(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년02월11일
(11) 등록번호 10-2362795
(24) 등록일자 2022년02월09일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/06* (2006.01)
H04W 12/06 (2021.01) *H04W 76/10* (2018.01)
(52) CPC특허분류
H04L 9/3236 (2013.01)
H04L 9/0643 (2013.01)
(21) 출원번호 10-2017-0124853
(22) 출원일자 2017년09월27일
심사청구일자 2020년01월14일
(65) 공개번호 10-2019-0036068
(43) 공개일자 2019년04월04일
(56) 선행기술조사문헌
US20050038707 A1*
(뒷면에 계속)
전체 청구항 수 : 총 10 항

(73) 특허권자
삼성에스디에스 주식회사
서울특별시 송파구 올림픽로35길 125 (신천동)
(72) 발명자
김도형
서울특별시 송파구 올림픽로35길 125 (신천동, 삼성SDS West Campus)
황순형
서울특별시 송파구 올림픽로35길 125 (신천동, 삼성SDS West Campus)
(뒷면에 계속)
(74) 대리인
특허법인가산

심사관 : 나용수

(54) 발명의 명칭 **해시 체인을 이용한 단말 간 인증 절차를 거치는 단말 간 통신 방법**

(57) 요 약

단말 간의 통신 방법이 제공된다. 본 발명의 일 실시예에 따른 단말 간의 통신 방법은, 제1 단말이 해시값들의 순차적인 연결인 해시 체인을 포함하는 제1 인증 데이터를 저장하고, 제2 단말이 상기 해시 체인의 최초 해시값을 포함하는 제2 인증 데이터를 저장하는 단계와, 상기 제1 단말이, 상기 해시 체인의 최후 해시값을 상기 제2 단말에 송신하는 단계와, 상기 제2 단말이, 상기 최후 해시값과 일치되는 값이 나올때까지 상기 제2 단말에 저장된 상기 최초 해시값을 반복적으로 해시함으로써, 상기 제1 단말과 상기 제2 단말 간의 인증 성공 여부를 판정하는 단계와, 상기 판정의 결과 인증 성공의 경우, 상기 제1 단말 및 상기 제2 단말이 상기 제1 단말과 상기 제2 단말 간의 커넥션 설립 프로세스를 수행하는 단계를 포함한다.

대 표 도 - 도5

(52) CPC특허분류
H04W 12/06 (2021.01)
H04W 76/10 (2018.02)
H04L 2209/38 (2013.01)

(72) 발명자
노세혁
서울특별시 송파구 올림픽로35길 125 (신천동, 삼성SDS West Campus)
전남수
서울특별시 송파구 올림픽로35길 125 (신천동, 삼성SDS West Campus)
김원경
서울특별시 송파구 올림픽로35길 125 (신천동, 삼성SDS West Campus)
정재성
서울특별시 송파구 올림픽로35길 125 (신천동, 삼성SDS West Campus)
김미란
서울특별시 송파구 올림픽로35길 125 (신천동, 삼성SDS West Campus)
최주희
서울특별시 송파구 올림픽로35길 125 (신천동, 삼성SDS West Campus)

(56) 선행기술조사문헌
US08984602 B1*
US20090024848 A1*
KR1020170057576 A*
US20070266244 A1*
US20050283444 A1*
*는 심사관에 의하여 인용된 문헌

명 세 서

청구범위

청구항 1

제1 단말이 해시값들의 순차적인 연결인 해시 체인을 포함하는 제1 인증 데이터를 저장하고, 제2 단말이 상기 해시 체인의 최초 해시값을 포함하는 제2 인증 데이터를 저장하는 단계;

상기 제1 단말이, 상기 해시 체인의 최후 해시값을 상기 제2 단말에 송신하는 단계;

상기 제2 단말이, 상기 최후 해시값과 일치되는 값이 나올때까지 상기 제2 단말에 저장된 상기 최초 해시값을 반복적으로 해시함으로써, 상기 제1 단말과 상기 제2 단말 간의 인증 성공 여부를 판정하는 단계;

상기 판정의 결과 인증 성공의 경우, 상기 제1 단말 및 상기 제2 단말이 상기 제1 단말과 상기 제2 단말 간의 커넥션 설립 프로세스를 수행하는 단계;

상기 제1 단말과 상기 제2 단말 간의 인증이 실패한 것으로 판정되면, 상기 제1 단말이 상기 해시 체인의 다른 해시값을 상기 제2 단말로 송신하는 단계;

상기 제2 단말이, 상기 다른 해시값과 동일한 해시값이 나올때까지 상기 최초 해시값을 반복적으로 해시하는 단계; 및

상기 다른 해시값과 동일한 해시값이 나오지 않으면, 상기 제1 단말과 상기 제2 단말 간에 인증에 실패한 것으로 판정하는 단계를 포함하고,

상기 다른 해시값은 상기 최후 해시값과 상이한 것인,

단말 간 통신 방법.

청구항 2

제1 항에 있어서,

상기 제1 인증 데이터는 최대 카운트 값을 더 포함하고,

상기 최후 해시값은 상기 해시 체인에 포함된 해시값들 중 상기 최대 카운트를 오프셋(offset)으로 하는 해시값이며,

상기 해시 체인의 해시값이 상기 제1 단말에서 상기 제2 단말로 전송될 때마다 상기 최대 카운트가 1씩 차감되고,

상기 제1 단말은 상기 최대 카운트가 설정 값 이하가 되면, 키 토큰의 갱신을 요청하고,

상기 키 토큰의 갱신 요청에 대한 응답으로 상기 키 토큰이 갱신되고,

상기 제1 단말에 저장된 상기 해시 체인 및 상기 제2 단말에 저장된 상기 최초 해시값은, 상기 키 토큰을 이용하여 생성되는 것인,

단말 간 통신 방법.

청구항 3

제1 항에 있어서,

상기 제1 인증 데이터는 최대 카운트 값을 더 포함하고,

상기 최후 해시값은 상기 해시 체인에 포함된 해시값들 중 상기 최대 카운트를 오프셋(offset)으로 하는 해시값이며,

상기 해시 체인의 해시값이 상기 제1 단말에서 상기 제2 단말로 전송될 때마다 상기 최대 카운트가 1씩 차감되고,

상기 제1 단말은 상기 최대 카운트가 설정 값 이하가 되면, 키 토큰의 폐기를 요청하고,

상기 제1 단말에 저장된 상기 해시 체인 및 상기 제2 단말에 저장된 상기 최초 해시값은, 상기 키 토큰을 이용하여 생성되는 것인,

단말 간 통신 방법.

청구항 4

제1 항에 있어서,

상기 커넥션 설립 프로세스는 블루투스 페어링 프로세스이고,

해시 체인을 포함하는 제1 인증 데이터를 저장하는 단계는,

서비스 서버로부터 상기 해시 체인을 수신하여 저장하는 단계를 포함하고,

상기 해시 체인의 최후 해시값을 상기 제2 단말에 송신하는 단계는,

블루투스 페어링 요청 신호에 상기 최후 해시값을 수납하여 상기 제2 단말에 송신하는 단계를 포함하는,

단말 간 통신 방법.

청구항 5

제1 항에 있어서,

제1 단말이 해시값들의 순차적인 연결인 해시 체인을 포함하는 제1 인증 데이터를 저장하고, 제2 단말이 상기 해시 체인의 최초 해시값을 포함하는 제2 인증 데이터를 저장하는 단계는,

상기 제1 단말의 사용자에 의하여 서비스 서버에 요청 된 예약 요청의 결과로, 상기 제1 단말이 상기 제1 인증 데이터를 상기 서비스 서버로부터 수신하여 저장하고, 상기 제2 단말이 상기 제2 인증 데이터를 상기 서비스 서버로부터 수신하여 저장하는 단계를 포함하고,

상기 제1 단말과 상기 제2 단말 간의 인증 성공 여부를 판정하는 단계는, 상기 서비스 서버와의 데이터 송수신 없이 상기 제1 단말과 상기 제2 단말 간의 인증 성공 여부를 판정하는 단계를 포함하고,

커넥션 설립 프로세스를 수행하는 단계는, 상기 서비스 서버와의 데이터 송수신 없이 커넥션 설립 프로세스를 수행하는 단계를 포함하는,

단말 간 통신 방법.

청구항 6

제5 항에 있어서,

상기 제1 인증 데이터는, 상기 제2 단말의 식별 정보를 더 포함하고,

상기 제1 단말이, 상기 해시 체인의 상기 최후 해시값을 상기 제2 단말에 송신하는 단계는,

상기 제2 단말이, 상기 제2 단말의 식별 정보가 수납된 광고(advertising) 신호를 송출하는 단계; 및

상기 제1 단말이, 상기 광고 신호를 감지하여, 상기 광고 신호에 수납된 식별 정보를 상기 제1 인증 데이터에 포함된 식별 정보와 비교하고, 비교 결과 두개의 식별 정보가 일치하는 것으로 판정된 경우, 상기 최후 해시값을 상기 제2 단말에 송신하는 단계를 포함하는,

단말 간 통신 방법.

청구항 7

제6 항에 있어서,

상기 예약 요청은 유효 기간에 대한 정보를 포함하고,

상기 제2 인증 데이터는 상기 유효 기간에 대한 정보를 더 포함하며,

상기 제2 단말이, 상기 제2 단말의 식별 정보가 수납된 광고(advertising) 신호를 송출하는 단계는,

상기 유효 기간 동안 상기 제2 단말의 식별 정보가 수납된 광고(advertising) 신호를 송출하는 단계를 포함하는,

단말 간 통신 방법.

청구항 8

제6 항에 있어서,

상기 예약 요청은 유효 기간에 대한 정보를 포함하고,

상기 제1 인증 데이터는 상기 유효 기간에 대한 정보를 더 포함하며,

상기 제1 단말이, 상기 광고 신호를 감지하여, 상기 광고 신호에 수납된 식별 정보를 상기 제1 인증 데이터에 포함된 식별 정보와 비교하고, 비교 결과 두개의 식별 정보가 일치하는 것으로 판정된 경우, 상기 최후 해시값을 상기 제2 단말에 송신하는 단계는,

상기 제1 단말이, 상기 광고 신호를 감지하기 위한 스캐닝을 상기 유효 기간 도중에 활성화 하는 단계를 포함하는,

단말 간 통신 방법.

청구항 9

제1 항에 있어서,

상기 제1 단말 및 상기 제2 단말이 상기 제1 단말과 상기 제2 단말 간의 커넥션 설립 프로세스를 수행하는 단계는,

상기 커넥션 설립 프로세스의 성공 시, 상기 제1 단말 및 상기 제2 단말 중 적어도 하나가 상기 제1 단말에 대한 사용자 입력 없이 디폴트 프로세스를 수행하는 단계를 포함하는,

단말 간 통신 방법.

청구항 10

제9 항에 있어서,

상기 제2 단말은, 차량에 구비된 상기 차량을 제어 하는 단말이고,

상기 커넥션 설립 프로세스의 성공 시, 상기 제1 단말 및 상기 제2 단말 중 적어도 하나가 상기 제1 단말에 대한 사용자 입력 없이 디폴트 프로세스를 수행하는 단계는,

상기 제2 단말이 상기 차량의 문을 오픈하는 제어 신호를 송신하는 단계; 및

상기 제1 단말이 디바이스 간 근거리 무선 통신 기반의 차량 제어 앱을 실행하는 단계를 포함하는,

단말 간 통신 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 단말 간 통신 방법에 관한 것이다. 보다 자세하게는, 해시값들의 순차적인 연결인 해시 체인을 이용하여 단말 간 커넥션 연결을 위한 단말 간 인증을 수행한 후 데이터가 송수신 되는 단말 간 통신 방법에 관한 것이다.

배 경 기 술

[0002] 블루투스(Bluetooth), 와이파이(WiFi), 지그비(Zig bee) 및 NFC(Near Field Communication) 등의 근거리 무선 통신(Short-range Wireless Communication) 기술이 알려져 있다. 상기 근거리 무선 통신 기술을 이용하여 단말 간에 데이터를 송수신 하기 위하여, 커넥션 설립 프로세스가 선행 되어야 한다. 예를 들어, 블루투스 기술을 이

용하여 단말 간 데이터 통신을 위하여, 페어링(pairing) 절차를 거쳐야 한다.

[0003] 상기 커넥션 설립 프로세스에서 수행되는 단말 간의 상호 인증 방법 중 빠르면서도 높은 보안성을 만족시킬 수 있는 방법의 제공이 요청되고 있다.

[0004] 한편, 단말 간 근거리 무선 통신 기술에 기반한 다양한 서비스가 제공 될 수 있다. 예를 들어, 차량 공유 서비스는 스마트 폰 등의 사용자 단말과 차량 내부에 설치된 차량 단말 사이의 근거리 무선 통신 기술을 기반으로 하여, 사용자의 차량 제어를 지원할 수 있다. 이 때, 근거리 무선 통신을 수행해야 하는 위치가 통신 음영 지역인 경우, 단말과 서비스 서버 사이의 데이터 송수신을 통한 단말 인증이 불가능할 것이기 때문에, 서비스 서버에 의하여 중개 되는 단말 간 근거리 무선 통신의 커넥션 설립 프로세스가 상기 서비스 서버와의 네트워크 연결이 불가능한 경우에도 수행될 수 있도록 지원할 필요가 있다.

선행기술문헌

특허문헌

[0005] (특허문헌 0001) 한국공개특허 제2013-0057373호

발명의 내용

해결하려는 과제

[0006] 본 발명이 해결하고자 하는 기술적 과제는, 해시값들의 순차적인 연결인 해시 체인을 이용하여 단말 간의 통신 연결을 위한 인증 절차를 거치는 단말 간 통신 방법, 그 단말 장치 및 상기 서비스 서버를 제공하는 것이다.

[0007] 본 발명이 해결하고자 하는 기술적 과제는, 서비스 서버에 의하여 중개 되는 단말 간 근거리 무선 통신의 커넥션 설립 프로세스가 상기 서비스 서버와의 네트워크 연결이 불가능한 경우에도 수행될 수 있는, 단말 간 통신 방법, 그 단말 장치 및 상기 서비스 서버를 제공하는 것이다.

[0008] 본 발명이 해결하고자 하는 다른 기술적 과제는, 서비스 서버에 의하여 중개 되는 단말 간 근거리 무선 통신의 커넥션 설립 프로세스를 단말의 사용자의 별도 사용자 입력 없이, 각 단말의 위치가 근접한 경우 자동적으로 개시하는, 단말 간 통신 방법, 그 단말 장치 및 상기 서비스 서버를 제공하는 것이다.

[0009] 본 발명이 해결하고자 하는 또 다른 기술적 과제는, 서비스 서버에 의하여 중개 되는 단말 간 근거리 무선 통신의 커넥션 설립 프로세스를 단말의 사용자의 별도 사용자 입력 없이, 각 단말의 위치가 근접한 경우 자동적으로 개시하되, 상기 커넥션 설립 프로세스가 자동적으로 개시되기 위한 전력 소모를 절감하는, 단말 간 통신 방법 및 그 단말 장치를 제공하는 것이다.

[0010] 본 발명의 기술적 과제들은 이상에서 언급한 기술적 과제들로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 본 발명의 기술분야에서의 통상의 기술자에게 명확하게 이해 될 수 있을 것이다.

과제의 해결 수단

[0011] 상기 언급된 문제점들을 해결하기 위한 본 발명의 일 실시예에 따른 단말 간 통신 방법은, 제1 단말이 해시값들의 순차적인 연결인 해시 체인을 포함하는 제1 인증 데이터를 저장하고, 제2 단말이 상기 해시 체인의 최초 해시값을 포함하는 제2 인증 데이터를 저장하는 단계와, 상기 제1 단말이, 상기 해시 체인의 최후 해시값을 상기 제2 단말에 송신하는 단계와, 상기 제2 단말이, 상기 최후 해시값과 일치되는 값이 나올때까지 상기 제2 단말에 저장된 상기 최초 해시값을 반복적으로 해시함으로써, 상기 제1 단말과 상기 제2 단말 간의 인증 성공 여부를 판정하는 단계와, 상기 판정의 결과 인증 성공의 경우, 상기 제1 단말 및 상기 제2 단말이 상기 제1 단말과 상기 제2 단말 간의 커넥션 설립 프로세스를 수행하는 단계를 포함한다.

[0012] 일 실시예에서, 상기 제1 인증 데이터는 최대 카운트 값을 더 포함하고, 상기 최후 해시값은 상기 해시 체인에 포함된 해시값들 중 상기 최대 카운트를 오프셋(offset)으로 하는 해시값이며, 상기 해시 체인의 최후 해시값을 상기 제2 단말에 송신하는 단계는, 상기 최대 카운트 값을 상기 최후 해시값과 함께 상기 제2 단말에 송신하는 단계를 포함하고, 상기 제1 단말과 상기 제2 단말 간의 인증 통과 여부를 판정하는 단계는, 상기 최후 해시값과 일치되는 값이 나올때까지 상기 제2 단말에 저장된 상기 최초 해시값을 반복적으로 해시하되, 해시 반복의 횟수

가 상기 최대 카운트 값이 될 때까지 해시의 결과가 상기 최후 해시값이 되는 경우가 발생하지 않는 경우, 상기 제1 단말과 상기 제2 단말 간의 인증이 실패한 것으로 판정하는 단계를 포함한다. 이 때, 상기 제1 단말과 상기 제2 단말 간의 인증이 실패한 것으로 판정하는 단계는, 상기 제2 단말이 상기 제1 단말에 인증 실패 메시지를 송신하는 단계와, 상기 제1 단말이 상기 최대 카운트 값을 감소 시키는 단계와, 상기 제1 단말이 상기 감소된 최대 카운트 값에 따른 최후 해시값과, 상기 감소된 최대 카운트 값을 상기 제2 단말에 송신하는 단계와, 상기 제2 단말이 상기 감소된 최대 카운트 값에 따른 최후 해시값과 일치되는 값이 나올때까지 상기 제2 단말에 저장된 상기 최초 해시값을 반복적으로 해시함으로써, 상기 제1 단말과 상기 제2 단말 간의 인증 통과 여부를 판정하되, 해시 반복의 횟수가 상기 감소된 최대 카운트 값이 될 때까지 해시의 결과가 상기 최후 해시값이 되는 경우가 발생하지 않는 경우, 상기 제1 단말과 상기 제2 단말 간의 인증이 실패한 것으로 판정하는 단계를 포함할 수 있다.

[0013] 일 실시예에서, 상기 커넥션 설립 프로세스는 블루투스 페어링 프로세스이고, 해시 체인을 포함하는 제1 인증 데이터를 저장하는 단계는, 서비스 서버로부터 상기 해시 체인을 수신하여 저장하는 단계를 포함하고, 상기 해시 체인의 최후 해시값을 상기 제2 단말에 송신하는 단계는, 블루투스 페어링 요청 신호에 상기 최후 해시값을 수납하여 상기 제2 단말에 송신하는 단계를 포함한다.

[0014] 일 실시예에서, 제1 단말이 해시값들의 순차적인 연결인 해시 체인을 포함하는 제1 인증 데이터를 저장하고, 제2 단말이 상기 해시 체인의 최초 해시값을 포함하는 제2 인증 데이터를 저장하는 단계는, 상기 제1 단말의 사용자에 의하여 서비스 서버에 요청 된 예약 요청의 결과로, 상기 제1 단말이 상기 제1 인증 데이터를 상기 서비스 서버로부터 수신하여 저장하고, 상기 제2 단말이 상기 제2 인증 데이터를 상기 서비스 서버로부터 수신하여 저장하는 단계를 포함하고, 상기 제1 단말과 상기 제2 단말 간의 인증 성공 여부를 판정하는 단계는, 상기 서비스 서버와의 데이터 송수신 없이 상기 제1 단말과 상기 제2 단말 간의 인증 성공 여부를 판정하는 단계를 포함하고, 커넥션 설립 프로세스를 수행하는 단계는, 상기 서비스 서버와의 데이터 송수신 없이 커넥션 설립 프로세스를 수행하는 단계를 포함한다. 이 때, 상기 제1 인증 데이터는, 상기 제2 단말의 식별 정보를 더 포함하고, 상기 제1 단말이, 상기 해시 체인의 상기 최후 해시값을 상기 제2 단말에 송신하는 단계는, 상기 제2 단말이, 상기 제2 단말의 식별 정보가 수납된 광고(advertising) 신호를 송출하는 단계와, 상기 제1 단말이, 상기 광고 신호를 감지하여, 상기 광고 신호에 수납된 식별 정보를 상기 제1 인증 데이터에 포함된 식별 정보와 비교하고, 비교 결과 두개의 식별 정보가 일치하는 것으로 판정된 경우, 상기 최후 해시값을 상기 제2 단말에 송신하는 단계를 포함할 수 있다. 이 때, 상기 예약 요청은 유효 기간에 대한 정보를 포함하고, 상기 제2 인증 데이터는 상기 유효 기간에 대한 정보를 더 포함하며, 상기 제2 단말이, 상기 제2 단말의 식별 정보가 수납된 광고(advertising) 신호를 송출하는 단계는, 상기 유효 기간 동안 상기 제2 단말의 식별 정보가 수납된 광고(advertising) 신호를 송출하는 단계를 포함할 수 있다. 또한, 상기 제1 인증 데이터는 상기 유효 기간에 대한 정보를 더 포함하며, 상기 제1 단말이, 상기 광고 신호를 감지하여, 상기 광고 신호에 수납된 식별 정보를 상기 제1 인증 데이터에 포함된 식별 정보와 비교하고, 비교 결과 두개의 식별 정보가 일치하는 것으로 판정된 경우, 상기 최후 해시값을 상기 제2 단말에 송신하는 단계는, 상기 제1 단말이, 상기 광고 신호를 감지하기 위한 스캐닝을 상기 유효 기간 도중에 활성화 하는 단계를 포함할 수도 있다.

