(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0017455
(43) 공개일자 2017년02월15일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
H04L 9/3213 (2013.01)
H04L 9/0819 (2013.01)
(21) 출원번호 10-2015-0111389
(22) 출원일자 2015년08월07일
심사청구일자 2015년08월07일

(71) 출원인
주식회사 엘지씨엔에스
서울특별시 영등포구 여의대로 24 (여의도동)
(72) 발명자
엄정용
서울특별시 영등포구 여의대로 24 (여의도동)
공동현
서울특별시 영등포구 여의대로 24 (여의도동)
박진기
서울특별시 영등포구 여의대로 24 (여의도동)
(74) 대리인
특허법인 무한

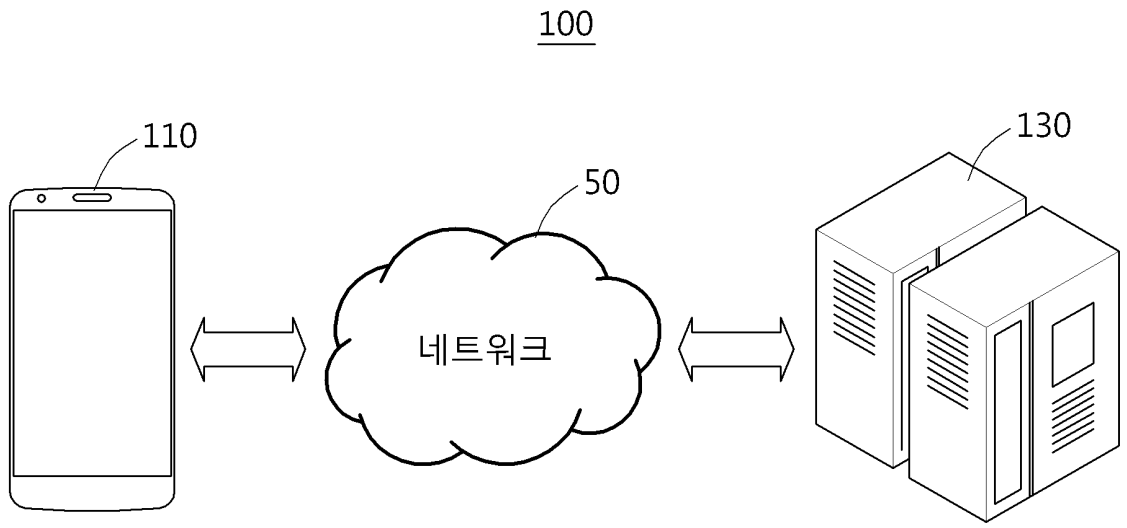
전체 청구항 수 : 총 23 항

(54) 발명의 명칭 **세션 키 및 인증 토큰에 기반한 상호 인증 장치들 간의 상호 인증 방법 및 상호 인증 장치들**

(57) 요 약

미리 공유된 마스터 키에 기초한 제1 세션 키를 이용하여 미리 공유된 인증 토큰을 제1 암호화하여 제1 장치에게 전송하고, 제1 암호화된 인증 토큰에 대한 제1 장치의 검증 결과에 따라 전송된, 제2 암호화된 인증 토큰을 제1 세션 키를 이용하여 복호화하여 검증하는, 상호 인증 방법을 제공할 수 있다.

대 표 도 - 도1



명 세 서

청구범위

청구항 1

제1 장치와 상호 인증하는 제2 장치를 위한 상호 인증 방법에 있어서,

미리 공유된 마스터 키에 기초한 제1 세션 키를 이용하여 미리 공유된 인증 토큰을 제1 암호화하는 단계;

상기 제1 암호화된 인증 토큰을 상기 제1 장치에게 전송하는 단계;

상기 제1 암호화된 인증 토큰에 대한 상기 제1 장치의 검증 결과에 따라 전송된, 제2 암호화된 인증 토큰을 수신하는 단계;

상기 제1 세션 키를 이용하여 상기 제2 암호화된 인증 토큰을 복호화하는 단계; 및

상기 복호화된 인증 토큰을 검증하는 단계

를 포함하는, 상호 인증 방법.

청구항 2

제1항에 있어서,

상기 제1 암호화하는 단계는

상기 제2 장치를 위한 제1 변조 알고리즘에 기초하여 상기 미리 공유된 인증 토큰을 제1 변조하는 단계; 및

상기 제1 변조된 인증 토큰을 상기 제1 세션 키를 이용하여 상기 제1 암호화하는 단계

를 포함하는, 상호 인증 방법.

청구항 3

제2항에 있어서,

상기 제1 변조하는 단계는

상기 제1 변조 알고리즘에 기초하여 상기 미리 공유된 인증 토큰의 일부를 상기 제1 변조하는 단계

를 포함하는, 상호 인증 방법.

청구항 4

제1항에 있어서,

상기 복호화된 인증 토큰을 검증하는 단계는

상기 제1 장치를 위한 제2 변조 알고리즘에 기초하여 상기 복호화된 인증 토큰을 검증하는 단계

를 포함하는, 상호 인증 방법.

청구항 5

제4항에 있어서,

상기 복호화된 인증 토큰을 검증하는 단계는

상기 제2 변조 알고리즘에 기초하여 상기 미리 공유된 인증 토큰을 제2 변조하는 단계; 및

상기 제2 변조된 인증 토큰을 이용하여 상기 복호화된 인증 토큰을 검증하는 단계

를 포함하는, 상호 인증 방법.

청구항 6

제1항에 있어서,

세션 키 생성을 위한 랜덤 정보를 생성하는 단계; 및

상기 미리 공유된 마스터 키 및 상기 랜덤 정보를 이용하여 제1 세션 키를 생성하는 단계

를 더 포함하는, 상호 인증 방법.

청구항 7

제1항에 있어서,

상기 제1 장치의 인증 요청을 수신하는 단계; 및

상기 인증 요청에 응답하여, 상기 제1 장치를 검증하는 단계

를 더 포함하는, 상호 인증 방법.

청구항 8

제5항에 있어서,

상기 인증 요청은

상기 제1 장치의 MAC 정보 및 상기 제1 장치의 칩 정보를 포함하는 식별 정보를 포함하고,

상기 제1 장치를 검증하는 단계는

상기 식별 정보를 이용하여 상기 제1 장치를 검증하는 단계

를 포함하는, 상호 인증 방법.

