



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0089491
(43) 공개일자 2020년07월27일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) H04L 29/08 (2006.01)
H04W 12/04 (2009.01)
(52) CPC특허분류
H04L 9/0838 (2013.01)
H04L 67/02 (2013.01)
(21) 출원번호 10-2019-0006295
(22) 출원일자 2019년01월17일
심사청구일자 없음

(71) 출원인
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
임태형
경기도 수원시 영통구 삼성로 129(매탄동)
신인영
경기도 수원시 영통구 삼성로 129(매탄동)
(뒷면에 계속)
(74) 대리인
리앤목특허법인

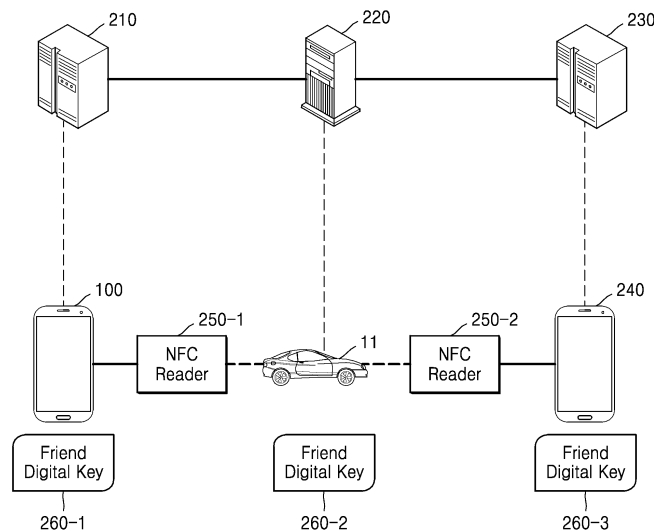
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 공유된 디지털 키를 관리하기 위한 장치 및 방법

(57) 요약

본 개시는 공유된 디지털 키를 관리하는 방법에 관한 것으로, 본 개시의 다양한 실시 예에 따른 디지털 키를 관리하는 전자 디바이스의 동작 방법은, 공유된 디지털 키를 관리하기 위한 요청 메시지에 대한 응답 메시지를 수신하는 단계; 수신된 응답 메시지에 포함된 정보를 확인하는 단계; 및 확인된 정보에 기초하여 공유된 디지털 키를 관리하는 단계를 포함할 수 있다.

대표도 - 도2



(52) CPC특허분류

H04L 9/0891 (2013.01)

H04W 12/04033 (2019.01)

H04L 2209/80 (2013.01)

(72) 발명자

이덕기

경기도 수원시 영통구 삼성로 129(매탄동)

이종효

경기도 수원시 영통구 삼성로 129(매탄동)

정수연

경기도 수원시 영통구 삼성로 129(매탄동)

명세서

청구범위

청구항 1

디지털 키를 관리하는 전자 디바이스의 동작 방법에 있어서,
공유된 디지털 키를 관리하기 위한 요청 메시지에 대한 응답 메시지를 수신하는 단계;
상기 수신된 응답 메시지에 포함된 정보를 확인하는 단계; 및
상기 확인된 정보에 기초하여 상기 공유된 디지털 키를 관리하는 단계를 포함하는, 방법.

청구항 2

제1항에 있어서,
상기 요청 메시지는, 상기 공유된 디지털 키의 정보, 요청 정보, 라우팅 정보, 또는 상기 요청 메시지를 송신하는 디바이스의 서명 중 적어도 하나를 포함하고,
상기 응답 메시지는, 상기 공유된 디지털 키의 정보, 응답 정보, 라우팅 정보, 또는 상기 응답 메시지를 송신하는 디바이스의 서명 중 적어도 하나를 포함하는, 방법.

청구항 3

제2항에 있어서,
상기 요청 정보는, 상기 공유된 디지털 키의 관리를 요청하는 정보를 포함하고,
상기 응답 정보는, 상기 공유된 디지털 키의 관리에 대한 결과를 포함하고,
상기 공유된 디지털 키의 관리는, 상기 공유된 디지털 키의 삭제 또는 갱신 중 적어도 하나를 포함하는, 방법.

청구항 4

제3항에 있어서,
상기 공유된 디지털 키의 삭제는, 상기 공유된 디지털 키의 공유 권한의 삭제를 포함하고,
상기 공유된 디지털 키의 갱신은, 상기 공유된 디지털 키의 사용 기한 또는 사용 권한에 관한 정보를 갱신하는 것을 나타내는 방법.

청구항 5

제3항에 있어서,
상기 공유된 디지털 키의 관리에 대한 정보를 제3 전자 디바이스로 송신하는 단계를 더 포함하는, 방법.

청구항 6

제3항에 있어서,
상기 요청 메시지 또는 상기 응답 메시지는, NFC(near field communication)를 이용한 통신 방식 또는

HTTP(hypertext transfer protocol)를 이용한 통신 방식을 통해 송신되고,

상기 HTTP를 이용한 통신 방식이 사용되는 경우, 상기 요청 메시지 또는 상기 응답 메시지는, 제1 백엔드 서버 또는 제2 백엔드 서버를 통해 송신되는, 방법.

청구항 7

제6항에 있어서,

상기 공유된 디지털 키를 관리하기 위한 요청 메시지를 생성하는 단계;

상기 생성된 요청 메시지를 타겟 디바이스로 송신하는 단계를 더 포함하는, 방법.

청구항 8

제6항에 있어서,

상기 제1 백엔드 서버에 의해 상기 공유된 디지털 키의 관리가 트리거링되는 경우,

상기 요청 메시지는, 상기 제1 백엔드 서버에서 생성되고,

상기 생성된 요청 메시지는, 상기 제2 백엔드 서버로 송신되고,

상기 응답 메시지는, 상기 제2 백엔드 서버로 송신된 요청 메시지에 기초하여 변경된 요청 메시지에 대한 응답 메시지인, 방법.

청구항 9

제6항에 있어서,

상기 제2 백엔드 서버에 의해 상기 공유된 디지털 키의 관리가 트리거링되는 경우,

상기 요청 메시지는, 상기 제2 백엔드 서버에 의해 생성되고,

상기 생성된 요청 메시지는, 타겟 디바이스로 송신되고,

상기 응답 메시지는, 상기 타겟 디바이스로 송신된 요청 메시지에 대한 응답 메시지인, 방법.

청구항 10

타겟 디바이스의 디지털 키 관리 방법에 있어서,

공유된 디지털 키를 관리하기 위한 요청 메시지에 포함된 정보를 확인하는 단계;

상기 확인된 정보에 기초하여 상기 요청 메시지에 대한 응답 메시지를 생성하는 단계; 및

상기 생성된 응답 메시지를 송신하는 단계를 포함하는, 방법.

청구항 11

제10항에 있어서,

상기 공유된 디지털 키를 관리하기 위한 요청 메시지를 수신하는 단계를 더 포함하고,

상기 요청 메시지는, 상기 공유된 디지털 키의 정보, 요청 정보, 라우팅 정보, 또는 상기 요청 메시지를 송신하는 디바이스의 서명 중 적어도 하나를 포함하고,

상기 응답 메시지는, 상기 공유된 디지털 키의 정보, 응답 정보, 라우팅 정보, 또는 상기 응답 메시지를 송신하

는 디바이스의 서명 중 적어도 하나를 포함하는, 방법.

청구항 12

전자 디바이스에 있어서,

공유된 디지털 키를 관리하기 위한 요청 메시지에 대한 응답 메시지를 수신하는 통신부; 및

상기 수신된 응답 메시지에 포함된 정보를 확인하고,

상기 확인된 정보에 기초하여 상기 공유된 디지털 키를 관리하는 적어도 하나의 프로세서를 포함하는, 전자 디바이스.

청구항 13

제12항에 있어서,

상기 요청 메시지는, 상기 공유된 디지털 키의 정보, 요청 정보, 라우팅 정보, 또는 상기 요청 메시지를 송신하는 디바이스의 서명 중 적어도 하나를 포함하고,

상기 응답 메시지는, 상기 공유된 디지털 키의 정보, 응답 정보, 라우팅 정보, 또는 상기 응답 메시지를 송신하는 디바이스의 서명 중 적어도 하나를 포함하는, 전자 디바이스.

청구항 14

제13항에 있어서,

상기 요청 정보는, 상기 공유된 디지털 키의 관리를 요청하는 정보를 포함하고,

상기 응답 정보는, 상기 공유된 디지털 키의 관리에 대한 결과를 포함하고,

상기 공유된 디지털 키의 관리는, 상기 공유된 디지털 키의 삭제 또는 갱신 중 적어도 하나를 포함하는, 전자 디바이스.

청구항 15

제14항에 있어서,

상기 공유된 디지털 키의 삭제는, 상기 공유된 디지털 키의 공유 권한의 삭제를 포함하고,

상기 공유된 디지털 키의 갱신은, 상기 공유된 디지털 키의 사용 기한 또는 사용 권한에 관한 정보를 갱신하는 것을 나타내는, 전자 디바이스.

청구항 16

제14항에 있어서,

상기 적어도 하나의 프로세서는,

상기 공유된 디지털 키의 관리에 대한 정보를 제3 전자 디바이스로 송신하는, 전자 디바이스.

청구항 17

제14항에 있어서,

상기 요청 메시지 또는 상기 응답 메시지는, NFC(near field communication)를 이용한 통신 방식 또는 HTTP(hypertext transfer protocol)를 이용한 통신 방식을 통해 송신되고,

상기 HTTP를 이용한 통신 방식이 사용되는 경우, 상기 요청 메시지 또는 상기 응답 메시지는, 제1 백엔드 서버 또는 제2 백엔드 서버를 통해 송신되는, 전자 디바이스.

청구항 18

제17항에 있어서,

상기 적어도 하나의 프로세서는,

상기 공유된 디지털 키를 관리하기 위한 요청 메시지를 생성하고,

상기 생성된 요청 메시지를 타겟 디바이스로 송신하는 단계를 더 포함하는, 전자 디바이스.

청구항 19

제17항에 있어서,

상기 제1 백엔드 서버에 의해 상기 디지털 키의 관리가 트리거링되는 경우,

상기 요청 메시지는, 상기 제1 백엔드 서버에서 생성되고,

상기 생성된 요청 메시지는, 상기 제2 백엔드 서버로 송신되고,

상기 응답 메시지는, 상기 제2 백엔드 서버로 송신된 요청 메시지에 기초하여 변경된 요청 메시지에 대한 응답 메시지인, 전자 디바이스.

청구항 20

제17항에 있어서,

상기 제2 백엔드 서버에 의해 상기 공유된 디지털 키의 관리가 트리거링되는 경우,

상기 요청 메시지는, 상기 제2 백엔드 서버에 의해 생성되고,

상기 생성된 요청 메시지는, 타겟 디바이스로 송신되고,

상기 응답 메시지는, 상기 타겟 디바이스로 송신된 요청 메시지에 대한 응답 메시지인, 전자 디바이스.

발명의 설명

기술 분야

[0001] 본 개시(disclosure)는 공유된 디지털 키를 관리하기 위한 장치 및 방법에 관한 것이다.

배경 기술

[0002] 스마트 폰, 태블릿 PC와 같은 개인화된 전자 기기가 보급됨에 따라, 디지털화된 가상의 키(즉, 디지털 키)를 이용한 보안, 인증 등을 수행하기 위한 기술이 개발되고 있다. 이러한 디지털 키 기술의 한 방안으로, NFC(Near Field Communication)와 같은 무선 통신 기술을 사용하여 디지털 키를 모바일 디바이스, 예를 들어, 스마트 폰에 통합하는 형태의 기술이 개발되고 있다.

[0003] 디지털 키가 모바일 디바이스에 삽입됨으로써, 모바일 디바이스의 사용자는 물리적 키를 대체하는 디지털 키를 이용하여 문을 열고 닫을 수 있다. 또한, 디지털 키의 기능이 보다 확장됨으로써, 모바일 디바이스의 사용자는 디바이스로의 접근 및 디바이스의 제어를 위해 디지털 키를 이용할 수 있다.

[0004] 디지털 키의 사용은 사용자 편의 및 산업적 효과에 있어 큰 개선을 가져올 수 있는 반면, 보안에 대한 우려 역

시 제기되고 있다. 전자 디바이스와 결합이 필요한 디지털 키의 특성 상, 전자 디바이스에 대한 해킹과 같은 위험에 노출될 수 있다. 따라서, 보안 수준이 높은 영역에서의 디지털 키의 관리가 필요하다.

발명의 내용

해결하려는 과제

[0005] 본 개시의 다양한 실시 예는 공유된 디지털 키를 관리하기 위한 장치 및 방법을 제공한다.

과제의 해결 수단

[0006] 본 개시의 다양한 실시 예에 따르면, 전자 디바이스의 동작 방법은, 공유된 디지털 키를 관리하기 위한 요청 메시지에 대한 응답 메시지를 수신하는 단계와, 수신된 응답 메시지에 포함된 정보를 확인하는 단계와, 확인된 정보에 기초하여 공유된 디지털 키를 관리하는 단계를 포함할 수 있다.

[0007] 본 개시의 다양한 실시 예에 따르면, 타겟 디바이스의 동작 방법은, 공유된 디지털 키를 관리하기 위한 요청 메시지에 포함된 정보를 확인하는 단계와, 확인된 정보에 기초하여 상기 요청 메시지에 대한 응답 메시지를 생성하는 단계와, 생성된 응답 메시지를 송신하는 단계를 포함할 수 있다.

[0008] 본 개시의 다양한 실시 예에 따르면, 전자 디바이스는, 공유된 디지털 키를 관리하기 위한 요청 메시지에 대한 응답 메시지를 수신하는 통신부; 및 수신된 응답 메시지에 포함된 정보를 확인하고, 확인된 정보에 기초하여 공유된 디지털 키를 관리하는 적어도 하나의 프로세서를 포함할 수 있다.

도면의 간단한 설명

[0009] 도 1은 본 개시의 다양한 실시 예들에 따른 디지털 키가 적용되는 환경을 설명하기 위한 도면이다.

도 2는 본 개시의 다양한 실시 예들에 따른 디지털 키를 이용한 서비스를 구현하기 위한 시스템을 설명하기 위한 도면이다.

도 3은 본 개시의 다양한 실시 예들에 따른 공유된 디지털 키의 관리 방법을 개략적으로 설명하기 위한 시퀀스 다이어그램이다.

도 4는 본 개시의 다양한 실시 예들에 따른 요청 메시지 및 응답 메시지에 포함된 정보의 예시이다.

도 5는 본 개시의 다양한 실시 예들에 따른 전자 디바이스의 동작 과정의 순서도를 도시한 도면이다.

도 6은 본 개시의 다양한 실시 예들에 따른 타겟 디바이스의 동작 과정의 순서도를 도시한 도면이다.

도 7은 본 개시의 다양한 실시 예들에 따른 전자 디바이스에 의해 개시(initiated) 또는 트리거링(triggered)된 디지털 키 관리 방법을 개략적으로 설명하기 위한 시퀀스 다이어그램이다.

도 8은 본 개시의 다양한 실시 예들에 따른 타겟 디바이스에 의해 개시 또는 트리거링된 디지털 키 관리 방법을 개략적으로 설명하기 위한 시퀀스 다이어그램이다.

도 9는 본 개시의 다양한 실시 예들에 따른 제1 백엔드 서버에 의해 개시 또는 트리거링된 디지털 키 관리 방법을 개략적으로 설명하기 위한 시퀀스 다이어그램이다.

도 10은 본 개시의 다양한 실시 예들에 따른 제2 백엔드 서버에 의해 개시 또는 트리거링된 디지털 키 관리 방법을 개략적으로 설명하기 위한 시퀀스 다이어그램이다.

도 11은 본 개시의 다양한 실시 예들에 따른 전자 디바이스의 구성을 도시한 도면이다.

도 12는 본 개시의 다양한 실시 예들에 따른 타겟 디바이스의 구성을 도시한 도면이다.

도 13은 본 개시의 다양한 실시 예들에 따른 보안 요소의 구성을 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0010] 아래에서는 첨부한 도면을 참조하여 본 개시가 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 개시의 실시예를 상세히 설명한다. 그러나 본 개시는 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 또한, 도면에서 본 개시를 명확하게 설명하기 위해서 설명과 관

계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

- [0011] 본 개시의 일부 실시예는 기능적인 블록 구성들 및 다양한 처리 단계들로 나타내어질 수 있다. 이러한 기능 블록들의 일부 또는 전부는, 특정 기능들을 실행하는 다양한 개수의 하드웨어 및/또는 소프트웨어 구성들로 구현될 수 있다. 예를 들어, 본 개시의 기능 블록들은 하나 이상의 마이크로프로세서들에 의해 구현되거나, 소정의 기능을 위한 회로 구성들에 의해 구현될 수 있다. 또한, 예를 들어, 본 개시의 기능 블록들은 다양한 프로그래밍 또는 스크립팅 언어로 구현될 수 있다. 기능 블록들은 하나 이상의 프로세서들에서 실행되는 알고리즘으로 구현될 수 있다. 또한, 본 개시는 전자적인 환경 설정, 신호 처리, 및/또는 데이터 처리 등을 위하여 종래 기술을 채용할 수 있다.
- [0012] 또한, 도면에 도시된 구성 요소들 간의 연결 선 또는 연결 부재들은 기능적인 연결 및/또는 물리적 또는 회로적 연결들을 예시적으로 나타낸 것일 뿐이다. 실제 장치에서는 대체 가능하거나 추가된 다양한 기능적인 연결, 물리적인 연결, 또는 회로 연결들에 의해 구성 요소들 간의 연결이 나타내어질 수 있다.
- [0013] 이하 첨부된 도면을 참고하여 본 개시를 상세히 설명하기로 한다.
- [0015] 도 1은 본 개시의 다양한 실시 예들에 따른 디지털 키가 적용되는 환경을 설명하기 위한 도면이다.
- [0016] 도 1을 참고하면, 오너 디바이스(100), 오너 디바이스(100)의 사용자(1) 및 오너 디바이스(100)에 저장된 디지털 키를 이용하여 접근 및 제어를 수행하기 위한 전자 디바이스들(11, 12, 13)이 개시되어 있다. 다양한 실시 예에서, 오너 디바이스(100)를 사용하는 사용자(1)는 오너(owner)로 지칭될 수 있다.
- [0017] 오너 디바이스(100)는 개인화된 모바일 디바이스를 포함할 수 있으나 이에 한정되지 않고, 다양한 종류의 전자 디바이스를 포함할 수 있다. 예를 들어, 오너 디바이스(100)는 스마트폰, 태블릿 PC, PC, 카메라 및 웨어러블 장치 등을 포함할 수 있다. 오너 디바이스(100)는, 전자 디바이스들(11, 12, ...)에게 접근하고 전자 디바이스들(11, 12, ...)을 제어하기 위한 디지털 키를 생성, 삭제, 관리 등의 처리를 수행할 수 있으며, 디지털 키에 대한 인증을 수행할 수 있다.
- [0018] 전자 디바이스들(11, 12, ...)은, 오너 디바이스(100)와 상호 작용하여 디지털 키의 생성을 위한 동작을 수행할 수 있고, 디지털 키를 이용하여 제어되고 접근 될 수 있다.
- [0019] 일 예로서, 오너 디바이스(100)는 자동차에 탑재되는 전자 디바이스(11)와 상호 작용하기 위한 디지털 키를 저장할 수 있다. 오너 디바이스(100)는 저장된 디지털 키를 이용하여, 자동차의 다양한 동작을 제어할 수 있다. 예를 들어, 오너 디바이스(100)는 디지털 키를 이용하여, 자동차의 문을 개폐할 수 있고, 시동을 걸 수도 있으며, 자동차에 탑재된 다양한 디바이스들을 제어할 수도 있다. 나아가, 자동 주차 시스템과 같은 자율 주행과 관련한 동작을 제어할 수도 있다.
- [0020] 다른 예로서, 오너 디바이스(100)는, 도어락(12)과 상호 작용하기 위한 디지털 키를 저장할 수 있다. 오너 디바이스(100)는 저장된 디지털 키를 이용하여 문을 개폐할 수 있다.
- [0021] 오너 디바이스(100)가 디지털 키를 이용하여 제어할 수 있는 전자 디바이스는 도 1에 도시된 예에 제한되지 않으며, 다양한 전자 디바이스들에 디지털 키 기술이 적용될 수 있다. 이하에서는 설명의 편의를 위하여, 오너 디바이스(100)가 자동차에 탑재되는 전자 디바이스(11)와 상호 작용하는 경우를 예로 들어 설명한다. 그러나, 이하의 설명은 오너 디바이스(100)가 자동차의 전자 디바이스(11) 이외의 다양한 전자 디바이스와 상호 작용하는 경우에도 적용될 수 있다.
- [0023] 도 2는 본 개시의 다양한 실시 예들에 따른 디지털 키를 이용한 서비스를 구현하기 위한 시스템을 설명하기 위한 도면이다.
- [0024] 도 2를 참고하면, 오너 디바이스 백엔드 서버(210), 타겟 디바이스 백엔드 서버(220), 다른 사용자의 전자 디바이스에 대한 백엔드 서버(230), 오너 디바이스(100), 제1 NFC(near field communication) 리더기(reader)(250-1), 전자 디바이스(11), 제2 NFC 리더기(250-2), 다른 사용자의 전자 디바이스(240), 다른 사용자의 디지털 키들(260-1, 260-2 및 260-3)이 도시된다. 본 개시의 다양한 실시 예들에서, 전자 디바이스(11)는 타겟 디바이스(11)로 지칭될 수 있다.