[0015] 일 실시예에서, 상기 제1 단말 및 상기 제2 단말이 상기 제1 단말과 상기 제2 단말 간의 커넥션 설립 프로세스를 수행하는 단계는, 상기 커넥션 설립 프로세스의 성공 시, 상기 제1 단말 및 상기 제2 단말 중 적어도 하나가 상기 제1 단말에 대한 사용자 입력 없이 디폴트 프로세스를 수행하는 단계를 포함할 수 있다. 이 때, 상기 제2 단말은, 차량에 구비된 상기 차량을 제어 하는 단말이고, 상기 커넥션 설립 프로세스의 성공 시, 상기 제1 단말 및 상기 제2 단말 중 적어도 하나가 상기 제1 단말에 대한 사용자 입력 없이 디폴트 프로세스를 수행하는 단계는, 상기 제2 단말이 상기 차량의 문을 오픈하는 제어 신호를 송신하는 단계와, 상기 제1 단말이 디바이스 간 근거리 무선 통신 기반의 차량 제어 앱을 실행하는 단계를 포함할 수 있다.

도면의 간단한 설명

[0016] 도 1은 본 발명의 일 실시예에 따른 단말 간 근거리 무선 통신 서비스 제공 시스템의 제1 구성도이다.

도 2는 본 발명의 일 실시예에 따른 단말 간 근거리 무선 통신 서비스 제공 시스템의 제2 구성도이다.

도 3은 본 발명의 일 실시예에 따른 단말 간 통신 방법의 신호 흐름도이다.

도 4는 본 발명의 몇몇 실시예들에서 참조될 수 있는 제2 단말 관련 정보의 데이터 구성을 예시한 도면이다.

도 5는 본 발명의 몇몇 실시예들에서, 단말 간 근거리 무선 통신을 위한 커넥션 설립 프로세스가 성공한 경우,

사용자 단말에 표시될 수 있는 화면의 예시도이다.

도 6은 본 발명의 일 실시예에 따른 서비스 서버의 상세 구성을 나타낸 블록도이다.

도 7은 본 발명의 일 실시예에 따른 제1 디바이스의 상세 구성을 나타낸 블록도이다.

도 8은 본 발명의 일 실시예에 따른 제2 디바이스의 상세 구성을 나타낸 블록도이다.

도 9는 본 발명의 일 실시예에 따른 중개 장치의 상세 구성을 나타낸 블록도이다.

도 10은 본 발명의 일 실시예에 따른 키 토큰의 생성 및 해시 코드의 분배 과정을 설명하기 위한 흐름도이다.

도 11은 본 발명의 제1 실시예에 따른 디바이스 간 인증 과정을 설명하기 위한 흐름도이다.

도 12는 본 발명의 제2 실시예에 따른 디바이스 간 인증 과정을 설명하기 위한 흐름도이다.

도 13은 본 발명의 제1 실시예에 따른 키 토큰의 갱신 과정을 설명하기 위함 흐름도이다.

도 14는 본 발명의 제2 실시예에 따른 키 토큰의 갱신 과정을 설명하기 위함 흐름도이다.

도 15는 도 14에서의 키 토큰의 갱신에 따른 이전 키 토큰의 폐기 과정을 설명하기 위한 흐름도이다.

도 16은 본 발명의 제1 실시예에 따른 키 토큰의 폐기 과정을 설명하기 위함 흐름도이다.

도 17은 본 발명의 제2 실시예에 따른 키 토큰의 폐기 과정을 설명하기 위함 흐름도이다.

도 18은 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위한 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0017] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예들을 상세히 설명한다. 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시 예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 게시되는 실시 예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시 예들은 본 발명의 게시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭한다.

[0018] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다. 본 명세서에서 사용된 용어는 실시예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 본 명세서에서, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다.

[0019] 이하, 도면들을 참조하여 본 발명의 몇몇 실시예들을 설명한다.

[0020] 먼저, 도 1 및 도 2를 참조하여, 본 발명의 일 실시예에 따른 단말 간 통신 서비스 제공 시스템의 구성 및 동작을 설명한다. 도 1은 본 발명의 일 실시예에 따른 단말 간 통신 서비스 제공 시스템의 구성도이다. 본 실시예에 따른 단말 간 통신 서비스 제공 시스템은 다양한 형태의 단말 간 통신을 제공한다. 예를 들어, 유선 통신, 3G, 4G, 5G 등의 이동통신, 블루투스, WIFI, NFC 등의 근거리 무선 통신(Short-range wireless communication) 등의 단말 간 통신이 제공될 수 있다. 본 발명의 몇몇 실시예들에서 근거리 무선 통신 형태의 단말 간 통신(40)이 제공되는 경우, 서비스 서버(102) 등 외부 장치 및 네트워크(30) 등 퍼블릭 네트워크에 대한 커넥션 없이도 단말 간 통신 서비스가 제공될 수 있으므로, 활용성 측면에서 큰 효과를 얻을 수 있다. 이하, 이해를 돕기 위하여 단말 간의 근거리 무선 통신 방법을 예로 들어 설명한다. 다만, 본 발명의 범위가 근거리 무선 통신 형태의 단말 간 통신으로 한정되어서는 아니된다.

[0021] 도 1을 참조하면, 본 실시예에 따른 시스템은 근거리 무선 통신 인터페이스를 구비한 제1 단말(104), 근거리 무선 통신 인터페이스를 구비한 제2 단말(106)과 및 서비스 서버(102)를 포함한다. 허가 된 근거리 무선 통신 만이 허용되도록, 제1 단말(104) 및 제2 단말(106)은 인증을 거쳐 근거리 무선 통신을 위한 커넥션(connection)을 설립(establishment)한다. 상기 커넥션이 정상적으로 설립된 후에, 근거리 무선 통신을 이용하여 데이터를 P2P(Peer-To-Peer) 방식으로 송수신 한다.

[0022] 서비스 서버(102)는 제1 단말(104)과 제2 단말(106) 간의 상기 커넥션을 설립하기 위한 상기 인증에 사용되는 인증 데이터를 제1 단말(104)과 제2 단말(106)에 제공한다. 상기 인증 데이터에 대하여는 도 3을 참조하여 보다 자세히 설명한다.

[0023] 서비스 서버(102)는, 제1 단말(104)의 예약 요청을 수신하면, 상기 예약 요청에 따른 예약 대상으로서 관리 대상인 복수의 단말 중 하나인 제2 단말(106)을 선정하는 것과, 제1 단말(104)에 네트워크(30)를 통해 제1 인증 데이터를 송신하는 것과, 제2 단말(106)에 네트워크(30)를 통해 제2 인증 데이터를 송신하는 것을 수행한다.

[0024] 제1 단말(104)은 상기 제1 인증 데이터를 저장한다. 제2 단말(106)도 상기 제2 인증 데이터를 저장한다.

[0025] 일 실시예에서, 제1 단말(104)과 제2 단말(106)은 해시값들의 순차적인 연결인 해시 체인을 이용하여 상호 인증 절차를 수행한다. 이 경우, 상기 제1 인증 데이터에는 상기 해시 체인이 포함된다. 또한, 상기 제2 인증 데이터에는 상기 해시 체인의 최초 해시값이 포함된다. 이 때, 상기 상호 인증 절차는, 제1 단말이 해시값들의 순차적인 연결인 해시 체인을 포함하는 제1 인증 데이터를 저장하고, 제2 단말이 상기 해시 체인의 최초 해시값을 포함하는 제2 인증 데이터를 저장하는 것, 상기 제1 단말이 상기 해시 체인의 최후 해시값을 상기 제2 단말에 송신하는 것, 상기 제2 단말이, 상기 최후 해시값과 일치되는 값이 나올때까지 상기 제2 단말에 저장된 상기 최초 해시값을 반복적으로 해시함으로써, 상기 제1 단말과 상기 제2 단말 간의 인증 성공 여부를 판정하는 것, 제1 단말(104)과 제2 단말(106)은, 제1 단말(104)과 제2 단말(106) 간의 근거리 무선 통신 커넥션 설립 프로세스 수행 요건이 완성되면, 상기 제1 인증 데이터 및 상기 제2 인증 데이터를 이용하여 상기 인증을 수행하는 것을 포함한다. 이 때, 상기 제1 인증 데이터는 최대 카운트 값을 더 포함하고, 상기 최후 해시값은 상기 해시 체인에 포함된 해시값들 중 상기 최대 카운트를 오프셋(offset)으로 하는 해시값일 수 있다. 또한, 상기 해시 체인의 최후 해시값을 상기 제2 단말에 송신하는 것은, 상기 최대 카운트 값을 상기 최후 해시값과 함께 상기 제2 단말에 송신하는 것을 포함하고, 상기 제1 단말과 상기 제2 단말 간의 인증 통과 여부를 판정하는 것은, 상기 최후 해시값과 일치되는 값이 나올때까지 상기 제2 단말에 저장된 상기 최초 해시값을 반복적으로 해시하되, 해시 반복의 횟수가 상기 최대 카운트 값이 될 때까지 해시의 결과가 상기 최후 해시값이 되는 경우가 발생하지 않는 경우, 상기 제1 단말과 상기 제2 단말 간의 인증이 실패한 것으로 판정하는 것을 포함한다.

[0026] 상기 제1 단말과 상기 제2 단말 간의 인증이 실패한 것으로 판정한다는 것은, 종국적인 인증 실패를 의미하는 것은 아니다. 상기 최대 카운트 값을 감소시킨 후, 인증을 재시도할 수 있다. 예를 들어, 상기 최대 카운트 값이 100이라고 할 때, H^{100} 에 해당하는 최후 해시값이 제2 단말 측의 반복 해시에서 유도되지 않았다고 하면, 다음 번에는 최대 카운트 값을 99로 감소시키고 H^{99} 에 해당하는 최후 해시값이 제2 단말 측의 반복 해시에서 유도되는 것을 시도할 수 있는 것이다. 해시체인을 이용한 단말 간 상호 인증 과정에 대하여 도 10 내지 도 17을 참조하여 추후 보다 자세히 설명한다.

[0027] 상기 근거리 무선 통신 커넥션 설립 프로세스 수행 요건은, 제1 단말(104)의 위치 정보가 상기 예약 요청에 포함된 정보에 매칭되는 것을 가리키거나, 현재 시간이 상기 예약 요청에 포함된 유효 시간에 해당하는 것을 가리키거나, 제1 단말(104)의 위치 정보가 상기 예약 요청에 포함된 정보에 매칭되면서 동시에 현재 시간이 상기 예약 요청에 포함된 유효 시간에 해당하는 것을 가리킬 수 있다.

[0028] 상기 인증을 수행하기 위하여 필요한 인증 데이터는 이미 서비스 서버(102)로부터 제1 단말(104) 및 제2 단말(106)에 다운로드 되어 있으므로, 상기 인증이 수행되는 시점에 제1 단말(104) 및 제2 단말(106)은 서비스 서버(102)에 연결 될 필요가 없다. 따라서, 제1 단말(104)과 제2 단말(106)이 제1 단말(104)과 제2 단말(106) 간의 근거리 무선 통신을 위한 커넥션 설립 시점에 통신 음영 지역에 위치하더라도, 정상적으로 상기 인증이 수행될 수 있고, 결과적으로 정상적으로 근거리 무선 통신을 위한 커넥션이 설립된다. 또한, 상기 인증 과정에서 서비스 서버(102)와의 연결에 소요되는 시간을 절감할 수 있으므로, 결과적으로 제1 단말(1104) 및 제2 단말(106) 사이에 데이터를 송수신하는데 소요되는 시간이 절감된다.

[0029] 이하, 이해의 편의를 돕기 위하여 제1 단말(104)은 사용자가 사용하는 단말이고, 제1 단말(104)과 근거리 무선 통신(40)을 수행하는 단말을 제2 단말(106)인 것으로 한다. 이미 언급한 바와 같이, 제1 단말(104)을 통하여 상기 예약 요청이 송신된다. 그리고, 제1 단말(104)과 제2 단말(106) 간의 근거리 무선 통신을 위한 커넥션을 설립하는데 있어서, 제1 단말(104)에 대한 사용자 입력이 있을 것을 요구하지 않는다. 즉, 제1 단말(104)의 사용자는 상기 예약 요청을 서비스 서버(102)에 송신하기만 하면 되고, 제2 단말(106)에 근접한 위치에 제1 단말(104)을 가져가기만 하면, 제1 단말(104)과 제2 단말(106) 사이의 근거리 무선 통신을 위한 커넥션이 자동으로 설립되는 것을 의미한다.

[0030] 예를 들어, 제2 단말(106)이 제1 단말(104)에 의하여 제어되는 피제어 장치라면, 제1 단말(104)의 사용자는 서비스 서버(102)에 제2 단말(106)에 대한 예약 요청을 송신하기만 하면, 제2 단말(106)에 가까이 접근하여, 별도의 절차 없이 바로 제1 단말(104)을 이용하여 제2 단말(106)을 제어할 수 있다. 제1 단말(104) 및 제2 단말(106)이 통신 음영 지역에 위치하더라도, 제1 단말(104)과 제2 단말(106) 사이의 근거리 무선 통신을 위한 커넥션 설립에 따른 인증에는 아무런 문제가 없다. 제1 단말(104)과 제2 단말(106)이 제1 단말(104)의 예약 요청 송신 시점에 서비스 서버(102)와 연결되기만 하면, 그 시점에 상기 커넥션 설립에 따른 인증을 위한 인증 데이터가 미리 제1 단말(104) 및 제2 단말(106)에 다운로드 되기 때문이다.

[0031] 도 2는 제2 단말(106)이 제1 단말(104)에 의하여 제어되는 피제어 장치인 경우의, 단말 간 근거리 무선 통신 서비스 제공 시스템의 구성도이다. 도 2에 도시된 시스템은, 차량이 제1 단말(104)로부터 블루투스(40a) 방식으로 제2 단말(106)에 제공되는 제어 신호를 통하여 제어되도록 지원한다. 도 2에는 제1 단말(104)과 제2 단말(106) 사이의 근거리 무선 통신(40a)으로서 블루투스 기술이 사용되는 것이 도시되어 있다.

[0032] 이미 설명된 바와 같이, 제1 단말(104)과 제2 단말(106) 사이의 근거리 무선 통신의 커넥션 설립(즉, 페어링) 시점에는 제1 단말(104)과 제2 단말(106)이 서비스 서버(102)에 연결될 필요가 없다. 그러나, 제2 단말(106)을 구비한 차량이 주차되어 있는 차고지가 통신 음영 지역이거나, 통신비 또는 제조 단가 문제로 제2 단말(106)이 이동 통신 인터페이스(예를 들어, LTE 또는 5G 이동통신 기반의 데이터 통신을 지원하는 네트워크 모듈)를 구비하고 있지 않은 등의 이유로 네트워크(30)에 직접 연결 될 수 없는 경우를 위해, 제2 단말(106)과 네트워크(30)의 연결을 지원하는 중개 장치(108)가 상기 시스템에 포함될 수 있다.

[0033] 중개 장치(108)는, 예를 들어 제2 단말(106)이 WiFi를 통해 네트워크(30)에 연결될 수 있도록 하는 억세스 포인트(AP; Access Point)일 수 있다. 이 때, 제2 단말(106)은 WiFi 모듈을 구비한 것이다. 중개 장치(108)는 서비스 서버(102)로부터 데이터를 수신하고, 이를 제2 디바이스(106)가 수신 가능한 형태로 변환하여 제2 디바이스(106)로 전송할 수 있다. 또한, 중개 장치(108)는 제2 디바이스(106)로부터 데이터를 수신하고, 이를 서비스 서버(102)가 수신 가능한 형태로 변환하여 서비스 서버(102)로 전송할 수 있다. 한편, 여기서는 중개 장치(108)가 서비스 서버(102)와 제2 디바이스(106)의 사이에서 데이터를 중개하는 것으로 설명하였으나 이는 일 예시에 불과하며, 서비스 서버(102)와 제2 디바이스(106)가 별도의 중개 장치(108) 없이 상호 간에 데이터를 직접 송수신할 수도 있다.

[0034] 이하, 도 3을 참조하여 본 발명의 일 실시예에 따른 단말 간 통신 방법을 설명한다. 도 3은 본 발명의 일 실시예에 따른 단말 간 통신 방법의 신호 흐름도이다.

[0035] 먼저, 서비스 서버(102)가 복수의 제2 단말(106)들에 대한 정보를 관리하는 것과 관련된 설명을 하기로 한다. 도 4는 본 발명의 몇몇 실시예들에서 참조될 수 있는 제2 단말 관련 정보의 데이터 구성(50)을 예시한 도면이다. 도 4에 도시된 바와 같이, 서비스 서버(102)는 각각의 제2 단말(106)에 대하여, 단말 ID(51) 및 단말의 부가 정보를 관리한다. 상기 단말의 부가 정보는, 단말 속성(52), MAC(Media Access Control) 주소(53) 및 서비스 가능 시간(54) 중 적어도 하나의 필드 정보를 포함한다.

[0036] 단말 ID(51)는 예를 들어, UUID 형식의 데이터로서 각각의 제2 단말들을 고유하게 식별할 수 있는 식별자이다.

[0037] 또한, 단말 속성(52)은 단말의 위치, 기종 등 단말과 관련된 정보를 포함한다. 서비스 서버는 제1 단말로부터 수신된 예약 요청에 포함된 예약 희망 단말의 요건에 대한 정보를 관리 대상인 각각의 제2 단말들의 단말 속성(52) 정보와 비교하고, 상기 요건에 부합하는 제2 단말을 선정한다. 추가적으로, 각각의 제2 단말에 대하여 서비스 가능 시간이 정의될 수 있다. 즉, 각각의 제2 단말은 상기 서비스 가능 시간에만 제1 단말과 데이터를 송수신 할 수 있고, 그 이외 시간에는 근거리 무선 통신 기능이 비활성화 되거나, 전원 자체가 OFF 될 수 있다. 따라서, 예약 요청에 포함되는 예약 희망 단말의 요건은 단말 속성(52)에 존재하는 정보 및 서비스 가능 시간(54) 중에서 선택되는 것이 바람직하다. 일 실시예에서, 각각의 제2 단말의 MAC 주소(53)는 제1 단말에 송신되는 제1 인증 데이터에 포함될 수 있다. 이와 관련하여 보다 자세한 설명은 후술한다.

[0038] 다시 도 3을 참조하여 설명한다. 제1 단말(104)이 서비스 서버(102)에 예약 요청을 송신한다(S10). 상기 예약 요청에는, 제1 단말(104)이 단말 간 근거리 무선 통신을 하고자 하는 상대 단말인 제2 단말(106)을 지정하는 요건에 대한 정보와, 제1 단말(104)이 제2 단말(106)과 통신하고자 하는 기간인 유효 기간에 대한 정보가 포함될 수 있다. 이미 도 4를 참조하여 설명한 바와 같이, 상기 제2 단말(106)을 지정하는 요건은 제2 단말 관련 정보의 데이터(50)의 단말 속성 필드(52) 및 서비스 가능 시간 필드(54)에 포함된 정보와 비교된다.

[0039] 서비스 서버(102)는 상기 예약 요청을 수신하여 예약 승인 처리 프로세스를 실행한다(S12). 상기 예약 승인 처

리 프로세스는 상기 예약 요청에 포함된 정보를 이용하여 제2 단말(106)을 선정하는 것과, 제1 단말(104)에 송신할 제1 인증 데이터 및 제2 단말(106)에 송신할 제2 인증 데이터를 생성하는 것을 포함한다. 상기 제2 인증 데이터는 상기 제1 인증 데이터에 대응되는 것이다.

[0040] 일 실시예에서, 상기 제1 인증 데이터는 해시 값들의 순차적인 연결인 해시 체인을 포함한다.

[0041] 상기 해시 체인은 토큰을 해시 함수에 입력하여 출력되는 제1 해시 값, 상기 제2 해시 값을 상기 해시 함수에 입력하여 출력되는 제3 해시 값, 상기 제3 해시 값을 상기 해시 함수에 입력하여 출력되는 제4 해시 값을 순차적으로 연결한 것이다. 상기 해시 체인이 상기 제4 해시 값 이후에도, 상기 제2 내지 제4 해시 값과 동일한 방식으로 생성되는 제5 내지 제N 해시 값(N은 6 이상의 자연수)을 추가적으로 더 포함할 수 있음은 물론이다. 서비스 서버(102)는 상기 토큰을 주기적으로 또는 비주기적으로 재생성할 수 있다.

[0042] 또한, 상기 제2 인증 데이터는 상기 해시 체인의 최초 해시 값을 포함한다. 상기 제1 인증 데이터가 상기 해시 체인을 포함하고, 상기 제2 인증 데이터가 상기 해시 체인의 최초 해시 값, 즉 토큰을 해시 함수에 입력하여 출력되는 제1 해시 값을 포함하는 점에서, 상기 제2 인증 데이터는 상기 제1 인증 데이터에 대응되는 것이다. 상기 제1 인증 데이터는 제2 단말(106)의 MAC 주소를 더 포함할 수도 있다.

[0043] 서비스 서버(102)는 예약 승인 처리 프로세스의 실행 결과, 예약 가능한 제2 단말이 존재하지 않는 경우, 제1 단말(104)에 예약 실패 메시지를 송신할 수 있다(미도시).

[0044] 서비스 서버(102)는 상기 제1 인증 데이터 및 상기 예약 요청에 포함되어 있던 유효 기간에 대한 정보를 제1 단말(104)에 송신하고(S14), 제1 단말(104)은 수신된 정보를 저장한다(S16). 서비스 서버(102)는 상기 제2 인증 데이터 및 상기 예약 요청에 포함되어 있던 유효 기간에 대한 정보를 제2 단말(106)에 송신하고(S18), 제1 단말(104)은 수신된 정보를 저장한다(S20).

[0045] 지금까지 예약 프로세스(S1)를 설명하였다. 상기 예약 요청이 서비스 서버(102)에 송신 되어야 하고, 상기 제1 인증 데이터 및 상기 제2 인증 데이터가 서비스 서버(102)에 의하여 제1 단말(104) 및 제2 단말(106)에 송신되어야 하므로, 예약 프로세스(S1)가 수행되는 도중에는 제1 단말(104) 및 제2 단말(106)이 서비스 서버(102)와의 연결 상태를 유지하여야 한다.

[0046] 이미 설명한 바와 같이, 서비스 서버(102)는 인증 데이터와 함께 상기 유효 기간에 대한 정보를 제1 단말(104) 및 제2 단말(106)에 송신한다. 제1 단말(104) 및 제2 단말(106)은 유효 기간이 아닌 기간 동안에는 근거리 무선 통신 커넥션이 설립되기 위한 프로세스를 활성화하지 않음으로써, 전력 소모를 절감할 수 있다.