청구항 9

제7항에 있어서,

상기 인증 요청에 앞서, 상기 제2 장치 및 상기 제1 장치 간에 상기 마스터 키 및 상기 인증 토큰을 공유하는 단계

를 더 포함하는, 상호 인증 방법.

청구항 10

제9항에 있어서,

상기 공유하는 단계는

상기 제1 장치의 등록 요청에 응답하여, 상기 제1 장치를 위한 인증 토큰(Token)을 생성하는 단계;

랜덤 정보 및 이니셜 키(initial key)를 이용하여 임시 키를 생성하는 단계; 및

상기 임시 키를 이용하여 암호화한 암호학적 정보(credential)- 상기 암호학적 정보는 상기 마스터 키, 및 상기 인증 토큰을 포함함-를 상기 랜덤 정보와 함께 상기 제1 장치에게 전송하는 단계

를 포함하는, 상호 인증 방법.

청구항 11

제10항에 있어서,

상기 인증 토큰은

상기 제1 장치의 권한 정보, 상기 랜덤 정보, 상기 제2 장치의 식별 정보 및 상기 제1 장치의 식별 정보 중 적어도 하나를 포함하는, 상호 인증 방법.

청구항 12

제11항에 있어서,

상기 제1 장치의 권한 정보가 변경된 경우, 상기 인증 토큰을 갱신하는 단계

를 더 포함하는, 상호 인증 방법.

청구항 13

제10항에 있어서,

상기 제1 장치로부터 상기 암호학적 정보의 공유가 완료되었음을 나타내는 신호를 수신함에 따라 상기 제1 장치를 등록하는 단계

를 더 포함하는, 상호 인증 방법.

청구항 14

제2 장치와 상호 인증하는 제1 장치를 위한 상호 인증 방법에 있어서,

인증 요청에 응답하여 상기 제2 장치로부터 전송된, 제1 암호화된 인증 토큰을 수신하는 단계;

미리 공유된 마스터 키에 기초한 제2 세션 키를 이용하여 상기 제1 암호화된 인증 토큰을 복호화하는 단계;

상기 복호화된 인증 토큰을 검증하는 단계;

상기 검증 결과에 따라, 미리 공유된 인증 토큰을 제2 암호화하는 단계; 및

상기 제2 암호화된 인증 토큰을 상기 제2 장치에게 전송하는 단계

를 포함하는, 상호 인증 방법.

청구항 15

제14항에 있어서,

상기 복호화된 인증 토큰을 검증하는 단계는

상기 제2 장치를 위한 제1 변조 알고리즘에 기초하여 상기 복호화된 인증 토큰을 검증하는 단계

를 포함하는, 상호 인증 방법.

청구항 16

제15항에 있어서,

상기 복호화된 인증 토큰을 검증하는 단계는

상기 미리 공유된 인증 토큰을 상기 제1 변조 알고리즘을 이용하여 제1 변조하는 단계; 및

상기 제1 변조된 인증 토큰을 이용하여 상기 복호화한 인증 토큰을 검증하는 단계

를 포함하는, 상호 인증 방법.

청구항 17

제14항에 있어서,

상기 제2 암호화하는 단계는

상기 제1 장치를 위한 제2 변조 알고리즘에 기초하여 상기 미리 공유된 인증 토큰을 제2 변조하는 단계; 및

상기 제2 변조된 인증 토큰을 상기 제2 세션 키를 이용하여 상기 제2 암호화하는 단계

를 포함하는, 상호 인증 방법.

청구항 18

제17항에 있어서,

상기 제2 변조하는 단계는

상기 제2 변조 알고리즘에 기초하여 상기 미리 공유된 인증 토큰의 일부를 제2 변조하는 단계

를 포함하는, 상호 인증 방법.

청구항 19

제14항에 있어서,

상기 인증 요청에 앞서, 상기 제2 장치 및 상기 제1 장치 간에 상기 마스터 키 및 상기 인증 토큰을 공유하는 단계

를 더 포함하는, 상호 인증 방법.

청구항 20

제19항에 있어서,

상기 공유하는 단계는

상기 제2 장치에게 등록을 요청하는 단계;

상기 등록 요청에 응답하여, 상기 제2 장치에서 암호화된 암호학적 정보- 상기 암호학적 정보는 상기 제2 장치가 생성한 마스터 키, 및 인증 토큰을 포함함-를 수신하는 단계;

상기 암호학적 정보를 복호화하여 상기 마스터 키 및 상기 인증 토큰을 추출하는 단계;

상기 마스터 키 및 상기 인증 토큰을 저장하는 단계; 및

상기 제2 장치에게, 상기 암호학적 정보의 공유가 완료되었음을 알리는 신호를 전송하는 단계

를 포함하는, 상호 인증 방법.

청구항 21

하드웨어와 결합되어 제1항 내지 제20항 중 어느 하나의 항의 방법을 실행시키기 위하여 매체에 저장된 컴퓨터 프로그램.

청구항 22

미리 공유된 마스터 키에 기초한 제1 세션 키를 이용하여 미리 공유된 인증 토큰을 제1 암호화하고, 제1 장치가 전송한 제2 암호화된 인증 토큰을 상기 제1 세션 키에 의해 복호화하여 검증하는 프로세서;

상기 제1 암호화된 인증 토큰을 상기 제1 장치에게 전송하고, 상기 제1 암호화된 인증 토큰에 대한 제1 장치의 검증 결과에 따라 전송된 제2 암호화된 인증 토큰을 수신하는 송수신부; 및

상기 미리 공유된 마스터 키 및 상기 미리 공유된 인증 토큰을 저장하는 메모리

를 포함하는, 제1 장치와 상호 인증하는 제2 장치.

청구항 23

인증 요청에 응답하여 제2 장치로부터 전송된 제1 암호화된 인증 토큰을 수신하고, 제2 암호화된 인증 토큰을 상기 제2 장치에게 전송하는 송수신부;

미리 공유된 마스터 키에 기초한 제2 세션 키를 이용하여 상기 제1 암호화된 인증 토큰을 복호화하여 검증하고, 상기 검증 결과에 따라, 미리 공유된 인증 토큰을 제2 암호화하는 프로세서; 및

상기 미리 공유된 마스터 키 및 상기 미리 공유된 인증 토큰을 저장하는 메모리

를 포함하는, 제2 장치와 상호 인증하는 제1 장치.

