14. Find KU$_H$ by Serial Number$_H$
15. D$_{KU_H}$[E$_{KR_H}$[Nonce$_A$]]