[0047] 물론, 일 실시예에서, 제1 단말(104) 및 제2 단말(106) 중 적어도 어느 하나는, 근거리 무선 통신 커넥션이 설립되기 위한 프로세스를 수행하기 위해, 유효 기간인지 여부와 무관하게 상대 단말로부터 수신되는 신호를 감지할 수도 있다.

[0048] 제1 단말(104) 및 제2 단말(106)은 유효 기간이 아닌 기간 동안에는 근거리 무선 통신 커넥션이 설립되기 위한 프로세스를 활성화하지 않는 실시예를 좀더 설명한다. 제2 단말(106)은 서버로부터 상기 제2 인증 데이터와 함께 유효 기간 정보를 수신하면, 상기 유효 기간에 도달 했는지 여부를 확인하고(S22), 유효 기간에 도달한 경우에 광고 신호(ADVERTISING SIGNAL)를 근거리 무선 통신 방식으로 송출한다(S25). 제1 단말(104)도, 서버로부터 상기 제2 인증 데이터와 함께 유효 기간 정보를 수신하면, 상기 유효 기간에 도달 했는지 여부를 확인하고(S23), 유효 기간에 도달한 경우에 제2 단말로부터 송출되는 상기 광고 신호를 스캐닝하는 것을 시작한다(S24).

[0049] 제1 단말(104)이 제2 단말(106)로부터의 광고 신호를 감지하면(S26), 제1 단말(104)에 저장된 상기 제1 인증 데이터를, 제2 단말(106)에 근거리 무선 통신 방식으로 송신한다(S27).

[0050] 한편, 이미 설명한 바와 같이, 일 실시예에서, 제1 인증 데이터에는 제2 단말(106)의 MAC 주소가 포함될 수 있다. 본 실시예에서는, 광고 신호에 제2 단말(106)의 MAC 주소가 포함된다. 그러면, 제1 단말(104)은 감지 된 상기 광고 신호에 포함된 MAC 주소와 상기 저장된 제1 인증 데이터에 포함된 MAC 주소를 비교하는 제1 단말에 대한 인증을 수행할 수 있다. 이 때, 제1 단말(104)은 감지 된 상기 광고 신호에 포함된 MAC 주소와 상기 저장된 제1 인증 데이터에 포함된 MAC 주소가 동일한 경우에 한하여, 상기 해시 체인에 속한 복수의 해시 값들 중 하나의 해시 값을 제2 단말(106)에 송신한다(S27).

[0051] 제2 단말(106)은 상기 제1 인증 데이터 및 상기 제2 인증 데이터를 이용하여 제1 단말(104)에 대한 인증을 처리한다. 보다 자세하게는, 제2 단말(106)은 제1 단말(104)로부터 수신된 해시 값이, 제2 단말(106)에 기 저장되어 있는 최초 해시 값을 기 정의된 해시 함수에 반복하여 입력함으로써 유도되는지 여부에 따라 제1 단말(104)에

대한 인증을 처리할 수 있다(S28). 제2 단말(106)은 제1 단말(104)에 대한 인증 성공 시, Ack 신호를 제1 단말(104)에 송신할 수 있다(S30).

[0052] 일 실시예에서, 상기 근거리 무선 통신 커넥션 설립 프로세스는 블루투스(Bluetooth) 세션을 설립하기 위한 프로세스이고, 단계 S27에서 제1 단말(104)이 제2 단말에 송신하는 신호는 블루투스 페어링 요청 신호일 수 있다.

[0053] 일 실시예에서, 단말 간 근거리 무선 통신을 위한 커넥션 설립이 성공한 경우, 제1 단말(104) 및 제2 단말(106) 중 적어도 어느 하나에서 사전 정의된 디폴트 프로세스가 사용자 입력 없이 수행될 수 있다(S32, S34). 예를 들어, 도 2에 도시된 것과 같이 본 실시예에 따른 단말 간 통신 방법이 차량 공유 서비스의 일환으로서 수행된다면, 제2 단말(106)의 디폴트 프로세스(S34)는 차량의 도어를 오픈하는 제어 신호를 도어 컨트롤러에 송신하는 것이고, 제1 단말(104)의 디폴트 프로세스(S32)는 디바이스 간 근거리 무선 통신 기반의 차량 제어 앱을 실행하는 것일 수 있다.

[0054] 또한, 일 실시예에서, 제2 단말(106)은 디지털 도어락이고, 디폴트 프로세스(S34)는 도어 오픈일 수 있다.

[0055] 또한, 일 실시예에서, 제2 단말(106)은 아파트 현관문 도어락이고, 디폴트 프로세스(S34)는 도어 오픈 및 제1 단말(104)의 사용자에 대한 알림 메시지 표시일 수 있다.

[0056] 이상 설명한 근거리 무선 통신을 위한 커넥션 설립 프로세스(S2)가 수행된 이후, 제1 단말(104)과 제2 단말(106) 사이의 근거리 무선 통신 데이터 송수신이 수행된다(S36).

[0057] 도 5는 본 발명의 몇몇 실시예들에서, 단말 간 근거리 무선 통신을 위한 커넥션 설립 프로세스가 성공한 경우, 사용자 단말에 표시될 수 있는 화면의 예시도이다. 단말 간 근거리 무선 통신을 위한 커넥션 설립이 성공한 경우, 제1 단말(104)은 도 5에 도시된 것과 같이 디바이스 간 근거리 무선 통신 기반의 차량 제어 앱(60)을 실행하고, 그 화면을 디스플레이 할 수 있다. 차량 제어 앱(60)은 제2 단말(106)을 통하여 차량을 제어하기 위한 다양한 커맨드 생성 버튼을 포함할 수 있다.

[0058] 예를 들어, 제1 단말(104)의 사용자가 상기 버튼을 선택하는 경우, 제1 단말(104)과 제2 단말(106) 사이의 근거리 무선 통신 커넥션을 통하여 상기 커맨드가 송신 될 것이다.

[0059] 이하, 서비스 서버(102)에 대한 기능 측면의 추가 설명을 부가한다.

[0060] 서비스 서버(102)는 제1 디바이스(104)와 제2 디바이스(106) 간의 D2D 통신을 위한 키 토큰(key token)을 생성하고, 이를 관리하는 장치이다. 본 실시예들에 있어서, 키 토큰은 양 디바이스(104, 106) 중 어느 하나가 상대방 디바이스를 인증하고 설정된 정책에 따른 커맨드(예를 들어, 도어락의 잠금 해제, 차량의 도어 개폐/시동 오프 등)를 수행하는 데 사용되는 스마트 키(smart key)의 일종일 수 있다. 상기 키 토큰은 제1 디바이스(104)의 정보, 제2 디바이스(106)의 정보, 입력된 정책의 아이디, 사용자 아이디 등에 기초하여 생성될 수 있다.

[0061] 서비스 서버(102)는 기간계 시스템(legacy system, 미도시) 등으로부터 정책을 입력 받고, 입력된 정책에 따라 키 토큰을 생성할 수 있다. 여기서, 기간계 시스템은 서비스 서버(102)와 연동하여 각종 서비스를 사용자에게 제공하는 시스템으로서, 미리 정의된 복수 개의 정책들 중 사용자의 요청에 대응되는 하나 이상의 정책을 서비스 서버(102)로 제공할 수 있다. 일 예시로서, 서비스 서버(102)는 사용자의 도어락 접근시 도어락의 잠금을 자동으로 해제하는 내용의 정책을 홈 네트워크 시스템(미도시)으로부터 입력 받을 수 있다. 다른 예시로서, 서비스 서버(102)는 사용자가 차량의 사용을 예약하는 경우 사용자에 의해 입력된 예약 기간 동안 사용자의 입력에 따라 차량의 도어 개폐/시동 온, 오프 등을 원격 제어할 수 있는 내용의 정책을 차량 공유 시스템(미도시)으로부터 입력 받을 수 있다. 이때, 상기 키 토큰은 설정된 유효 기간(예를 들어, 5일)을 가질 수 있으며, 상기 유효 기간은 입력된 정책(예를 들어, 상술한 예약 기간)에 따라 달라질 수 있다. 후술할 바와 같이, 제2 디바이스(106)는 서비스 서버(102)로부터 상기 유효 기간에 관한 정보를 수신하고, 상기 유효 기간 내에만 제1 디바이스(104)의 인증 및 커맨드 수행이 가능하다.

[0062] 또한, 서비스 서버(102)는 서비스를 제공받는 사용자, 상기 사용자가 소지하는 디바이스의 정보(예를 들어, 디바이스의 유형, 식별 정보 등), 제어 대상이 되는 디바이스의 정보(예를 들어, 디바이스의 유형, 식별 정보, 제어 가능한 커맨드 정보 등), 입력 가능한 정책들의 정보, 생성된 키 토큰 및 유효 기간에 관한 정보(예를 들어, 시작 시간 및 종료 시간에 관한 정보), 후술할 해시 코드 등을 데이터베이스에 저장하고 관리할 수 있다.

[0063] 또한, 서비스 서버(102)는 생성된 하나의 키 토큰을 이용하여 해시 코드(hash code)를 생성하고, 생성된 해시 코드를 제1 디바이스(104) 및 제2 디바이스(106)로 각각 전송한다. 구체적으로, 서비스 서버(102)는 키 토큰(또는 키 토큰의 최초 해시 값)을 설정된 최대 카운트(maximum count)만큼 반복적으로 해시함으로써 복수 개의 제1

해시 값들을 생성할 수 있다. 또한, 서비스 서버(102)는 생성된 제1 해시 값들을 해시 함수가 적용된 횟수 순(또는 제1 해시 값들이 생성된 순)으로 순차적으로 연결하여 상기 제1 해시 값들의 체인(chain)을 생성할 수 있다. 이때, 최대 카운트는 순차적으로 연결된 제1 해시 값들의 개수로서, 입력된 정책, 키 토큰의 유효 기간 등에 따라 달라질 수 있다. 일 예시로서, 사용자가 차량의 사용을 5일 동안 예약하는 경우, 키 토큰의 유효 기간은 5일이며 최대 카운트는 100이 될 수 있다. 다른 예시로서, 사용자가 차량의 사용을 3일 동안 예약하는 경우, 키 토큰의 유효 기간은 3일이며 최대 카운트는 50이 될 수 있다. 이와 같은 방법으로 순차적으로 연결된 제1 해시 값들의 예시는 아래와 같다.

[0064] $H^{1}(T) - H^{2}(T) - H^{3}(T) \ldots H^{99}(T) - H^{100}(T)$ (최대 카운트 = 100이라 가정)

[0065] 여기서, $H^{1}(T)$는 키 토큰(또는 키 토큰의 최초 해시 값)에 해시 함수가 1번 적용된 해시 값, $H^{2}(T)$는 키 토큰(또는 키 토큰의 최초 해시 값)에 해시 함수가 2번 적용된 해시 값(즉, $H^{2}(T)$의 해시 값)... $H^{100}(T)$은 키 토큰(또는 키 토큰의 최초 해시 값)에 해시 함수가 100번 적용된 해시 값(즉, $H^{99}(T)$의 해시 값)일 수 있다. 또한, T는 키 토큰을 나타낸다. 즉, $H^{N}(T)$은 키 토큰(T) 또는 키 토큰(T)의 최초 해시 값을 입력값으로 하여 해시 함수를 N번 적용한 값이다. 상기 HN(T)은 서비스 서버(102)의 개입 없이 제1 디바이스(104)와 제2 디바이스(106) 간 싱크(sync)를 맞추기 어려운 환경에서 양 디바이스 간의 D2D 통신을 위한 일회용 키로서 사용될 수 있다.

[0066] 서비스 서버(102)는 상기 순차적으로 연결된 제1 해시 값들을 제1 디바이스(104)로 전송할 수 있다. 이때, 서비스 서버(102)는 입력된 정책, 최대 카운트에 관한 정보, 키 토큰의 유효 기간에 관한 정보 등을 상기 제1 해시 값들과 함께 제1 디바이스(104)로 전송할 수 있다.

[0067] 또한, 서비스 서버(102)는 키 토큰에 관한 정보, 최대 카운트에 관한 정보, 입력된 정책, 키 토큰의 유효 기간에 관한 정보 등을 제2 디바이스(106)로 전송할 수 있다. 여기서, 상기 키 토큰에 관한 정보는, 상기 키 토큰 또는 상기 키 토큰을 설정된 횟수만큼 해시한 값을 포함할 수 있다. 본 실시예들에 있어서, 상기 키 토큰을 설정된 횟수만큼 해시한 값은 예를 들어, 키 토큰의 최초 해시 값일 수 있으며, 이하에서는 키 토큰에 관한 정보가 상기 키 토큰의 최초 해시 값인 것으로 가정한다. 이때, 서비스 서버(102)는 중개 장치(108)를 통해 상기 정보들을 제2 디바이스(106)로 전송할 수 있다. 서비스 서버(102)와 제2 디바이스(106) 간의 통신 채널은 서비스 서버(102)와 제1 디바이스(104) 간의 통신 채널에 비해 상대적으로 그 보안이 취약할 수 있으므로, 서비스 서버(102)는 키 토큰에 대한 해시 값들, 예를 들어 $H^{1}(T) - H^{2}(T) - H^{3}(T) \ldots H^{99}(T) - H^{100}(T)$ 모두를 제2 디바이스(106)로 전송하는 것이 아니라 키 토큰에 대한 최초 해시 값과 설정된 최대 카운트만을 제2 디바이스(106)로 전송할 수 있다. 후술할 바와 같이, 제2 디바이스(106)는 제1 디바이스(104)로부터 제1 해시 값들 중 하나를 수신하고, 제1 디바이스(104)로부터 수신된 제1 해시 값, 서비스 서버(102)로부터 수신된 최초 해시 값 및 최대 카운트에 관한 정보를 이용하여 제1 디바이스(104)를 인증할 수 있다.

[0068] 또한, 서비스 서버(102)는 제1 디바이스(104) 및 제2 디바이스(106) 측 최대 카운트를 이용하여 양 디바이스(104, 106)에 저장된 해시 값들의 체인을 동기화할 수 있다.

[0069] 또한, 서비스 서버(102)는 키 토큰의 유효 기간, 제1 디바이스(104) 측 최대 카운트의 수(또는 제1 디바이스(104)에 저장된 제1 해시 값들의 개수) 및 서비스 서버(102)에 입력된 정책 중 하나 이상을 고려하여 키 토큰 및 최대 카운트 중 하나 이상을 갱신할 수 있다.

[0070] 또한, 서비스 서버(102)는 키 토큰 또는 정책의 유효 기간 만료 여부에 따라 생성된 키 토큰을 폐기할 수 있다. 상기 키 토큰의 생성 및 양 디바이스(104, 106)에 저장된 체인의 동기화, 키 토큰의 갱신 및 폐기에 대해서는 도 10 내지 12를 참조하여 구체적으로 후술하기로 한다. 한편, 이하에서는 설명의 편의상 제1 디바이스(104)에 저장되는 최대 카운트를 제1 최대 카운트, 제2 디바이스(106)에 저장되는 최대 카운트를 제2 최대 카운트로 각각 칭하기로 한다. 상기 제1 최대 카운트 및 제2 최대 카운트는 서비스 서버(102)에서 최초로 생성되어 제1 디바이스(104) 및 제2 디바이스(106)로 분배될 수 있으나 반드시 이에 한정되는 것은 아니다. 후술할 바와 같이, 제1 디바이스(104)는 제1 최대 카운트에 대응되는 제1 해시 값을 제2 디바이스(106)로 전송하고, 상기 제1 해시 값이 전송될 때마다 제1 최대 카운트를 1씩 차감할 수 있다. 또한, 제2 디바이스(106)는 N번 해시된 제2 해시 값이 제1 디바이스(104)로부터 수신된 제1 해시 값과 일치하는 경우 제2 최대 카운트를 상기 N으로 차감할 수 있다.

[0071] 제1 디바이스(104)는 제2 디바이스(106)와 D2D 통신하여 제2 디바이스(106)의 동작을 제어하는 데 사용되는 장

치로서, 예를 들어 스마트폰, 태블릿 PC, 스마트 워치 등과 같은 웨어러블 디바이스 등이 될 수 있다. 본 실시예들에 있어서, 제1 디바이스(104)는 사용자가 휴대 가능한 모바일 디바이스일 수 있다. 또한, 제1 디바이스(104)는 보안 관련 애플리케이션을 구비할 수 있으며, 상기 애플리케이션을 통해 이하에서 설명할 각종 기능들을 수행할 수 있다.

[0072] 상술한 바와 같이, 제1 디바이스(104)는 상기 순차적으로 연결된 제1 해시 값들(예를 들어, $H^{1}(T) - H^{2}(T) - H^{3}(T) \ldots H^{99}(T) - H^{100}(T)$), 서비스 서버(102)에 입력된 정책, 제1 최대 카운트 및 키 토큰의 유효 기간에 관한 정보를 서비스 서버(102)로부터 수신할 수 있다. 또한, 제1 디바이스(104)는 수신된 상기 제1 해시 값들, 정책, 제1 최대 카운트 및 키 토큰의 유효 기간에 관한 정보를 암호화하여 내부 보안 영역(즉, 스토리지)에 저장할 수 있다.

[0073] 이후, 제1 디바이스(104)는 제2 디바이스(106)와의 D2D 통신을 위해 순차적으로 연결된 제1 해시 값들 중 제1 최대 카운트에 대응되는 제1 해시 값을 제2 디바이스(106)로 전송하고, 제1 해시 값이 전송될 때마다 제1 최대 카운트를 1씩 차감할 수 있다. 일 예시로서, 제1 디바이스(104)는 순차적으로 연결된 제1 해시 값들 중 마지막에 연결된 제1 해시 값을 가장 먼저 제2 디바이스(106)로 전송하고, 상기 마지막에 연결된 제1 해시 값의 바로 이전 제1 해시 값을 그 다음에 제2 디바이스(106)로 전송할 수 있다. 위 예시에서, 제1 디바이스(104)는 $H^{100}(T)$, $H^{99}(T)$, $H^{98}(T)$... 을 하나씩 제2 디바이스(106)로 전송할 수 있으며, $H^{100}(T)$, $H^{99}(T)$, $H^{98}(T)$... 을 제2 디바이스(106)로 전송할 때마다 제1 최대 카운트를 100→99, 99→98, 98→97, ... 로 각각 차감할 수 있다. 이와 같이, 제1 디바이스(104)는 제2 디바이스(106)와의 통신을 시도할 때마다 체인의 가장 끝단에 연결된 제1 해시 값을 하나씩 소진하게 되며, 이에 따라 제1 디바이스(104) 측 최대 카운트를 1씩 차감하게 된다.

[0074] 만약, 키 토큰의 유효 기간이 설정된 기간을 초과하여 남은 상태에서 제1 디바이스(104) 측 최대 카운트의 수(또는 체인에 연결된 제1 해시 값들의 개수)가 설정된 값(예를 들어, 1) 이하가 되는 경우, 제1 디바이스(104)는 서비스 서버(102)로 상기 키 토큰 및 제1 최대 카운트의 갱신을 요청할 수 있다. 일 예시로서, 키 토큰의 유효 기간이 5월 1일 ~ 5월 10일이라 가정할 때 현재 날짜(예를 들어, 5월 3일)로부터 상기 유효 기간의 만료일까지의 남은 기한이 5일 이상 초과하여 남은 상태에서 제1 디바이스(104) 측 최대 카운트의 수가 1이 되는 경우, 제1 디바이스(104)는 서비스 서버(102)로 상기 키 토큰 및 제1 최대 카운트의 갱신을 요청할 수 있다. 이 경우, 서비스 서버(102)는 제1 디바이스(104)의 요청에 따라 키 토큰 및 제1 최대 카운트를 갱신하고, 갱신된 키 토큰 및 갱신된 제1 최대 카운트로부터 생성되는 새로운 제1 해시 값들, 상기 새로운 제1 해시 값들의 순차적인 연결 관계 및 갱신된 제1 최대 카운트에 관한 정보를 제1 디바이스(104)로 전송할 수 있다.

[0075] 또한, 키 토큰의 유효 기간이 설정된 기간 이하로 남은 상태에서 제1 디바이스(104) 측 최대 카운트의 수가 설정된 값(예를 들어, 1) 이하가 되는 경우(또는 체인에 연결된 제1 해시 값들이 모두 소진되는 경우) 또는 키 토큰의 남은 유효 기간이 만료되는 경우, 제1 디바이스(104)는 서비스 서버(102)로 상기 키 토큰의 폐기를 요청할 수 있다. 일 예시로서, 키 토큰의 유효 기간이 5월 1일 ~ 5월 10일이라 가정할 때 현재 날짜(예를 들어, 5월 9일)로부터 상기 유효 기간의 만료일까지의 남은 기한이 2일 이하로 남은 상태에서 제1 디바이스(104) 측 최대 카운트의 수가 1이 되는 경우, 제1 디바이스(104)는 서비스 서버(102)로 상기 키 토큰의 폐기를 요청할 수 있다. 이 경우, 서비스 서버(102)는 제1 디바이스(104) 및 제2 디바이스(106)로 남은 해시 코드(즉, 해시 값들의 체인)의 폐기를 각각 요청하고, 제1 디바이스(104) 및 제2 디바이스(106)에서 해시 코드의 폐기가 완료되는 경우 서비스 서버(102)에 저장된 키 토큰을 폐기할 수 있다.

[0076] 제2 디바이스(106)는 제어 대상이 되는 디바이스로서, 예를 들어 도어락, 차량, 센서 등과 같은 IoT 디바이스 또는 상기 IoT 디바이스에 내장된 보안 모듈일 수 있다.

[0077] 상술한 바와 같이, 제2 디바이스(106)는 키 토큰의 최초 해시 값, 제2 최대 카운트에 관한 정보, 서비스 서버(102)에 입력된 정책, 키 토큰의 유효 기간에 관한 정보 등을 서비스 서버(102)로부터 수신할 수 있다. 이때, 제2 디바이스(106)는 중개 장치(108)를 통해 상기 정보들을 서비스 서버(102)로부터 수신할 수 있다. 또한, 제2 디바이스(106)는 수신된 키 토큰의 최초 해시 값, 제2 최대 카운트에 관한 정보, 서비스 서버(102)에 입력된 정책, 키 토큰의 유효 기간에 관한 정보 등을 내부 보안 영역(즉, 스토리지)에 저장할 수 있다.