- [0025] 도 2에 도시되지는 아니하였으나, 서비스 제공자 서버는 디지털 키 서비스를 사용자에게 제공하고자 하는 서비스 제공자에 의해 운영되는 서버이다. 서비스 제공자는, 예를 들어, 자동차, 호텔, 집, 빌딩 등과 관련된 서비스를 제공하는 사업자를 지칭하며, 주된 서비스에 따른 부가 서비스로서 사용자에게 디지털 키 서비스를 제공할 수 있다. 예를 들어, 자동차 회사는 자동차를 판매하고, 호텔, 집, 빌딩 회사는 호텔, 집, 빌딩 관련 서비스를 제공한다. 예를 들어, 서비스 제공자 서버는 자동차 회사에 의해 운영될 수 있다. 예를 들어, 서비스 제공자 서버는 문 개폐, 시동, 제어 등과 같은 액세스 기능을 위해 디지털 키 서비스를 제공할 수 있다.
- [0026] 서비스 제공자 서버는 사용자의 ID, 패스워드 와 같은 사용자 계정 정보, 판매 상품 또는 서비스 정보와 같은 사용자 정보 데이터베이스를 포함할 수 있다. 예를 들어, 자동차 회사는 자동차를 판매하면 사용자의 ID, 패스워드, 판매한 자동차 식별 번호, 디지털 키 서비스 사용 유무 등에 대한 정보를 저장할 수 있다.
- [0027] 오너 디바이스 백엔드 서버(또는, 백엔드 서버)(210)는 오너 디바이스(100)에게 디지털 키를 안전하게 발급하고 저장할 수 있는 기술 및 서비스를 제공한다. 오너 디바이스 백엔드 서버(210)는, 예를 들어, 오너 디바이스(100)의 제조사(Original Equipment Manufacturer, OEM)에 의해 운영되는 서버이거나, 이동 통신 서비스를 제공하는 통신 회사에 의해 운영되는 서버이거나, 디지털 키 서비스를 제공하는 서비스 제공 업체에 의해 운영되는 서버일 수 있다.
- [0028] 예를 들어, 사용자(1)가 자동차를 구매하고, 오너 디바이스(100) 상에 자동차의 디지털 키를 저장하고자 할 때, 오너 디바이스(100)는 인증 절차를 수행할 수 있다. 예를 들어, 오너 디바이스(100)는 사용자(1)가 유효한 사용자인지, 유효한 자동차인지 여부 등을 확인하는 인증 절차를 수행할 수 있는데, 오너 디바이스 백엔드 서버(210)는 이러한 인증 절차를 지원할 수 있다.
- [0029] 타겟 디바이스 백엔드 서버(220)는 타겟 디바이스와 관련된 디지털 키 서비스를 제공할 수 있다. 예를 들어, 타겟 디바이스 백엔드 서버(220)는 문 개폐, 시동, 제어 등과 같은 액세스 기능을 위한 디지털 키 서비스를 제공할 수 있다. 일 실시 예에서, 타겟 디바이스 백엔드 서버(220)는, 디지털 키 서비스를 사용자에게 제공하고자 하는 서비스 제공자에 의해 운영되는 서버일 수 있다. 보다 구체적으로, 타겟 디바이스(11)의 제조사가 운영하는 서버일 수 있다. 서비스 제공자는, 예를 들어, 자동차, 호텔, 집, 빌딩 등과 관련된 서비스를 제공하는 사업자를 지칭할 수 있으며, 주된 서비스에 따른 부가 서비스로서 사용자에게 디지털 키 서비스를 제공할 수 있다. 예를 들어, 자동차 회사가 자동차를 판매하고, 호텔, 집, 빌딩 회사가 호텔, 집, 빌딩 관련 서비스를 제공하는 경우, 타겟 디바이스 백엔드 서버(220)는, 각각의 자동차 회사 또는 호텔, 집, 빌딩 회사에 의해 운영될 수 있다.
- [0030] 일 실시 예에서, 타겟 디바이스 백엔드 서버(220)는 사용자의 ID, 패스워드 와 같은 사용자 계정 정보, 판매 상품 또는 서비스 정보와 같은 사용자 정보 데이터베이스를 포함할 수 있다. 예를 들어, 자동차 회사는 자동차를 판매하면 사용자의 ID, 패스워드, 판매한 자동차 식별 번호, 디지털 키 서비스 사용 유무 등에 대한 정보를 저장할 수 있다.
- [0031] 일 실시 예에서, 타겟 디바이스 백엔드 서버(220)는 디지털 키 서비스를 사용자에게 제공하기 위하여, 오너 디바이스 백엔드 서버(210)로 디지털 키의 서비스를 위한 정보를 송신할 수도 있다. 또한, 타겟 디바이스 백엔드 서버(220)는 디지털 키 서비스를 다른 사용자(예: 친구)에게 제공하기 위하여, 다른 사용자의 전자 디바이스에 대한 백엔드 서버(230)로 디지털 키의 서비스를 위한 정보를 송신할 수 있다.
- [0032] 다른 사용자의 전자 디바이스에 대한 백엔드 서버(230)는, 오너가 아닌 다른 사용자(예: 친구)의 전자 디바이스(240)의 제조사가 운영하는 서버일 수 있다. 오너 디바이스(100)와, 다른 사용자(예: 친구)의 전자 디바이스(240)의 제조사는 동일할 수도 있고 다를 수도 있다.
- [0033] 전자 디바이스(11)는 서비스 제공자가 사용자에게 판매하는 상품 및 서비스에 상응하는 엔티티(entity)이다. 예를 들어, 전자 디바이스(11)는 자동차, 호텔, 집, 빌딩 등의 게이트를 포함할 수 있다. 보다 구체적으로, 전자 디바이스(11)는 자동차에서 차량 도어, 트렁크 게이트, 주유구 뿐만 아니라, 시동 및 차량 제어를 위한 액세스 게이트 등을 포함할 수 있다.
- [0034] 본 개시의 다양한 실시 예에서, 오너 디바이스(100), 타겟 디바이스(11) 및 다른 사용자의 전자 디바이스(240)는, 다른 사용자의 디지털 키를 공유할 수 있다. 예를 들면, 오너 디바이스는 다른 사용자의 디지털 키(260-1)를 저장할 수 있고, 타겟 디바이스는 다른 사용자의 디지털 키(260-2)를 저장할 수 있고, 다른 사용자는 자신의 디지털 키(260-3)를 저장할 수 있다. 다양한 실시 예에서, 오너 디바이스(100)는 제1 NFC 리더기(250-1)를 통해 타겟 디바이스(11)와 디지털 키를 관리할 수 있다. 다른 사용자의 전자 디바이스(240)는 제2 NFC 리더기

(250-2)를 통해 타겟 디바이스(11)와 디지털 키를 관리할 수 있다.

- [0035] 본 개시의 다양한 실시 예들은, 다른 사용자의 디지털 키가 오너 디바이스(100), 타겟 디바이스(11) 및 다른 사용자의 전자 디바이스(240)에 의해 공유되어 있는 경우, 디바이스들 간 공유된 디지털 키를 관리하기 위한 방법을 설명한다. 즉, 본 개시의 다양한 실시 예들은 타겟 디바이스(11)에 저장된 다른 사용자의 디지털 키(260-2)를 관리하는 방법을 설명한다. 이때, 공유된 디지털 키의 관리는, 공유된 디지털 키의 삭제(revocation) 또는 갱신(update)을 의미할 수 있다. 다양한 실시 예들에서, 상술한 공유된 디지털 키의 관리는, 사용자(1)(예: 오너) 또는 다른 사용자(예: 친구)에 의해 요청(request)될 수 있다. 다양한 실시 예들에서, 상술한 공유된 디지털 키의 관리는 오너 디바이스(100), 다른 사용자의 전자 디바이스(240), 타겟 디바이스(11), 오너 디바이스 백엔드 서버(210), 다른 사용자의 전자 디바이스에 대한 백엔드 서버(230) 또는 타겟 디바이스 백엔드 서버(220)에 의해 개시되거나(initiated) 트리거링(triggered)될 수 있다. 본 개시의 다양한 실시 예들에서, 개시(initiate) 또는 트리거링(triggering)은 공유된 디지털 키의 관리가 시작되는 것을 의미할 수 있다.
- [0036] 본 개시의 다양한 실시 예들에서, 사용자(1)(예: 오너) 또는 다른 사용자(예: 친구)는 타겟 디바이스(11)에 저장된 다른 사용자의 디지털 키(260-2)를 삭제하는 것을 요청할 수 있다. 이 경우, 다른 사용자의 디지털 키(260-2)에 대한 삭제 동작은, 오너 디바이스(100), 다른 사용자의 전자 디바이스(240), 타겟 디바이스(11), 오너 디바이스 백엔드 서버(210), 다른 사용자의 전자 디바이스에 대한 백엔드 서버(230) 또는 타겟 디바이스 백엔드 서버(220)에 의해 개시 또는 트리거링 될 수 있다. 다양한 실시 예에서, 공유된 디지털 키의 삭제는, 다른 사용자에게 공유된 디지털 키의 공유 권한의 삭제를 의미할 수 있다.
- [0037] 본 개시의 다양한 실시 예들에서, 사용자(1)(예: 오너)는 타겟 디바이스(11)에 저장된 다른 사용자의 디지털 키(260-2)를 갱신하는 것을 요청할 수 있다. 이 경우, 다른 사용자의 디지털 키(260-2)에 대한 갱신 동작은, 오너 디바이스(100), 타겟 디바이스(11), 오너 디바이스 백엔드 서버(210) 또는 타겟 디바이스 백엔드 서버(220)에 의해 또는 트리거링 될 수 있다. 다양한 실시 예에서, 공유된 디지털 키의 갱신은, 다른 사용자에게 공유된 디지털 키의 사용 기한의 변경 또는 사용 권한의 변경을 의미할 수 있다. 일 실시 예에서, 공유된 디지털 키의 사용 권한은, 자동차의 문 개폐, 트렁크 문 개폐 또는 자동차의 시동을 거는 것에 대한 권한을 의미할 수 있다. 일 실시 예에서, 공유된 디지털 키의 사용 권한 이외에 대한 갱신 요청은 다른 사용자(예: 친구)에 의해서도 요청될 수 있다. 그러나, 본 개시는 여러 가지 상이한 형태로 구현될 수 있으며, 여기에서 설명되는 실시 예에 한정되지 않는다. 아래에서는, 미리 공유된 디지털 키를 관리하는 방법을 설명한다.
- [0039] 도 3은 본 개시의 다양한 실시 예들에 따른 공유된 디지털 키의 관리 방법을 개략적으로 설명하기 위한 시퀀스 다이어그램이다.
- [0040] 도 3을 참고하면, 전자 디바이스(310)는 오너 디바이스(100) 또는 다른 사용자의 전자 디바이스(240)를 의미할 수 있다. 타겟 디바이스(320)는 전자 디바이스(11)를 의미할 수 있다. 예를 들면, 전자 디바이스(11)는 자동차 또는, 자동차에 탑재되는 전자 장치를 의미할 수 있다. 다양한 실시 예에서, 전자 디바이스(310)는 개시자(initiator)로 지칭될 수 있다.
- [0041] 301 단계에서, 전자 디바이스(310)는 요청 메시지를 생성할 수 있다. 예를 들면, 전자 디바이스(310)는 공유된 디지털 키의 관리를 요청하는 메시지를 생성할 수 있다. 다양한 실시 예에서, 요청 메시지는 공유된 디지털 키에 대한 정보, 요청 정보, 라우팅 정보 또는 요청 메시지를 송신한 발신자의 서명을 포함할 수 있다. 예를 들면, 발신자의 서명은 전자 디바이스(310)의 사용자의 서명을 의미할 수 있다.
- [0042] 303 단계에서, 전자 디바이스(310)는 요청 메시지를 송신할 수 있다. 예를 들면, 전자 디바이스(310)는 생성된 요청 메시지를 타겟 디바이스(320)로 송신할 수 있다.
- [0043] 305 단계에서, 타겟 디바이스(320)는 수신된 요청 메시지를 확인할 수 있다. 예를 들면, 타겟 디바이스(320)는 수신된 요청 메시지에 포함된, 공유된 디지털 키에 대한 정보, 요청 정보 또는 요청 메시지를 송신한 발신자 서명을 확인할 수 있다.
- [0044] 307 단계에서, 타겟 디바이스(320)는 요청에 따른 동작을 수행할 수 있다. 즉, 타겟 디바이스(320)는 요청 메시지에 포함된 정보에 기초하여 공유된 디지털 키 관리를 수행할 수 있다. 예를 들면, 요청 메시지의 요청 정보가, 공유된 디지털 키의 삭제와 관련된 정보를 포함하고 있는 경우, 타겟 디바이스(320)는 타겟 디바이스(320)에 저장된 공유된 디지털 키를 삭제할 수 있다. 요청 메시지의 요청 정보가, 공유된 디지털 키의 갱신과 관련된 정보를 포함하고 있는 경우, 타겟 디바이스(320)는 타겟 디바이스(320)에 저장된 공유된 디지털 키를 갱

신할 수 있다.

- [0045] 309 단계에서, 타겟 디바이스(320)는 응답 메시지를 생성할 수 있다. 다양한 실시 예에서, 응답 메시지는 공유된 디지털 키에 대한 정보, 응답 정보, 라우팅 정보 또는 응답 메시지를 송신한 발신자의 서명을 포함할 수 있다. 예를 들면, 발신자의 서명은 타겟 디바이스(320)의 사용자의 서명을 의미할 수 있다.
- [0046] 311 단계에서, 타겟 디바이스(320)는 응답 메시지를 송신할 수 있다. 예를 들면, 타겟 디바이스(320)는 생성된 응답 메시지를 전자 디바이스(310)로 송신할 수 있다.
- [0047] 313 단계에서, 전자 디바이스(310)는 응답 메시지를 확인할 수 있다. 예를 들면, 전자 디바이스(310)는 응답 메시지에 포함된, 공유된 디지털 키에 대한 정보, 응답 정보 또는 응답 메시지를 송신한 발신자 서명을 확인할 수 있다.
- [0048] 315 단계에서, 전자 디바이스(310)는 응답에 따른 동작을 수행할 수 있다. 예를 들면, 응답 메시지의 응답 정보가, 공유된 디지털 키의 삭제와 관련된 정보를 포함하고 있는 경우, 전자 디바이스(310)는 전자 디바이스(310)에 저장된 공유된 디지털 키를 삭제할 수 있다. 응답 메시지의 응답 정보가, 공유된 디지털 키의 갱신과 관련된 정보를 포함하고 있는 경우, 전자 디바이스(310)는 전자 디바이스(310)에 저장된 공유된 디지털 키를 갱신할 수 있다.
- [0049] 상술한 동작들을 통해, 전자 디바이스(310)와 타겟 디바이스(320)에서, 다른 사용자의 공유된 디지털 키가 관리될 수 있다. 도 4는, 상술한 요청 메시지 및 응답 메시지에 포함된 정보의 의미를 구체적으로 설명한다.
- [0051] 도 4는 본 개시의 다양한 실시 예들에 따른 요청 메시지 및 응답 메시지에 포함된 정보의 예시이다.
- [0052] 도 4를 참고하면, 요청 메시지(410)는 디지털 키 정보(412), 요청 정보(414), 라우팅 정보(416) 및 발신자 서명(418)을 포함할 수 있다. 응답 메시지(420)는 디지털 키 정보(422), 응답 정보(424), 라우팅 정보(426) 및 발신자 서명(428)을 포함할 수 있다.
- [0053] 다양한 실시 예에서, 요청 메시지(410)에 포함된 디지털 키 정보는, 공유된 디지털 키와 관련된 정보를 포함할 수 있다. 예를 들면, 디지털 키 정보는, 공유된 디지털 키의 고유한 식별자(identifier, ID)를 포함할 수 있다. 이러한 식별자를 통해, 공유된 디지털 키는, 다른 디지털 키와 구별될 수 있다.
- [0054] 다양한 실시 예에서, 요청 메시지(410)에 포함된 요청 정보(414)는, 공유된 디지털 키의 관리를 요청하는 정보를 의미할 수 있다. 예를 들면, 공유된 디지털 키의 관리는, 공유된 디지털 키의 삭제 또는 갱신을 의미할 수 있다. 일 실시 예에서, 요청 정보는 공유된 디지털 키를 삭제하기 위한 데이터(revocation_request)를 포함할 수 있다. 다른 실시 예에서, 요청 정보는 공유된 디지털 키를 갱신하기 위한 데이터(update_request)를 포함할 수 있다. 본 개시는 디지털 키의 관리 방법으로, 디지털 키의 삭제 또는 갱신을 설명하나, 본 개시는 이에 한정되지 않는다.
- [0055] 다양한 실시 예에서, 요청 메시지(410)에 포함된 라우팅 정보(416)는 요청 메시지(410)의 전송 경로와 관련된 정보를 포함할 수 있다. 예를 들면, 라우팅 정보(416)는 요청 메시지(410)가 송신되어야 할 목적지에 대한 주소를 포함할 수 있다. 일 실시 예에서, 요청 메시지(410)가 송신되어야 할 목적지에 대한 주소는, 데이터 패킷이 전송되는 패킷 주소를 의미할 수 있다.
- [0056] 다양한 실시 예에서, 요청 메시지(410)에 포함된 발신자 서명(418)은, 요청 메시지를 송신한 발신자의 서명과 관련된 정보를 포함할 수 있다. 예를 들면, 요청 메시지(410)가 전자 디바이스(310)에서 송신되는 경우, 발신자 서명(418)은 전자 디바이스(310)의 사용자의 서명을 의미할 수 있다. 다양한 실시 예에서, 요청 메시지(410)를 수신한 디바이스는, 요청 메시지(410)에 포함된 발신자 서명(418)을 통해 요청 메시지(410)가 올바른 발신자에 의해 송신되었는지 여부를 확인할 수 있다.
- [0057] 다양한 실시 예에서, 응답 메시지(420)에 포함된 디지털 키 정보는, 공유된 디지털 키와 관련된 정보를 포함할 수 있다. 예를 들면, 디지털 키 정보는, 공유된 디지털 키의 고유한 식별자를 포함할 수 있다. 이러한 식별자를 통해, 공유된 디지털 키는, 다른 디지털 키와 구별될 수 있다.
- [0058] 다양한 실시 예에서, 응답 메시지(420)에 포함된 응답 정보(424)는, 공유된 디지털 키의 관리에 대한 응답을 의미할 수 있다. 예를 들면, 공유된 디지털 키의 관리에 대한 응답은, 공유된 디지털 키의 삭제 또는 갱신 수행의 결과를 의미할 수 있다. 즉, 요청 메시지(410)에 포함된 요청 정보(414)가 공유된 디지털 키의 삭제를 지시하는

경우, 타겟 디바이스(320)는 공유된 디지털 키를 삭제하고, 이에 대한 결과를 응답 정보(424)에 포함시킬 수 있다. 요청 메시지(410)에 포함된 요청 정보(414)가 공유된 디지털 키의 갱신을 지시하는 경우, 타겟 디바이스(320)는 공유된 디지털 키를 갱신하고, 이에 대한 결과를 응답 정보(424)에 포함시킬 수 있다.