발명의 설명

기 술 분 야

[0001] 아래의 실시예들은 세션 키 및 인증 토큰에 기반한 상호 인증 장치들 간의 상호 인증 방법 및 상호 인증 장치들에 관한 것이다.

배 경 기 술

[0002] 마스터 키를 이용한 인증 방식은 상호 인증하고자 하는 객체들이 동일한 마스터 키를 공유하고 있어야 상호 인증을 수행할 수 있으므로 마스터 키에 대한 의존도가 매우 높다. 때문에 마스터 키를 소프트웨어 방식으로 보관해야 하는 다양한 IoT(Internet of Thing) 기기들에서 마스터 키만을 이용한 인증은 보안이 취약하다는 위험이 있다. 뿐만 아니라, 다양한 서비스를 제공하는 IoT 기기는 각각의 객체에 대한 서로 다른 서비스를 위한 권한 관리를 필요로 하므로 권한 관리를 위한 방안 또한 요구된다.

발명의 내용

해결하려는 과제

[0003] 일 실시예에 따르면, 상호 인증 장치들 간의 상호 인증을 통해 보안 수준을 높일 수 있다.

[0004] 일 실시예에 따르면, 권한 확인(authorization check) 및 상호 인증(mutual authentication)을 한 번에 수행함으로써 권한 확인 절차를 간소화하는 한편, IoT 자원을 효율적으로 이용할 수 있다.

과제의 해결 수단

[0005] 일 측에 따른 제1 장치와 상호 인증하는 제2 장치를 위한 상호 인증 방법은 미리 공유된 마스터 키에 기초한 제1 세션 키를 이용하여 미리 공유된 인증 토큰을 제1 암호화하는 단계; 상기 제1 암호화된 인증 토큰을 상기 제1 장치에게 전송하는 단계; 상기 제1 암호화된 인증 토큰에 대한 상기 제1 장치의 검증 결과에 따라 전송된, 제2 암호화된 인증 토큰을 수신하는 단계; 상기 제1 세션 키를 이용하여 상기 제2 암호화된 인증 토큰을 복호화하는 단계; 및 상기 복호화된 인증 토큰을 검증하는 단계를 포함한다.

[0006] 상기 제1 암호화하는 단계는 상기 제2 장치를 위한 제1 변조 알고리즘에 기초하여 상기 미리 공유된 인증 토큰을 제1 변조하는 단계; 및 상기 제1 변조된 인증 토큰을 상기 제1 세션 키를 이용하여 상기 제1 암호화하는 단계를 포함할 수 있다.

[0007] 상기 제1 변조하는 단계는 상기 제1 변조 알고리즘에 기초하여 상기 미리 공유된 인증 토큰의 일부를 상기 제1 변조하는 단계를 포함할 수 있다.

[0008] 상기 복호화된 인증 토큰을 검증하는 단계는 상기 제1 장치를 위한 제2 변조 알고리즘에 기초하여 상기 복호화된 인증 토큰을 검증하는 단계를 포함할 수 있다.

[0009] 상기 복호화된 인증 토큰을 검증하는 단계는 상기 제2 변조 알고리즘에 기초하여 상기 미리 공유된 인증 토큰을 제2 변조하는 단계; 및 상기 제2 변조된 인증 토큰을 이용하여 상기 복호화된 인증 토큰을 검증하는 단계를 포함할 수 있다.

[0010] 상기 제2 장치를 위한 상호 인증 방법은 세션 키 생성을 위한 랜덤 정보를 생성하는 단계; 및 상기 미리 공유된 마스터 키 및 상기 랜덤 정보를 이용하여 제1 세션 키를 생성하는 단계를 더 포함할 수 있다.

[0011] 상기 제2 장치를 위한 상호 인증 방법은 상기 제1 장치의 인증 요청을 수신하는 단계; 및 상기 인증 요청에 응답하여, 상기 제1 장치를 검증하는 단계를 더 포함할 수 있다.

[0012] 상기 인증 요청은 상기 제1 장치의 MAC 정보 및 상기 제1 장치의 칩 정보를 포함하는 식별 정보를 포함하고, 상기 제1 장치를 검증하는 단계는 상기 식별 정보를 이용하여 상기 제1 장치를 검증하는 단계를 포함할 수 있다.

[0013] 상기 제2 장치를 위한 상호 인증 방법은 상기 인증 요청에 앞서, 상기 제2 장치 및 상기 제1 장치 간에 상기 마스터 키 및 상기 인증 토큰을 공유하는 단계를 더 포함할 수 있다.

[0014] 상기 공유하는 단계는 상기 제1 장치의 등록 요청에 응답하여, 상기 제1 장치를 위한 인증 토큰(Token)을 생성하는 단계; 랜덤 정보 및 이니셜 키(initial key)를 이용하여 임시 키를 생성하는 단계; 및 상기 임시 키를 이용하여 암호화한 암호학적 정보(credential)- 상기 암호학적 정보는 상기 마스터 키, 및 상기 인증 토큰을 포함함-를 상기 랜덤 정보와 함께 상기 제1 장치에게 전송하는 단계를 포함할 수 있다.

[0015] 상기 인증 토큰은 상기 제1 장치의 권한 정보, 상기 랜덤 정보, 상기 제2 장치의 식별 정보 및 상기 제1 장치의 식별 정보 중 적어도 하나를 포함할 수 있다.

[0016] 상기 제2 장치를 위한 상호 인증 방법은 상기 제1 장치의 권한 정보가 변경된 경우, 상기 인증 토큰을 갱신하는 단계를 더 포함할 수 있다.

[0017] 상기 제2 장치를 위한 상호 인증 방법은 상기 제1 장치로부터 상기 암호학적 정보의 공유가 완료되었음을 나타내는 신호를 수신함에 따라 상기 제1 장치를 등록하는 단계를 더 포함할 수 있다.

[0018] 일 측에 따르면, 제2 장치와 상호 인증하는 제1 장치를 위한 상호 인증 방법은 인증 요청에 응답하여 상기 제2 장치로부터 전송된, 제1 암호화된 인증 토큰을 수신하는 단계; 미리 공유된 마스터 키에 기초한 제2 세션 키를 이용하여 상기 제1 암호화된 인증 토큰을 복호화하는 단계; 상기 복호화된 인증 토큰을 검증하는 단계; 상기 검증 결과에 따라, 미리 공유된 인증 토큰을 제2 암호화하는 단계; 및 상기 제2 암호화된 인증 토큰을 상기 제2 장치에게 전송하는 단계를 포함한다.