[0078] 또한, 제2 디바이스(106)는 제1 디바이스(104)로부터 상기 제1 해시 값들 중 하나를 수신할 수 있다. 상술한 바와 같이, 제1 디바이스(104)는 제1 해시 값들 중 현재 제1 최대 카운트에 대응되는 제1 해시 값을 제2 디바이스(106)로 전송할 수 있다. 제2 디바이스(106)는 제1 디바이스(104)로부터 상기 제1 해시 값들 중 하나를 수신함에 따라 제1 디바이스(104)로부터 수신된 제1 해시 값, 서비스 서버(102)로부터 수신된 최초 해시 값 및 제2 최

대 카운트에 관한 정보를 이용하여 제1 디바이스(104)를 인증할 수 있다.

[0079] 구체적으로, 제2 디바이스(106)는 제1 디바이스(104)로부터 수신된 제1 해시 값과 일치하는 값이 나올 때까지 상기 최초 해시 값을 제2 최대 카운트 이하만큼 반복적으로 해시함으로써 생성되는 제2 해시 값들을 상기 제1 해시 값과 각각 비교하여 제1 디바이스(104)를 인증할 수 있다. 이때, 제2 디바이스(106)는 서비스 서버(102)에서 사용된 해시 함수와 동일한 해시 함수를 이용하여 제2 해시 값들을 생성하게 된다. 일 예시로서, 제2 디바이스(106)는 최초 해시 값에 해시 함수를 한 번 적용한 값과 상기 제1 해시 값을 비교하고, 비교 결과 일치하지 않는 경우 최초 해시 값에 해시 함수를 두 번 적용한 값과 상기 제2 해시 값을 비교할 수 있다. 이와 같이, 제2 디바이스(106)는 제1 해시 값과 일치하는 값이 나올 때까지 상기 최초 해시 값을 제2 최대 카운트 이하만큼 반복적으로 해시할 수 있으며, 이렇게 생성된 제2 해시 값들을 상기 제1 해시 값과 각각 비교할 수 있다.

[0080] 만약, 상기 제1 해시 값과 일치하는 제2 해시 값이 나오는 경우, 제2 디바이스(106)는 제1 디바이스(104)의 인증이 완료된 것으로 판단할 수 있다.

[0081] 또한, 제2 디바이스(106)는 상기 제1 해시 값과 일치하는 제2 해시 값에 기초하여 상기 제2 최대 카운트를 차감할 수 있다. 구체적으로, 제2 디바이스(106)는 N번 해시된 제2 해시 값이 상기 제1 해시 값과 일치하는 경우 제2 최대 카운트를 상기 N으로 차감할 수 있다. 여기서, N < 제2 최대 카운트이다. 예를 들어, 해시 함수가 50번 적용된 제2 해시 값이 상기 제1 해시 값과 일치하는 경우, 제2 디바이스(106)는 제2 최대 카운트를 50으로 차감할 수 있다. 본 발명의 실시예들에 따르면, 제1 디바이스(104)와 제2 디바이스(106)가 현재 서로 다른 최대 카운트를 가지고 있다 하더라도 제1 디바이스(104)의 인증이 가능하다.

[0082] 도 6은 본 발명의 일 실시예에 따른 서비스 서버(102)의 상세 구성을 나타낸 블록도이다. 도 6에 도시된 바와 같이, 본 발명의 일 실시예에 따른 서비스 서버(102)는 정책 매니저(202), 토큰 매니저(204), 제1 디바이스 매니저(206), 제2 디바이스 매니저(208), 인터페이스(210), 커맨드 매니저(212), 권한 설정 매니저(214) 및 인증 매니저(216)를 포함하며, 실시예에 따라 데이터베이스(218)와 연결될 수 있다.

[0083] 정책 매니저(202)는 기간계 시스템(미도시)으로부터 정책을 입력 받는다. 또한, 정책 매니저(202)는 각 정책별 식별 코드를 관리하고, 정책이 입력될 때마다 입력된 정책의 식별 코드를 확인하여 해당 정책을 식별할 수 있다. 또한, 정책 매니저(202)는 정책의 입력, 변경 및 만료시 토큰 매니저(204)로 키 토큰의 생성, 갱신 및 폐기를 각각 요청할 수 있다. 구체적으로, 정책 매니저(202)는 정책이 새롭게 입력되거나 입력된 정책이 변경되는 경우 토큰 매니저(204)로 키 토큰의 생성 또는 갱신을 요청하고, 입력된 정책의 유효 기간이 만료되는 경우 토큰 매니저(204)로 키 토큰의 폐기를 요청할 수 있다.

[0084] 토큰 매니저(204)는 키 토큰의 생성, 갱신 및 폐기를 관리한다. 토큰 매니저(204)는 정책 매니저(202)를 통해 정책이 입력됨에 따라 키 토큰을 생성할 수 있다. 또한, 토큰 매니저(204)는 키 토큰의 유효 기간, 제1 디바이스(104) 측 최대 카운트의 수 및 서비스 서버(102)에 입력된 정책 중 하나 이상을 고려하여 키 토큰 및 최대 카운트 중 하나 이상을 갱신 또는 폐기할 수 있다. 즉, 토큰 매니저(204)는 입력된 정책에 종속적인 키 토큰의 라이프사이클(life cycle)을 관리할 수 있다.

[0085] 또한, 토큰 매니저(204)는 생성된 키 토큰을 기반으로 해시 코드를 생성할 수 있다. 구체적으로, 토큰 매니저(204)는 키 토큰을 설정된 최대 카운트만큼 반복적으로 해시함으로써 복수 개의 제1 해시 값들을 생성하고, 생성된 제1 해시 값들을 해시 함수가 적용된 횟수 순으로 순차적으로 연결하여 상기 제1 해시 값들의 체인을 생성할 수 있다. 이때, 최대 카운트는 순차적으로 연결된 제1 해시 값들의 개수로서, 입력된 정책, 키 토큰의 유효 기간 등에 따라 달라질 수 있다. 또한, 토큰 매니저(204)는 키 토큰의 갱신시 상기 해시 코드를 갱신하고, 키 토큰의 폐기시 상기 해시 코드를 폐기할 수 있다.

[0086] 또한, 토큰 매니저(204)는 제1 디바이스(104) 및 제2 디바이스(106) 측 최대 카운트를 이용하여 양 디바이스(104, 106)에 저장된 해시 값들의 체인을 동기화할 수 있다.

[0087] 제1 디바이스 매니저(206)는 제1 디바이스(104)와 데이터를 송수신한다. 제1 디바이스 매니저(206)는 순차적으로 연결된 제1 해시 값들(즉, 제1 해시 값들의 체인), 입력된 정책, 최대 카운트에 관한 정보, 키 토큰의 유효 기간에 관한 정보 등을 제1 디바이스(104)로 전송할 수 있다. 또한, 제1 디바이스 매니저(206)는 제1 디바이스(104)로 해시 코드의 동기화를 요청하고, 제1 디바이스(104)에 저장된 최대 카운트에 관한 정보를 제1 디바이스(104)로부터 수신할 수 있다. 또한, 제1 디바이스 매니저(206)는 토큰 매니저(204)의 요청에 따라 제1 디바이스(104)로 해시 코드의 폐기를 요청할 수 있다.

[0088] 제2 디바이스 매니저(208)는 제2 디바이스(106)와 데이터를 송수신한다. 제2 디바이스 매니저(208)는 키 토큰의

최초 해시 값, 최대 카운트에 관한 정보, 입력된 정책, 키 토큰의 유효 기간에 관한 정보 등을 제2 디바이스(106)로 전송할 수 있다. 또한, 제2 디바이스 매니저(208)는 제2 디바이스(106)로 해시 코드의 동기화를 요청하고, 제2 디바이스(106)에 저장된 최대 카운트에 관한 정보를 제2 디바이스(106)로부터 수신할 수 있다. 또한, 제2 디바이스 매니저(208)는 토큰 매니저(204)의 요청에 따라 제2 디바이스(106)로 해시 코드의 폐기를 요청할 수 있다.

[0089] 인터페이스(210)는 기간계 시스템, 제1 디바이스(104) 및 제2 디바이스(106)와의 데이터 송수신을 위한 모듈이다. 정책 매니저(202)는 인터페이스(210)를 통해 기간계 시스템으로부터 정책을 입력 받을 수 있다. 또한, 제1 디바이스 매니저(206)는 인터페이스(210)를 통해 제1 디바이스(104)와 각종 데이터를 송수신할 수 있다. 또한, 제2 디바이스 매니저(208)는 인터페이스(210)를 통해 제2 디바이스(106)와 각종 데이터를 송수신할 수 있다. 이때, 제2 디바이스 매니저(208)는 중개 장치(108)를 거쳐 제2 디바이스(106)와 각종 데이터를 송수신할 수 있으며, 이 경우 인터페이스(210)는 서비스 서버(102)와 중개 장치(108) 간의 데이터를 중개하는 데 사용될 수 있다.

[0090] 커맨드 매니저(212)는 제2 디바이스(106)의 제어를 위한 각종 커맨드를 관리한다. 커맨드 매니저(212)는 각 정책에 대응되는 하나 이상의 커맨드를 구비할 수 있으며, 각 정책별 커맨드의 수정이 필요한 경우 이를 업데이트 할 수 있다. 상기 각 정책별 커맨드는 해당 정책에 매핑되어 있을 수 있으며, 제1 디바이스(104) 및 제2 디바이스(106)는 서비스 서버(102)로부터 수신된 정책에 관한 정보를 참조하여 대응되는 하나 이상의 커맨드를 식별할 수 있다. 상기 커맨드는 예를 들어, 예약된 차량의 도어 잠금/도어 잠금 해제, 시동 온/오프, 운행 정보 조회, 위치 정보 조회 등이 될 수 있다.

[0091] 권한 설정 매니저(214)는 서비스를 제공받는 사용자, 제1 디바이스(104)의 정보 및 제2 디바이스(106)의 정보를 관리한다. 권한 설정 매니저(214)는 제1 디바이스(104) 및 제2 디바이스(106)의 정보를 등록할 수 있다. 여기서, 제1 디바이스(104)의 정보는 예를 들어, 제1 디바이스(104)의 유형, 식별 정보, 제1 디바이스(104)를 소지하는 사용자의 아이디/비밀번호 등이 될 수 있다. 또한, 제2 디바이스(106)의 정보는 예를 들어, 제2 디바이스(106)의 유형, 식별 정보, 제어 가능한 제2 디바이스(106)의 동작 정보(예를 들어, 도어 개폐/시동 온, 오프 등), 기타 정보(예를 들어, 제2 디바이스(106)가 차량인 경우 차량의 운행 정보, 위치 정보 등) 등이 될 수 있다.

[0092] 인증 매니저(216)는 권한 설정 매니저(214)와 연동하여 제1 디바이스(104) 및 제2 디바이스(106)를 인증한다. 인증 매니저(216)는 제1 디바이스(104) 및 제2 디바이스(106)의 로그인 요청시 상술한 제1 디바이스(104) 및 제2 디바이스(106)의 정보를 이용하여 제1 디바이스(104) 및 제2 디바이스(106)를 각각 인증할 수 있다.

[0093] 데이터베이스(218)는 제1 디바이스(104)와 제2 디바이스(106) 간 D2D 통신에 필요한 각종 정보가 저장되는 저장소이다. 데이터베이스(218)에는 예를 들어, 하나 이상의 정책, 각 정책별 커맨드, 토큰 키, 토큰 키의 해시 코드, 제1 디바이스(104) 및 제2 디바이스(106)의 정보 등이 저장될 수 있다. 도 1에서는 설명의 편의상 데이터베이스(218)가 서비스 서버(102)와 연결되는 것으로 도시하였으나 이는 일 예시에 불과하며, 데이터베이스(218)는 서비스 서버(102)의 일 구성으로서 서비스 서버(102)의 내부에 존재할 수도 있다.

[0094] 도 7은 본 발명의 일 실시예에 따른 제1 디바이스(104)의 상세 구성을 나타낸 블록도이다. 도 7에 도시된 바와 같이, 본 발명의 일 실시예에 따른 제1 디바이스(104)는 제1 인터페이스(302), 접속 매니저(304), 커맨드 매니저(306), 스마트 키 매니저(308), 제2 인터페이스(310) 및 스토리지(312)를 포함한다.

[0095] 제1 인터페이스(302)는 서비스 서버(102)와의 데이터 송수신을 위한 모듈이다. 제1 디바이스(104)는 제1 인터페이스(302)를 통해 서비스 서버(102)와 각종 데이터를 송수신할 수 있다.

[0096] 접속 매니저(304)는 사용자의 요청에 따라 서비스 서버(102)로 로그인을 요청한다. 또한, 접속 매니저(304)는 제1 디바이스(104)의 정보를 서비스 서버(102)로 제공할 수 있으며, 서비스 서버(102)는 접속 매니저(304)로부터 수신된 제1 디바이스(104)의 정보를 이용하여 제1 디바이스(104)를 인증할 수 있다.

[0097] 커맨드 매니저(306)는 제2 디바이스(106)의 제어를 위한 각종 커맨드를 관리한다. 커맨드 매니저(306)는 각 정책에 대응되는 하나 이상의 커맨드를 구비할 수 있으며, 서비스 서버(102)로부터 수신된 정책에 대응되는 커맨드에 관한 정보를 상기 정책과 함께 제2 디바이스(106)로 전송할 수 있다.

[0098] 스마트 키 매니저(208)는 순차적으로 연결된 제1 해시 값들(즉, 제1 해시 값들의 체인), 입력된 정책, 제1 최대 카운트에 관한 정보, 키 토큰의 유효 기간에 관한 정보 등을 서비스 서버(102)로부터 수신한다. 또한, 스마트 키 매니저(208)는 순차적으로 연결된 제1 해시 값들을 제2 디바이스(106)로 하나씩 전송하며, 상기 제1 해시 값

이 전송된 이후 전송된 상기 제1 해시 값을 상기 제1 해시 값들의 연결에서 삭제하여 상기 제1 해시 값들을 하나씩 소진할 수 있다. 즉, 스마트 키 매니저(208)가 해시 함수가 N번 적용된 제1 해시 값(즉, $H^N(T)$)을 제2 디바이스(106)로 전송한 경우, 스마트 키 매니저(208)는 상기 $H^N(T)$을 상술한 체인에서 삭제하여 소진하고, 저장된 제1 최대 카운트를 N에서 N-1로 차감할 수 있다.

[0099] 또한, 키 토큰의 유효 기간이 설정된 기간 이상 남은 상태에서 체인에 연결된 제1 해시 값들의 개수(또는 제1 디바이스(104) 측 최대 카운트의 수)가 설정된 값(예를 들어, 1) 이하가 되는 경우, 스마트 키 매니저(208)는 서비스 서버(102)로 상기 키 토큰 및 제1 최대 카운트의 갱신을 요청할 수 있다.

[0100] 제2 인터페이스(310)는 제2 디바이스(106)와의 데이터 송수신을 위한 모듈이다. 제1 디바이스(104)는 제2 인터페이스(310)를 통해 제2 디바이스(106)로 각종 데이터를 송신할 수 있다. 제2 인터페이스(310)는 예를 들어, 와이파이(Wifi) 모듈, BLE(Bluetooth Low Energy) 모듈, NFC(Near Field Communication) 모듈, 지그비(Zigbee) 모듈 등과 같은 무선 통신 모듈일 수 있다.

[0101] 스토리지(312)는 제1 디바이스(104)와 제2 디바이스(106) 간 D2D 통신에 필요한 각종 정보가 저장되는 저장소이다. 스마트 키 매니저(208)는 예를 들어, 서비스 서버(102)로부터 수신된 상기 제1 해시 값들, 정책 및 제1 최대 카운트에 관한 정보를 암호화하여 스토리지(312)에 저장할 수 있다.

[0102] 도 8은 본 발명의 일 실시예에 따른 제2 디바이스(106)의 상세 구성을 나타낸 블록도이다. 도 8에 도시된 바와 같이, 본 발명의 일 실시예에 따른 제2 디바이스(106)는 제1 인터페이스(402), 제2 인터페이스(404), 스마트 키 매니저(406) 및 커맨드 매니저(408)을 포함한다.

[0103] 제1 인터페이스(402)는 서비스 서버(102)와의 데이터 송수신을 위한 모듈이다. 제2 디바이스(106)는 제1 인터페이스(402)를 통해 서비스 서버(102)와 각종 데이터를 송수신할 수 있다. 이때, 제2 디바이스(106)는 중개 장치(108)를 거쳐 서비스 서버(102)와 각종 데이터를 송수신할 수 있으며, 이 경우 제1 인터페이스(402)는 제2 디바이스(106)와 중개 장치(108) 간의 데이터를 중개하는 데 사용될 수 있다.

[0104] 제2 인터페이스(404)는 제1 디바이스(104)와의 데이터 송수신을 위한 모듈이다. 제2 디바이스(106)는 제2 인터페이스(404)를 통해 제1 디바이스(104)로부터 각종 데이터를 수신할 수 있다. 제2 인터페이스(404)는 예를 들어, 와이파이 모듈, BLE 모듈, NFC 모듈, 지그비 모듈 등과 같은 무선 통신 모듈일 수 있다.

[0105] 스마트 키 매니저(406)는 키 토큰의 최초 해시 값, 제2 최대 카운트에 관한 정보, 입력된 정책, 키 토큰의 유효 기간에 관한 정보 등을 서비스 서버(102)로부터 수신한다. 또한, 스마트 키 매니저(406)는 제1 디바이스(104)로부터 제1 해시 값들 중 하나를 수신하고, 제1 디바이스(104)로부터 수신된 제1 해시 값, 서비스 서버(102)로부터 수신된 최초 해시 값 및 제2 최대 카운트에 관한 정보를 이용하여 제1 디바이스(104)를 인증할 수 있다.

[0106] 구체적으로, 스마트 키 매니저(406)는 제1 디바이스(104)로부터 수신된 제1 해시 값과 일치하는 값이 나올 때까지 상기 최초 해시 값을 제2 최대 카운트 이하만큼 반복적으로 해시함으로써 생성되는 제2 해시 값들을 상기 제1 해시 값과 각각 비교하여 제1 디바이스(104)를 인증할 수 있다.

[0107] 또한, 스마트 키 매니저(406)는 상기 제1 해시 값과 일치하는 제2 해시 값에 기초하여 상기 제2 최대 카운트를 차감할 수 있다. 일 예시로서, N번 해시된 제2 해시 값이 상기 제1 해시 값과 일치하는 경우, 스마트 키 매니저(406)는 상기 제2 최대 카운트를 상기 N으로 차감할 수 있다.

[0108] 커맨드 매니저(408)는 스마트 키 매니저(406)에서 제1 디바이스(104)의 인증이 성공하는 경우 제1 디바이스(104)로부터 수신된 정책에 대응되는 커맨드를 수행한다. 일 예시로서, 제1 디바이스(104)로부터 수신된 제1 해시 값과 제2 디바이스(106)에서 생성된 제2 해시 값이 일치하는 경우, 커맨드 매니저(408)는 차량의 도어 잠금을 해제할 수 있다.

[0109] 도 9는 본 발명의 일 실시예에 따른 중개 장치(108)의 상세 구성을 나타낸 블록도이다. 도 9에 도시된 바와 같이, 본 발명의 일 실시예에 따른 중개 장치(108)는 제1 인터페이스(502), 제2 인터페이스(504), 세션 매니저(506) 및 데이터 변환 모듈(506)을 포함하며, 실시예에 따라 데이터베이스(510)와 연결될 수 있다.

[0110] 제1 인터페이스(502)는 서비스 서버(102)와의 데이터 송수신을 위한 모듈이다. 중개 장치(108)는 제1 인터페이스(502)를 통해 서비스 서버(102)와 각종 데이터를 송수신할 수 있다.

[0111] 제2 인터페이스(504)는 제2 디바이스(106)와의 데이터 송수신을 위한 모듈이다. 중개 장치(108)는 제2 인터페이스(504)를 통해 제2 디바이스(106)와 각종 데이터를 송수신할 수 있다. 또한, 중개 장치(108)는 예를 들어,

MQTT(Message Queuing Telemetry Transport) 프로토콜을 지원할 수 있으며, 상기 MQTT 프로토콜을 통해 제2 디바이스(106)와 각종 데이터를 송수신할 수 있다.

[0112] 세션 매니저(506)는 제2 디바이스(106)의 세션 정보를 관리한다.

[0113] 데이터 변환 모듈(508)은 서비스 서버(102)로부터 수신된 데이터를 제2 디바이스(106)가 수신 가능한 형태로 변환하거나 제2 디바이스(106)로부터 수신된 데이터를 서비스 서버(102)가 수신 가능한 형태로 변환한다.

[0114] 데이터베이스(510)는 서비스 서버(102)와 제2 디바이스(106) 간 통신에 필요한 각종 정보가 저장되는 저장소이다. 데이터베이스(510)에는 예를 들어, 제2 디바이스(106)의 정보, 세션 정보(예를 들어, 세션 아이디 등) 등이 저장될 수 있다.

[0115] 도 10은 본 발명의 일 실시예에 따른 키 토큰의 생성 및 해시 코드의 분배 과정을 설명하기 위한 흐름도이다. 도 10 내지 도 16에 도시된 흐름도에서는 상기 방법을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0116] 단계 102에서, 정책 매니저(202)는 정책 입력에 따라 토큰 매니저(204)로 키 토큰(T)의 생성을 요청한다.

[0117] 단계 104에서, 토큰 매니저(204)는 키 토큰(T)을 생성한다.

[0118] 단계 106에서, 토큰 매니저(204)는 상기 키 토큰(T)(또는 키 토큰(T)의 최초 해시 값)을 설정된 최대 카운트만큼 반복적으로 해시함으로써 획득되는 제1 해시 값들을 해시 함수가 적용된 횟수 순으로 순차적으로 연결한다. 여기서는, 설명의 편의상 최대 카운트가 100인 것으로 가정한다.