[0059] 일 실시 예에서, 응답 정보(424)는 공유된 디지털 키의 삭제에 대한 결과를 나타내는 데이터(revocation_attestation)를 포함할 수 있다. 다른 실시 예에서, 응답 정보(424)는 공유된 디지털 키의 갱신에 대한 결과를 나타내는 데이터(update_confirmation)를 포함할 수 있다. 본 개시는 디지털 키의 관리 방법으로, 디지털 키의 삭제 또는 갱신을 설명하나, 본 개시는 이에 한정되지 않는다.

[0060] 다양한 실시 예에서, 응답 메시지(420)에 포함된 라우팅 정보(426)는 응답 메시지(420)의 전송 경로와 관련된 정보를 포함할 수 있다. 예를 들면, 라우팅 정보(426)는 응답 메시지(420)가 송신되어야 할 목적지에 대한 주소를 포함할 수 있다. 일 실시 예에서, 응답 메시지(420)가 송신되어야 할 목적지에 대한 주소는, 데이터 패킷이 전송되는 패킷 주소를 의미할 수 있다.

[0061] 다양한 실시 예에서, 응답 메시지(420)에 포함된 발신자 서명(428)은, 응답 메시지를 송신한 발신자의 서명과 관련된 정보를 포함할 수 있다. 예를 들면, 응답 메시지(420)가 타겟 디바이스(320)에서 송신되는 경우, 발신자 서명(428)은 타겟 디바이스(320)의 사용자의 서명을 의미할 수 있다. 다양한 실시 예에서, 응답 메시지(420)를 수신한 디바이스는, 응답 메시지(420)에 포함된 발신자 서명(428)을 통해 응답 메시지(420)가 올바른 발신자에 의해 송신되었는지 여부를 확인할 수 있다. 본 개시는, 요청 메시지(410)가 디지털 키 정보(412), 요청 정보(414), 라우팅 정보(416) 및 발신자 서명(418)을 포함할 수 있고, 응답 메시지(420)가 디지털 키 정보(422), 응답 정보(424), 라우팅 정보(426) 및 발신자 서명(428)을 포함할 수 있다고 설명하고 있으나, 이에 한정되지 않는다.

[0063] 도 5는 본 개시의 다양한 실시 예들에 따른 전자 디바이스의 동작 과정의 순서도를 도시한 도면이다. 이하, 전자 디바이스(310)는 오너 디바이스(100) 또는 다른 사용자의 전자 디바이스(240)를 의미할 수 있다. 또한, 제1 백엔드 서버는 전자 디바이스(310)의 백엔드 서버를 의미할 수 있고, 제2 백엔드 서버는 타겟 디바이스(320)의 백엔드 서버를 의미할 수 있다. 여기서, 전자 디바이스(310)의 백엔드 서버는, 오너 디바이스의 백엔드 서버(210) 또는 다른 사용자의 전자 디바이스에 대한 백엔드 서버(230)를 의미할 수 있다.

[0064] 도 5를 참고하면, 501 단계에서, 전자 디바이스(310)는 공유된 디지털 키를 관리하기 위한 요청 메시지에 대한 응답 메시지를 수신할 수 있다. 도 5에는 도시되지 아니하였으나, 일 실시 예에서, 전자 디바이스(310)에 의해 공유된 디지털 키의 관리가 개시 또는 트리거링되는 경우, 전자 디바이스(310)는 공유된 디지털 키를 관리하기 위한 요청 메시지를 생성하고, 생성된 요청 메시지를 타겟 디바이스(320)로 송신할 수 있다. 다른 실시 예에서, 타겟 디바이스(320)에 의해 공유된 디지털 키의 관리가 개시 또는 트리거링되는 경우, 전자 디바이스(310)에 의한 요청 메시지 생성 및 송신 동작이 생략될 수 있다. 또 다른 실시 예에서, 제1 백엔드 서버에 의해 공유된 디지털 키의 관리가 개시 또는 트리거링되는 경우, 제1 백엔드 서버가 요청 메시지를 생성할 수 있다. 또 다른 실시 예에서, 제2 백엔드 서버에 의해 공유된 디지털 키의 관리가 개시 또는 트리거링되는 경우, 제2 백엔드 서버가 요청 메시지를 생성할 수 있다. 이후, 전자 디바이스(310)는 공유된 디지털 키를 관리하기 위한 요청 메시지에 대한 응답 메시지를 수신할 수 있다.

[0065] 503 단계에서, 전자 디바이스(310)는 수신된 응답 메시지에 포함된 정보를 확인할 수 있다. 예를 들면, 수신된 응답 메시지는, 디지털 키 정보, 응답 정보, 라우팅 정보 또는 발신자 서명 중 적어도 하나를 포함할 수 있다. 다양한 실시 예에서, 응답 정보는, 공유된 디지털 키의 관리에 대한 응답을 의미할 수 있다. 예를 들면, 공유된 디지털 키의 관리에 대한 응답은, 공유된 디지털 키의 삭제 또는 갱신 수행의 결과를 의미할 수 있다. 또한, 전자 디바이스(310)는 발신자 서명을 통해 응답 메시지가 올바른 발신자에 의해 송신되었는지 여부를 확인할 수 있다.

[0066] 505 단계에서, 전자 디바이스(310)는 확인된 정보에 기초하여 공유된 디지털 키를 관리할 수 있다. 예를 들면, 응답 메시지의 응답 정보가, 공유된 디지털 키의 삭제와 관련된 정보를 포함하고 있는 것으로 확인되는 경우, 전자 디바이스(310)는 전자 디바이스(310)에 저장된 공유된 디지털 키를 삭제할 수 있다. 응답 메시지의 응답 정보가, 공유된 디지털 키의 갱신과 관련된 정보를 포함하고 있는 것으로 확인되는 경우, 전자 디바이스(310)는 전자 디바이스(310)에 저장된 공유된 디지털 키를 갱신할 수 있다. 505 단계에서 공유된 디지털 키의 관리 방법으로, 공유된 디지털 키의 삭제 또는 갱신이 설명되어 있으나, 본 개시는 이에 한정되지 않는다.

- [0068] 도 6은 본 개시의 다양한 실시 예들에 따른 타겟 디바이스의 동작 과정의 순서도를 도시한 도면이다. 이하, 전자 디바이스(310)는 오너 디바이스(100) 또는 다른 사용자의 전자 디바이스(240)를 의미할 수 있다. 또한, 제1 백엔드 서버는 전자 디바이스(310)의 백엔드 서버를 의미할 수 있고, 제2 백엔드 서버는 타겟 디바이스(320)의 백엔드 서버를 의미할 수 있다. 여기서, 전자 디바이스(310)의 백엔드 서버는, 오너 디바이스의 백엔드 서버(210) 또는 다른 사용자의 전자 디바이스에 대한 백엔드 서버(230)를 의미할 수 있다.
- [0069] 도 6에는 도시되지 아니하였으나, 일 실시 예에서, 전자 디바이스(310)에 의해 공유된 디지털 키의 관리가 개시 또는 트리거링되는 경우, 타겟 디바이스(320)는 상술한 요청 메시지를 전자 디바이스(310)로부터 수신할 수 있다. 다른 실시 예에서, 타겟 디바이스(320)에 의해 공유된 디지털 키의 관리가 개시 또는 트리거링되는 경우, 601 단계는, 공유된 디지털 키를 관리하는 단계로 대체될 수 있다. 또 다른 실시 예에서, 제1 백엔드 서버에 의해 공유된 디지털 키의 관리가 개시 또는 트리거링되는 경우, 타겟 디바이스(320)는 제1 백엔드 서버에서 송신된 요청 메시지로부터 변경된 요청 메시지를 제2 백엔드 서버로부터 수신할 수 있다. 또 다른 실시 예에서, 제2 백엔드 서버에 의해 공유된 디지털 키의 관리가 개시 또는 트리거링되는 경우, 타겟 디바이스(320)는 제2 백엔드 서버에 의해 생성된 요청 메시지를 수신할 수 있다.
- [0070] 도 6을 참고하면, 601 단계에서, 타겟 디바이스(320)는 공유된 디지털 키를 관리하기 위한 요청 메시지에 포함된 정보를 확인할 수 있다. 예를 들면, 요청 메시지는, 디지털 키 정보, 요청 정보, 라우팅 정보 또는 발신자 서명 중 적어도 하나를 포함할 수 있다. 다양한 실시 예에서, 요청 정보는, 공유된 디지털 키의 관리를 요청하는 정보를 의미할 수 있다. 예를 들면, 공유된 디지털 키의 관리는, 공유된 디지털 키의 삭제 또는 갱신을 의미할 수 있다. 또한, 타겟 디바이스(320)는 발신자 서명을 통해 요청 메시지가 올바른 발신자에 의해 송신되었는지 여부를 확인할 수 있다.
- [0071] 603 단계에서, 타겟 디바이스(320)는 확인된 정보에 기초하여 요청 메시지에 대한 응답 메시지를 생성할 수 있다. 예를 들면, 타겟 디바이스(320)는, 공유된 디지털 키에 대한 정보, 응답 정보, 라우팅 정보 또는 응답 메시지를 송신한 발신자의 서명을 포함하는 응답 메시지를 생성할 수 있다. 다양한 실시 예에서, 응답 정보는, 공유된 디지털 키의 관리에 대한 응답을 의미할 수 있다. 예를 들면, 공유된 디지털 키의 관리에 대한 응답은, 공유된 디지털 키의 삭제 또는 갱신 수행의 결과를 의미할 수 있다. 다양한 실시 예에서, 응답 메시지를 송신한 발신자의 서명은 타겟 디바이스(320)의 사용자 서명을 의미할 수 있다.
- [0072] 605 단계에서, 타겟 디바이스(320)는 생성된 응답 메시지를 송신할 수 있다. 일 실시 예에서, NFC를 이용한 통신 방식이 사용되는 경우, 생성된 응답 메시지는 전자 디바이스(310)으로 직접 송신될 수 있다. 다른 실시 예에서, HTTP(hypertext transfer protocol)를 이용한 통신 방식이 사용되는 경우, 생성된 응답 메시지는 제2 백엔드 서버를 통해 제1 백엔드 서버 또는 전자 디바이스(310)로 송신될 수 있다. 이하, 도 7 내지 도 10은, 공유된 디지털 키의 관리를 개시 또는 트리거링하는 디바이스에 따른, 디지털 키 관리 동작의 실시 예들을 도시한다.
- [0074] 도 7은 본 개시의 다양한 실시 예들에 따른 전자 디바이스에 의해 개시 또는 트리거링된 디지털 키 관리 방법을 개략적으로 설명하기 위한 시퀀스 다이어그램이다.
- [0075] 도 7을 참고하면, 전자 디바이스(310)는 오너 디바이스(100) 또는 다른 사용자의 전자 디바이스(240)를 의미할 수 있다. 타겟 디바이스(320)는 전자 디바이스(11)를 의미할 수 있다. 예를 들면, 전자 디바이스(11)는 자동차 또는, 자동차에 탑재되는 전자 장치를 의미할 수 있다. 또한, 제1 백엔드 서버(710)는 전자 디바이스(310)의 백엔드 서버를 의미할 수 있고, 제2 백엔드 서버(720)는 타겟 디바이스(320)의 백엔드 서버를 의미할 수 있다. 여기서, 전자 디바이스(310)의 백엔드 서버는, 오너 디바이스의 백엔드 서버(210) 또는 다른 사용자의 전자 디바이스에 대한 백엔드 서버(230)를 의미할 수 있다.
- [0076] 701 단계에서, 전자 디바이스(310)는 요청 메시지를 생성할 수 있다. 즉, 전자 디바이스(310)는 다른 사용자(예: 친구)의 공유된 디지털 키를 관리하기 위한 요청 메시지를 생성할 수 있다. 다양한 실시 예에서, 요청 메시지는 공유된 디지털 키에 대한 정보, 요청 정보, 라우팅 정보 또는 요청 메시지를 송신한 발신자의 서명을 포함할 수 있다. 일 실시 예에서, 생성된 요청 메시지는, 전자 디바이스(310) 및 타겟 디바이스(320) 간의 NFC 연결을 통해 전송될 수 있다. 이하, NFC 연결을 통한 통신 시나리오는 옵션 1(option 1) 시나리오로 지칭될 수 있다. 다른 실시 예에서, 생성된 요청 메시지는, 제1 백엔드 서버(710) 또는 제2 백엔드 서버(720)를 통한 HTTP 통신 방식을 통해 송신될 수 있다. 이때, HTTP 통신 방식은 인터넷 연결을 통한 통신 방식을 의미할 수

있다. 이하, HTTP 연결을 통한 통신 시나리오는 옵션 2(option 2) 시나리오로 지칭될 수 있다. 다양한 실시 예에서, 옵션 1 시나리오의 경우, 701 단계 이후, 703 단계 내지 715 단계가 수행될 수 있다.

- [0077] 703 단계에서, 전자 디바이스(310)는 요청 메시지를 송신할 수 있다. 예를 들면, 전자 디바이스(310)는 생성된 요청 메시지를 타겟 디바이스(320)로 송신할 수 있다. 이때, 요청 메시지는 전자 디바이스(310) 및 타겟 디바이스(320) 간의 NFC연결을 통해 전송될 수 있다.
- [0078] 705 단계에서, 타겟 디바이스(320)는 수신된 요청 메시지를 확인할 수 있다. 예를 들면, 타겟 디바이스(320)는 수신된 요청 메시지에 포함된, 공유된 디지털 키에 대한 정보, 요청 정보 또는 요청 메시지를 송신한 발신자 서명을 확인할 수 있다.
- [0079] 707 단계에서, 타겟 디바이스(320)는 요청에 따른 동작을 수행할 수 있다. 즉, 타겟 디바이스(320)는 요청 메시지에 포함된 정보에 기초하여 공유된 디지털 키의 관리를 수행할 수 있다. 예를 들면, 요청 메시지의 요청 정보가, 공유된 디지털 키의 삭제와 관련된 정보를 포함하고 있는 경우, 타겟 디바이스(320)는 타겟 디바이스(320)에 저장된 공유된 디지털 키를 삭제할 수 있다. 요청 메시지의 요청 정보가, 공유된 디지털 키의 갱신과 관련된 정보를 포함하고 있는 경우, 타겟 디바이스(320)는 타겟 디바이스(320)에 저장된 공유된 디지털 키를 갱신할 수 있다.
- [0080] 709 단계에서, 타겟 디바이스(320)는 응답 메시지를 생성할 수 있다. 다양한 실시 예에서, 응답 메시지는 공유된 디지털 키에 대한 정보, 응답 정보, 라우팅 정보 또는 응답 메시지를 송신한 발신자의 서명을 포함할 수 있다. 예를 들면, 발신자의 서명은 타겟 디바이스(320)의 사용자의 서명을 의미할 수 있다. 다양한 실시 예들에서, 응답 정보는 공유된 디지털 키의 삭제 또는 갱신 수행의 결과에 대한 정보를 포함할 수 있다.
- [0081] 711 단계에서, 타겟 디바이스(320)는 응답 메시지를 송신할 수 있다. 예를 들면, 타겟 디바이스(320)는 생성된 응답 메시지를 전자 디바이스(310)로 송신할 수 있다. 이때, 응답 메시지는 전자 디바이스(310) 및 타겟 디바이스(320) 간의 NFC연결을 통해 전송될 수 있다.
- [0082] 713 단계에서, 전자 디바이스(310)는 응답 메시지를 확인할 수 있다. 예를 들면, 전자 디바이스(310)는 응답 메시지에 포함된, 공유된 디지털 키에 대한 정보, 응답 정보 또는 응답 메시지를 송신한 발신자 서명을 확인할 수 있다.
- [0083] 715 단계에서, 전자 디바이스(310)는 응답에 따른 동작을 수행할 수 있다. 즉, 전자 디바이스(310)는 확인된 응답 메시지에 포함된 정보에 기초하여, 공유된 디지털 키의 관리를 수행할 수 있다. 예를 들면, 응답 메시지의 응답 정보가, 공유된 디지털 키의 삭제와 관련된 정보를 포함하고 있는 경우, 전자 디바이스(310)는 전자 디바이스(310)에 저장된 공유된 디지털 키를 삭제할 수 있다. 응답 메시지의 응답 정보가, 공유된 디지털 키의 갱신과 관련된 정보를 포함하고 있는 경우, 전자 디바이스(310)는 전자 디바이스(310)에 저장된 공유된 디지털 키를 갱신할 수 있다. 다양한 실시 예에서, 전자 디바이스(310)의 공유된 디지털 키의 관리와 관련된 정보는 제1 백엔드 서버(710) 또는 제2 백엔드 서버(720)로 전송될 수 있다. 예를 들면, 전자 디바이스(310)는 공유된 디지털 키의 삭제 또는 갱신을 수행하고, 삭제 또는 갱신 수행의 결과와 관련된 정보를 제2 백엔드 서버(720)로 송신할 수 있다. 이후, 제1 백엔드 서버(710)는 제2 백엔드 서버(720)로 삭제 또는 갱신 수행의 결과와 관련된 정보를 송신할 수 있다. 다양한 실시 예에서, 옵션 2 시나리오의 경우, 701 단계 이후, 717 단계 내지 737 단계가 수행될 수 있다. 이때, 723 단계 내지 727 단계는 705 단계 내지 709 단계와 동일한 절차로 수행될 수 있다. 또한, 735 단계 및 737 단계는 713 단계 및 715 단계와 동일한 절차로 수행될 수 있다.
- [0084] 717 단계에서, 전자 디바이스(310)는 요청 메시지를 송신할 수 있다. 즉, 전자 디바이스(310)는 생성된 요청 메시지를 제1 백엔드 서버(710)로 송신할 수 있다. 이때, 전자 디바이스(310) 및 제1 백엔드 서버(710) 간의 상호 인증(mutual authentication) 절차가 수행될 수 있다.
- [0085] 719 단계에서, 제1 백엔드 서버(710)는 제2 백엔드 서버(720)로 요청 메시지를 송신할 수 있다. 예를 들면, 제1 백엔드 서버(710)는 요청 메시지에 포함된 라우팅 정보를 이용하여 제2 백엔드 서버(720)를 식별하고, 제2 백엔드 서버(720)로 요청 메시지를 송신할 수 있다. 이때, 제1 백엔드 서버(710)와 제2 백엔드 서버(720) 간의 상호 인증 절차가 수행될 수 있다.
- [0086] 721 단계에서, 제2 백엔드 서버(720)는 타겟 디바이스(320)로 요청 메시지를 송신할 수 있다. 이때, 제2 백엔드 서버(720)와 타겟 디바이스(320) 간의 상호 인증 절차가 수행될 수 있다.
- [0087] 723 단계에서, 타겟 디바이스(320)는 요청 메시지를 확인할 수 있다. 예를 들면, 타겟 디바이스(320)는 수신된

요청 메시지에 포함된, 공유된 디지털 키에 대한 정보, 요청 정보 또는 요청 메시지를 송신한 발신자 서명을 확인할 수 있다.