[0019] 상기 복호화된 인증 토큰을 검증하는 단계는 상기 제2 장치를 위한 제1 변조 알고리즘에 기초하여 상기 복호화된 인증 토큰을 검증하는 단계를 포함할 수 있다.

[0020] 상기 복호화된 인증 토큰을 검증하는 단계는 상기 미리 공유된 인증 토큰을 상기 제1 변조 알고리즘을 이용하여 제1 변조하는 단계; 및 상기 제1 변조된 인증 토큰을 이용하여 상기 복호화한 인증 토큰을 검증하는 단계를 포함할 수 있다.

[0021] 상기 제2 암호화하는 단계는 상기 제1 장치를 위한 제2 변조 알고리즘에 기초하여 상기 미리 공유된 인증 토큰을 제2 변조하는 단계; 및 상기 제2 변조된 인증 토큰을 상기 제2 세션 키를 이용하여 상기 제2 암호화하는 단계를 포함할 수 있다.

[0022] 상기 제2 변조하는 단계는 상기 제2 변조 알고리즘에 기초하여 상기 미리 공유된 인증 토큰의 일부를 제2 변조하는 단계를 포함할 수 있다.

[0023] 상기 제1 장치를 위한 상호 인증 방법은 상기 인증 요청에 앞서, 상기 제2 장치 및 상기 제1 장치 간에 상기 마스터 키 및 상기 인증 토큰을 공유하는 단계를 더 포함할 수 있다.

[0024] 상기 공유하는 단계는 상기 제2 장치에게 등록을 요청하는 단계; 상기 등록 요청에 응답하여, 상기 제2 장치에서 암호화된 암호학적 정보- 상기 암호학적 정보는 상기 제2 장치가 생성한 마스터 키, 및 인증 토큰을 포함함-를 수신하는 단계; 상기 암호학적 정보를 복호화하여 상기 마스터 키 및 상기 인증 토큰을 추출하는 단계; 상기 마스터 키 및 상기 인증 토큰을 저장하는 단계; 및 상기 제2 장치에게, 상기 암호학적 정보의 공유가 완료되었음을 알리는 신호를 전송하는 단계를 포함할 수 있다.

[0025] 일 측에 따르면, 제1 장치와 상호 인증하는 제2 장치는 미리 공유된 마스터 키에 기초한 제1 세션 키를 이용하여 미리 공유된 인증 토큰을 제1 암호화하고, 제1 장치가 전송한 제2 암호화된 인증 토큰을 상기 제1 세션 키에 의해 복호화하여 검증하는 프로세서; 상기 제1 암호화된 인증 토큰을 상기 제1 장치에게 전송하고, 상기 제1 암호화된 인증 토큰에 대한 제1 장치의 검증 결과에 따라 전송된 제2 암호화된 인증 토큰을 수신하는 송수신부; 및 상기 미리 공유된 마스터 키 및 상기 미리 공유된 인증 토큰을 저장하는 메모리를 포함한다.

[0026] 일 측에 따르면, 제2 장치와 상호 인증하는 제1 장치는 인증 요청에 응답하여 제2 장치로부터 전송된 제1 암호화된 인증 토큰을 수신하고, 제2 암호화된 인증 토큰을 상기 제2 장치에게 전송하는 송수신부; 미리 공유된 마스터 키에 기초한 제2 세션 키를 이용하여 상기 제1 암호화된 인증 토큰을 복호화하여 검증하고, 상기 검증 결과에 따라, 미리 공유된 인증 토큰을 제2 암호화하는 프로세서; 및 상기 미리 공유된 마스터 키 및 상기 미리 공유된 인증 토큰을 저장하는 메모리를 포함한다.

발명의 효과

[0027] 본 발명의 일 측에 따르면, 마스터 키 및 인증 토큰을 함께 이용하여 상호 인증을 수행함으로써 보안 수준을 강

화할 수 있다.

[0028] 본 발명의 일 측에 따르면, 권한 확인(authorization check) 및 상호 인증(mutual authentication)을 한 번에 수행함으로써 권한 확인 절차를 간소화하는 한편, 원격 통신 절차 및 서버의 부하를 줄일 수 있다.

[0029] 본 발명의 일 측에 따르면, 마스터 키 및 인증 토큰을 함께 이용하여 상호 인증을 수행함으로써 별도의 장치가 없이도 IoT 기기에서 자체적으로 권한을 확인할 수 있다.

도면의 간단한 설명

[0030] 도 1은 일 실시예에 따른 상호 인증 방법이 수행되는 시스템 환경을 나타낸 도면.

도 2는 일 실시예에 따른 서버를 위한 상호 인증 방법을 나타낸 흐름도.

도 3은 다른 실시예에 따른 서버를 위한 상호 인증 방법을 나타낸 흐름도.

도 4는 일 실시예에 따른 마스터 키 및 인증 토큰을 공유하기 위한 서버의 동작을 나타낸 흐름도.

도 5는 일 실시예에 따른 대상 기기를 위한 상호 인증 방법을 나타낸 흐름도.

도 6은 다른 실시예에 따른 대상 기기를 위한 상호 인증 방법을 나타낸 흐름도.

도 7은 일 실시예에 따른 마스터 키 및 인증 토큰을 공유하기 위한 대상 기기의 동작을 나타낸 흐름도.

도 8은 일 실시예에 따른 대상 기기와 서버 간의 기기 등록 절차를 설명하기 한 도면.

도 9는 일 실시예에 따른 대상 기기와 서버 간의 상호 인증 절차를 설명하기 한 도면.

도 10은 일 실시예에 따른 서버의 블록도.

도 11은 일 실시예에 따른 대상 기기의 블록도.

발명을 실시하기 위한 구체적인 내용

[0031] 이하에서, 첨부된 도면을 참조하여 실시예들을 상세하게 설명한다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.

[0032] 아래 설명하는 실시예들에는 다양한 변경이 가해질 수 있다. 아래 설명하는 실시예들은 실시 형태에 대해 한정하려는 것이 아니며, 이들에 대한 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[0033] 실시예에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 실시예를 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 명세서 상에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0034] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 실시예가 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0035] 또한, 첨부 도면을 참조하여 설명함에 있어, 도면 부호에 관계없이 동일한 구성 요소는 동일한 참조 부호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다. 실시예를 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 실시예의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

[0037] 도 1은 일 실시예에 따른 장치들 간의 상호 인증 방법이 수행되는 시스템 환경을 나타낸 도면이다.