[0119] 단계 108에서, 토큰 매니저(204)는 제2 디바이스 매니저(208)로 해시 코드의 동기화를 요청한다.

[0120] 단계 110에서, 토큰 매니저(204)는 제2 디바이스(106)를 검색하고, 키 토큰의 최초 해시 값, 최대 카운트에 관한 정보, 입력된 정책, 키 토큰의 유효 기간에 관한 정보 등을 제2 디바이스(106)로 전송하면서 해시 코드의 동기화를 요청한다.

[0121] 단계 112에서, 제2 디바이스(106)는 키 토큰의 최초 해시 값, 최대 카운트에 관한 정보, 입력된 정책, 키 토큰의 유효 기간에 관한 정보 등을 저장한다. 여기서, 제2 디바이스(106)에 저장된 최대 카운트를 제2 최대 카운트라 칭하기로 한다.

[0122] 단계 114에서, 제2 디바이스(106)는 제2 디바이스(106)에 저장된 제2 최대 카운트에 관한 정보(예를 들어, Max Count = 100)를 제2 디바이스 매니저(208)로 전송한다.

[0123] 단계 116에서, 제2 디바이스 매니저(208)는 제2 디바이스(106)로부터 수신된 제2 최대 카운트에 관한 정보(예를 들어, Max Count = 100)를 토큰 매니저(204)로 전송한다.

[0124] 단계 118에서, 토큰 매니저(204)는 제1 디바이스 매니저(206)로 해시 코드의 동기화를 요청한다.

[0125] 단계 120에서, 제1 디바이스 매니저(206)는 제1 디바이스(104)를 검색하고, 순차적으로 연결된 제1 해시 값들(즉, 제1 해시 값들의 체인), 입력된 정책, 최대 카운트에 관한 정보, 키 토큰의 유효 기간에 관한 정보 등을 제1 디바이스(104)로 전송하면서 해시 코드의 동기화를 요청한다.

[0126] 단계 122에서, 제1 디바이스(104)는 순차적으로 연결된 제1 해시 값들(즉, 제1 해시 값들의 체인), 입력된 정책, 최대 카운트에 관한 정보, 키 토큰의 유효 기간에 관한 정보 등을 암호화하여 저장한다. 여기서, 제1 디바이스(104)에 저장된 최대 카운트를 제1 최대 카운트라 칭하기로 한다.

[0127] 단계 124에서, 제1 디바이스(104)는 제1 디바이스(104)에 저장된 제1 최대 카운트에 관한 정보(예를 들어, Max Count = 100)를 제1 디바이스 매니저(206)로 전송한다.

[0128] 단계 126에서, 제1 디바이스 매니저(206)는 제1 디바이스(104)로부터 수신된 제1 최대 카운트에 관한 정보(예를 들어, Max Count = 100)를 토큰 매니저(204)로 전송한다.

[0129] 단계 128에서, 토큰 매니저(204)는 제1 디바이스(104)로부터 수신된 제1 최대 카운트(예를 들어, Max Count = 100)와 제2 디바이스(106)로부터 수신된 제2 최대 카운트(예를 들어, Max Count = 100)를 비교한다. 만약, 제1 디바이스(104)로부터 수신된 제1 최대 카운트(예를 들어, Max Count = 100)와 제2 디바이스(106)로부터 수신된 제2 최대 카운트(예를 들어, Max Count = 100)가 일치하는 경우, 토큰 매니저(204)는 해시 코드의 동기화가 성

공한 것으로 판단한다. 반면, 제1 디바이스(104)로부터 수신된 제1 최대 카운트와 제2 디바이스(106)로부터 수신된 제2 최대 카운트가 일치하지 않는 경우, 토큰 매니저(204)는 해시 코드의 동기화가 실패한 것으로 판단하고, 제1 디바이스 매니저(206) 및 제2 디바이스 매니저(208)로 해시 코드의 동기화를 재요청할 수 있다.

[0130] 단계 130에서, 토큰 매니저(204)는 해시 코드의 동기화 결과를 정책 매니저(202)로 전송한다.

[0131] 한편, 여기서는 서비스 서버(102)가 해시 코드를 제1 디바이스(104) 및 제2 디바이스(106)에 각각 분배하는 과정에서 제1 디바이스(104) 및 제2 디바이스(106)에 저장된 해시 코드를 동기화하는 것으로 설명하였으나 이는 일 예시에 불과하다. 서비스 서버(102)는 해시 코드가 제1 디바이스(104) 및 제2 디바이스(106)에 각각 분배된 이후 어느 때라도 상술한 동기화 작업을 수행할 수 있다. 예를 들어, 서비스 서버(102)는 후술할 도 11의 디바이스 간 인증 과정 중 제1 디바이스(104) 및 제2 디바이스(106)로 동기화 요청 메시지를 전송하여 제1 디바이스(104) 및 제2 디바이스(106)에 저장된 해시 코드의 동기화 작업을 수행할 수 있다.

[0132] 도 11은 본 발명의 제1 실시예에 따른 디바이스(104, 106) 간 인증 과정을 설명하기 위한 흐름도이다.

[0133] 단계 202에서, 제1 디바이스(104)는 제1 해시 값들 중 제1 최대 카운트에 대응되는 제1 해시 값을 전송한다. 여기서, 제1 최대 카운트는 예를 들어, 100인 것으로 가정한다. 제1 디바이스(104)는 예를 들어, 제1 해시 값들 중 제1 최대 카운트에 대응되는 제1 해시 값인 $H^{100}(T)$를 입력된 정책, 현재 시간, 제1 디바이스(104)의 아이디 등과 함께 제2 디바이스(106)로 전송할 수 있다. 이때, 상기 $H^{100}(T)$은 네트워크 상의 문제로 제2 디바이스(106)로 제대로 전달되지 않은 것으로 가정한다.

[0134] 단계 204에서, 제1 디바이스(104)는 전송된 제1 해시 값, 즉 $H^{100}(T)$을 상기 제1 해시 값들의 연결에서 삭제하고 제1 디바이스(104)에 저장된 제1 최대 카운트를 100에서 99로 차감한다. 즉, 제1 디바이스(104)가 해시 함수가 N번 적용된 제1 해시 값(즉, $H^{N}(T)$)을 제2 디바이스(106)로 전송한 경우, 제1 디바이스(104)는 상기 $H^{N}(T)$을 상술한 체인에서 삭제하여 소진하고, 저장된 제1 최대 카운트를 N에서 N-1로 차감할 수 있다.

[0135] 단계 206에서, 제1 디바이스(104)는 제1 해시 값들 중 제1 최대 카운트에 대응되는 제1 해시 값을 전송한다. 여기서, 제1 최대 카운트는 99이므로, 제1 디바이스(104)는 제1 최대 카운트에 대응되는 제1 해시 값인 $H^{99}(T)$를 입력된 정책, 현재 시간, 제1 디바이스(104)의 아이디 등과 함께 제2 디바이스(106)로 전송할 수 있다. 이때, 상기 $H^{99}(T)$은 제2 디바이스(106)로 정상적으로 전달된 것으로 가정한다.

[0136] 단계 208에서, 제1 디바이스(104)는 전송된 제1 해시 값, 즉 $H^{99}(T)$을 상기 제1 해시 값들의 연결에서 삭제하고 제1 디바이스(104)에 저장된 제1 최대 카운트를 99에서 98로 차감한다.

[0137] 단계 210에서, 제2 디바이스(106)는 상기 제1 해시 값과 일치하는 값이 나올 때까지 상기 최초 해시 값을 제2 최대 카운트 이하만큼 반복적으로 해시함으로써 생성되는 제2 해시 값들을 상기 제1 해시 값과 각각 비교한다. 일 예시로서, 제2 디바이스(106)는 제1 해시 값 $H^{99}(T)$와 제2 해시 값 $H^{1}(T)$, 제1 해시 값 $H^{99}(T)$와 제2 해시 값 $H^{2}(T)$, 제1 해시 값 $H^{99}(T)$와 제2 해시 값 $H^{3}(T)$... 을 각각 비교할 수 있다. 이때, 제2 디바이스(106)는 상기 제1 해시 값과 일치하는 값이 나올 때까지 상기 최초 해시 값을 제2 최대 카운트 이하만큼 반복적으로 해시할 수 있다.

[0138] 단계 S212에서, 제1 해시 값과 일치하는 제2 해시 값이 나오는 경우, 제2 디바이스(106)는 제1 디바이스(104)의 인증이 성공한 것으로 판단한다.

[0139] 단계 S214에서, 제2 디바이스(106)는 N번 해시된 제2 해시 값이 상기 제1 해시 값과 일치하는 경우 상기 제2 최대 카운트를 상기 N으로 차감한다. 위 예시에서, 99번 해시된 제2 해시 값 $H^{99}(T)$이 제1 해시 값 $H^{99}(T)$과 일치하므로, 제2 디바이스(106)는 제2 최대 카운트를 100에서 99로 차감할 수 있다.

[0140] 단계 216에서, 제2 디바이스(106)는 제1 디바이스(104)로부터 수신된 정책에 대응되는 커맨드를 수행한다.

[0141] 도 12는 본 발명의 제2 실시예에 따른 디바이스 간 인증 과정을 설명하기 위한 흐름도이다.

[0142] S218 단계에서, 제1 디바이스(104)는 제1 해시 값과 상기 제1 해시 값에 대응되는 해시 넘버(M)를 제2 디바이스(106)로 전송한다. 여기서, 해시 넘버(M)는 해시 함수가 적용된 횟수를 나타낸다. 일 예시로서, 제1 디바이스

(104)는 제1 해시 값 $H^{50}(T)$과 제1 해시 값 $H^{50}(T)$에 대응되는 해시 넘버 M = 50을 제3 디바이스(106)로 전송할 수 있다.

[0143] S220 단계에서, 제1 디바이스(104)는 제1 디바이스(104)는 전송된 제1 해시 값, 즉 $H^{50}(T)$을 상기 제1 해시 값들의 연결에서 삭제하고 제1 디바이스(104)에 저장된 제1 최대 카운트를 50에서 49로 차감한다.

[0144] 단계 222에서, 제2 디바이스(106)는 상기 최초 해시 값을 해시 넘버(M)만큼 반복적으로 해시함으로써 생성되는 제2 해시 값들을 상기 제1 해시 값과 각각 비교한다. 이때, 제2 디바이스(106)는 먼저 해시 넘버(M)가 제2 최대 카운트보다 작은지의 여부를 확인할 수 있다. 일 예시로서, 해시 넘버 M = 50 이고 제2 최대 카운트가 51인 경우, 제2 디바이스(106)는 M = 50 < 제2 최대 카운트 = 51임을 확인할 수 있다. 이 경우, 제2 디바이스(106)는 제1 해시 값 $H^{50}(T)$와 제2 해시 값 $H^{1}(T)$, 제1 해시 값 H50(T)와 제2 해시 값 $H^{2}(T)$, 제1 해시 값 $H^{50}(T)$와 제2 해시 값 $H^{3}(T)$... $H^{50}(T)$와 제2 해시 값 $H^{50}(T)$을 각각 비교할 수 있다.

[0145] 단계 S224에서, 제1 해시 값과 일치하는 제2 해시 값이 나오는 경우, 제2 디바이스(106)는 제1 디바이스(104)의 인증이 성공한 것으로 판단한다.

[0146] 단계 S226에서, 제2 디바이스(106)는 N번 해시된 제2 해시 값이 상기 제1 해시 값과 일치하는 경우 상기 제2 최대 카운트를 상기 N으로 차감한다. 위 예시에서, 50번 해시된 제2 해시 값 $H^{50}(T)$이 제1 해시 값 $H^{50}(T)$과 일치하므로, 제2 디바이스(106)는 제2 최대 카운트를 51에서 50으로 차감할 수 있다.

[0147] 단계 228에서, 제2 디바이스(106)는 제1 디바이스(104)로부터 수신된 정책에 대응되는 커맨드를 수행한다.

[0148] 도 13은 본 발명의 제1 실시예에 따른 키 토큰의 갱신 과정을 설명하기 위함 흐름도이다.

[0149] 단계 302에서, 제1 디바이스(104)는 서비스 서버(102)에서 생성된 키 토큰을 갱신할 필요가 있는지 확인한다. 일 예시로서, 키 토큰의 유효 기간이 설정된 기간 이상 남은 상태에서 체인에 연결된 제1 해시 값들의 개수(또는 제1 디바이스(104)에 저장된 최대 카운트의 수)가 설정된 값(예를 들어, 1) 이하가 되는 경우, 제1 디바이스(104)는 키 토큰의 갱신이 필요한 것으로 판단할 수 있다.

[0150] 단계 304에서, 제1 디바이스(104)는 토큰 매니저(204)로 키 토큰 및 최대 카운트의 갱신을 요청한다.

[0151] 단계 306에서, 토큰 매니저(204)는 새로운 키 토큰(T')을 생성한다.

[0152] 단계 308에서, 토큰 매니저(204)는 상기 키 토큰(T')을 설정된 최대 카운트(예를 들어, Max Count' = 50)만큼 반복적으로 해시함으로써 획득되는 제1 해시 값들을 해시 함수가 적용된 횟수 순으로 순차적으로 연결한다. 여기서는, 설명의 편의상 갱신된 최대 카운트가 50인 것으로 가정한다.

[0153] 단계 310에서, 토큰 매니저(204)는 제2 디바이스 매니저(208)로 해시 코드의 동기화를 요청한다.

[0154] 단계 312에서, 토큰 매니저(204)는 제2 디바이스(106)를 검색하고, 갱신된 키 토큰(T')의 최초 해시 값, 갱신된 최대 카운트에 관한 정보, 입력된 정책, 갱신된 키 토큰(T')의 유효 기간에 관한 정보 등을 제2 디바이스(106)로 전송하면서 해시 코드의 동기화를 요청한다.

[0155] 단계 314에서, 제2 디바이스(106)는 (T')의 최초 해시 값, 갱신된 최대 카운트에 관한 정보, 입력된 정책, 갱신된 키 토큰(T')의 유효 기간에 관한 정보 등을 저장한다. 여기서, 제2 디바이스(106)에 저장된 갱신된 최대 카운트를 갱신된 제2 최대 카운트라 칭하기로 한다.

[0156] 단계 316에서, 제2 디바이스(106)는 제2 디바이스(106)에 저장된 제2 최대 카운트에 관한 정보(예를 들어, Max Count' = 50)를 제2 디바이스 매니저(208)로 전송한다.

[0157] 단계 318에서, 제2 디바이스 매니저(208)는 제2 디바이스(106)로부터 수신된 제2 최대 카운트에 관한 정보(예를 들어, Max Count' = 50)를 토큰 매니저(204)로 전송한다.

[0158] 단계 320에서, 토큰 매니저(204)는 제1 디바이스 매니저(206)로 해시 코드의 동기화를 요청한다.

[0159] 단계 322에서, 제1 디바이스 매니저(206)는 제1 디바이스(104)를 검색하고, 순차적으로 연결된 제1 해시 값들(즉, 제1 해시 값들의 체인), 입력된 정책, 갱신된 최대 카운트에 관한 정보, 갱신된 키 토큰(T')의 유효 기간에 관한 정보 등을 제1 디바이스(104)로 전송하면서 해시 코드의 동기화를 요청한다.

[0160] 단계 324에서, 제1 디바이스(104)는 순차적으로 연결된 제1 해시 값들(즉, 제1 해시 값들의 체인), 입력된 정책, 갱신된 최대 카운트에 관한 정보, 갱신된 키 토큰(T')의 유효 기간에 관한 정보 등을 암호화하여 저장한다. 여기서, 제1 디바이스(104)에 저장된 갱신된 최대 카운트를 갱신된 제1 최대 카운트라 칭하기로 한다.

[0161] 단계 326에서, 제1 디바이스(104)는 제1 디바이스(104)에 저장된 제1 최대 카운트에 관한 정보(예를 들어, Max Count' = 50)를 제1 디바이스 매니저(206)로 전송한다.

[0162] 단계 328에서, 제1 디바이스 매니저(206)는 제1 디바이스(104)로부터 수신된 제1 최대 카운트에 관한 정보(예를 들어, Max Count' = 50)를 토큰 매니저(204)로 전송한다.

[0163] 단계 330에서, 토큰 매니저(204)는 제1 디바이스(104)로부터 수신된 제1 최대 카운트에 관한 정보(예를 들어, Max Count' = 50)와 제2 디바이스(106)로부터 수신된 제2 최대 카운트에 관한 정보(예를 들어, Max Count' = 50)를 비교한다. 만약, 제1 디바이스(104)로부터 수신된 제1 최대 카운트에 관한 정보(예를 들어, Max Count' = 50)와 제2 디바이스(106)로부터 수신된 제2 최대 카운트에 관한 정보(예를 들어, Max Count' = 50)가 일치하는 경우, 토큰 매니저(204)는 해시 코드의 동기화가 성공한 것으로 판단한다.

[0164] 단계 332에서, 토큰 매니저(204)는 해시 코드의 동기화 결과를 정책 매니저(202)로 전송한다.

[0165] 한편, 여기서는 S302 단계 및 S304 단계가 제1 디바이스(104)에서 수행되는 것으로 기재하였으나 이에 한정되는 것은 아니며, 실시예에 따라 상기 S302 단계 및 S304 단계는 제2 디바이스(106)에서 수행될 수도 있다.

[0166] 도 14는 본 발명의 제2 실시예에 따른 키 토큰의 갱신 과정을 설명하기 위함 흐름도이다.

[0167] S402 단계에서, 정책 매니저(202)는 기간계 시스템으로부터 변경된 정책을 입력 받는다.

[0168] S404 단계에서, 정책 매니저(202)는 정책 변경에 따라 토큰 매니저(204)로 키 토큰 및 최대 카운트의 갱신을 요청한다.

[0169] 이후, S406 단계 내지 S432 단계가 수행된다. S406 단계 내지 S432 단계는 앞선 S306 단계 내지 S332 단계와 동일하므로, 여기서는 그 자세한 설명을 생략하기로 한다.

[0170] 도 15는 도 14에서의 키 토큰의 갱신에 따른 이전 키 토큰의 폐기 과정을 설명하기 위한 흐름도이다.

[0171] S434 단계에서, 정책 매니저(202)는 토큰 매니저(204)로 키 토큰의 갱신 완료 메시지를 전송한다.

[0172] S436 단계에서, 토큰 매니저(204)는 제1 디바이스 매니저(206)로 제1 디바이스(104)에 저장된 이전 해시 코드에 대한 폐기를 요청한다.

[0173] S438 단계에서, 제1 디바이스 매니저(206)는 제1 디바이스(104)로 제1 디바이스(104)에 저장된 이전 해시 코드에 대한 폐기를 요청한다.

[0174] S440 단계에서, 제1 디바이스(104)는 제1 디바이스(104)에 저장된 이전 해시 코드를 폐기한다.

[0175] S442 단계에서, 토큰 매니저(204)는 제2 디바이스 매니저(208)로 제2 디바이스(106)에 저장된 이전 해시 코드에 대한 폐기를 요청한다.

[0176] S444 단계에서, 제2 디바이스 매니저(208)는 제2 디바이스(106)로 제2 디바이스(106)에 저장된 이전 해시 코드에 대한 폐기를 요청한다.

[0177] S446 단계에서, 제2 디바이스(106)는 제1 디바이스(104)에 저장된 이전 해시 코드를 폐기한다.

[0178] 도 16은 본 발명의 제1 실시예에 따른 키 토큰의 폐기 과정을 설명하기 위함 흐름도이다.

[0179] S502 단계에서, 제1 디바이스(104)는 서비스 서버(102)에서 생성된 키 토큰에 대한 유효성의 만료 여부를 확인한다. 일 예시로서, 키 토큰의 유효 기간이 설정된 기간 이하로 남은 상태에서 제1 디바이스(104)에 저장된 최대 카운트의 수가 설정된 값(예를 들어, 1) 이하가 되는 경우(또는 체인에 연결된 제1 해시 값들이 모두 소진되는 경우), 제1 디바이스(104)는 키 토큰의 폐기가 필요한 것으로 판단할 수 있다.

[0180] S504 단계에서, 제1 디바이스(104)는 토큰 매니저(204)로 키 토큰의 폐기를 요청한다.

[0181] S506 단계에서, 토큰 매니저(204)는 제2 디바이스 매니저(208)로 제2 디바이스(106)에 저장된 해시 코드의 폐기를 요청한다.

[0182] S508 단계에서, 제2 디바이스 매니저(208)는 제2 디바이스(106)로 제2 디바이스(106)에 저장된 남은 해시 코드의 폐기를 요청한다.

[0183] S510 단계에서, 제2 디바이스(106)는 제2 디바이스(106)에 저장된 남은 해시 코드를 폐기한다.

[0184] S512 단계에서, 제2 디바이스(106)는 해시 코드의 폐기 완료 메시지를 제2 디바이스 매니저(208)로 전송한다.

[0185] S514 단계에서, 제2 디바이스 매니저(208)는 제2 디바이스(106)로부터 수신된 해시 코드의 폐기 완료 메시지를 토큰 매니저(204)로 전송한다.

[0186] S516 단계에서, 토큰 매니저(204)는 제1 디바이스 매니저(206)로 제1 디바이스(104)에 저장된 해시 코드의 폐기를 요청한다.

[0187] S518 단계에서, 제1 디바이스 매니저(206)는 제1 디바이스(104)로 제1 디바이스(104)에 저장된 남은 해시 코드의 폐기를 요청한다.

[0188] S520 단계에서, 제1 디바이스(104)는 제1 디바이스(104)에 저장된 남은 해시 코드를 폐기한다.

[0189] S522 단계에서, 제1 디바이스(104)는 해시 코드의 폐기 완료 메시지를 제1 디바이스 매니저(206)로 전송한다.

[0190] S524 단계에서, 제1 디바이스 매니저(206)는 제1 디바이스(104)로부터 수신된 해시 코드의 폐기 완료 메시지를 토큰 매니저(204)로 전송한다.

[0191] S526 단계에서, 토큰 매니저(204)는 토큰 매니저(204)는 해시 코드의 동기화 결과를 정책 매니저(202)로 전송한다.