- [0088] 725 단계에서, 타겟 디바이스(320)는 요청에 따른 동작을 수행할 수 있다. 즉, 타겟 디바이스(320)는 요청 메시지에 포함된 정보에 기초하여 공유된 디지털 키의 관리를 수행할 수 있다. 예를 들면, 요청 메시지의 요청 정보가, 공유된 디지털 키의 삭제와 관련된 정보를 포함하고 있는 경우, 타겟 디바이스(320)는 타겟 디바이스(320)에 저장된 공유된 디지털 키를 삭제할 수 있다. 요청 메시지의 요청 정보가, 공유된 디지털 키의 갱신과 관련된 정보를 포함하고 있는 경우, 타겟 디바이스(320)는 타겟 디바이스(320)에 저장된 공유된 디지털 키를 갱신할 수 있다.
- [0089] 727 단계에서, 타겟 디바이스(320)는 응답 메시지를 생성할 수 있다. 다양한 실시 예에서, 응답 메시지는 공유된 디지털 키에 대한 정보, 응답 정보, 라우팅 정보 또는 응답 메시지를 송신한 발신자의 서명을 포함할 수 있다. 예를 들면, 발신자의 서명은 타겟 디바이스(320)의 사용자의 서명을 의미할 수 있다. 다양한 실시 예들에서, 응답 정보는 공유된 디지털 키의 삭제 또는 갱신 수행의 결과에 대한 정보를 포함할 수 있다.
- [0090] 729 단계에서, 타겟 디바이스(320)는 제2 백엔드 서버(720)로 응답 메시지를 송신할 수 있다. 이때, 타겟 디바이스(320) 및 제2 백엔드 서버(720) 간의 상호 인증 절차가 수행될 수 있다.
- [0091] 731 단계에서, 제2 백엔드 서버(720)는 응답 메시지를 송신할 수 있다. 예를 들면, 제2 백엔드 서버(720)는 응답 메시지에 포함된 라우팅 정보를 이용하여 제1 백엔드 서버(710)를 식별하고, 제1 백엔드 서버(710)로 응답 메시지를 송신할 수 있다. 이때, 제1 백엔드 서버(710)와 제2 백엔드 서버(720) 간의 상호 인증 절차가 수행될 수 있다.
- [0092] 733 단계에서, 제1 백엔드 서버(710)는 응답 메시지를 송신할 수 있다. 즉, 제1 백엔드 서버(710)는 수신된 응답 메시지를 전자 디바이스(310)로 송신할 수 있다. 이때, 전자 디바이스(310)와 제1 백엔드 서버(710) 간의 상호 인증 절차가 수행될 수 있다.
- [0093] 735 단계에서, 전자 디바이스(310)는 응답 메시지를 확인할 수 있다. 예를 들면, 전자 디바이스(310)는 응답 메시지에 포함된, 공유된 디지털 키에 대한 정보, 응답 정보 또는 응답 메시지를 송신한 발신자 서명을 확인할 수 있다.
- [0094] 737 단계에서, 전자 디바이스(310)는 응답에 따른 동작을 수행할 수 있다. 즉, 전자 디바이스(310)는 확인된 응답 메시지에 포함된 정보에 기초하여, 공유된 디지털 키의 관리를 수행할 수 있다. 예를 들면, 응답 메시지의 응답 정보가, 공유된 디지털 키의 삭제와 관련된 정보를 포함하고 있는 경우, 전자 디바이스(310)는 전자 디바이스(310)에 저장된 공유된 디지털 키를 삭제할 수 있다. 응답 메시지의 응답 정보가, 공유된 디지털 키의 갱신과 관련된 정보를 포함하고 있는 경우, 전자 디바이스(310)는 전자 디바이스(310)에 저장된 공유된 디지털 키를 갱신할 수 있다.
- [0095] 상술한 옵션 1 시나리오 및 옵션 2 시나리오에서 도 7에서 설명된 바와 같은 디지털 키 관리 절차가 수행되는 경우, 아래와 같은 동작이 수행될 수 있다.
- [0096] 일 실시 예에서, 다른 사용자의 공유된 디지털 키의 관리(예: 삭제 또는 갱신)가 오너 디바이스(100)에 의해 개시 또는 트리거링 되는 경우, 공유된 디지털 키의 관리에 대한 알림(notification)이 다른 사용자의 전자 디바이스(240) 또는 다른 사용자의 전자 디바이스에 대한 백엔드 서버(230)로 전송될 수 있다.
- [0097] 다른 실시 예에서, 다른 사용자의 공유된 디지털 키의 관리(예: 삭제)가 다른 사용자의 전자 디바이스(240)에 의해 개시 또는 트리거링 되는 경우, 공유된 디지털 키의 관리에 대한 알림이 오너 디바이스(100) 또는 오너 디바이스의 백엔드 서버(210)로 전송될 수 있다. 상술한 바와 같은 절차들을 통해, 전자 디바이스(310)에 의해 개시 또는 트리거링된 디지털 키 관리 동작이 수행될 수 있다.
- [0099] 도 8은 본 개시의 다양한 실시 예들에 따른 타겟 디바이스에 의해 개시 또는 트리거링된 디지털 키 관리 방법을 개략적으로 설명하기 위한 시퀀스 다이어그램이다.
- [0100] 도 8을 참고하면, 전자 디바이스(310)는 오너 디바이스(100) 또는 다른 사용자의 전자 디바이스(240)를 의미할 수 있다. 타겟 디바이스(320)는 전자 디바이스(11)를 의미할 수 있다. 예를 들면, 전자 디바이스(11)는 자동차 또는, 자동차에 탑재되는 전자 장치를 의미할 수 있다. 또한, 제1 백엔드 서버(810)는 전자 디바이스(310)의 백

엔드 서버를 의미할 수 있고, 제2 백엔드 서버(820)는 타겟 디바이스(320)의 백엔드 서버를 의미할 수 있다. 여기서, 전자 디바이스(310)의 백엔드 서버는, 오너 디바이스의 백엔드 서버(210) 또는 다른 사용자의 전자 디바이스에 대한 백엔드 서버(230)를 의미할 수 있다.

[0101] 801 단계에서, 타겟 디바이스(320)는 디지털 키 관리를 수행할 수 있다. 도 8에는 도시되지 아니하였으나, 타겟 디바이스(320)가 디지털 키 관리를 수행하기 전에, 디지털 키 관리를 요청하는 요청자(requester)의 요청에 의해 디지털 키 관리 동작이 개시 또는 트리거링될 수 있다. 예를 들면, 요청자는 오너 디바이스(100)의 사용자(1) 또는 오너가 아닌 다른 사용자(예: 친구)를 의미할 수 있다. 일 실시 예에서, 요청자는 타겟 디바이스(320)의 물리적인 버튼, 사용자 인터페이스 상의 버튼 또는 패스워드 입력을 통해, 공유된 디지털 키의 관리를 요청할 수 있다. 타겟 디바이스(320)의 시동이 걸려있는 경우, 공유된 디지털 키 관리 요청을 위한 추가적인 인증 절차는 필요하지 아니할 수 있다. 다양한 실시 예에서, 타겟 디바이스(320)로의 요청자의 공유된 디지털 키 관리 요청은, 공유된 디지털 키를 관리하기 위한 요청 메시지 형태로 구현될 수 있다. 상술한 바와 같이, 공유된 디지털 키의 관리가 요청된 이후, 타겟 디바이스(320)는 디지털 키 관리 동작을 수행할 수 있다. 예를 들면, 요청자의 요청이 공유된 디지털 키의 삭제인 경우, 타겟 디바이스(320)는 타겟 디바이스(320)에 저장된 공유된 디지털 키를 삭제할 수 있다. 요청자의 요청이 공유된 디지털 키의 갱신인 경우, 타겟 디바이스(320)는 타겟 디바이스(320)에 저장된 공유된 디지털 키를 갱신할 수 있다.

[0102] 803 단계에서, 타겟 디바이스(320)는 응답 메시지를 생성할 수 있다. 예를 들면, 타겟 디바이스(320)는 공유된 디지털 키에 대한 관리 동작을 수행하고, 이에 대한 결과를 응답 메시지 형태로 생성할 수 있다. 다양한 실시 예에서, 응답 메시지는 공유된 디지털 키에 대한 정보, 응답 정보, 라우팅 정보 또는 응답 메시지를 송신한 발신자의 서명을 포함할 수 있다. 예를 들면, 발신자의 서명은 타겟 디바이스(320)의 사용자의 서명을 의미할 수 있다. 다양한 실시 예들에서, 응답 정보는 공유된 디지털 키의 삭제 또는 갱신 수행의 결과에 대한 정보를 포함할 수 있다. 일 실시 예에서, 생성된 응답 메시지는, 전자 디바이스(310) 및 타겟 디바이스(320) 간의 NFC 연결을 통해 전송될 수 있다. 이하, NFC 연결을 통한 통신 시나리오는 옵션 1(option 1) 시나리오로 지칭될 수 있다. 다른 실시 예에서, 생성된 응답 메시지는, 제1 백엔드 서버(810) 또는 제2 백엔드 서버(820)를 통한 HTTP 통신 방식을 통해 송신될 수 있다. 이때, HTTP 통신 방식은 인터넷 연결을 통한 통신 방식을 의미할 수 있다. 이하, HTTP 연결을 통한 통신 시나리오는 옵션 2(option 2) 시나리오로 지칭될 수 있다. 일 실시 예에서, 요청자가 오너인 경우, 응답 메시지는, 전자 디바이스(310)와 타겟 디바이스(320) 간의 NFC 연결을 통해 전송되거나, 제1 백엔드 서버(810) 또는 제2 백엔드 서버(820)를 통한 HTTP 연결을 통해 전송될 수 있다. 다른 실시 예에서, 요청자가 오너가 아닌 다른 사용자인 경우, 응답 메시지는, 제1 백엔드 서버(810) 또는 제2 백엔드 서버(820)를 통한 HTTP 연결을 통해 전송될 수 있다. 다양한 실시 예에서, 옵션 1 시나리오의 경우, 803 단계 이후, 805 단계 내지 809 단계가 수행될 수 있다.

[0103] 805 단계에서, 타겟 디바이스(320)는 응답 메시지를 송신할 수 있다. 예를 들면, 타겟 디바이스(320)는 생성된 응답 메시지를 전자 디바이스(310)로 송신할 수 있다. 이때, 응답 메시지는 전자 디바이스(310) 및 타겟 디바이스(320) 간의 NFC 연결을 통해 전송될 수 있다.

[0104] 807 단계에서, 전자 디바이스(310)는 응답 메시지를 확인할 수 있다. 예를 들면, 전자 디바이스(310)는 응답 메시지에 포함된, 공유된 디지털 키에 대한 정보, 응답 정보 또는 응답 메시지를 송신한 발신자 서명을 확인할 수 있다.

[0105] 809 단계에서, 전자 디바이스(310)는 응답에 따른 동작을 수행할 수 있다. 즉, 전자 디바이스(310)는 확인된 응답 메시지에 포함된 정보에 기초하여, 공유된 디지털 키의 관리를 수행할 수 있다. 예를 들면, 응답 메시지의 응답 정보가, 공유된 디지털 키의 삭제와 관련된 정보를 포함하고 있는 경우, 전자 디바이스(310)는 전자 디바이스(310)에 저장된 공유된 디지털 키를 삭제할 수 있다. 응답 메시지의 응답 정보가, 공유된 디지털 키의 갱신과 관련된 정보를 포함하고 있는 경우, 전자 디바이스(310)는 전자 디바이스(310)에 저장된 공유된 디지털 키를 갱신할 수 있다. 다양한 실시 예에서, 전자 디바이스(310)의 공유된 디지털 키의 관리와 관련된 정보는 제1 백엔드 서버(810) 또는 제2 백엔드 서버(820)로 전송될 수 있다. 예를 들면, 전자 디바이스(310)는 공유된 디지털 키의 삭제 또는 갱신을 수행하고, 삭제 또는 갱신 수행의 결과와 관련된 정보를 제1 백엔드 서버(810)로 송신할 수 있다. 이후, 제1 백엔드 서버(810)는 제2 백엔드 서버(820)로 삭제 또는 갱신 수행의 결과와 관련된 정보를 송신할 수 있다. 다양한 실시 예에서, 옵션 2 시나리오의 경우, 803 단계 이후, 811 단계 내지 819 단계가 수행될 수 있다. 이때, 817 단계 및 819 단계는, 807 단계 및 809 단계와 동일한 절차로 수행될 수 있다.

[0106] 811 단계에서, 타겟 디바이스(320)는 응답 메시지를 송신할 수 있다. 예를 들면, 타겟 디바이스(320)는 생성된

응답 메시지를 제2 백엔드 서버(820)로 송신할 수 있다. 이때, 타겟 디바이스(320)와 제2 백엔드 서버(820) 간의 상호 인증 절차가 수행될 수 있다.

- [0107] 813 단계에서, 제2 백엔드 서버(820)는 응답 메시지를 송신할 수 있다. 예를 들면, 제2 백엔드 서버(820)는 응답 메시지에 포함된 라우팅 정보를 이용하여 제1 백엔드 서버(810)를 식별하고, 제1 백엔드 서버(810)로 응답 메시지를 송신할 수 있다. 이때, 제1 백엔드 서버(810)와 제2 백엔드 서버(820) 간의 상호 인증 절차가 수행될 수 있다.
- [0108] 815 단계에서, 제1 백엔드 서버(810)는 응답 메시지를 송신할 수 있다. 즉, 제1 백엔드 서버(810)는 수신된 응답 메시지를 전자 디바이스(310)로 송신할 수 있다. 이때, 전자 디바이스(310)와 제1 백엔드 서버(810) 간의 상호 인증 절차가 수행될 수 있다.
- [0109] 817 단계에서, 전자 디바이스(310)는 응답 메시지를 확인할 수 있다. 예를 들면, 전자 디바이스(310)는 응답 메시지에 포함된, 공유된 디지털 키에 대한 정보, 응답 정보 또는 응답 메시지를 송신한 발신자 서명을 확인할 수 있다.
- [0110] 819 단계에서, 전자 디바이스(310)는 응답에 따른 동작을 수행할 수 있다. 즉, 전자 디바이스(310)는 확인된 응답 메시지에 포함된 정보에 기초하여, 공유된 디지털 키의 관리를 수행할 수 있다. 예를 들면, 응답 메시지의 응답 정보가, 공유된 디지털 키의 삭제와 관련된 정보를 포함하고 있는 경우, 전자 디바이스(310)는 전자 디바이스(310)에 저장된 공유된 디지털 키를 삭제할 수 있다. 응답 메시지의 응답 정보가, 공유된 디지털 키의 갱신과 관련된 정보를 포함하고 있는 경우, 전자 디바이스(310)는 전자 디바이스(310)에 저장된 공유된 디지털 키를 갱신할 수 있다.
- [0111] 상술한 옵션 1 시나리오 및 옵션 2 시나리오에서 도 8에서 설명된 바와 같은 디지털 키 관리 절차가 수행되는 경우, 아래와 같은 동작이 수행될 수 있다.
- [0112] 일 실시 예에서, 다른 사용자의 공유된 디지털 키의 관리(예: 삭제 또는 갱신)가 오너에 의해 요청되는 경우, 공유된 디지털 키의 관리에 대한 알림이 다른 사용자의 전자 디바이스(240) 또는 다른 사용자의 전자 디바이스에 대한 백엔드 서버(230)로 전송될 수 있다.
- [0113] 다른 실시 예에서, 다른 사용자의 공유된 디지털 키의 관리(예: 삭제)가 다른 사용자에 의해 요청되는 경우, 공유된 디지털 키의 관리에 대한 알림이 오너 디바이스(100) 또는 오너 디바이스의 백엔드 서버(210)로 전송될 수 있다. 상술한 바와 같은 절차들을 통해, 타겟 디바이스(320)에 의해 개시 또는 트리거링된 디지털 키 관리 동작이 수행될 수 있다.
- [0115] 도 9는 본 개시의 다양한 실시 예들에 따른 제1 백엔드 서버에 의해 개시 또는 트리거링된 디지털 키 관리 방법을 개략적으로 설명하기 위한 시퀀스 다이어그램이다.
- [0116] 도 9를 참고하면, 전자 디바이스(310)는 오너 디바이스(100) 또는 다른 사용자의 전자 디바이스(240)를 의미할 수 있다. 타겟 디바이스(320)는 전자 디바이스(11)를 의미할 수 있다. 예를 들면, 전자 디바이스(11)는 자동차 또는, 자동차에 탑재되는 전자 장치를 의미할 수 있다. 또한, 제1 백엔드 서버(910)는 전자 디바이스(310)의 백엔드 서버를 의미할 수 있고, 제2 백엔드 서버(920)는 타겟 디바이스(320)의 백엔드 서버를 의미할 수 있다. 여기서, 전자 디바이스(310)의 백엔드 서버는, 오너 디바이스의 백엔드 서버(210) 또는 다른 사용자의 전자 디바이스에 대한 백엔드 서버(230)를 의미할 수 있다.
- [0117] 901 단계에서, 제1 백엔드 서버(910)는 요청 메시지를 생성할 수 있다. 다양한 실시 예에서, 요청자는 제1 백엔드 서버(910)로 공유된 디지털 키의 관리를 요청할 수 있다. 일 실시 예에서, 요청은 요청자의 통화 또는, 요청자의 전자 디바이스 상의 어플리케이션을 통한 요청을 의미할 수 있다. 상술한 요청 메시지는, 공유된 디지털 키에 대한 정보, 요청 정보, 라우팅 정보 또는 요청 메시지를 송신한 발신자의 서명을 포함할 수 있다. 제1 백엔드 서버(910)가 요청 메시지를 송신하므로, 요청 메시지에는 제1 백엔드 서버(910)의 서명이 포함될 수 있다.
- [0118] 903 단계에서, 제1 백엔드 서버(910)는 요청 메시지를 송신할 수 있다. 다양한 실시 예들에서, 제1 백엔드 서버(910)는 요청 메시지에 포함된 라우팅 정보를 이용하여 제2 백엔드 서버(920)를 식별할 수 있다. 제1 백엔드 서버(910)는 요청 메시지를 식별된 제2 백엔드 서버(920)로 송신할 수 있다. 이때, 제1 백엔드 서버(910)와 제2 백엔드 서버(920) 간의 상호 인증 절차가 수행될 수 있다.