[0038] 도 1을 참조하면, 일 실시예에 따른 시스템 환경은 네트워크(50), 상호 인증 대상 장치(110, 이하 '제1 장치') 및 상기 제1 장치와 상호 인증을 하는 상호 인증 장치(130, 이하 '제2 장치')를 포함한다.

[0039] 네트워크(50)는, 예를 들면, 인터넷, 인트라넷들, 익스트라넷들, 광역 네트워크들(WANs), 근거리 네트워크들

(LANs), 유선 네트워크들, 무선 네트워크들, 혹은 그 외 적합한 네트워크들, 등 혹은 상기 네트워크들의 둘 이상의 임의의 조합을 포함할 수 있다.

[0040] 제1 장치(110)는 예를 들어, 퍼스널 컴퓨터(Personal Computer), 스마트 폰(smart phone), PDA(Personal Digital Assistant), 게이트웨이(Gateway) 등과 같은 통신 장치, 또는 CCTV(Closed Circuit Television), 출입 통제 단말기, 가정 내 전자 기기 등과 같이 사물 인터넷(Internet of Thing; IoT) 서비스가 가능한 다양한 전자 장치 등으로 구현될 수 있다. 제1 장치(110)는 제2 장치(130)에 직접 또는 간접적으로 연결된 단순 에지 디바이스(Edge Device)일 수 있다.

[0041] 제1 장치(110)는 제2 장치(130)와의 상호 인증을 거친 후 일정 정보를 주고 받고자 하는 기기일 수 있다.

[0042] 제2 장치(130)는 예를 들어, 퍼스널 컴퓨터(Personal Computer), 스마트 폰(smart phone), PDA(Personal Digital Assistant), 게이트웨이(Gateway) 등과 같은 통신 장치, 또는 CCTV(Closed Circuit Television), 출입 통제 단말기, 가정 내 전자 기기 등과 같이 사물 인터넷(Internet of Thing; IoT) 서비스가 가능한 다양한 전자 장치 등으로 구현될 수 있다. 제2 장치(130)는 제1 장치(110)에 직접 또는 간접적으로 연결된 단순 에지 디바이스(Edge Device)일 수 있다.

[0043] 이와 다르게, 제2 장치(130)는 예를 들어, 단일의 서버 컴퓨터 또는 이와 유사한 시스템이거나, 또는 하나 이상의 서버 뱅크들(server banks) 또는 그 외 다른 배열들로 배열되는 복수의 서버들일 수 있다. 제2 장치(130)는 서버 플랫폼으로서 단일 시설에 놓일 수도 있고, 혹은 많은 서로 다른 지리적 위치들 간에 분산된 서버 "클라우드(cloud)"일 수도 있다.

[0044] 제1 장치(110) 또한, 제2 장치(130)와 마찬가지로, 단일의 서버 컴퓨터 또는 이와 유사한 시스템이거나, 또는 하나 이상의 서버 뱅크들(server banks) 또는 그 외 다른 배열들로 배열되는 복수의 서버들일 수 있다. 제2 장치(130)는 서버 플랫폼으로서 단일 시설에 놓일 수도 있고, 혹은 많은 서로 다른 지리적 위치들 간에 분산된 서버 "클라우드(cloud)"일 수도 있다.

[0045] 이하, 제1 장치(110)가 통신 장치 또는 가정 내 전자 기기이고, 제2 장치(130)가 서버인 경우를 일 예로 들어 설명한다.

[0046] 제1 장치(110)는 단수 개일 수도 있고, 복수 개일 수도 있다. 제1 장치(110)와 제2 장치(130)는 1:1 또는 n:1의 관계로 서로 직접 또는 간접 연결될 수 있다.

[0047] 제1 장치(110)는 네트워크 망(50)을 통해 제2 장치(130)와 상호 인증을 수행할 수 있다. 일 실시예에 따른 제1 장치(110) 및 제2 장치(130)는 마스터 키(master key) 이외에도 인증 토큰(authentication token)이라는 독립적인 암호학적 정보(credential)를 함께 이용하여 상호 인증을 수행함으로써 보안성을 강화할 수 있다.

[0048] 제1 장치(110)는 제2 장치(130)에 기기를 최초 등록할 때 제2 장치(130)로부터 마스터 키와 인증 토큰을 부여받을 수 있다. 이와 같은 방식으로 시스템 내에 포함된 객체들은 서로 동일한 마스터 키 및 인증 토큰을 공유할 수 있다. 제1 장치(110)와 제2 장치(130) 간의 기기 등록 절차는 도 8을 참조하여 설명한다.

[0049] 제2 장치(130)는 제1 장치(110)와 상호 간에 공유된 마스터 키를 이용하여 세션 키(session key)를 생성하고, 세션 키로 인증 토큰을 암호화하여 제1 장치(110)에게 전달할 수 있다. 이하에서, 제2 장치(130)에서 생성되는 세션 키를 '제1 세션 키'라고 부르기로 한다. 또한, 제2 장치(130)에서 제1 세션 키에 의해 암호화된 인증 토큰을 '제1 암호화된 인증 토큰'이라 부르기로 한다.

[0050] 제1 장치(110) 또한 제2 장치(130)와 동일한 방식으로 세션 키를 생성하고, 세션 키를 이용하여 제2 장치(130)가 전송한 제1 암호화된 인증 토큰을 복호화하여 추출할 수 있다. 이하에서, 제1 장치(110)에서 생성된 세션 키를 '제2 세션 키'라고 부르기로 한다. 또한, 제1 장치(110)에서 제2 세션 키에 의해 암호화된 인증 토큰을 '제2 암호화된 인증 토큰'이라고 부르기로 한다.

[0051] 제1 장치(110)는 제2 장치(130)로부터 수신한 인증 토큰을 자신이 소유하고 있는 인증 토큰과 비교하여 인증을 수행할 수 있다. 이와 마찬가지로, 제2 장치(130) 또한, 제1 장치(110)로부터 수신한 인증 토큰을 자신이 소유하고 있는 인증 토큰과 비교하여 인증을 수행할 수 있다. 제1 장치(110)와 제2 장치(130) 간의 상호 인증 절차는 도 9를 참조하여 설명한다.