[0192] S528 단계에서, 정책 매니저(202)는 동기화 결과에 대한 확인 메시지를 토큰 매니저(204)로 전송한다.

[0193] S530 단계에서, 토큰 매니저(204)는 서비스 서버(102)에 저장된 키 토큰을 폐기한다.

[0194] 한편, 여기서는 S502 단계 및 S504 단계가 제1 디바이스(104)에서 수행되는 것으로 기재하였으나 이에 한정되는 것은 아니며, 실시예에 따라 상기 S502 단계 및 S504 단계는 제2 디바이스(106)에서 수행될 수도 있다.

[0195] 도 17은 본 발명의 제2 실시예에 따른 키 토큰의 폐기 과정을 설명하기 위함 흐름도이다.

[0196] S602 단계에서, 정책 매니저(202)는 입력된 정책에 대한 유효성의 만료 여부를 확인한다. 일 예시로서, 입력된 정책 또는 키 토큰의 남은 유효 기간이 만료되는 경우, 정책 매니저(202)는 키 토큰의 폐기가 필요한 것으로 판단할 수 있다.

[0197] S604 단계에서, 정책 매니저(202)는 토큰 매니저(204)로 키 토큰의 폐기를 요청한다.

[0198] 이후, S606 단계 내지 S630 단계가 수행된다. SS606 단계 내지 S630 단계는 앞선 S506 단계 내지 S530 단계와 동일하므로, 여기서는 그 자세한 설명을 생략하기로 한다. 한편, 여기서는 키 토큰 또는 입력된 정책의 유효성이 만료되는 경우 서비스 서버(102)가 키 토큰을 폐기하는 것으로 설명하였으나 이는 일 예시에 불과하며, 키 토큰이 폐기되는 경우가 이에 한정되는 것은 아니다. 예를 들어, 서비스 서버(102)는 제1 디바이스(104) 또는 제2 디바이스(106)에서 악성 코드가 감지되는 경우, 사용자의 아이디가 위조된 것으로 판별되는 경우 등과 같이 키 토큰의 유효성이 상실되는 경우 키 토큰을 폐기할 수 있다. 또한, 서비스 서버(102)는 관리자의 강제 조치에 의해 키 토큰을 폐기할 수도 있다.

[0199] 한편, 상술한 통신 시스템(100)은 차량 예약 및 제어 서비스, 도어락 제어 서비스 등과 같은 다양한 서비스에 적용될 수 있다. 일 예시로서, 통신 시스템(100)이 차량 예약 및 제어 서비스에 적용되는 경우, 제1 디바이스(104)는 사용자가 소지하는 사용자 단말, 예를 들어 스마트폰일 수 있으며, 제2 디바이스(106)는 차량에 탑재되는 보안 모듈, 예를 들어 CSM(Cypto Service Manager)일 수 있다.

[0200] 이 경우, 사용자는 제1 디바이스(104)에 설치된 모바일 애플리케이션을 통해 차량 사용에 대한 예약 요청 및 예약 기간을 입력할 수 있다. 서비스 서버(102)는 제1 디바이스(104)와 연동되는 기간계 시스템(미도시)로부터 상기 예약 요청 및 예약 기간에 관한 정보를 수신하고, 상기 차량에 대한 사용자의 예약이 완료됨에 따라 키 토큰 및 최대 카운트를 생성할 수 있다. 이때, 제1 최대 카운트 및 제2 최대 카운트는 차량에 대한 사용자의 예약 기간에 비례할 수 있다. 예를 들어, 사용자의 예약 기간이 5일인 경우 제1 최대 카운트 및 제2 최대 카운트는 100일 수 있으며, 사용자의 예약 기간이 3일인 경우 제1 최대 카운트 및 제2 최대 카운트는 50일 수 있다. 또한, 상기 차량에 대한 사용자의 예약이 변경되는 경우, 서비스 서버(102)는 생성된 키 토큰을 폐기하고 재생성할 수

있다.

[0201] 상기 차량에 대한 사용자의 예약 완료 또는 예약 변경시, 서비스 서버(102)는 상기 제1 해시 값들, 상기 제1 해시 값들의 순차적인 연결 관계 및 상기 제1 최대 카운트에 관한 정보를 제1 디바이스(104)로 전송하고, 상기 키 토큰의 최초 해시 값 및 상기 제2 최대 카운트에 관한 정보를 제2 디바이스(106)로 전송할 수 있다. 다만, 상기 키 토큰 및 최대 카운트가 반드시 서비스 서버(102)에서 생성되는 것은 아니며, 제1 디바이스(104) 및 제2 디바이스(106), 또는 이와 다른 별도의 장소에서 생성될 수도 있다.

[0202] 또한, 서비스 서버(102)는 상기 차량에 대한 사용자의 예약 취소시 생성된 키 토큰을 폐기하고, 제1 디바이스(104) 및 제2 디바이스(106)로 상기 제1 해시 값들 및 상기 제2 해시 값들의 폐기를 각각 요청할 수 있다.

[0203] 도 18은 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위한 블록도이다. 도시된 실시예에서, 각 컴포넌트들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술되지 것 이외에도 추가적인 컴포넌트를 포함할 수 있다.

[0204] 도시된 컴퓨팅 환경(10)은 컴퓨팅 장치(12)를 포함한다. 일 실시예에서, 컴퓨팅 장치(12)는 서비스 서버(102), 제1 디바이스(104), 제2 디바이스(106) 또는 중개 장치(108)에 포함되는 하나 이상의 컴포넌트일 수 있다.

[0205] 컴퓨팅 장치(12)는 적어도 하나의 프로세서(14), 컴퓨터 판독 가능 저장 매체(16) 및 통신 버스(18)를 포함한다. 프로세서(14)는 컴퓨팅 장치(12)로 하여금 앞서 언급된 예시적인 실시예에 따라 동작하도록 할 수 있다. 예컨대, 프로세서(14)는 컴퓨터 판독 가능 저장 매체(16)에 저장된 하나 이상의 프로그램들을 실행할 수 있다. 상기 하나 이상의 프로그램들은 하나 이상의 컴퓨터 실행 가능 명령어를 포함할 수 있으며, 상기 컴퓨터 실행 가능 명령어는 프로세서(14)에 의해 실행되는 경우 컴퓨팅 장치(12)로 하여금 예시적인 실시예에 따른 동작들을 수행하도록 구성될 수 있다.

[0206] 컴퓨터 판독 가능 저장 매체(16)는 컴퓨터 실행 가능 명령어 내지 프로그램 코드, 프로그램 데이터 및/또는 다른 적합한 형태의 정보를 저장하도록 구성된다. 컴퓨터 판독 가능 저장 매체(16)에 저장된 프로그램(20)은 프로세서(14)에 의해 실행 가능한 명령어의 집합을 포함한다. 일 실시예에서, 컴퓨터 판독 가능 저장 매체(16)는 메모리(랜덤 액세스 메모리와 같은 휘발성 메모리, 비휘발성 메모리, 또는 이들의 적절한 조합), 하나 이상의 자기 디스크 저장 디바이스들, 광학 디스크 저장 디바이스들, 플래시 메모리 디바이스들, 그 밖에 컴퓨팅 장치(12)에 의해 액세스되고 원하는 정보를 저장할 수 있는 다른 형태의 저장 매체, 또는 이들의 적합한 조합일 수 있다.

[0207] 통신 버스(18)는 프로세서(14), 컴퓨터 판독 가능 저장 매체(16)를 포함하여 컴퓨팅 장치(12)의 다른 다양한 컴포넌트들을 상호 연결한다.

[0208] 컴퓨팅 장치(12)는 또한 하나 이상의 입출력 장치(24)를 위한 인터페이스를 제공하는 하나 이상의 입출력 인터페이스(22) 및 하나 이상의 네트워크 통신 인터페이스(26)를 포함할 수 있다. 입출력 인터페이스(22) 및 네트워크 통신 인터페이스(26)는 통신 버스(18)에 연결된다. 입출력 장치(24)는 입출력 인터페이스(22)를 통해 컴퓨팅 장치(12)의 다른 컴포넌트들에 연결될 수 있다. 예시적인 입출력 장치(24)는 포인팅 장치(마우스 또는 트랙패드 등), 키보드, 터치 입력 장치(터치패드 또는 터치스크린 등), 음성 또는 소리 입력 장치, 다양한 종류의 센서 장치 및/또는 촬영 장치와 같은 입력 장치, 및/또는 디스플레이 장치, 프린터, 스피커 및/또는 네트워크 카드와 같은 출력 장치를 포함할 수 있다. 예시적인 입출력 장치(24)는 컴퓨팅 장치(12)를 구성하는 일 컴포넌트로서 컴퓨팅 장치(12)의 내부에 포함될 수도 있고, 컴퓨팅 장치(12)와는 구별되는 별개의 장치로 컴퓨팅 장치(12)와 연결될 수도 있다.

[0209] 지금까지 설명된 본 발명의 실시예에 따른 방법들은 컴퓨터가 읽을 수 있는 코드로 구현된 컴퓨터프로그램의 실행에 의하여 수행될 수 있다. 상기 컴퓨터프로그램은 인터넷 등의 네트워크를 통하여 제1 컴퓨팅 장치로부터 제2 컴퓨팅 장치에 전송되어 상기 제2 컴퓨팅 장치에 설치될 수 있고, 이로써 상기 제2 컴퓨팅 장치에서 사용될 수 있다. 상기 제1 컴퓨팅 장치 및 상기 제2 컴퓨팅 장치는, 서비스 서버 장치, 클라우드 서비스를 위한 서비스 서버 풀에 속한 물리 서비스 서버, 데스크탑 피씨와 같은 고정식 컴퓨팅 장치를 모두 포함한다.

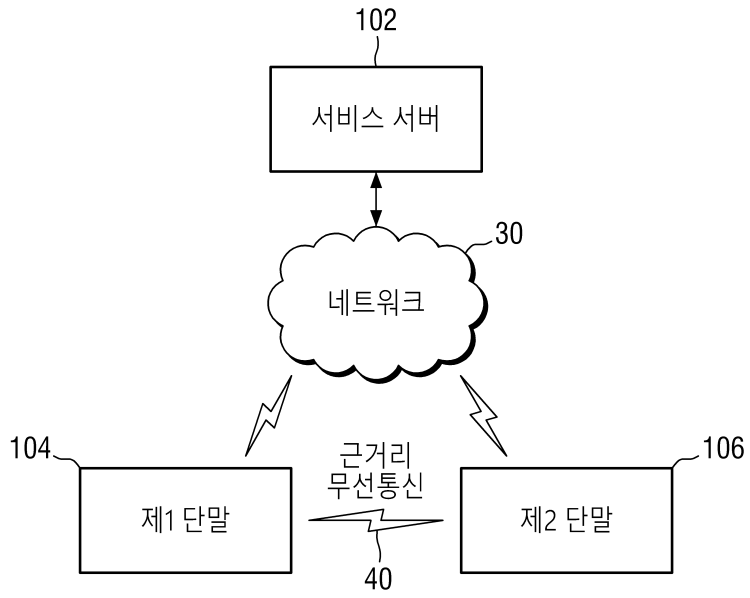
[0210] 상기 컴퓨터프로그램은 DVD-ROM, 플래시 메모리 장치 등의 기록매체에 저장된 것일 수도 있다.

[0211] 이상 첨부된 도면을 참조하여 본 발명의 실시예들을 설명하였지만, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정

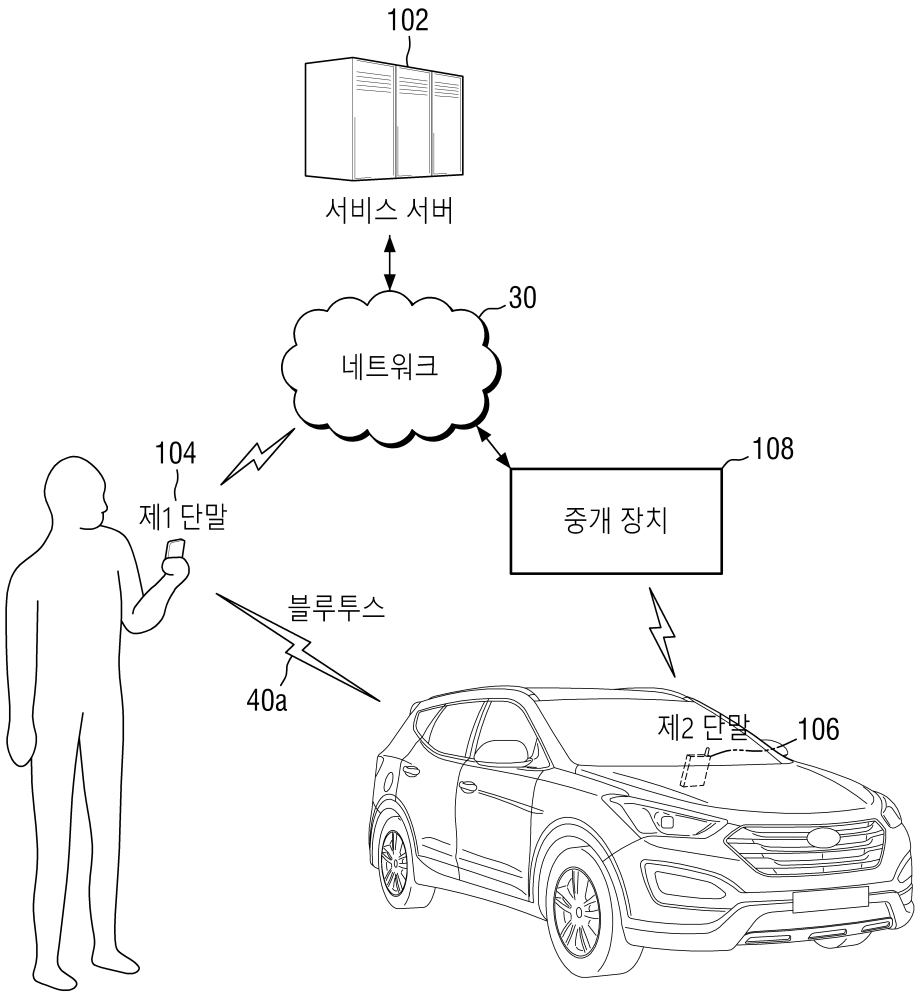
적인 것이 아닌 것으로 이해해야만 한다.

도면

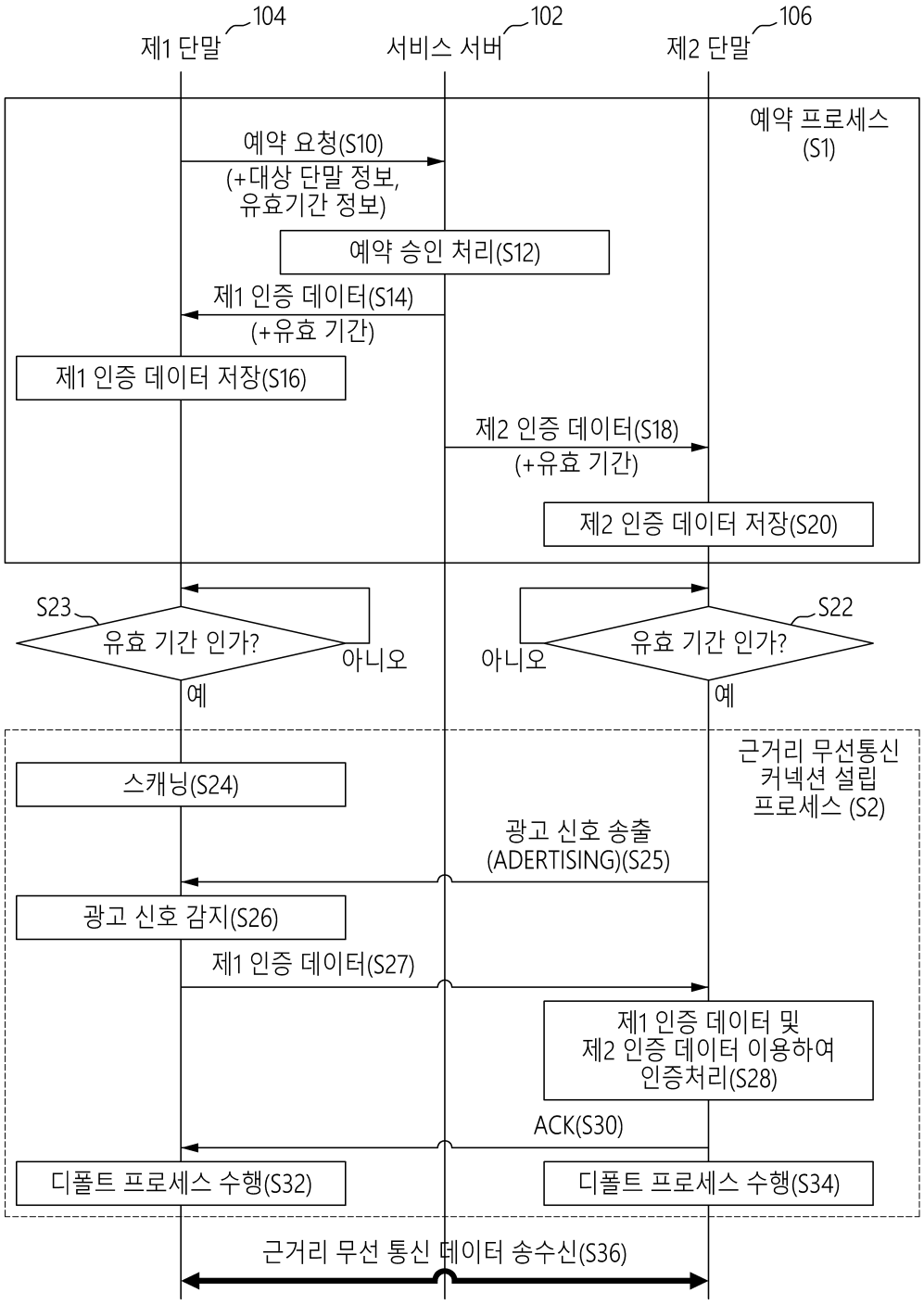
도면1



도면2



도면3


104
제1 단말
102
서비스 서버
106
제2 단말
예약 프로세스
(S1)
예약 요청(S10)
(+대상 단말 정보,
유효기간 정보)
예약 승인 처리(S12)
제1 인증 데이터(S14)
(+유효 기간)
제1 인증 데이터 저장(S16)
제2 인증 데이터(S18)
(+유효 기간)
제2 인증 데이터 저장(S20)
S23
유효 기간 인가?
아니오
예
S22
유효 기간 인가?
아니오
예
근거리 무선통신
커넥션 설립
프로세스 (S2)
스캐닝(S24)
광고 신호 송출
(ADERTISING)(S25)
광고 신호 감지(S26)
제1 인증 데이터(S27)
제1 인증 데이터 및
제2 인증 데이터 이용하여
인증처리(S28)
ACK(S30)
디폴트 프로세스 수행(S32)
디폴트 프로세스 수행(S34)
근거리 무선 통신 데이터 송수신(S36)

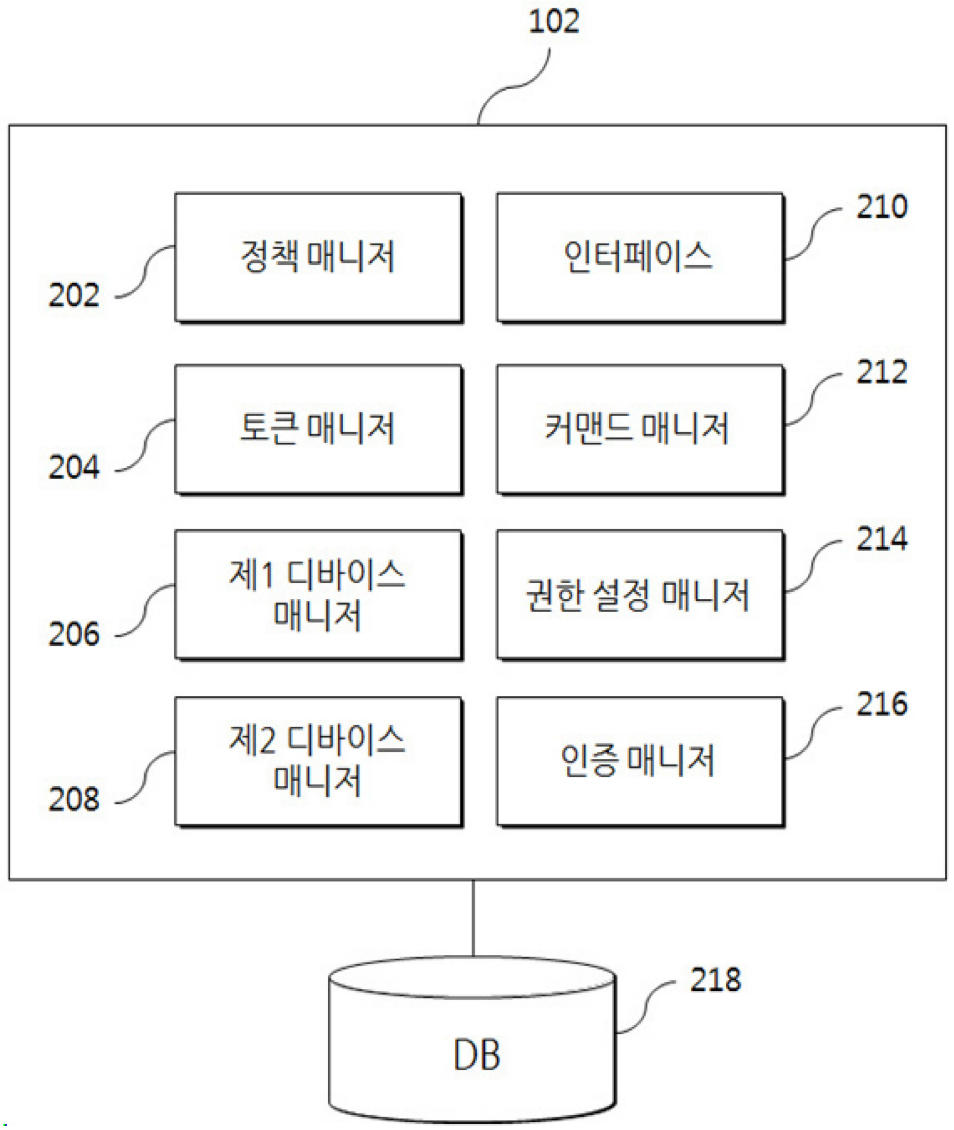
도면4

51 52 53 54 50

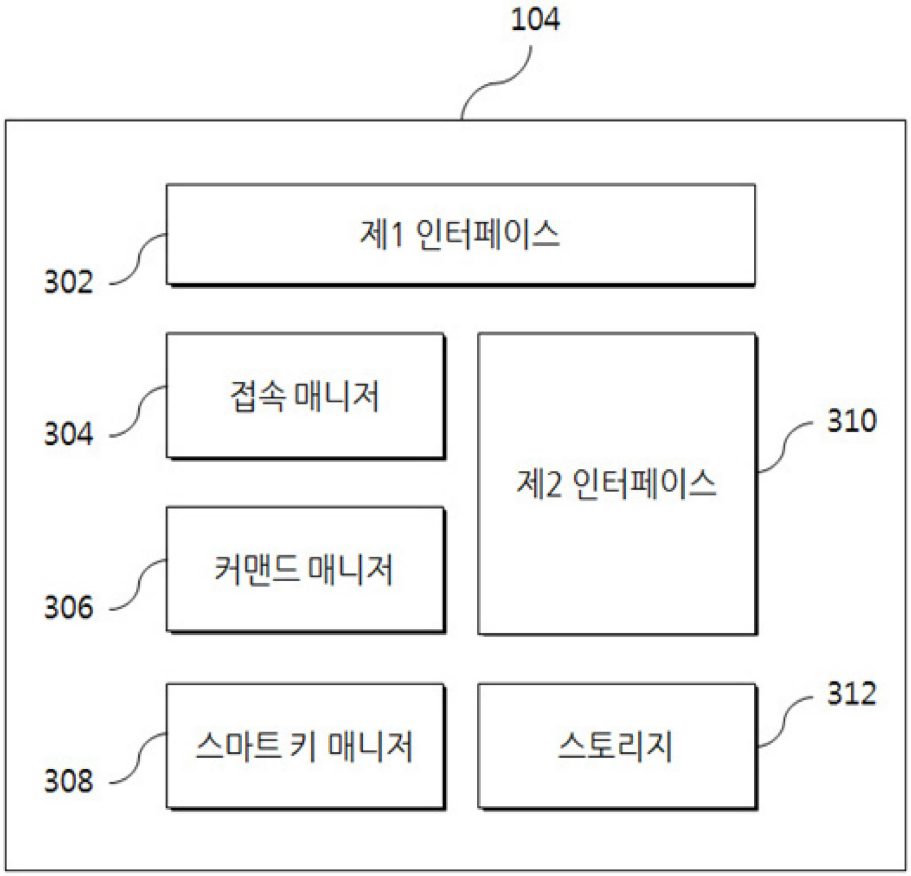
단말 ID	단말 속성	MAC 주소	서비스 가능 시간
550e8400-e29b-41d4-a716-446655440000	서울시 제1 차고지	4F-A8-F0-4B-21-3A	09:00 ~ 19:00
...	...	...	...