- [0119] 905 단계에서, 제2 백엔드 서버(920)는 요청 메시지를 확인할 수 있다. 예를 들면, 제2 백엔드 서버(920)는 요청 메시지에 포함된 공유된 디지털 키에 대한 정보, 요청 정보, 라우팅 정보 또는 요청 메시지를 송신한 발신자의 서명을 확인할 수 있다.
- [0120] 907 단계에서, 제2 백엔드 서버(920)는 요청 메시지를 생성할 수 있다. 즉, 제2 백엔드 서버(920)는 제1 백엔드 서버(910)로부터 수신한 요청 메시지에 포함된 정보들을 이용하여 새로운 요청 메시지를 생성할 수 있다. 제1 백엔드 서버(910)에 의해 공유된 디지털 키 관리 동작이 개시 또는 트리거링되는 경우, 일 실시 예에서, 제2 백엔드 서버(920)는 수신된 요청 메시지에 포함된 제1 백엔드 서버(910)의 서명을 자신의 서명으로 대체할 수 있다. 다른 실시 예에서, 제2 백엔드 서버(920)는 수신된 요청 메시지에 포함된 제1 백엔드 서버(910)의 서명에 더하여 자신의 서명을 추가할 수 있다. 또 다른 실시 예에서, 제2 백엔드 서버(920)는 새로운 요청 메시지를 생성하지 아니하고, 수신된 요청 메시지를 타겟 디바이스(320)로 송신할 수 있다. 즉, 제2 백엔드 서버(920)는 제1 백엔드 서버(910)로부터 수신된 요청 메시지에 기초하여 새로운 요청 메시지를 생성하지 아니하고, 제1 백엔드 서버(910)로부터 수신된 요청 메시지를 재사용할 수 있다. 상술한 바와 같이, 제2 백엔드 서버(920)가 새로운 요청 메시지를 생성하지 않는 경우, 907 단계는 생략될 수 있다.
- [0121] 909 단계에서, 제2 백엔드 서버(920)는 요청 메시지를 송신할 수 있다. 즉, 제2 백엔드 서버(920)는 자신의 서명이 포함된 요청 메시지를 타겟 디바이스(320)로 송신할 수 있다. 이때, 타겟 디바이스(320)와 제2 백엔드 서버(920) 간의 상호 인증 절차가 수행될 수 있다. 다른 실시 예에서, 제2 백엔드 서버(920)가 새로운 요청 메시지를 생성하지 아니하고, 제1 백엔드 서버(910)로부터 수신된 요청 메시지를 타겟 디바이스(320)로 송신하는 경우, 제2 백엔드 서버(920)는 자신의 서명 또는 제1 백엔드 서버(910)의 서명이 포함된 메시지를 타겟 디바이스(320)로 송신할 수 있다.
- [0122] 911 단계에서, 타겟 디바이스(320)는 수신된 요청 메시지를 확인할 수 있다. 예를 들면, 타겟 디바이스(320)는 수신된 요청 메시지에 포함된, 공유된 디지털 키에 대한 정보, 요청 정보 또는 요청 메시지를 송신한 발신자 서명을 확인할 수 있다. 예를 들면, 타겟 디바이스(320)는 요청 메시지에 포함된 요청 정보를 통해, 공유된 디지털 키의 삭제 또는 갱신에 대한 요청을 확인할 수 있다. 또한, 타겟 디바이스(320)는 요청 메시지에 포함된 발신자 서명이 제2 백엔드 서버(920)의 서명임을 확인할 수 있다. 다른 실시 예에서, 제2 백엔드 서버(920)가 새로운 요청 메시지를 생성하지 아니하고, 제1 백엔드 서버(910)로부터 수신된 요청 메시지를 타겟 디바이스(320)로 송신하는 경우, 타겟 디바이스(320)는 요청 메시지에 포함된 발신자 서명이, 제1 백엔드 서버(910) 또는 제2 백엔드 서버(920)의 서명임을 확인할 수 있다.
- [0123] 913 단계에서, 타겟 디바이스(320)는 요청에 따른 동작을 수행할 수 있다. 즉, 타겟 디바이스(320)는 요청 메시지에 포함된 정보에 기초하여 공유된 디지털 키의 관리를 수행할 수 있다. 예를 들면, 요청 메시지의 요청 정보가, 공유된 디지털 키의 삭제와 관련된 정보를 포함하고 있는 경우, 타겟 디바이스(320)는 타겟 디바이스(320)에 저장된 공유된 디지털 키를 삭제할 수 있다. 요청 메시지의 요청 정보가, 공유된 디지털 키의 갱신과 관련된 정보를 포함하고 있는 경우, 타겟 디바이스(320)는 타겟 디바이스(320)에 저장된 공유된 디지털 키를 갱신할 수 있다.
- [0124] 915 단계에서, 타겟 디바이스(320)는 응답 메시지를 생성할 수 있다. 다양한 실시 예에서, 응답 메시지는 공유된 디지털 키에 대한 정보, 응답 정보, 라우팅 정보 또는 응답 메시지를 송신한 발신자의 서명을 포함할 수 있다. 예를 들면, 발신자의 서명은 타겟 디바이스(320)의 사용자의 서명을 의미할 수 있다. 다양한 실시 예들에서, 응답 정보는 공유된 디지털 키의 삭제 또는 갱신 수행의 결과에 대한 정보를 포함할 수 있다.
- [0125] 917 단계에서, 타겟 디바이스(320)는 응답 메시지를 송신할 수 있다. 예를 들면, 타겟 디바이스(320)는 생성된 응답 메시지를 제2 백엔드 서버(920)로 송신할 수 있다. 이때, 타겟 디바이스(320) 및 제2 백엔드 서버(920) 간의 상호 인증 절차가 수행될 수 있다.
- [0126] 919 단계에서, 제2 백엔드 서버(920)는 응답 메시지를 확인할 수 있다. 예를 들면, 제2 백엔드 서버(920)는 응답 메시지에 포함된 라우팅 정보를 확인할 수 있다. 제2 백엔드 서버(920)는 확인된 라우팅 정보에 기초하여, 응답 메시지를 송신할 대상을 제1 백엔드 서버(910)로 식별할 수 있다.
- [0127] 921 단계에서, 제2 백엔드 서버(920)는 응답 메시지를 송신할 수 있다. 예를 들면, 제2 백엔드 서버(920)는 확인된 응답 메시지를 제1 백엔드 서버(910)로 송신할 수 있다. 이때, 제1 백엔드 서버(910)와 제2 백엔드 서버(920) 간의 상호 인증 절차가 수행될 수 있다.
- [0128] 다양한 실시 예에서, 공유된 디지털 키의 관리를 요청하는 요청 메시지에 대한 응답 메시지는, 디지털 키 관리

요청자의 전자 디바이스로 송신될 수 있다. 일 실시 예에서, 요청자가 오너인 경우, 응답 메시지는 전자 디바이스(310)와 타겟 디바이스(320) 간의 NFC 연결을 통해 전송되거나, 제1 백엔드 서버(910) 또는 제2 백엔드 서버(920)를 통한 HTTP 연결을 통해 전송될 수 있다. 다른 실시 예에서, 요청자가 오너가 아닌 다른 사용자인 경우, 응답 메시지는, 제1 백엔드 서버(910) 또는 제2 백엔드 서버(920)를 통한 HTTP 연결을 통해 전송될 수 있다. 일 실시 예에서, 915 단계에서 타겟 디바이스(320)에 의해 생성된 응답 메시지는, 전자 디바이스(310) 및 타겟 디바이스(320) 간의 NFC 연결을 통해 전송될 수 있다. 이하, NFC 연결을 통한 통신 시나리오는 옵션 1(option 1) 시나리오로 지칭될 수 있다. 다른 실시 예에서, 타겟 디바이스(320)에 의해 생성된 응답 메시지는, 제1 백엔드 서버(910) 또는 제2 백엔드 서버(920)를 통한 HTTP 통신 방식을 통해 송신될 수 있다. 이때, HTTP 통신 방식은 인터넷 연결을 통한 통신 방식을 의미할 수 있다. 이하, HTTP 연결을 통한 통신 시나리오는 옵션 2(option 2) 시나리오로 지칭될 수 있다. 다양한 실시 예에서, 옵션 1 시나리오의 경우, 921 단계 이후, 923 단계 내지 927 단계가 수행될 수 있다.

- [0129] 923 단계에서, 타겟 디바이스(320)는 응답 메시지를 송신할 수 있다. 예를 들면, 타겟 디바이스(320)는 생성된 응답 메시지를 전자 디바이스(310)로 송신할 수 있다. 이때, 응답 메시지는 전자 디바이스(310) 및 타겟 디바이스(320) 간의 NFC 연결을 통해 전송될 수 있다.
- [0130] 925 단계에서, 전자 디바이스(310)는 응답 메시지를 확인할 수 있다. 예를 들면, 전자 디바이스(310)는 응답 메시지에 포함된, 공유된 디지털 키에 대한 정보, 응답 정보 또는 응답 메시지를 송신한 발신자 서명을 확인할 수 있다.
- [0131] 927 단계에서, 전자 디바이스(310)는 응답에 따른 동작을 수행할 수 있다. 즉, 전자 디바이스(310)는 확인된 응답 메시지에 포함된 정보에 기초하여, 공유된 디지털 키의 관리를 수행할 수 있다. 예를 들면, 응답 메시지의 응답 정보가, 공유된 디지털 키의 삭제와 관련된 정보를 포함하고 있는 경우, 전자 디바이스(310)는 전자 디바이스(310)에 저장된 공유된 디지털 키를 삭제할 수 있다. 응답 메시지의 응답 정보가, 공유된 디지털 키의 갱신과 관련된 정보를 포함하고 있는 경우, 전자 디바이스(310)는 전자 디바이스(310)에 저장된 공유된 디지털 키를 갱신할 수 있다. 다양한 실시 예에서, 옵션 2 시나리오의 경우, 921 단계 이후, 929 단계 내지 933 단계가 수행될 수 있다. 이때, 931 단계 및 933 단계는, 925 단계 및 927 단계와 동일한 절차로 수행될 수 있다.
- [0132] 929 단계에서, 제1 백엔드 서버(910)는 응답 메시지를 송신할 수 있다. 예를 들면, 제1 백엔드 서버(910)는 921 단계에서 제2 백엔드 서버(920)로부터 수신된 응답 메시지를 전자 디바이스(310)로 송신할 수 있다. 이때, 제1 백엔드 서버(910)와 전자 디바이스(310) 간의 상호 인증 절차가 수행될 수 있다.
- [0133] 931 단계에서, 전자 디바이스(310)는 응답 메시지를 확인할 수 있다. 예를 들면, 전자 디바이스(310)는 응답 메시지에 포함된, 공유된 디지털 키에 대한 정보, 응답 정보 또는 응답 메시지를 송신한 발신자 서명을 확인할 수 있다.
- [0134] 933 단계에서, 전자 디바이스(310)는 응답에 따른 동작을 수행할 수 있다. 즉, 전자 디바이스(310)는 확인된 응답 메시지에 포함된 정보에 기초하여, 공유된 디지털 키의 관리를 수행할 수 있다. 예를 들면, 응답 메시지의 응답 정보가, 공유된 디지털 키의 삭제와 관련된 정보를 포함하고 있는 경우, 전자 디바이스(310)는 전자 디바이스(310)에 저장된 공유된 디지털 키를 삭제할 수 있다. 응답 메시지의 응답 정보가, 공유된 디지털 키의 갱신과 관련된 정보를 포함하고 있는 경우, 전자 디바이스(310)는 전자 디바이스(310)에 저장된 공유된 디지털 키를 갱신할 수 있다.
- [0135] 상술한 옵션 1 시나리오 및 옵션 2 시나리오에서 도 9에서 설명된 바와 같은 디지털 키 관리 절차가 수행되는 경우, 아래와 같은 동작이 수행될 수 있다.
- [0136] 일 실시 예에서, 다른 사용자의 공유된 디지털 키의 관리(예: 삭제 또는 갱신)가 오너에 의해 요청되는 경우, 공유된 디지털 키의 관리에 대한 알림이 다른 사용자의 전자 디바이스(240) 또는 다른 사용자의 전자 디바이스에 대한 백엔드 서버(230)로 전송될 수 있다.
- [0137] 다른 실시 예에서, 다른 사용자의 공유된 디지털 키의 관리(예: 삭제)가 다른 사용자에게 의해 요청되는 경우, 공유된 디지털 키의 관리에 대한 알림이 오너 디바이스(100) 또는 오너 디바이스의 백엔드 서버(210)로 전송될 수 있다. 상술한 바와 같은 절차들을 통해, 제1 백엔드 서버에 의해 개시 또는 트리거링된 디지털 키 관리 동작이 수행될 수 있다.

- [0139] 도 10은 본 개시의 다양한 실시 예들에 따른 제2 백엔드 서버에 의해 개시 또는 트리거링된 디지털 키 관리 방법을 개략적으로 설명하기 위한 시퀀스 다이어그램이다.
- [0140] 도 10을 참고하면, 전자 디바이스(310)는 오너 디바이스(100) 또는 다른 사용자의 전자 디바이스(240)를 의미할 수 있다. 타겟 디바이스(320)는 전자 디바이스(11)를 의미할 수 있다. 예를 들면, 전자 디바이스(11)는 자동차 또는, 자동차에 탑재되는 전자 장치를 의미할 수 있다. 또한, 제1 백엔드 서버(1010)는 전자 디바이스(310)의 백엔드 서버를 의미할 수 있고, 제2 백엔드 서버(1020)는 타겟 디바이스(320)의 백엔드 서버를 의미할 수 있다. 여기서, 전자 디바이스(310)의 백엔드 서버는, 오너 디바이스의 백엔드 서버(210) 또는 다른 사용자의 전자 디바이스에 대한 백엔드 서버(230)를 의미할 수 있다.
- [0141] 1001 단계에서, 제2 백엔드 서버(1020)는 요청 메시지를 생성할 수 있다. 다양한 실시 예에서, 요청자는 제2 백엔드 서버(1020)로 공유된 디지털 키의 관리를 요청할 수 있다. 일 실시 예에서, 요청은 요청자의 통화 또는, 요청자의 전자 디바이스 상의 어플리케이션을 통한 요청을 의미할 수 있다. 상술한 요청 메시지는, 공유된 디지털 키에 대한 정보, 요청 정보, 라우팅 정보 또는 요청 메시지를 송신한 발신자의 서명을 포함할 수 있다. 제2 백엔드 서버(1020)가 요청 메시지를 송신하므로, 요청 메시지에는 제2 백엔드 서버(1020)의 서명이 포함될 수 있다.
- [0142] 1003 단계에서, 제2 백엔드 서버(1020)는 요청 메시지를 송신할 수 있다. 즉, 제2 백엔드 서버(1020)는 자신의 서명이 포함된 요청 메시지를 타겟 디바이스(320)로 송신할 수 있다. 이때, 타겟 디바이스(320)와 제2 백엔드 서버(1020) 간의 상호 인증 절차가 수행될 수 있다.
- [0143] 1005 단계에서, 타겟 디바이스(320)는 수신된 요청 메시지를 확인할 수 있다. 예를 들면, 타겟 디바이스(320)는 수신된 요청 메시지에 포함된, 공유된 디지털 키에 대한 정보, 요청 정보 또는 요청 메시지를 송신한 발신자 서명을 확인할 수 있다. 예를 들면, 타겟 디바이스(320)는 요청 메시지에 포함된 요청 정보를 통해, 공유된 디지털 키의 삭제 또는 갱신에 대한 요청을 확인할 수 있다. 또한, 타겟 디바이스(320)는 요청 메시지에 포함된 발신자 서명이 제2 백엔드 서버(920)의 서명임을 확인할 수 있다.
- [0144] 1007 단계에서, 타겟 디바이스(320)는 요청에 따른 동작을 수행할 수 있다. 즉, 타겟 디바이스(320)는 요청 메시지에 포함된 정보에 기초하여 공유된 디지털 키의 관리를 수행할 수 있다. 예를 들면, 요청 메시지의 요청 정보가, 공유된 디지털 키의 삭제와 관련된 정보를 포함하고 있는 경우, 타겟 디바이스(320)는 타겟 디바이스(320)에 저장된 공유된 디지털 키를 삭제할 수 있다. 요청 메시지의 요청 정보가, 공유된 디지털 키의 갱신과 관련된 정보를 포함하고 있는 경우, 타겟 디바이스(320)는 타겟 디바이스(320)에 저장된 공유된 디지털 키를 갱신할 수 있다.
- [0145] 1009 단계에서, 타겟 디바이스(320)는 응답 메시지를 생성할 수 있다. 다양한 실시 예에서, 응답 메시지는 공유된 디지털 키에 대한 정보, 응답 정보, 라우팅 정보 또는 응답 메시지를 송신한 발신자의 서명을 포함할 수 있다. 예를 들면, 발신자의 서명은 타겟 디바이스(320)의 사용자의 서명을 의미할 수 있다. 다양한 실시 예들에서, 응답 정보는 공유된 디지털 키의 삭제 또는 갱신 수행의 결과에 대한 정보를 포함할 수 있다.
- [0146] 1011 단계에서, 타겟 디바이스(320)는 응답 메시지를 송신할 수 있다. 예를 들면, 타겟 디바이스(320)는 생성된 응답 메시지를 제2 백엔드 서버(1020)로 송신할 수 있다. 이때, 타겟 디바이스(320) 및 제2 백엔드 서버(1020) 간의 상호 인증 절차가 수행될 수 있다.
- [0147] 1013 단계에서, 제2 백엔드 서버(1020)는 응답 메시지를 확인할 수 있다. 예를 들면, 제2 백엔드 서버(1020)는 응답 메시지에 포함된 라우팅 정보를 확인할 수 있다. 일 실시 예에서, 제2 백엔드 서버(1020)는 확인된 라우팅 정보에 기초하여, 응답 메시지를 송신할 대상을 제1 백엔드 서버(1010)로 식별할 수 있다.
- [0148] 다양한 실시 예에서, 공유된 디지털 키의 관리를 요청하는 요청 메시지에 대한 응답 메시지는, 디지털 키 관리 요청자의 전자 디바이스로 송신될 수 있다. 일 실시 예에서, 요청자가 오너인 경우, 응답 메시지는 전자 디바이스(310)와 타겟 디바이스(320) 간의 NFC 연결을 통해 전송되거나, 제1 백엔드 서버(910) 또는 제2 백엔드 서버(920)를 통한 HTTP 연결을 통해 전송될 수 있다. 다른 실시 예에서, 요청자가 오너가 아닌 다른 사용자인 경우, 응답 메시지는, 제1 백엔드 서버(910) 또는 제2 백엔드 서버(920)를 통한 HTTP 연결을 통해 전송될 수 있다. 일 실시 예에서, 1009 단계에서 타겟 디바이스(320)에 의해 생성된 응답 메시지는, 전자 디바이스(310) 및 타겟 디바이스(320) 간의 NFC 연결을 통해 전송될 수 있다. 이하, NFC 연결을 통한 통신 시나리오는 옵션 1(option 1) 시나리오로 지칭될 수 있다. 다른 실시 예에서, 타겟 디바이스(320)에 의해 생성된 응답 메시지는, 제1 백엔드 서버(910) 또는 제2 백엔드 서버(920)를 통한 HTTP 통신 방식을 통해 송신될 수 있다. 이때, HTTP 통신 방식은

인터넷 연결을 통한 통신 방식을 의미할 수 있다. 이하, HTTP 연결을 통한 통신 시나리오는 옵션 2(option 2) 시나리오로 지칭될 수 있다. 다양한 실시 예에서, 옵션 1 시나리오의 경우, 1013 단계 이후, 1015 단계 내지 1019 단계가 수행될 수 있다.