[0052] 일 실시예에서 상호 인증을 수행하고자 하는 객체들은 모두 사전에 동일한 마스터 키와 인증 토큰을 가지고 있어야 인증을 성공적으로 수행할 수 있다. 이를 통해, 허가 받지 않은 사용자가 제1 장치(110) 또한 제2 장치

(130)에 접근하는 것을 방지할 수 있다.

[0053] 이 밖에도, 제1 장치(110)는 제2 장치(130)가 생성한 인증 토큰에 포함된 제1 장치(110)의 권한 정보를 통해 자체적으로 자신(제1 장치(110))의 권한을 확인할 수 있다. 제1 장치(110)의 권한 정보가 변경된 경우, 제2 장치(130)는 인증 토큰을 갱신하여 제1 장치(110)에게 전송할 수 있다. 이하, 도면들을 통해 상호 인증을 위한 제1 장치(110) 및 제2 장치(130)의 동작을 살펴본다.

[0055] 도 2는 일 실시예에 따른 제2 장치를 위한 상호 인증 방법을 나타낸 흐름도이다.

[0056] 도 2를 참조하면, 일 실시예에 따른 제2 장치는 미리 공유된 마스터 키에 기초한 제1 세션 키를 이용하여 미리 공유된 인증 토큰을 제1 암호화한다(210). 단계(210)에서 제2 장치는 제1 변조 알고리즘에 기초하여 미리 공유된 인증 토큰을 제1 변조하고, 제1 변조된 인증 토큰을 제1 세션 키를 이용하여 제1 암호화할 수 있다. 이때, 제1 변조 알고리즘을 제2 장치에서 사용되는 변조 알고리즘으로서 제2 장치와 제1 장치 간에 미리 약속된 것일 수 있다. 제1 변조 알고리즘은 제1 장치에서 사용되는 제2 변조 알고리즘과는 상이한 것일 수 있다.

[0057] 제2 장치는 제1 변조 알고리즘에 기초하여 미리 공유된 인증 토큰의 일부를 제1 변조할 수 있다. 제2 장치는 예를 들어, 미리 공유된 인증 토큰의 앞 1/3만을 제1 변조하거나, 인증 토큰의 앞 1/2부분 중 짝수 위치에 해당하는 값만을 제1 변조할 수 있다.

[0058] 제2 장치는 예를 들어, 스크램블, 마스킹 등 다양한 암호화 기법에 의해 제1 세션 키로 제1 변조된 인증 토큰을 제2 암호화할 수 있다.

[0059] 제2 장치는 제1 암호화된 인증 토큰을 제1 장치에게 전송한다(220).

[0060] 제2 장치는 제1 장치로부터 제2 암호화된 인증 토큰을 수신한다(230). 이때, 제2 암호화된 인증 토큰은 제1 암호화된 인증 토큰에 대한 제1 장치의 검증 결과가 성공인 경우에 전송될 수 있다. 예를 들어, 제2 장치가 제1 장치에게 전송한 제1 암호화된 인증 토큰이 제1 장치에서 검증에 실패한 경우, 제1 장치는 제1 암호화된 인증 토큰을 전송한 제2 장치가 상호 인증을 위한 적절한 제2 장치가 아니라고 판단하여 제2 암호화된 인증 토큰을 전송하지 않을 수 있다.

[0061] 제2 장치는 제1 세션 키를 이용하여 제2 암호화된 인증 토큰을 복호화하고(240), 복호화된 인증 토큰을 검증함으로써 상호 인증을 완료할 수 있다(250). 단계(250)에서, 제2 장치는 제1 장치를 위한 제2 변조 알고리즘에 기초하여 복호화된 인증 토큰을 검증할 수 있다. 제2 장치는 예를 들어, 제2 변조 알고리즘에 기초하여 미리 공유된 인증 토큰을 제2 변조하고, 제2 변조된 인증 토큰을 이용하여 복호화된 인증 토큰을 검증할 수 있다. 제2 암호화된 인증 토큰은 제1 장치에 의해 암호화된 것일 수 있다.

[0062] 만약, 제2 암호화된 인증 토큰이 상호 인증을 위한 정당한 상대방으로부터 전송된 경우, 제2 장치가 사전에 약속된 제2 변조 알고리즘에 의해 미리 공유된 인증 토큰을 제2 변조한 결과(제2 변조된 인증 토큰)와 복호화된 인증 토큰이 동일한 값을 가질 수 있다. 제2 장치는 제2 변조된 인증 토큰과 복호화된 인증 토큰의 값이 동일한 경우, 제1 장치에 대한 검증을 성공한 것으로 판단할 수 있다.

[0064] 도 3은 다른 실시예에 따른 제2 장치를 위한 상호 인증 방법을 나타낸 흐름도이다.

[0065] 도 3을 참조하면, 제2 장치는 제1 장치와 마스터 키 및 인증 토큰을 공유할 수 있다(305). 제2 장치와 제1 장치 간에 마스터 키 및 인증 토큰을 공유하기 위한 제2 장치의 동작은 도 4를 참조하여 설명한다.

[0066] 제2 장치는 제1 장치의 인증 요청을 수신할 수 있다(310). 이때, 인증 요청에는 제1 장치의 식별 정보가 함께 포함될 수 있다. 제1 장치의 식별 정보는 예를 들어, 제1 장치의 MAC(Media Access Control) 정보 및 제1 장치의 칩 정보(예를 들어, 시리얼 번호) 등을 포함할 수 있다.

[0067] 제2 장치는 단계(310)의 인증 요청에 응답하여, 제1 장치를 검증할 수 있다(315). 단계(315)에서의 검증은 제1 장치 자체에 대한 검증으로서, 제2 장치는 제1 장치의 인증 요청 시에 인증 요청과 함께 포함된 제1 장치의 식별 정보를 이용하여 제1 장치를 검증할 수 있다.

[0068] 제2 장치는 랜덤 정보를 생성할 수 있다(320). 여기서, 랜덤 정보는 세션 키 생성을 위한 것으로서, 예를 들어, 랜덤 함수 등에 생성되는 랜덤 값일 수 있다.

[0069] 제2 장치는 미리 공유된 마스터 키 및 단계(320)에서 생성된 랜덤 정보를 이용하여 제1 세션 키를 생성할 수 있다(325).