도면5

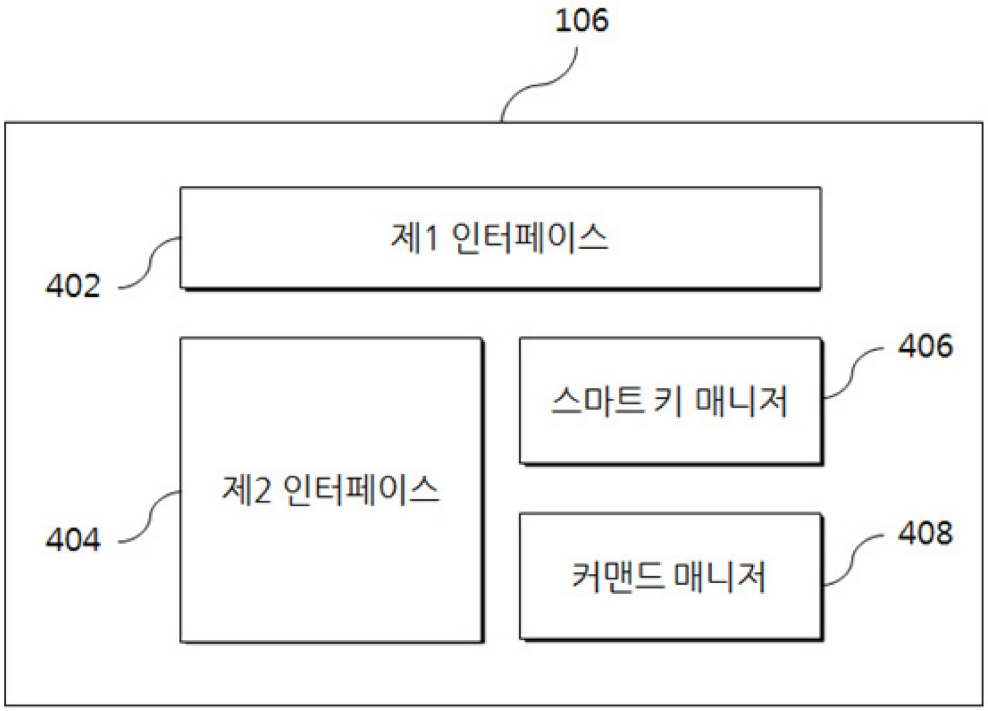
도면6


102
202
정책 매니저
210
인터페이스
204
토큰 매니저
212
커맨드 매니저
206
제1 디바이스 매니저
214
권한 설정 매니저
208
제2 디바이스 매니저
216
인증 매니저
218
DB

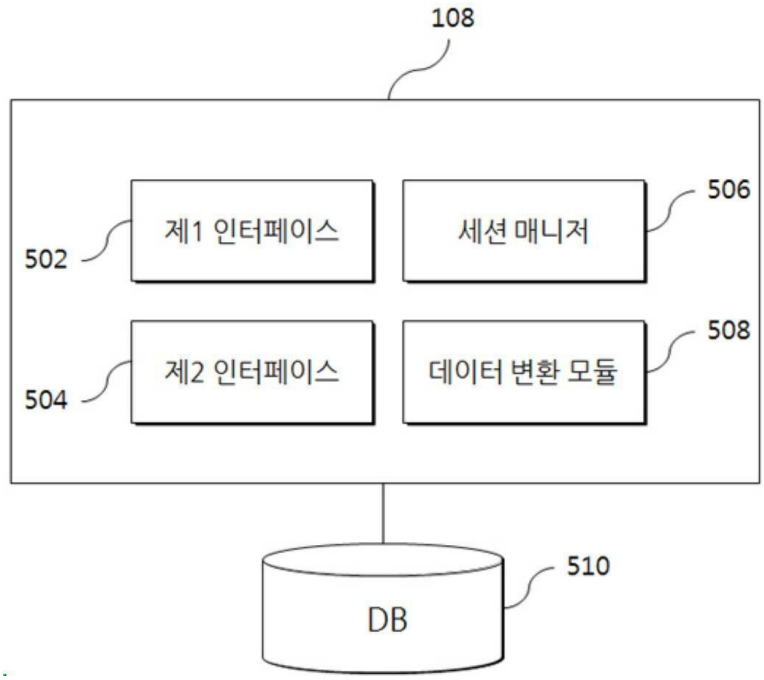
도면7


104
제1 인터페이스
302
접속 매니저
304
제2 인터페이스
310
커맨드 매니저
306
스마트 키 매니저
308
스토리지
312

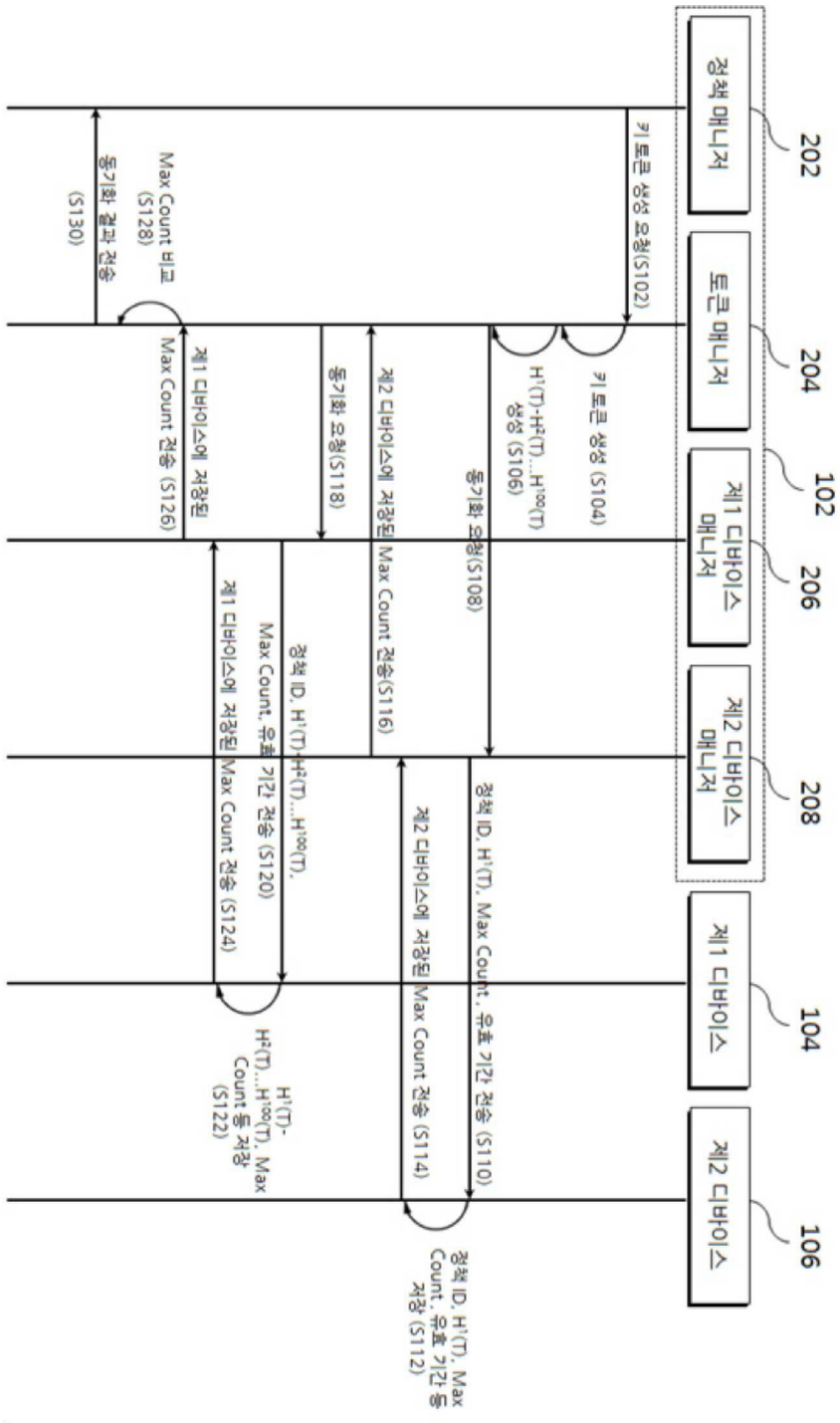
도면8


106
제1 인터페이스
402
제2 인터페이스
404
스마트 키 매니저
406
커맨드 매니저
408

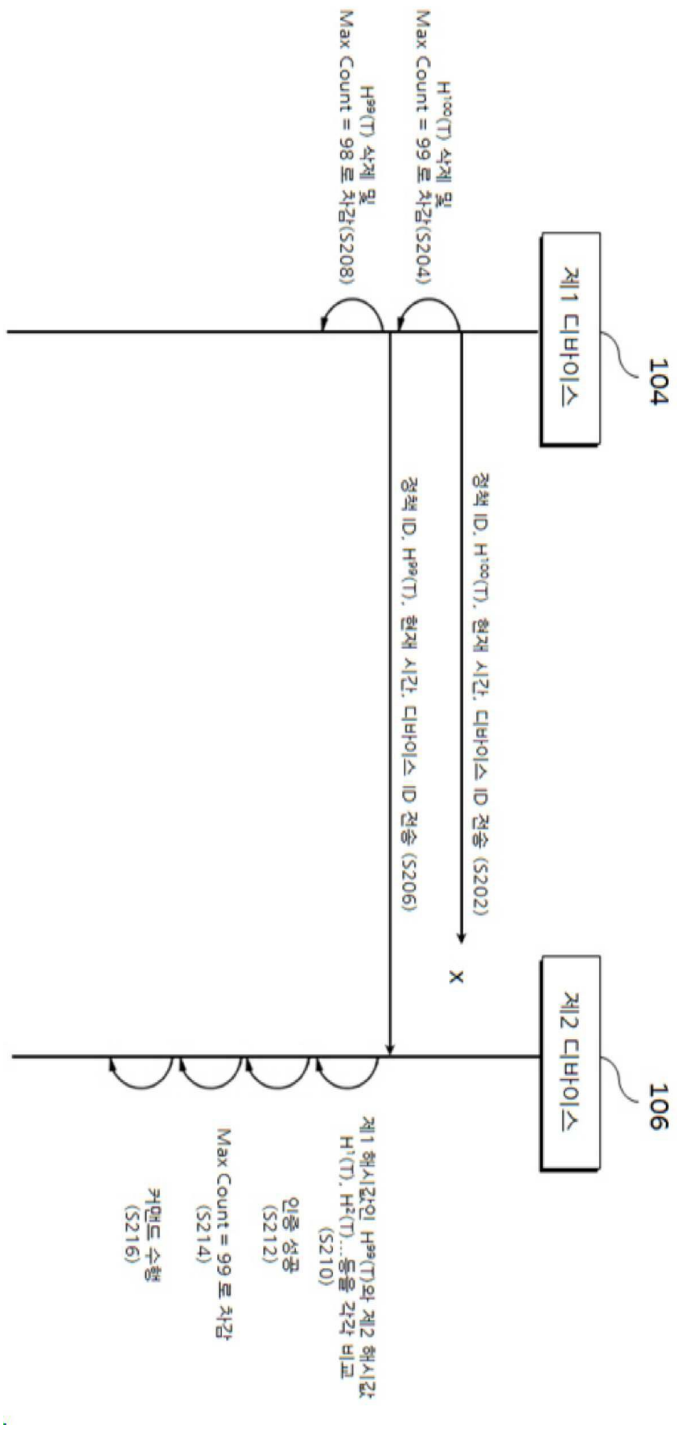
도면9



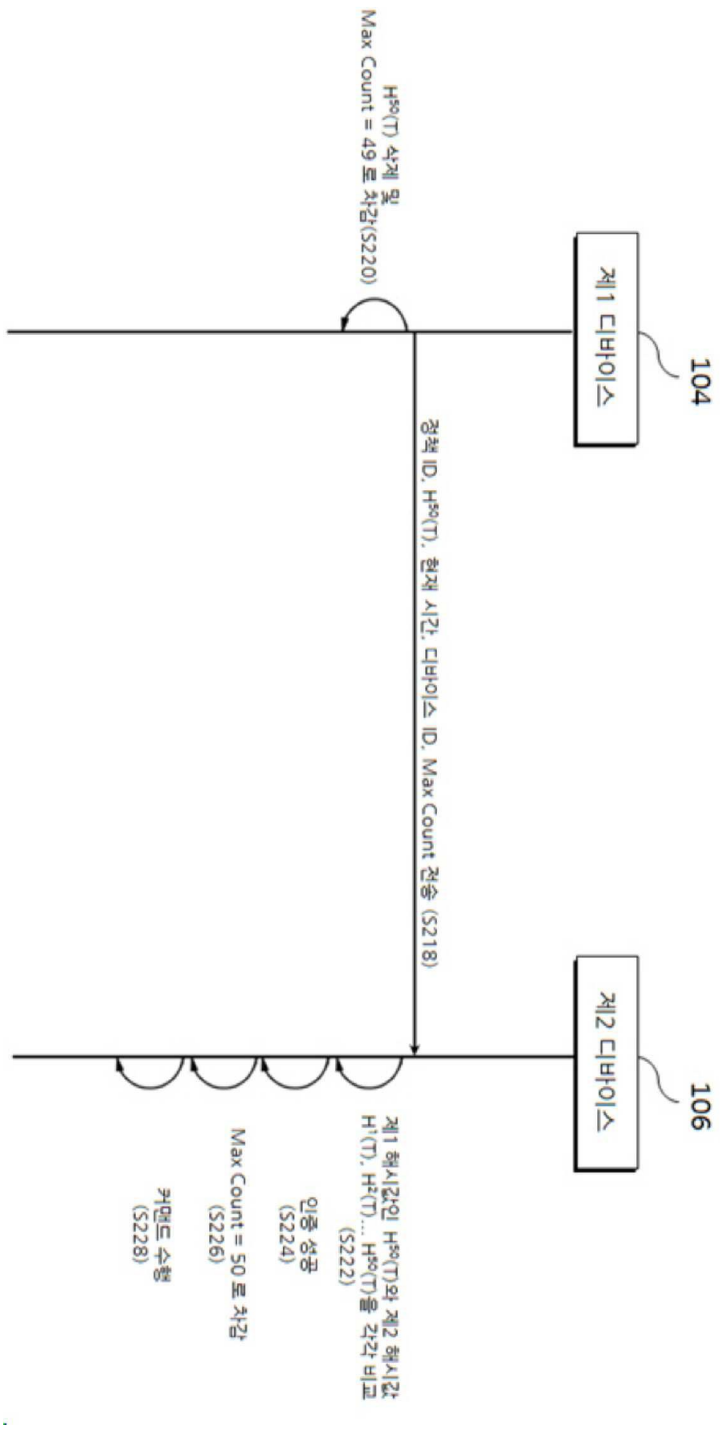
도면10


정책 매니저
202
토큰 매니저
204
제1 디바이스 매니저
102
206
제2 디바이스 매니저
208
제1 디바이스
104
제2 디바이스
106
키 토큰 생성 요청(S102)
키 토큰 생성 (S104)
H1(T)-H2(T)...H100(T) 생성 (S106)
동기화 요청(S108)
정책 ID, H1(T), Max Count, 유효 기간 전송 (S110)
제2 디바이스에 저장된 Max Count 전송 (S114)
정책 ID, H1(T), Max Count, 유효 기간 등 저장 (S112)
제2 디바이스에 저장된 Max Count 전송(S116)
동기화 요청(S118)
정책 ID, H1(T)-H2(T)...H100(T), Max Count, 유효 기간 전송 (S120)
H1(T)-H2(T)...H100(T), Max Count 등 저장 (S122)
제1 디바이스에 저장된 Max Count 전송 (S124)
제1 디바이스에 저장된 Max Count 전송 (S126)
Max Count 비교 (S128)
동기화 결과 전송 (S130)

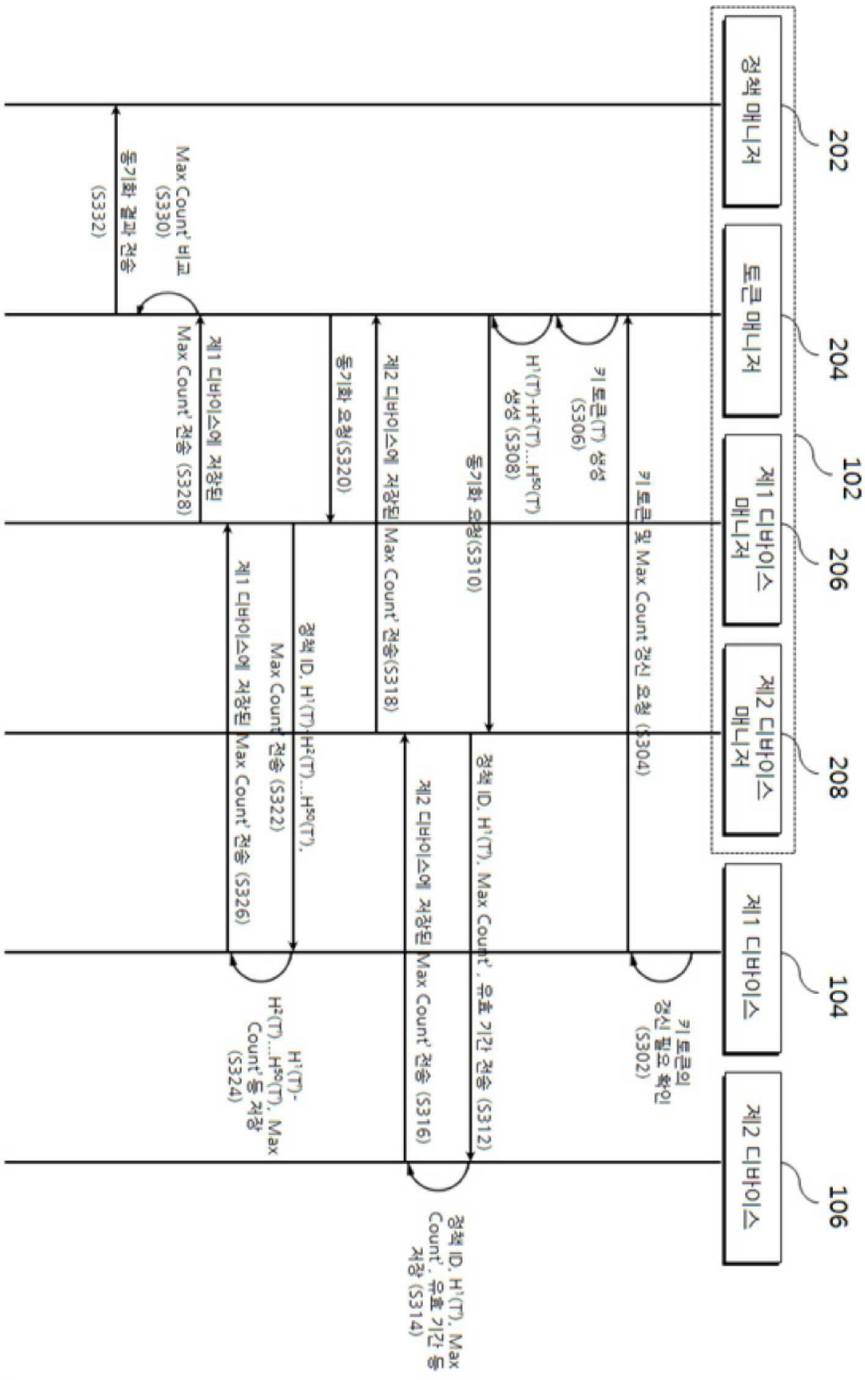
도면11


제1 디바이스
104
제2 디바이스
106
정책 ID, H'100(T), 현재 시간, 디바이스 ID 전송 (S202)
정책 ID, H99(T), 현재 시간, 디바이스 ID 전송 (S206)
H'100(T) 삭제 및
Max Count = 99 로 차감(S204)
H99(T) 삭제 및
Max Count = 98 로 차감(S208)
제1 해시값인 H99(T)와 제2 해시값
H'(T), H2(T)...등을 각각 비교
(S210)
인증 성공
(S212)
Max Count = 99 로 차감
(S214)
커맨드 수행
(S216)