- [0149] 1015 단계에서, 타겟 디바이스(320)는 응답 메시지를 송신할 수 있다. 예를 들면, 타겟 디바이스(320)는 생성된 응답 메시지를 전자 디바이스(310)로 송신할 수 있다. 이때, 응답 메시지는 전자 디바이스(310) 및 타겟 디바이스(320) 간의 NFC연결을 통해 전송될 수 있다.
- [0150] 1017 단계에서, 전자 디바이스(310)는 응답 메시지를 확인할 수 있다. 예를 들면, 전자 디바이스(310)는 응답 메시지에 포함된, 공유된 디지털 키에 대한 정보, 응답 정보 또는 응답 메시지를 송신한 발신자 서명을 확인할 수 있다.
- [0151] 1019 단계에서, 전자 디바이스(310)는 응답에 따른 동작을 수행할 수 있다. 즉, 전자 디바이스(310)는 확인된 응답 메시지에 포함된 정보에 기초하여, 공유된 디지털 키의 관리를 수행할 수 있다. 예를 들면, 응답 메시지의 응답 정보가, 공유된 디지털 키의 삭제와 관련된 정보를 포함하고 있는 경우, 전자 디바이스(310)는 전자 디바이스(310)에 저장된 공유된 디지털 키를 삭제할 수 있다. 응답 메시지의 응답 정보가, 공유된 디지털 키의 갱신과 관련된 정보를 포함하고 있는 경우, 전자 디바이스(310)는 전자 디바이스(310)에 저장된 공유된 디지털 키를 갱신할 수 있다. 다양한 실시 예에서, 전자 디바이스(310)의 공유된 디지털 키의 관리와 관련된 정보는 제1 백엔드 서버(1010)로 송신될 수 있다. 예를 들면, 전자 디바이스(310)는 공유된 디지털 키의 삭제 또는 갱신을 수행하고, 삭제 또는 갱신 수행의 결과와 관련된 정보를 제1 백엔드 서버(1010)로 송신할 수 있다.
- [0152] 다양한 실시 예에서, 옵션 2 시나리오의 경우, 1013 단계 이후, 1021 단계 내지 1027 단계가 수행될 수 있다. 이때, 1025 단계 및 1027 단계는, 1017 단계 및 1019 단계와 동일한 절차로 수행될 수 있다.
- [0153] 1021 단계에서, 제2 백엔드 서버(1020)는 응답 메시지를 송신할 수 있다. 예를 들면, 제2 백엔드 서버(1020)는 확인된 응답 메시지를 제1 백엔드 서버(1010)로 송신할 수 있다. 이때, 제1 백엔드 서버(1010)와 제2 백엔드 서버(1020) 간의 상호 인증 절차가 수행될 수 있다.
- [0154] 1023 단계에서, 제1 백엔드 서버(1010)는 응답 메시지를 송신할 수 있다. 예를 들면, 제1 백엔드 서버(1010)는 1021 단계에서 제2 백엔드 서버(1020)로부터 수신된 응답 메시지를 전자 디바이스(310)로 송신할 수 있다. 이때, 제1 백엔드 서버(1010)와 전자 디바이스(310) 간의 상호 인증 절차가 수행될 수 있다.
- [0155] 1025 단계에서, 전자 디바이스(310)는 응답 메시지를 확인할 수 있다. 예를 들면, 전자 디바이스(310)는 응답 메시지에 포함된, 공유된 디지털 키에 대한 정보, 응답 정보 또는 응답 메시지를 송신한 발신자 서명을 확인할 수 있다.
- [0156] 1027 단계에서, 전자 디바이스(310)는 응답에 따른 동작을 수행할 수 있다. 즉, 전자 디바이스(310)는 확인된 응답 메시지에 포함된 정보에 기초하여, 공유된 디지털 키의 관리를 수행할 수 있다. 예를 들면, 응답 메시지의 응답 정보가, 공유된 디지털 키의 삭제와 관련된 정보를 포함하고 있는 경우, 전자 디바이스(310)는 전자 디바이스(310)에 저장된 공유된 디지털 키를 삭제할 수 있다. 응답 메시지의 응답 정보가, 공유된 디지털 키의 갱신과 관련된 정보를 포함하고 있는 경우, 전자 디바이스(310)는 전자 디바이스(310)에 저장된 공유된 디지털 키를 갱신할 수 있다.
- [0157] 상술한 옵션 1 시나리오 및 옵션 2 시나리오에서 도 10에서 설명된 바와 같은 디지털 키 관리 절차가 수행되는 경우, 아래와 같은 동작이 수행될 수 있다.
- [0158] 일 실시 예에서, 다른 사용자의 공유된 디지털 키의 관리(예: 삭제 또는 갱신)가 오너에 의해 요청되는 경우, 공유된 디지털 키의 관리에 대한 알림이 다른 사용자의 전자 디바이스(240) 또는 다른 사용자의 전자 디바이스에 대한 백엔드 서버(230)로 전송될 수 있다.
- [0159] 다른 실시 예에서, 다른 사용자의 공유된 디지털 키의 관리(예: 삭제)가 다른 사용자에게 의해 요청되는 경우, 공유된 디지털 키의 관리에 대한 알림이 오너 디바이스(100) 또는 오너 디바이스의 백엔드 서버(210)로 전송될 수 있다. 상술한 바와 같은 절차들을 통해, 제2 백엔드 서버에 의해 개시 또는 트리거링된 디지털 키 관리 동작이 수행될 수 있다.
- [0161] 본 개시의 다양한 실시 예들에 따른 디지털 키를 관리하는 전자 디바이스(310)의 동작 방법은, 공유된 디지털

키를 관리하기 위한 요청 메시지에 대한 응답 메시지를 수신하는 단계와, 수신된 응답 메시지에 포함된 정보를 확인하는 단계와, 확인된 정보에 기초하여 공유된 디지털 키를 관리하는 단계를 포함할 수 있다.

- [0162] 본 개시의 다양한 실시 예들에 따른 요청 메시지는, 공유된 디지털 키의 정보, 요청 정보, 라우팅 정보, 또는 요청 메시지를 송신하는 디바이스의 서명 중 적어도 하나를 포함할 수 있고, 응답 메시지는, 공유된 디지털 키의 정보, 응답 정보, 라우팅 정보, 또는 응답 메시지를 송신하는 디바이스의 서명 중 적어도 하나를 포함할 수 있다.
- [0163] 본 개시의 다양한 실시 예들에 따른 요청 정보는, 공유된 디지털 키의 관리를 요청하는 정보를 포함할 수 있고, 응답 정보는, 공유된 디지털 키의 관리에 대한 결과를 포함할 수 있고, 공유된 디지털 키의 관리는, 공유된 디지털 키의 삭제 또는 갱신 중 적어도 하나를 포함할 수 있다.
- [0164] 본 개시의 다양한 실시 예들에 따른 공유된 디지털 키의 삭제는, 공유된 디지털 키의 공유 권한의 삭제를 포함할 수 있고, 공유된 디지털 키의 갱신은, 공유된 디지털 키의 사용 기한 또는 사용 권한에 관한 정보를 갱신하는 것을 나타낼 수 있다.
- [0165] 본 개시의 다양한 실시 예들에 따른 전자 디바이스(310)의 동작 방법은, 공유된 디지털 키의 관리에 대한 정보를 제3 전자 디바이스(310)로 송신하는 단계를 더 포함할 수 있다.
- [0166] 본 개시의 다양한 실시 예들에 따른 요청 메시지 또는 상기 응답 메시지는, NFC(near field communication)를 이용한 통신 방식 또는 HTTP(hypertext transfer protocol)를 이용한 통신 방식을 통해 송신될 수 있고, 일 실시 예에서, HTTP를 이용한 통신 방식이 사용되는 경우, 요청 메시지 또는 응답 메시지는, 제1 백엔드 서버 또는 제2 백엔드 서버를 통해 송신될 수 있다.
- [0167] 본 개시의 다양한 실시 예들에 따른 전자 디바이스(310)의 동작 방법은, 공유된 디지털 키를 관리하기 위한 요청 메시지를 생성하는 단계와, 생성된 요청 메시지를 타겟 디바이스(320)로 송신하는 단계를 더 포함할 수 있다.
- [0168] 본 개시의 다양한 실시 예들에 따라, 제1 백엔드 서버에 의해 공유된 디지털 키의 관리가 개시 또는 트리거링되는 경우, 요청 메시지는, 제1 백엔드 서버에서 생성될 수 있고, 생성된 요청 메시지는, 제2 백엔드 서버로 송신될 수 있고, 응답 메시지는, 제2 백엔드 서버로 송신된 요청 메시지에 기초하여 변경된 요청 메시지에 대한 응답 메시지일 수 있다.
- [0169] 본 개시의 다양한 실시 예들에 따라, 제2 백엔드 서버에 의해 공유된 디지털 키의 관리가 개시 또는 트리거링되는 경우, 요청 메시지는, 제2 백엔드 서버에 의해 생성될 수 있고, 생성된 요청 메시지는, 타겟 디바이스(320)로 송신될 수 있고, 응답 메시지는, 타겟 디바이스(320)로 송신된 요청 메시지에 대한 응답 메시지일 수 있다.
- [0171] 본 개시의 다양한 실시 예들에 따른 디지털 키를 관리하는 타겟 디바이스(320)의 동작 방법은, 공유된 디지털 키를 관리하기 위한 요청 메시지에 포함된 정보를 확인하는 단계와, 확인된 정보에 기초하여 상기 요청 메시지에 대한 응답 메시지를 생성하는 단계와, 생성된 응답 메시지를 송신하는 단계를 포함할 수 있다.
- [0172] 본 개시의 다양한 실시 예들에 따른 타겟 디바이스(320)의 동작 방법은, 공유된 디지털 키를 관리하기 위한 요청 메시지를 수신하는 단계를 더 포함할 수 있고, 요청 메시지는, 공유된 디지털 키의 정보, 요청 정보, 라우팅 정보, 또는 요청 메시지를 송신하는 디바이스의 서명 중 적어도 하나를 포함할 수 있고, 응답 메시지는, 공유된 디지털 키의 정보, 응답 정보, 라우팅 정보, 또는 응답 메시지를 송신하는 디바이스의 서명 중 적어도 하나를 포함할 수 있다.
- [0173] 후술하는 도 11 내지 도 13은 상술한 전자 디바이스 및 타겟 디바이스의 구성을 도시한다.
- [0175] 도 11은 본 개시의 다양한 실시 예들에 따른 전자 디바이스의 구성을 도시한 도면이다. 도 11에서 전자 디바이스(310)는, 오너 디바이스(100) 또는 다른 사용자의 전자 디바이스(240)를 의미할 수 있다.
- [0176] 도 11을 참고하면, 전자 디바이스(310)는 프로세서(1110), 통신부(1120), 메모리(1130), 보안 요소(1150)와 각 구성을 연결하는 버스(BUS)(1140)를 포함할 수 있다. 그러나, 도 11에 도시된 구성 요소 모두보다 많은 구성 요소에 의해 전자 디바이스(310)가 구현될 수도 있다.

- [0177] 도 11에서는 전자 디바이스(310)가 하나의 프로세서를 포함하는 것으로 도시되었으나, 본 개시의 실시 예는 이에 제한되지 않으며, 전자 디바이스(310)는 복수의 프로세서들을 포함할 수 있다. 이하, 서술되는 프로세서(1110)의 동작 및 기능들의 적어도 일부는 복수의 프로세서들에 의해 수행될 수 있다. 도 11에 도시된 전자 디바이스(310)는, 본 개시의 다양한 실시 예들에 따른 공유된 디지털 키의 관리 방법을 수행할 수 있으며, 도 3 내지 도 10에 대한 설명이 적용될 수 있다. 따라서, 상술한 바와 중복되는 내용은 생략한다.
- [0178] 통신부(1120)는, 다른 디바이스, 서버 또는 네트워크와 유무선 통신을 수행할 수 있다. 이를 위해, 통신부(1120)는 다양한 유무선 통신 방법 중 적어도 하나를 지원하는 통신 모듈을 포함할 수 있다. 예를 들어, 통신 모듈은 칩셋(chipset)의 형태일 수도 있고, 또는 통신에 필요한 정보를 포함하는 스티커/마코드를(e.g. NFC tag를 포함하는 스티커)등일 수도 있다.
- [0179] 무선 통신은, 예를 들어, 셀룰러 통신, Wi-Fi(wireless fidelity), Wi-Fi Direct, 블루투스(bluetooth), UWB(ultra wide band) 또는 NFC(near field communication) 중 적어도 하나를 포함할 수 있다. 유선 통신은, 예를 들어, USB 또는 HDMI(high definition multimedia interface) 중 적어도 하나를 포함할 수 있다.
- [0180] 일 실시예에서 통신부(1120)는 근거리 통신(short range communication)을 위한 통신 모듈을 포함할 수 있다. 예를 들어, 통신부(1120)는 위에서 설명한 Wi-Fi, Wi-Fi Direct, 블루투스, NFC 외에 적외선 통신, MST(magnetic secure transmission), 마그네틱 보안 통신과 같은 다양한 근거리 통신을 수행하기 위한 통신 모듈을 포함할 수 있다.
- [0181] 메모리(1130)에는 애플리케이션과 같은 프로그램 및 파일 등과 같은 다양한 종류의 데이터가 설치 및 저장될 수 있다. 프로세서(1110)는 메모리(1130)에 저장된 데이터에 접근하여 이를 이용하거나, 또는 새로운 데이터를 메모리(1130)에 저장할 수도 있다. 일 실시예에서, 메모리(1130)에는 디지털 키의 관리를 위한 프로그램 및 데이터가 설치 및 저장될 수 있다. 그러나 본 개시의 실시 예는 이에 제한되지 않으며, 디지털 키의 관리를 위한 프로그램 및 데이터는 보안 요소(1150)에 설치 및 저장될 수도 있다. 일 실시 예에서, 메모리(1130)에는 오너가 아닌 다른 사용자의 공유된 디지털 키에 대한 정보가 저장될 수 있다.
- [0182] 보안 요소(1150)는, 전자 디바이스(310)의 보안 저장 장치로서, 인증된 애플리케이션만 접근 가능한 보안 영역이다. 보안 요소(1150)는, 일반 저장 영역과 소프트웨어 적으로 분리되도록 구성되거나, 메모리(1130)와 물리적으로 분리되도록 구성될 수 있다.
- [0183] 프로세서(1110)는 전자 디바이스(310)의 전체적인 동작을 제어하며, CPU, GPU 등과 같은 프로세서를 적어도 하나 이상 포함할 수 있다. 프로세서(1110)는 공유된 디지털 키의 관리를 위한 동작을 수행하도록 전자 디바이스(310)에 포함된 다른 구성들을 제어할 수 있다.
- [0184] 프로세서(1110)는 메모리(1130) 및 보안 요소(1150)에 저장된 프로그램을 실행시키거나, 저장된 파일을 읽어오거나, 새로운 파일을 저장할 수도 있다.
- [0185] 버스(1140)는 통신부(1120), 메모리(1130), 보안 요소(1150) 및 프로세서(1110)를 연결하는 공통 데이터 전송 통로이다.
- [0186] 본 개시의 다양한 실시 예에서, 통신부(1120)는 공유된 디지털 키를 관리하기 위한 요청 메시지에 대한 응답 메시지를 수신할 수 있다. 프로세서(1110)는 수신된 응답 메시지에 포함된 정보를 확인하고, 확인된 정보에 기초하여 공유된 디지털 키를 관리할 수 있다.
- [0187] 본 개시의 다양한 실시 예에서, 요청 메시지는, 공유된 디지털 키의 정보, 요청 정보, 라우팅 정보, 또는 요청 메시지를 송신하는 디바이스의 서명 중 적어도 하나를 포함할 수 있다. 또한, 응답 메시지는, 공유된 디지털 키의 정보, 응답 정보, 라우팅 정보, 또는 응답 메시지를 송신하는 디바이스의 서명 중 적어도 하나를 포함할 수 있다.
- [0188] 본 개시의 다양한 실시 예에서, 요청 정보는, 공유된 디지털 키의 관리를 요청하는 정보를 포함할 수 있다. 응답 정보는, 공유된 디지털 키의 관리에 대한 결과를 포함할 수 있다. 또한, 공유된 디지털 키의 관리는, 공유된 디지털 키의 삭제 또는 갱신 중 적어도 하나를 포함할 수 있다.
- [0189] 본 개시의 다양한 실시 예에서, 공유된 디지털 키의 삭제는, 공유된 디지털 키의 공유 권한의 삭제를 포함할 수 있다. 공유된 디지털 키의 갱신은, 공유된 디지털 키의 사용 기한 또는 사용 권한에 관한 정보를 갱신하는 것을 의미할 수 있다.

- [0190] 본 개시의 다양한 실시 예에서, 프로세서(1110)는 공유된 디지털 키의 관리에 대한 정보를 제3 전자 디바이스로 송신할 수 있다. 이때, 제3 전자 디바이스는 오퍼 디바이스(100), 다른 사용자의 전자 디바이스(240), 오퍼 디바이스 백엔드 서버(210), 타겟 디바이스 백엔드 서버(220) 또는 다른 사용자의 전자 디바이스에 대한 백엔드 서버(230)를 의미할 수 있다.
- [0191] 본 개시의 다양한 실시 예에서, 요청 메시지 또는 응답 메시지는, NFC를 이용한 통신 방식 또는 HTTP를 이용한 통신 방식을 통해 송신될 수 있다. 일 실시 예에서, HTTP를 이용한 통신 방식이 사용되는 경우, 요청 메시지 또는 응답 메시지는, 제1 백엔드 서버 또는 제2 백엔드 서버를 통해 송신될 수 있다.
- [0192] 본 개시의 다양한 실시 예에서, 프로세서(1110)는 공유된 디지털 키를 관리하기 위한 요청 메시지를 생성할 수 있고, 통신부(1120)는 생성된 요청 메시지를 타겟 디바이스로 송신할 수 있다.
- [0193] 본 개시의 다양한 실시 예에서, 제1 백엔드 서버에 의해 디지털 키의 관리가 개시 또는 트리거링되는 경우, 요청 메시지는, 제1 백엔드 서버에서 생성될 수 있고, 생성된 요청 메시지는, 제2 백엔드 서버로 송신될 수 있다. 응답 메시지는, 제2 백엔드 서버로 송신된 요청 메시지에 기초하여 변경된 요청 메시지에 대한 응답 메시지일 수 있다.
- [0194] 본 개시의 다양한 실시 예에서, 제2 백엔드 서버에 의해 공유된 디지털 키의 관리가 개시 또는 트리거링되는 경우, 요청 메시지는, 제2 백엔드 서버에 의해 생성될 수 있고, 생성된 요청 메시지는, 타겟 디바이스로 송신될 수 있고, 응답 메시지는, 타겟 디바이스로 송신된 요청 메시지에 대한 응답 메시지일 수 있다.
- [0196] 도 12는 본 개시의 다양한 실시 예들에 따른 타겟 디바이스의 구성을 도시한 도면이다. 도 12에서 타겟 디바이스(320)는, 전자 디바이스(11)를 의미할 수 있다.
- [0197] 도 12를 참고하면, 타겟 디바이스(320)는 프로세서(1210), 통신부(1220), 메모리(1230), 보안 요소(1250)와 각 구성을 연결하는 버스(BUS)(1240)를 포함할 수 있다. 그러나, 도 12에 도시된 구성 요소 모두보다 많은 구성 요소에 의해 타겟 디바이스(320)가 구현될 수도 있다.
- [0198] 도 12에서는, 타겟 디바이스(320)가 하나의 프로세서를 포함하는 것으로 도시되었으나, 본 개시의 실시 예는 이에 제한되지 않으며, 타겟 디바이스(320)는 복수의 프로세서들을 포함할 수 있다. 이하, 서술되는 프로세서(1210)의 동작 및 기능들의 적어도 일부는 복수의 프로세서들에 의해 수행될 수 있다. 도 12에 도시된 타겟 디바이스(320)는, 본 개시의 다양한 실시 예들에 따른 공유된 디지털 키의 관리 방법을 수행할 수 있으며, 도 3 내지 도 10에 대한 설명이 적용될 수 있다. 따라서, 상술한 바와 중복되는 내용은 생략한다.
- [0199] 통신부(1220)는, 다른 디바이스, 서버 또는 네트워크와 유무선 통신을 수행할 수 있다. 이를 위해, 통신부(1220)는 다양한 유무선 통신 방법 중 적어도 하나를 지원하는 통신 모듈을 포함할 수 있다. 예를 들어, 통신 모듈은 칩셋(chipset)의 형태일 수도 있고, 또는 통신에 필요한 정보를 포함하는 스티커/마코드(e.g. NFC tag)를 포함하는 스티커)등일 수도 있다.
- [0200] 무선 통신은, 예를 들어, 셀룰러 통신, Wi-Fi(wireless fidelity), Wi-Fi Direct, 블루투스(bluetooth), UWB(ultra wide band) 또는 NFC(near field communication) 중 적어도 하나를 포함할 수 있다. 유선 통신은, 예를 들어, USB 또는 HDMI(high definition multimedia interface) 중 적어도 하나를 포함할 수 있다.
- [0201] 일 실시예에서 통신부(1220)는 근거리 통신(short range communication)을 위한 통신 모듈을 포함할 수 있다. 예를 들어, 통신부(1120)는 위에서 설명한 Wi-Fi, Wi-Fi Direct, 블루투스, NFC 외에 적외선 통신, MST(magnetic secure transmission), 마그네틱 보안 통신과 같은 다양한 근거리 통신을 수행하기 위한 통신 모듈을 포함할 수 있다.
- [0202] 메모리(1230)에는 애플리케이션과 같은 프로그램 및 파일 등과 같은 다양한 종류의 데이터가 설치 및 저장될 수 있다. 프로세서(1210)는 메모리(1230)에 저장된 데이터에 접근하여 이를 이용하거나, 또는 새로운 데이터를 메모리(1230)에 저장할 수도 있다. 일 실시예에서, 메모리(1230)에는 디지털 키의 관리를 위한 프로그램 및 데이터가 설치 및 저장될 수 있다. 그러나 본 개시의 실시 예는 이에 제한되지 않으며, 디지털 키의 관리를 위한 프로그램 및 데이터는 보안 요소(1250)에 설치 및 저장될 수도 있다. 일 실시 예에서, 메모리(1230)에는 오퍼가 아닌 다른 사용자의 공유된 디지털 키에 대한 정보가 저장될 수 있다.
- [0203] 보안 요소(1250)는, 타겟 디바이스(320)의 보안 저장 장치로서, 인증된 애플리케이션만 접근 가능한 보안 영역

이다. 보안 요소(1250)는, 일반 저장 영역과 소프트웨어 적으로 분리되도록 구성되거나, 메모리(1230)와 물리적으로 분리되도록 구성될 수 있다.