[0070] 제2 장치는 제1 변조 알고리즘에 기초하여 미리 공유된 인증 토큰을 제1 변조하고(330), 제1 변조된 인증 토큰을 단계(325)에서 생성된 제1 세션 키를 이용하여 제1 암호화할 수 있다(335).

[0071] 제2 장치는 단계(335)에서 제1 암호화된 인증 토큰을 제1 장치에게 전송할 수 있다(340).

[0072] 제2 장치는 제1 장치로부터 제2 암호화된 인증 토큰을 수신할 수 있다(345). 이때, 제2 암호화된 인증 토큰은 단계(340)에서 제2 장치가 전송한 제1 암호화된 인증 토큰에 대한 제1 장치의 검증 결과에 따라 전송된 것일 수 있다.

[0073] 제2 장치는 단계(325)에서 생성한 제1 세션 키를 이용하여 제2 암호화된 인증 토큰을 복호화할 수 있다(350).

[0074] 제2 장치는 제2 변조 알고리즘에 기초하여 미리 공유된 인증 토큰을 제2 변조하고(355), 제2 변조된 인증 토큰을 이용하여 단계(350)에서 복호화된 인증 토큰을 검증할 수 있다(360).

[0076] 도 4는 일 실시예에 따른 마스터 키 및 인증 토큰을 공유하기 위한 제2 장치의 동작을 나타낸 흐름도이다.

[0077] 도 4를 참조하면, 일 실시예에 따른 제2 장치는 제1 장치의 (기기) 등록 요청을 수신할 수 있다(410).

[0078] 제2 장치는 등록 요청에 응답하여, 임시 키 생성을 위한 랜덤 정보를 생성할 수 있다(420).

[0079] 제2 장치는 제1 장치를 위한 인증 토큰을 생성할 수 있다(430). 제2 장치는 제1 장치의 권한 정보에 기초하여 제1 장치를 위한 인증 토큰을 생성할 수 있다. 시스템 내에 포함된 제1 장치가 복수 개인 경우, 제2 장치는 제1 장치마다 서로 다른 인증 토큰을 생성할 수 있다. 제1 장치의 권한 정보는 제1 장치가 제공하는 서비스에 따라 제1 장치마다 서로 달라질 수 있다.

[0080] 인증 토큰은 예를 들어, 제1 장치의 권한 정보, 랜덤 정보, 제2 장치의 식별 정보(ID) 및 제1 장치의 식별 정보(ID) 등을 포함할 수 있다.

[0081] 제2 장치는 마스터 키를 생성할 수 있다(440). 제2 장치는 키 시드(Key Seed) 값을 이용하여 마스터 키를 생성할 수 있다. 제2 장치는 인증 토큰과 마스터 키를 서로 독립적인 방법으로 생성함으로써 서로 간의 관련성이 없도록 할 수 있다. 이에 따라, 마스터 키와 인증 토큰 중 어느 하나가 외부에 노출되더라도 다른 하나에 대한 보안성이 유지될 수 있다.

[0082] 제2 장치는 단계(420)에서 생성한 랜덤 정보 및 이니셜 키(initial key)를 이용하여 임시 키(temporary key)를 생성할 수 있다(450). 임시 키는 마스터 키 및 인증 토큰의 전송을 위해 1번만 사용되고 폐기되는 일회성의 키로서, '원-타임 키(One-Time key)'라고도 부를 수 있다. 이니셜 키는 제1 장치의 제작 시점에 제1 장치에 주입된 키일 수 있다. 제2 장치는 제1 장치의 이니셜 키에 대한 정보를 미리 파악할 수 있다.

[0083] 제2 장치는 단계(450)에서 생성된 임시 키를 이용하여 암호학적 정보(credential)를 암호화하고, 암호화한 암호학적 정보를 단계(420)에서 생성된 랜덤 정보와 함께 제1 장치에게 전송할 수 있다(460). 암호학적 정보는 예를 들어, 단계(430)에서 생성된 인증 토큰 및 단계(440)에서 생성된 마스터 키를 포함할 수 있다.

[0085] 도 5는 일 실시예에 따른 제1 장치를 위한 상호 인증 방법을 나타낸 흐름도이다.

[0086] 도 5를 참조하면, 일 실시예에 따른 제1 장치는 제2 장치에게 인증을 요청할 수 있다(510).

[0087] 제1 장치는 단계(510)의 인증 요청에 응답하여 제2 장치로부터 전송된, 제1 암호화된 인증 토큰을 수신한다(520).

[0088] 제1 장치는 제2 세션 키를 이용하여 제1 암호화된 인증 토큰을 복호화 한다(530). 제2 세션 키는 미리 공유된 마스터 키에 기초한 것일 수 있다.

[0089] 제1 장치는 단계(530)에서 복호화된 인증 토큰을 검증한다(540). 단계(540)에서, 제1 장치는 제2 장치를 위한 제1 변조 알고리즘에 기초하여 복호화된 인증 토큰을 검증할 수 있다.

[0090] 제1 장치는 단계(540)의 검증 결과에 따라, 미리 공유된 인증 토큰을 제2 암호화한다(550). 제1 장치는 제2 변

조 알고리즘에 기초하여 미리 공유된 인증 토큰을 제2 변조하고, 제2 변조된 인증 토큰을 제2 세션 키를 이용하여 제2 암호화할 수 있다 할 수 있다. 이때, 제1 장치는 미리 공유된 인증 토큰의 일부만을 제2 변조할 수 있다. 제1 장치는 예를 들어, 미리 공유된 인증 토큰의 뒤 1/3만을 제2 변조하거나, 앞 1/3 부분 중 홀수 위치에 해당하는 값만을 제2 변조할 수 있다.

[0091] 일 실시예에 따른 제2 장치 및 제1 장치는 도 5의 제2 암호화 과정에서 제1 장치가 암호화한 인증 토큰이 도 2의 제1 암호화 과정에서 제2 장치가 암호화하는 인증 토큰과 결합되는 경우, 인증 토큰 전체의 값이 드러나지 않는 범위 내에서 인증 토큰의 일부를 변조 및 암호화할 수 있다.

[0092] 제1 장치는 예를 들어, 스크램블, 마스킹 등 다양한 암호화 기법에 의해 제2 세션 키로 제2 변조된 인증 토큰을 제2 암호화할 수 있다.