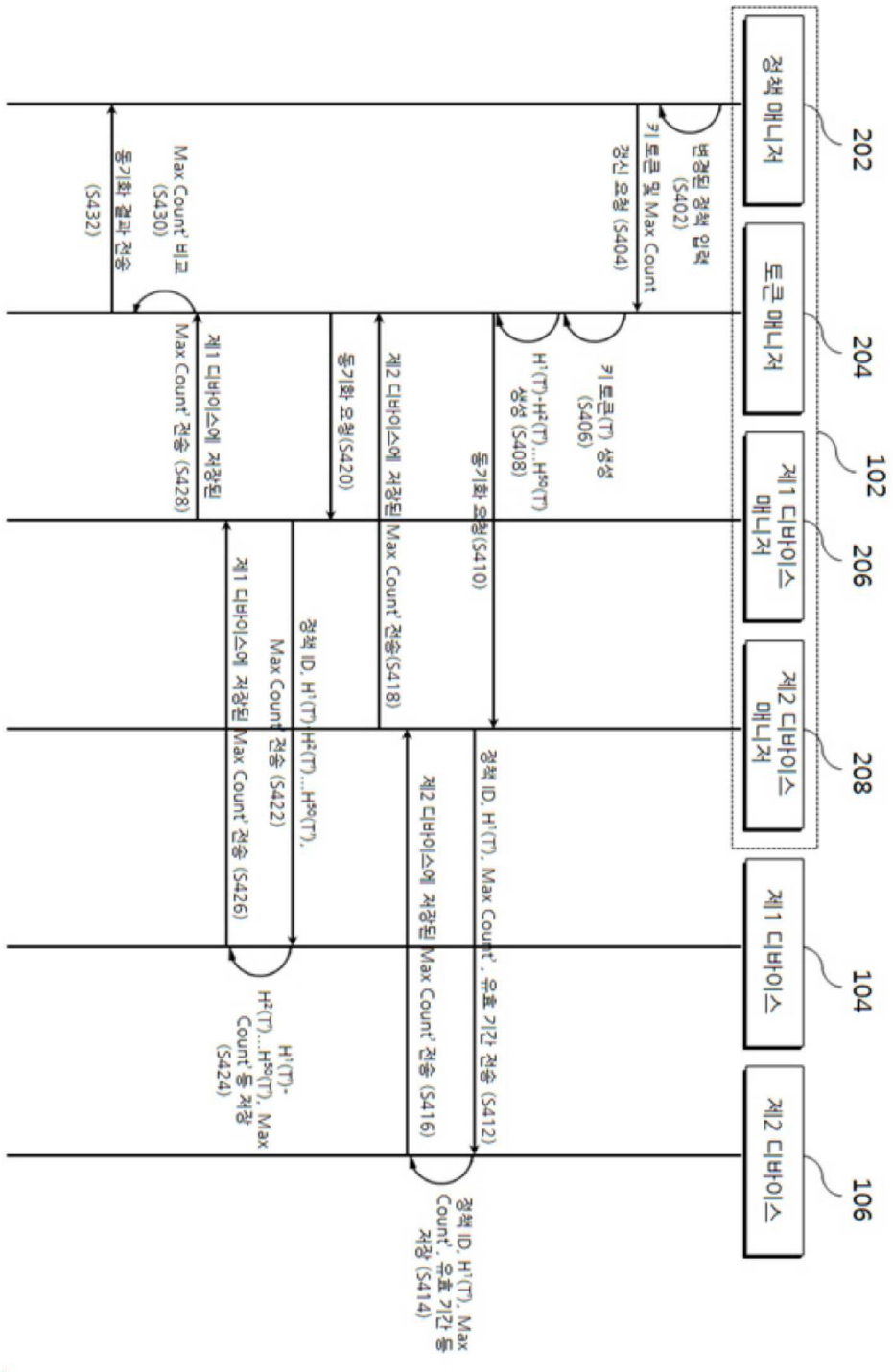
도면12


제1 디바이스
104
H^50(T) 삭제 및
Max Count = 49 로 차감(S220)
정책 ID, H^50(T), 현재 시간, 디바이스 ID, Max Count 전송 (S218)
제2 디바이스
106
제1 해시값인 H^50(T)와 제2 해시값
H^1(T), H^2(T)... H^50(T)를 각각 비교
(S222)
인증 성공
(S224)
Max Count = 50 로 차감
(S226)
커맨드 수행
(S228)

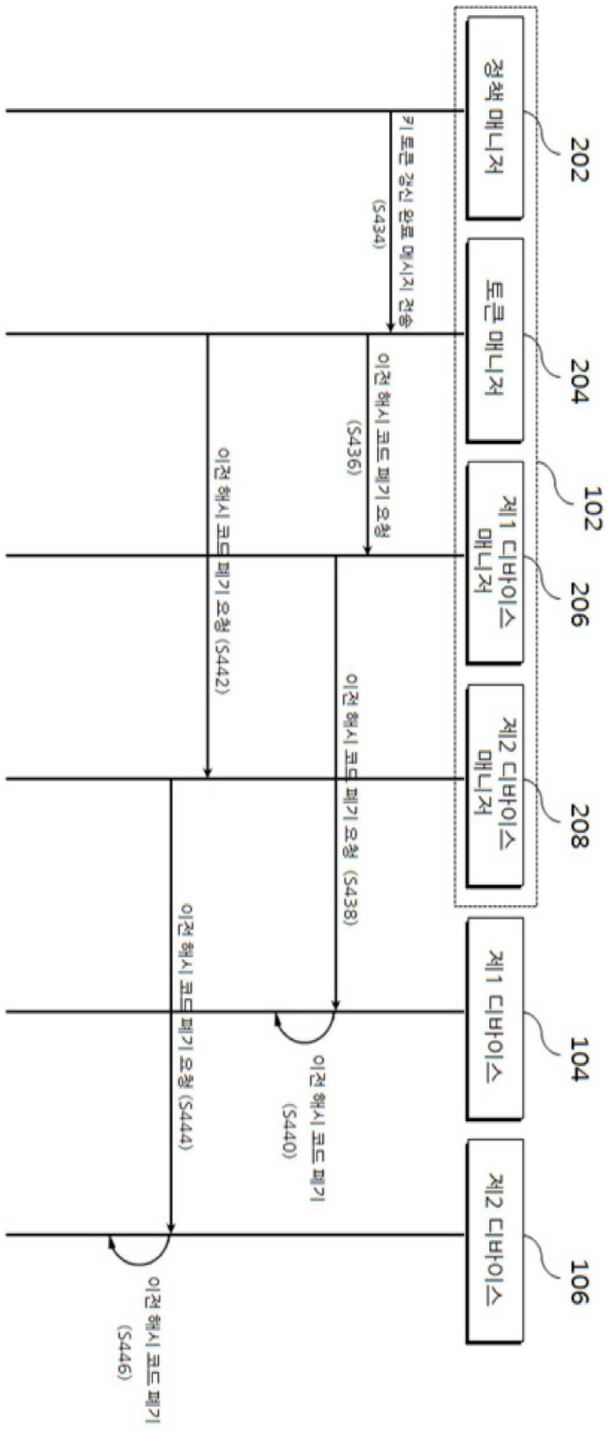
도면13


정책 매니저
202
토큰 매니저
204
제1 디바이스 매니저
102
206
제2 디바이스 매니저
208
제1 디바이스
104
제2 디바이스
106
키 토큰의 갱신 필요 확인 (S302)
키 토큰 및 Max Count 갱신 요청 (S304)
키 토큰(T) 생성 (S306)
H¹(T)-H²(T)...H⁵⁰(T) 생성 (S308)
동기화 요청(S310)
정책 ID, H¹(T), Max Count', 유효 기간 전송 (S312)
정책 ID, H¹(T), Max Count', 유효 기간 등 저장 (S314)
제2 디바이스에 저장된 Max Count' 전송 (S316)
제2 디바이스에 저장된 Max Count' 전송(S318)
동기화 요청(S320)
정책 ID, H¹(T), H²(T)...H⁵⁰(T), 제1 디바이스에 저장된 Max Count' 전송 (S322)
H¹(T)-H²(T)...H⁵⁰(T), Max Count' 등 저장 (S324)
제1 디바이스에 저장된 Max Count' 전송 (S326)
Max Count' 비교 (S330)
동기화 결과 전송 (S332)

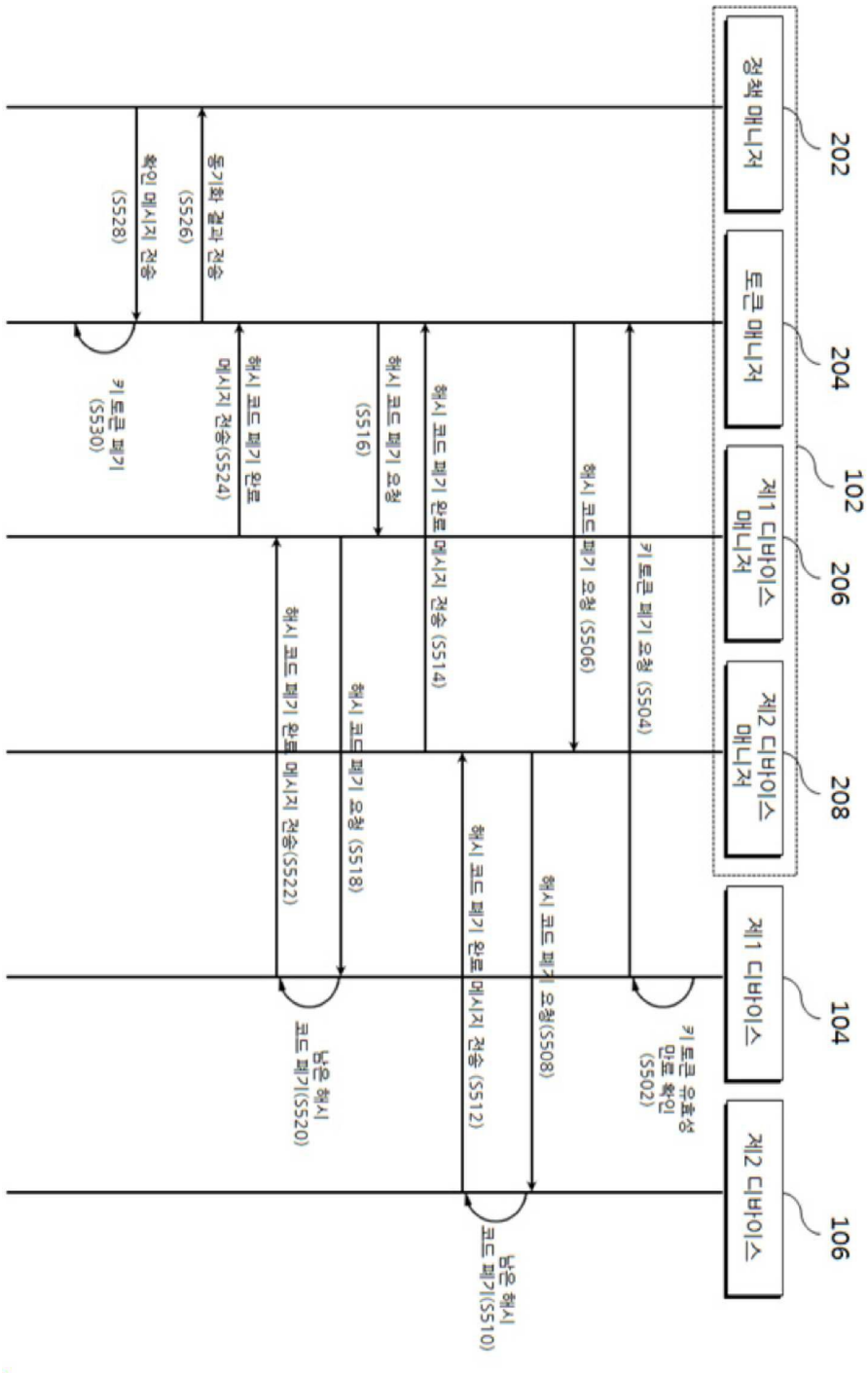
도면14


정책 매니저
202
토큰 매니저
204
제1 디바이스 매니저
102
206
제2 디바이스 매니저
208
제1 디바이스
104
제2 디바이스
106
변경된 정책 입력 (S402)
키 토큰 및 Max Count 갱신 요청 (S404)
키 토큰(T) 생성 (S406)
H¹(T)-H²(T)...H⁵⁰(T) 생성 (S408)
동기화 요청(S410)
정책 ID, H¹(T), Max Count', 유효 기간 전송 (S412)
제2 디바이스에 저장된 Max Count' 전송 (S416)
정책 ID, H¹(T), Max Count', 유효 기간 등 저장 (S414)
동기화 요청(S420)
제2 디바이스에 저장된 Max Count' 전송(S418)
정책 ID, H¹(T) H²(T)...H⁵⁰(T), Max Count' 전송 (S422)
제1 디바이스에 저장된 Max Count' 전송 (S426)
H¹(T)-H²(T)...H⁵⁰(T), Max Count' 등 저장 (S424)
제1 디바이스에 저장된 Max Count' 전송 (S428)
Max Count' 비교 (S430)
동기화 결과 전송 (S432)

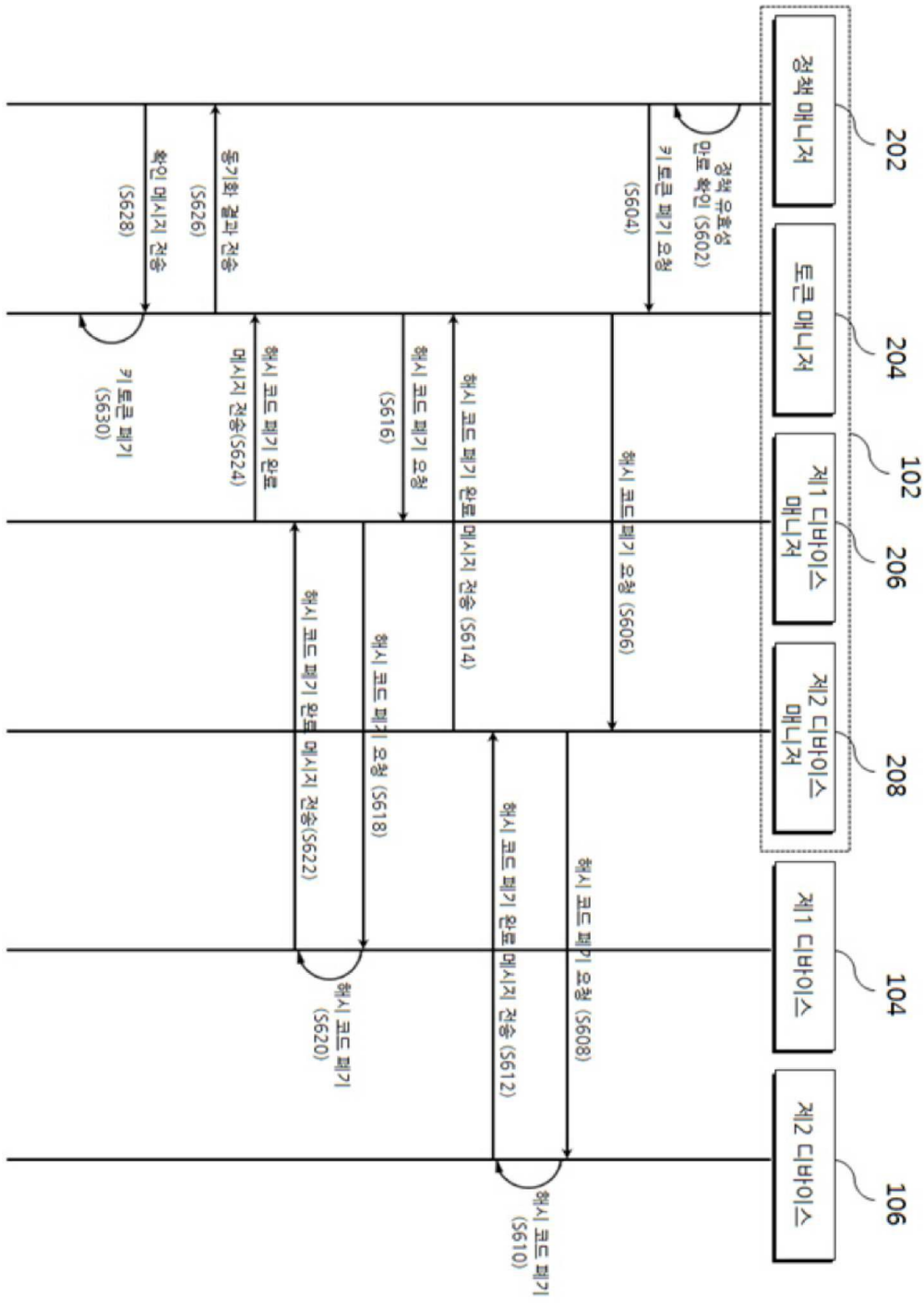
도면15


정책 매니저
202
토큰 매니저
204
제1 디바이스 매니저
102
206
제2 디바이스 매니저
208
제1 디바이스
104
제2 디바이스
106
키 토큰 갱신 완료 메시지 전송 (S434)
이전 해시 코드 폐기 요청 (S436)
이전 해시 코드 폐기 요청 (S442)
이전 해시 코드 폐기 요청 (S438)
이전 해시 코드 폐기 (S440)
이전 해시 코드 폐기 요청 (S444)
이전 해시 코드 폐기 (S446)

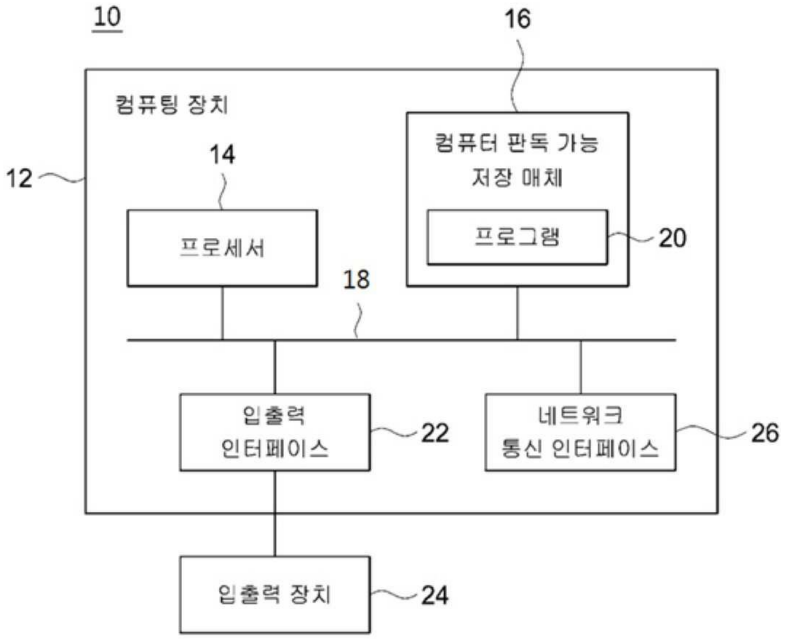
도면16


정책 매니저
202
토큰 매니저
204
제1 디바이스 매니저
102
206
제2 디바이스 매니저
208
제1 디바이스
104
제2 디바이스
106
키 토큰 유효성 만료 확인 (S502)
키 토큰 폐기 요청 (S504)
해시 코드 폐기 요청 (S506)
해시 코드 폐기 요청(S508)
남은 해시 코드 폐기(S510)
해시 코드 폐기 완료 메시지 전송 (S512)
해시 코드 폐기 요청 (S514)
해시 코드 폐기 완료 메시지 전송(S516)
해시 코드 폐기 요청 (S518)
남은 해시 코드 폐기(S520)
해시 코드 폐기 완료 메시지 전송(S522)
해시 코드 폐기 완료 메시지 전송(S524)
동기화 결과 전송 (S526)
확인 메시지 전송 (S528)
키 토큰 폐기 (S530)

도면17


정책 매니저
202
토큰 매니저
204
제1 디바이스 매니저
102
206
제2 디바이스 매니저
208
제1 디바이스
104
제2 디바이스
106
정책 유효성 만료 확인 (S602)
키 토큰 폐기 요청 (S604)
해시 코드 폐기 요청 (S606)
해시 코드 폐기 요청 (S608)
해시 코드 폐기 (S610)
해시 코드 폐기 완료 메시지 전송 (S612)
해시 코드 폐기 완료 메시지 전송 (S614)
해시 코드 폐기 요청 (S616)
해시 코드 폐기 요청 (S618)
해시 코드 폐기 (S620)
해시 코드 폐기 완료 메시지 전송(S622)
해시 코드 폐기 완료 메시지 전송(S624)
동기화 결과 전송 (S626)
확인 메시지 전송 (S628)
키 토큰 폐기 (S630)

도면18


10
16
컴퓨팅 장치
14
12
컴퓨터 판독 가능
저장 매체
프로세서
프로그램
20
18
입출력
인터페이스
22
네트워크
통신 인터페이스
26
입출력 장치
24