- [0204] 프로세서(1210)는 타겟 디바이스(320)의 전체적인 동작을 제어하며, CPU, GPU 등과 같은 프로세서를 적어도 하나 이상 포함할 수 있다. 프로세서(1210)는 공유된 디지털 키의 관리를 위한 동작을 수행하도록 타겟 디바이스(320)에 포함된 다른 구성들을 제어할 수 있다.
- [0205] 프로세서(1210)는 메모리(1230) 및 보안 요소(1250)에 저장된 프로그램을 실행시키거나, 저장된 파일을 읽어오거나, 새로운 파일을 저장할 수도 있다.
- [0206] 버스(1240)는 통신부(1220), 메모리(1230), 보안 요소(1250) 및 프로세서(1210)를 연결하는 공통 데이터 전송 통로이다.
- [0207] 본 개시의 다양한 실시 예에서, 프로세서(1210)는 공유된 디지털 키를 관리하기 위한 요청 메시지에 포함된 정보를 확인할 수 있다. 프로세서(1210)는 확인된 정보에 기초하여 요청 메시지에 대한 응답 메시지를 생성할 수 있다. 통신부(1220)는 생성된 응답 메시지를 송신할 수 있다.
- [0208] 본 개시의 다양한 실시 예에서, 통신부(1220)는 공유된 디지털 키를 관리하기 위한 요청 메시지를 수신할 수 있다. 이때, 요청 메시지는, 공유된 디지털 키의 정보, 요청 정보, 라우팅 정보, 또는 요청 메시지를 송신하는 디바이스의 서명 중 적어도 하나를 포함할 수 있고, 응답 메시지는, 공유된 디지털 키의 정보, 응답 정보, 라우팅 정보, 또는 응답 메시지를 송신하는 디바이스의 서명 중 적어도 하나를 포함할 수 있다.
- [0210] 도 13은 본 개시의 다양한 실시 예들에 따른 보안 요소의 구성을 도시한 도면이다.
- [0211] 도 13을 참고하면, 보안 요소(1150)는 통신 인터페이스(1310), 메모리(1320) 및 프로세서(1330)를 포함할 수 있다.
- [0212] 다양한 실시 예에서, 보안 요소(1150)는 전자 디바이스(310)의 보안 저장 장치로서, 인증된 애플리케이션만 접근 가능한 보안 영역이다. 일 실시예에서, 보안 요소(1150)는 embedded Secure Element(eSE), Universal Integrated Circuit Card(UICC), Secure Digital Card(SD Card), embedded UICC (eUICC), 및/또는 Trusted Execution Environment(TEE) 등을 포함할 수 있다.
- [0213] 통신 인터페이스(1310)는 호스트(Host, 101)와 통신할 수 있다. 일 실시예에서, 통신 인터페이스(1310)는 호스트(101)와 통신하기 위한 다양한 유무선 통신 인터페이스 중 적어도 하나를 포함할 수 있다. 여기서 호스트(101)는 전자 디바이스(310)에 포함된 장치들 중 하나일 수 있으며, 예를 들어, AP(Application Processor), 메모리 등을 포함할 수 있다. 통신 인터페이스(1310)는 예를 들어, ISO 7816, USB(Universal Serial Bus), I2C(Inter-Integrated Circuit), SPI(Serial Peripheral Interface), SWP(Single Wire Protocol), 및/또는 UWB(Ultra Wide Band)와 같은 직렬 인터페이스 또는 두 개의 하드웨어 장치들 사이의 통신에 일반적으로 사용되는 임의의 직렬 인터페이스일 수 있다. 또한, 안테나를 하드웨어 장치에 직접 연결시키는 ISO 14443, 지그비(Zigbee), 블루투스(Bluetooth) 등과 같은 무선 인터페이스일 수도 있다. 나아가, 통신 인터페이스(1310)는 전자 디바이스(310)의 중앙 버스(BUS)에 연결되는 병렬 인터페이스일 수도 있으며, 이 경우, 통신 인터페이스(1310)는 호스트(101)로부터의 커맨드와 데이터를 수신하기 위한 버퍼를 포함할 수도 있다.
- [0214] 메모리(1320)에는 애플리케이션과 같은 프로그램 및 파일 등과 같은 다양한 종류의 데이터가 설치 및 저장될 수 있다. 프로세서(1330)는 메모리(1320)에 저장된 데이터에 접근하여 이를 이용하거나, 또는 새로운 데이터를 메모리(1320)에 저장할 수도 있다. 일 실시예에서, 메모리(1320)에는 디지털 키를 처리하기 위한 프로그램 및 데이터가 설치 및 저장될 수 있다.
- [0215] 프로세서(1330)는 보안 요소(1150)의 전체적인 동작을 제어하며, CPU, GPU 등과 같은 프로세서를 적어도 하나 이상 포함할 수 있다. 프로세서(1330)는 디지털 키를 처리하기 위한 동작을 수행하도록 보안 요소(1150)에 포함된 다른 구성들을 제어할 수 있다. 예를 들어, 프로세서(1330)는 메모리(1320)에 저장된 프로그램을 실행시키거나, 저장된 파일을 읽어오거나, 새로운 파일을 저장할 수도 있다. 일 실시예에서, 프로세서(1330)는 메모리(1320)에 저장된 프로그램을 실행함으로써, 디지털 키를 처리하기 위한 동작을 수행할 수 있다.
- [0216] 한편, 도 11의 보안 요소(1150)는 도 12의 보안 요소(1250)에 대응된다. 도 12의 보안 요소(1250)와 관련하여서는 도 11의 설명이 동일하게 적용될 수 있다.

- [0218] 본 개시의 청구항 또는 명세서에 기재된 실시 예들에 따른 방법들은 하드웨어, 소프트웨어, 또는 하드웨어와 소프트웨어의 조합의 형태로 구현될(implemented) 수 있다.
- [0219] 소프트웨어로 구현하는 경우, 하나 이상의 프로그램(소프트웨어 모듈)을 저장하는 컴퓨터 판독 가능 저장 매체가 제공될 수 있다. 컴퓨터 판독 가능 저장 매체에 저장되는 하나 이상의 프로그램은, 전자장치(device) 내의 하나 이상의 프로세서에 의해 실행 가능하도록 구성된다(configured for execution). 하나 이상의 프로그램은, 전자장치로 하여금 본 개시의 청구항 또는 명세서에 기재된 실시 예들에 따른 방법들을 실행하게 하는 명령어(instructions)를 포함할 수 있다.
- [0220] 이러한 프로그램(소프트웨어 모듈, 소프트웨어)은 랜덤 액세스 메모리(random access memory), 플래시(flash) 메모리를 포함하는 불휘발성(non-volatile) 메모리, 롬(ROM: Read Only Memory), 전기적 삭제가능 프로그램가능 롬(EEPROM: Electrically Erasable Programmable Read Only Memory), 자기 디스크 저장 장치(magnetic disc storage device), 콤팩트 디스크 롬(CD-ROM: Compact Disc-ROM), 디지털 다목적 디스크(DVDs: Digital Versatile Discs) 또는 다른 형태의 광학 저장 장치, 마그네틱 카세트(magnetic cassette)에 저장될 수 있다. 또는, 이들의 일부 또는 전부의 조합으로 구성된 메모리에 저장될 수 있다. 또한, 각각의 구성 메모리는 다수 개 포함될 수도 있다.
- [0221] 또한, 프로그램은 인터넷(Internet), 인트라넷(Intranet), LAN(Local Area Network), WLAN(Wide LAN), 또는 SAN(Storage Area Network)과 같은 통신 네트워크, 또는 이들의 조합으로 구성된 통신 네트워크를 통하여 접근(access)할 수 있는 부착 가능한(attachable) 저장 장치(storage device)에 저장될 수 있다. 이러한 저장 장치는 외부 포트를 통하여 본 개시의 실시 예를 수행하는 장치에 접속할 수 있다. 또한, 통신 네트워크상의 별도의 저장장치가 본 개시의 실시 예를 수행하는 장치에 접속할 수도 있다.
- [0222] 한편, 본 개시의 상세한 설명에서는 구체적인 실시 예에 관해 설명하였으나, 본 개시의 범위에서 벗어나지 않는 한도 내에서 여러 가지 변형이 가능함은 물론이다. 그러므로, 본 개시의 범위는 설명된 실시 예에 국한되어 정해져서는 안되며 후술하는 특허청구의 범위뿐만 아니라 이 특허청구의 범위와 균등한 것들에 의해 정해져야 한다.
- [0223] 본 개시에서 개시된 블록도들은 본 개시의 원리들을 구현하기 위한 회로를 개념적으로 표현한 형태라고 당업자에게 해석될 수 있을 것이다. 유사하게, 임의의 흐름 차트, 흐름도, 상태 전이도, 의사코드 등은 컴퓨터 판독 가능 매체에서 실질적으로 표현되어, 컴퓨터 또는 프로세서가 명시적으로 도시되든지 아니든지 간에 이러한 컴퓨터 또는 프로세서에 의해 실행될 수 있는 다양한 프로세스를 나타낸다는 것이 당업자에게 인식될 것이다. 따라서, 상술한 본 개시의 실시예들은 컴퓨터에서 실행될 수 있는 프로그램으로 작성가능하고, 컴퓨터로 읽을 수 있는 기록매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다. 상기 컴퓨터로 읽을 수 있는 기록매체는 마그네틱 저장매체(예를 들면, 롬, 플로피 디스크, 하드디스크 등), 광학적 판독 매체(예를 들면, 시디롬, 디브이디 등)와 같은 저장매체를 포함한다.
- [0224] 도면들에 도시된 다양한 요소들의 기능들은 적절한 소프트웨어와 관련되어 소프트웨어를 실행할 수 있는 하드웨어뿐만 아니라 전용 하드웨어의 이용을 통해 제공될 수 있다. 프로세서에 의해 제공될 때, 이런 기능은 단일 전용 프로세서, 단일 공유 프로세서, 또는 일부가 공유될 수 있는 복수의 개별 프로세서에 의해 제공될 수 있다. 또한, 용어 "프로세서" 또는 "제어부"의 명시적 이용은 소프트웨어를 실행할 수 있는 하드웨어를 배타적으로 지칭하는 것으로 해석되지 말아야 하며, 제한 없이, 디지털 신호 프로세서(DSP) 하드웨어, 소프트웨어를 저장하기 위한 판독 전용 메모리(ROM), 랜덤 액세스 메모리(RAM), 및 비휘발성 저장장치를 명시적으로 포함할 수 있다.
- [0225] 본 명세서의 청구항들에서, 특정 기능을 수행하기 위한 수단으로서 표현된 요소는 특정 기능을 수행하는 임의의 방식을 포괄하고, 이러한 요소는 특정 기능을 수행하는 회로 요소들의 조합, 또는 특정 기능을 수행하기 위한 소프트웨어를 수행하기 위해 적합한 회로와 결합된, 펌웨어, 마이크로코드 등을 포함하는 임의의 형태의 소프트웨어를 포함할 수 있다.
- [0226] 본 명세서에서 본 개시의 원리들의 '일 실시예'와 이런 표현의 다양한 변형들의 지칭은 이 실시예와 관련되어 특정 특징, 구조, 특성 등이 본 개시의 원리의 적어도 하나의 실시예에 포함된다는 것을 의미한다. 따라서, 표현 '일 실시예에서'와, 본 명세서 전체를 통해 개시된 임의의 다른 변형체들은 반드시 모두 동일한 실시예를 지칭하는 것은 아니다.

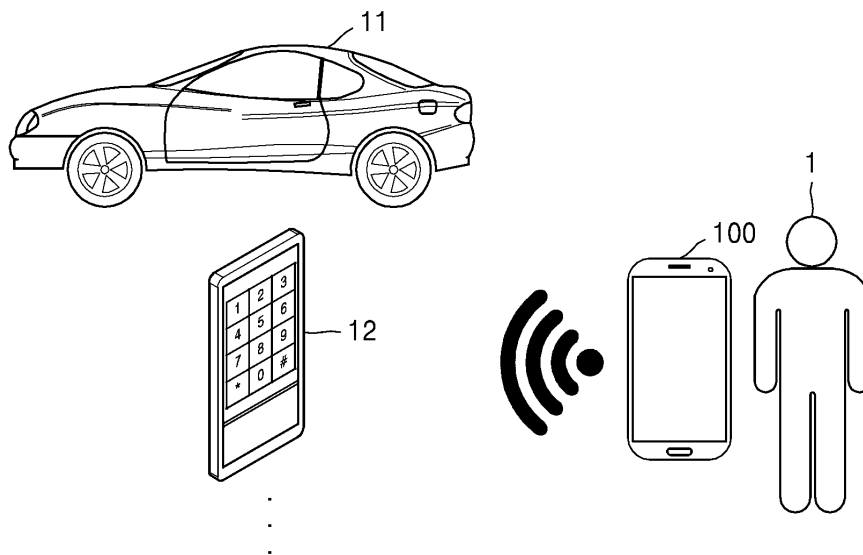
[0227] 본 명세서에서, 'A와 B 중 적어도 하나'의 경우에서 '~중 적어도 하나'의 표현은, 첫 번째 옵션 (A)의 선택만, 또는 두 번째 열거된 옵션 (B)의 선택만, 또는 양쪽 옵션들 (A와 B)의 선택을 포괄하기 위해 사용된다. 추가적인 예로 'A, B, 및 C 중 적어도 하나'의 경우는, 첫 번째 열거된 옵션 (A)의 선택만, 또는 두 번째 열거된 옵션 (B)의 선택만, 또는 세 번째 열거된 옵션 (C)의 선택만, 또는 첫 번째와 두 번째 열거된 옵션들 (A와 B)의 선택만, 또는 두 번째와 세 번째 열거된 옵션 (B와 C)의 선택만, 또는 모든 3개의 옵션들의 선택(A와 B와 C)이 포괄할 수 있다. 더 많은 항목들이 열거되는 경우에도 당업자에게 명백하게 확장 해석될 수 있다.

[0228] 이제까지 본 개시에 대하여 그 바람직한 실시예들을 중심으로 살펴보았다.

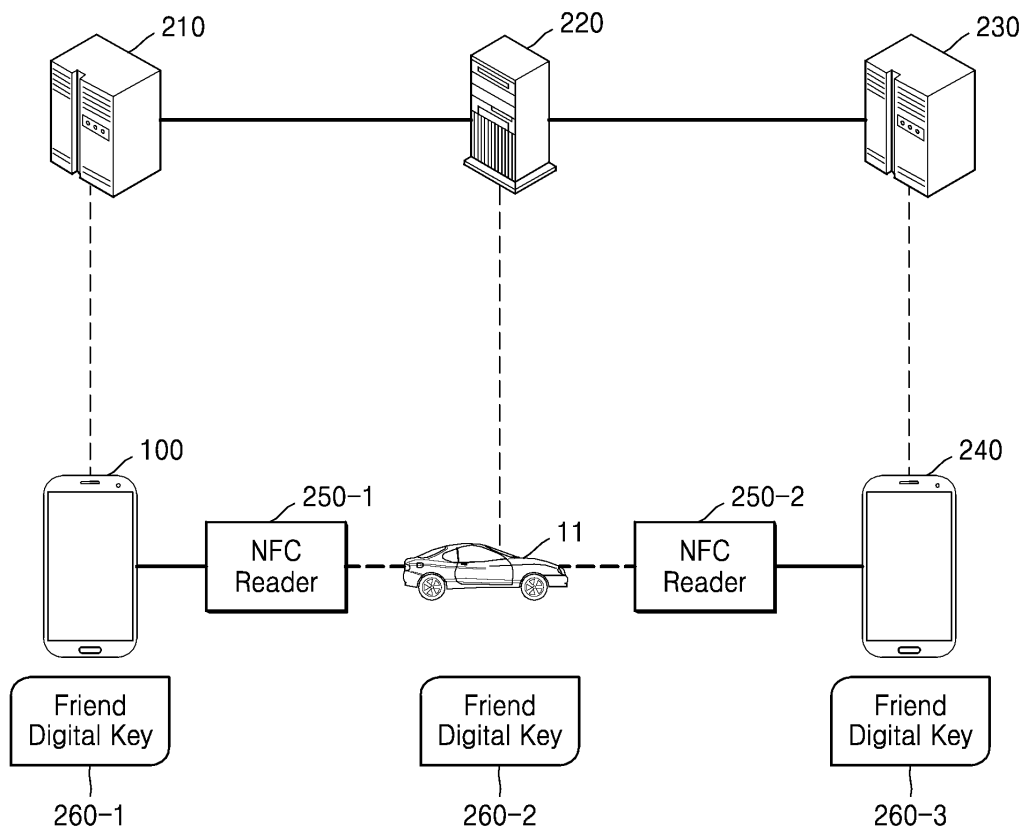
[0229] 본 명세서를 통해 개시된 모든 실시예들과 조건부 예시들은, 본 개시의 기술 분야에서 통상의 지식을 가진 당업자가 독자가 본 개시의 원리와 개념을 이해하도록 돕기 위한 의도로 기술된 것으로, 당업자는 본 개시가 본 개시의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 개시의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 개시에 포함된 것으로 해석되어야 할 것이다.

도면

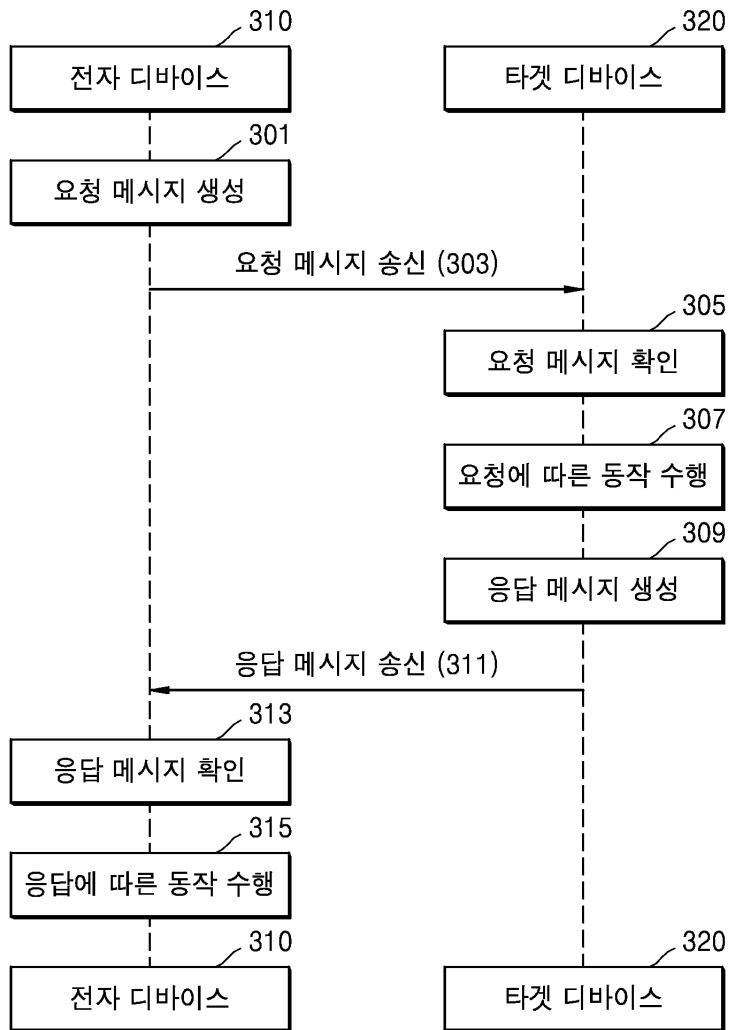
도면1



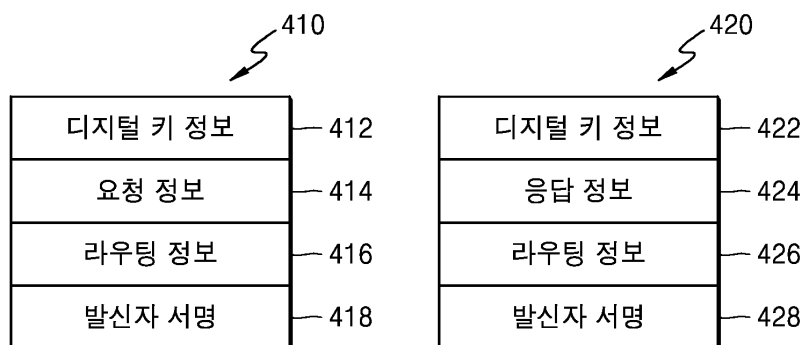
도면2



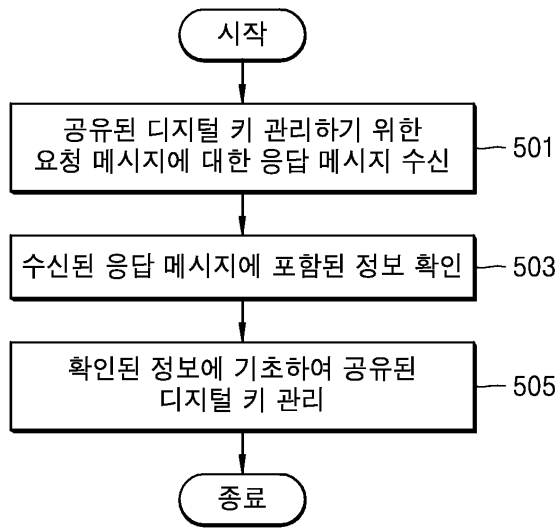
도면3



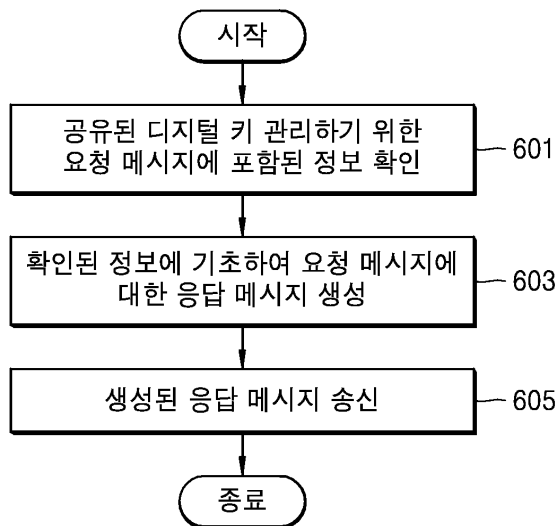
도면4



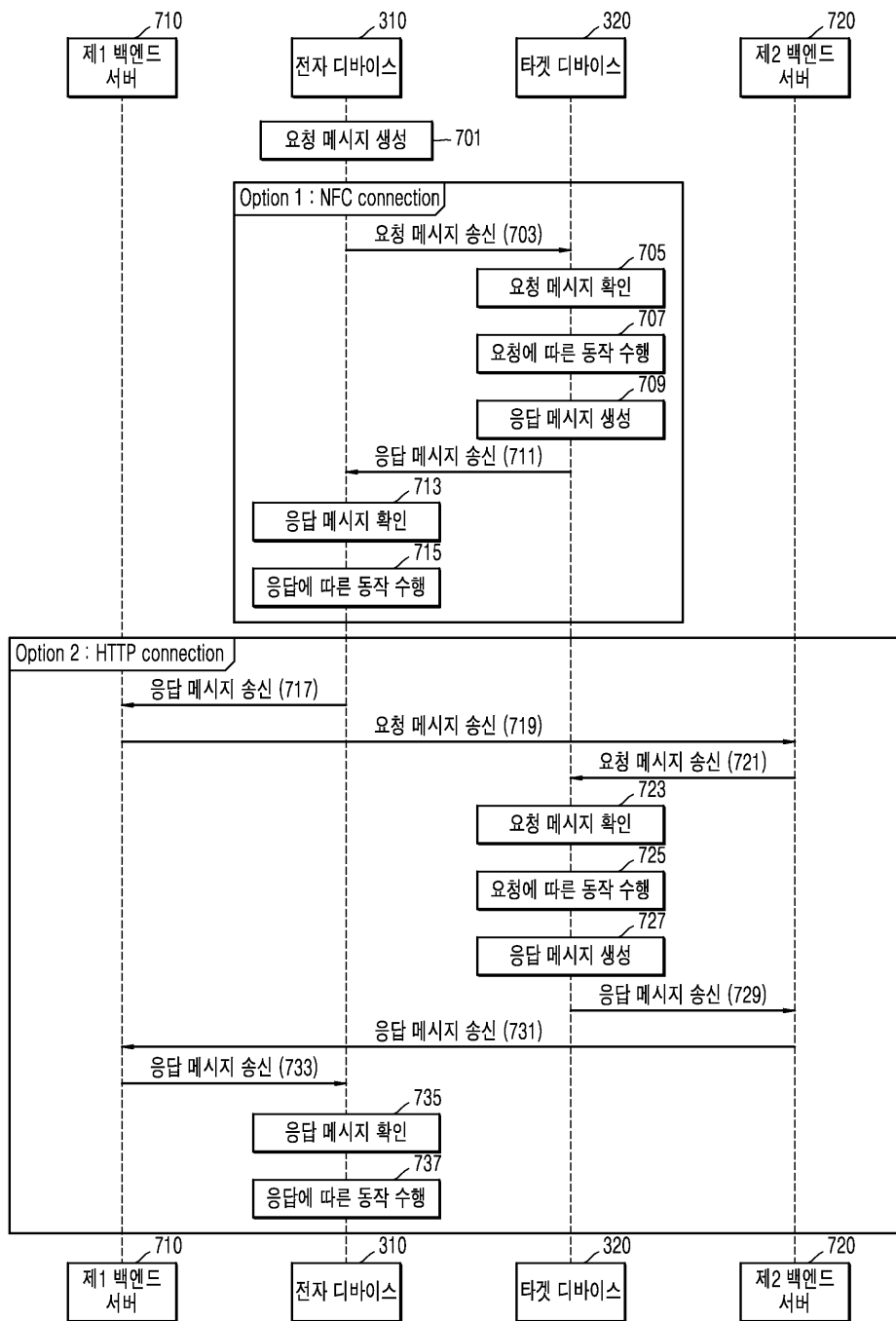
도면5



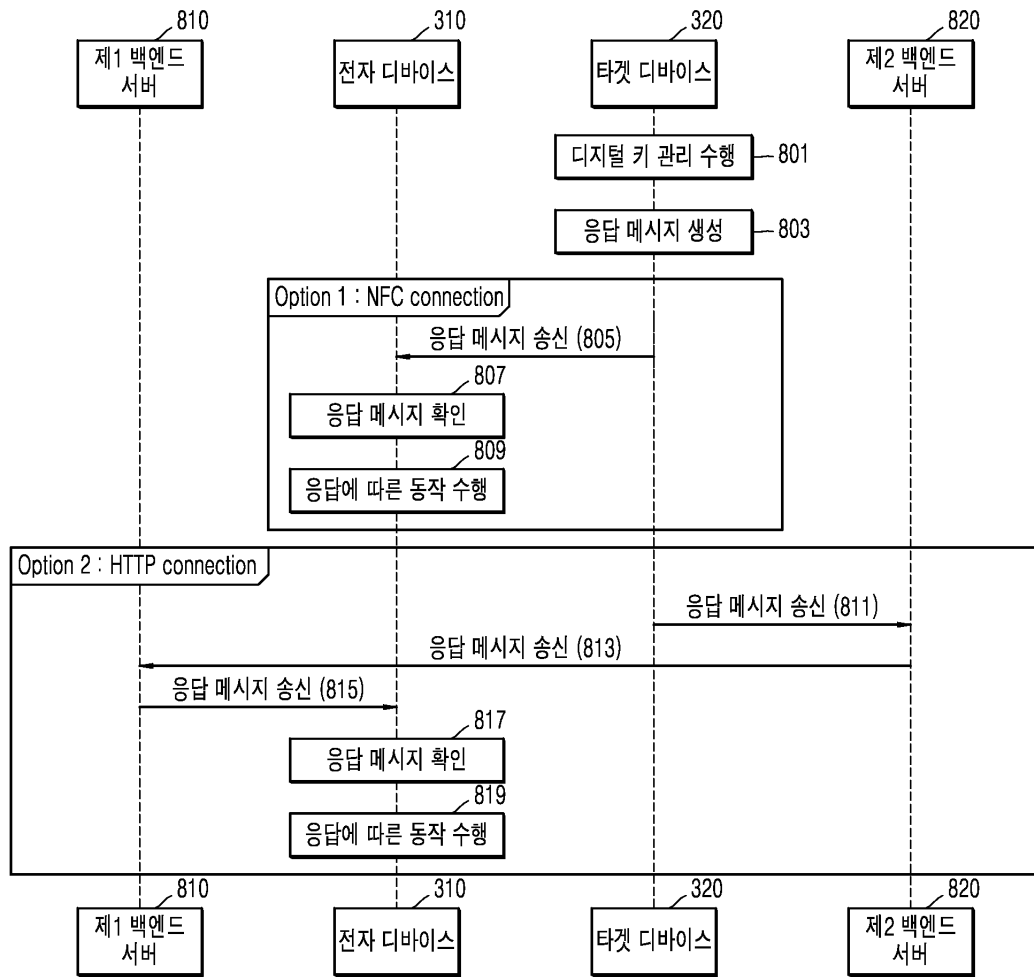
도면6



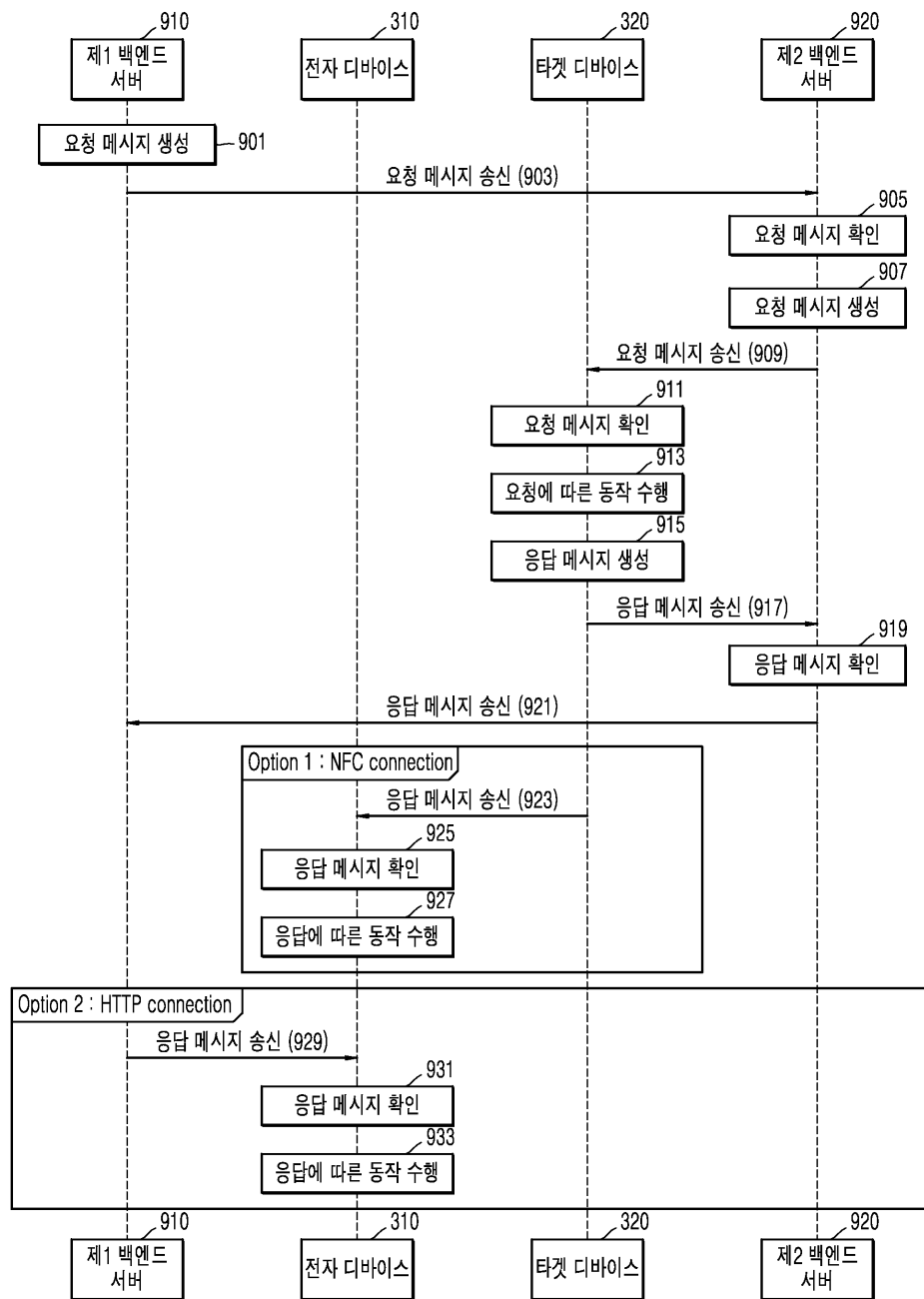
도면7



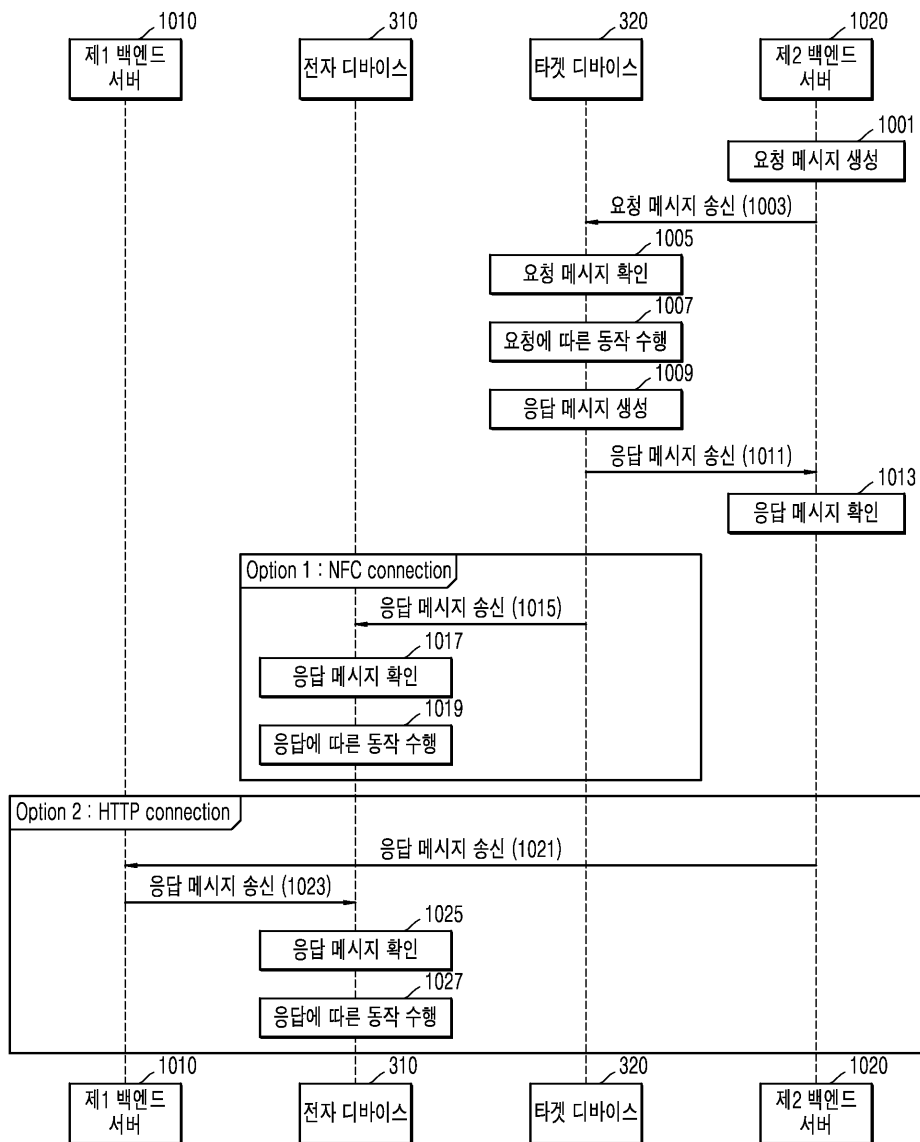
도면8



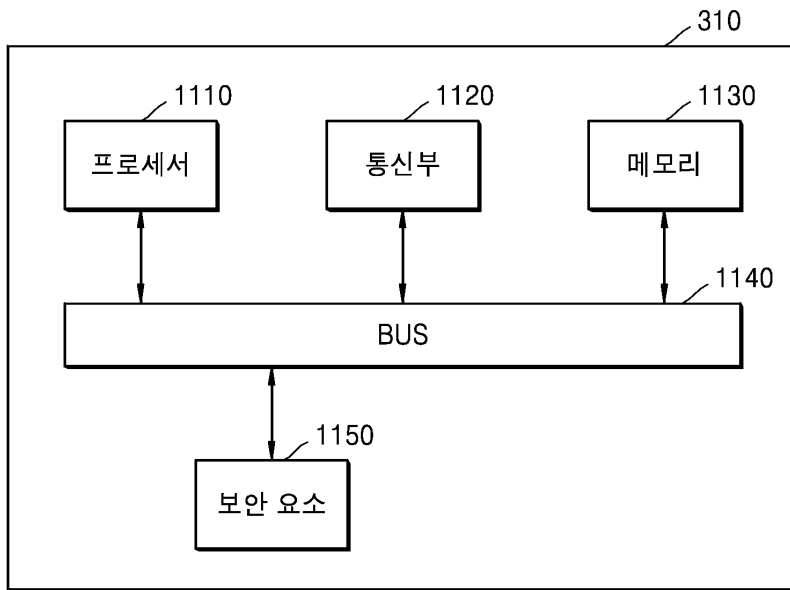
도면9



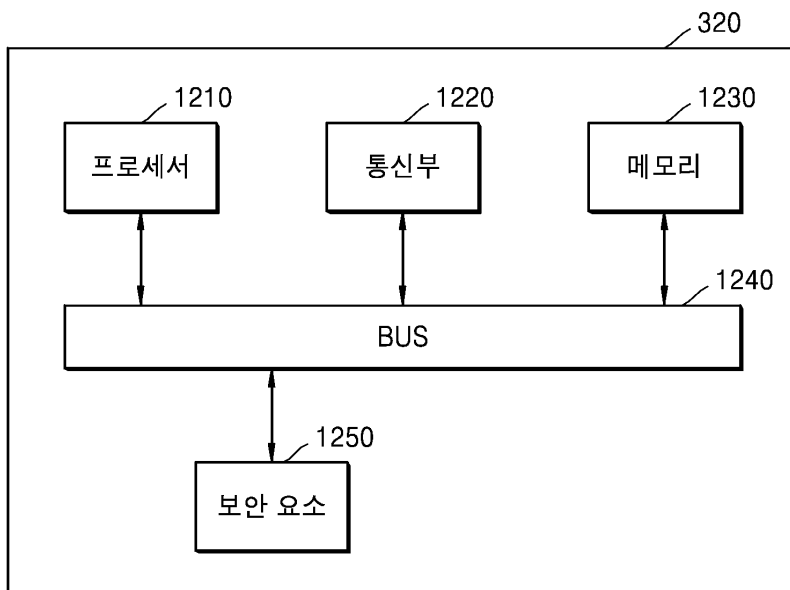
도면10



도면11



도면12



도면13