[0093] 제1 장치는 제2 암호화된 인증 토큰을 제2 장치에게 전송한다(560).

[0095] 도 6은 다른 실시예에 따른 제1 장치를 위한 상호 인증 방법을 나타낸 흐름도이다.

[0096] 도 6을 참조하면, 일 실시예에 따른 제1 장치는 마스터 키 및 인증 토큰을 제2 장치와 공유할 수 있다(605). 마스터 키 및 인증 토큰의 공유를 위한 제1 장치의 동작은 도 7을 참조하여 설명한다.

[0097] 제1 장치는 제2 장치에게 인증을 요청하고(610), 인증 요청에 응답하여 제2 장치로부터 전송된, 제1 암호화된 인증 토큰을 수신한다(615).

[0098] 제1 장치는 제2 세션 키를 이용하여 제1 암호화된 인증 토큰을 복호화 할 수 있다(620).

[0099] 제1 장치는 미리 공유된 인증 토큰을 제1 변조 알고리즘을 이용하여 제1 변조하고(625), 제1 변조된 인증 토큰을 이용하여 복호화한 인증 토큰을 검증할 수 있다(630). 제1 장치는 제1 변조된 인증 토큰이 단계(620)에서 복호화한 인증 토큰과 동일한지 여부에 따라 복호화한 인증 토큰을 검증할 수 있다.

[0100] 제1 장치는 복호화한 인증 토큰에 대한 검증이 성공인지 여부를 판단할 수 있다(635). 단계(635)에서 검증이 실패한 것으로 판단되면, 제1 장치는 동작을 종료할 수 있다.

[0101] 단계(635)에서 검증이 성공한 것으로 판단되면, 제1 장치는 제2 변조 알고리즘에 기초하여 미리 공유된 인증 토큰을 제2 변조할 수 있다(640). 이때, 제1 장치는 미리 공유된 인증 토큰의 일부만을 제2 변조할 수 있다.

[0102] 제1 장치는 제2 변조된 인증 토큰을 제2 세션 키를 이용하여 제2 암호화할 수 있다(645).

[0103] 제1 장치는 제2 암호화된 인증 토큰을 제2 장치에게 전송할 수 있다(650).

[0105] 도 7은 일 실시예에 따른 마스터 키 및 인증 토큰을 공유하기 위한 제1 장치의 동작을 나타낸 흐름도이다.

[0106] 도 7을 참조하면, 제1 장치는 제2 장치에게 (기기) 등록을 요청할 수 있다(710). 단계(710)에서, 제1 장치는 제2 장치에게 제1 장치의 식별 정보를 전송하여 기기 등록을 요청할 수 있다. 제1 장치의 식별 정보는 예를 들어, 제1 장치의 아이디, 칩 시리얼 번호, 및 제1 장치의 MAC 정보 등을 포함할 수 있다.

[0107] 제1 장치는 단계(710)의 등록 요청에 응답하여, 제2 장치가 생성한 랜덤 정보 및 제2 장치에서 암호화된 암호학적 정보를 수신할 수 있다(720). 암호학적 정보는 마스터 키, 및 인증 토큰을 포함할 수 있다. 암호학적 정보는 미리 저장된 이니셜 키 및 제2 장치에서 생성된 랜덤 정보를 이용하여 생성한 임시키를 이용하여 암호화된 것일 수 있다.

[0108] 제1 장치는 암호학적 정보를 복호화하여 마스터 키 및 인증 토큰을 추출하고(730), 마스터 키 및 인증 토큰을 저장할 수 있다(740).

[0109] 제1 장치는 제2 장치에게, 암호학적 정보의 공유가 완료되었음을 알리는 신호를 전송할 수 있다(750).

[0111] 도 8은 일 실시예에 따른 제1 장치와 제2 장치 간의 기기 등록 절차를 설명하기 한 도면이다.

[0112] 도 8을 참조하면, 제1 장치(801) 및 제2 장치(803) 간에 수행되는 기기 등록 절차가 도시된다.

[0113] 제1 장치(801)는 제2 장치(803)에게 제1 장치(801)의 기기 등록을 요청할 수 있다(810). 이때, 제1 장치(801)는 기기 등록 요청과 함께 제1 장치(801)를 식별할 수 있는 식별 정보(예를 들어, 디바이스 ID, 칩 시리얼 번호, MAC 등)를 전송할 수 있다.

[0114] 제2 장치(803)는 제1 장치(801)의 식별 정보가 사전에 등록된 기기 정보 목록에 있는지 확인하여 제1 장치(801)를 검증할 수 있다(815). 제1 장치(801)의 식별 정보는 일반적으로 제1 장치(801)가 공장에서 제조된 시점에 제2 장치(803)의 기기 정보 목록에 등록될 수 있다.

[0115] 제2 장치(803)는 임시 키를 생성하기 위한 랜덤 정보를 생성할 수 있다(820).

[0116] 제2 장치(803)는 제1 장치(801)에 대한 인증 토큰을 생성할 수 있다(825). 제1 장치(801)가 복수 개인 경우, 제2 장치(803)는 제1 장치(801)의 권한을 기준으로 제1 장치(801) 별로 인증 토큰을 생성할 수 있다. 여기서, 인증 토큰은 마스터 키와 동일한 수준의 보안이 요구되는 정보로 이해될 수 있다.

[0117] 제1 장치(801)의 권한 정보가 변경되는 경우, 제2 장치(803)는 인증 토큰을 갱신하여 제1 장치(801)를 재등록할 수 있다. 제1 장치(801)의 재등록 시 제2 장치(803)는 상호 인증에 따라 이미 생성된 세션 키를 이용하여 갱신된 인증 토큰을 암호화하여 제1 장치(801)에게 전송할 수 있다.

[0118] 제2 장치(803)는 예를 들어, 제1 장치(801)의 권한 정보, 제1 장치(801)의 식별 정보, 랜덤 정보 등을 조합하여 인증 토큰을 생성할 수 있다. 인증 토큰은 제1 장치(801)의 권한 정보, 제1 장치(801)의 식별 정보, 랜덤 정보, 제2 장치(803)의 식별 정보 중 적어도 하나를 포함할 수 있다.

[0119] 제2 장치(803)는 마스터 키를 생성할 수 있다(830). 제2 장치(803)는 별도의 키 시드(Key Seed) 값을 이용하여 마스터 키를 생성할 수 있다. 일 실시예에서는 인증 토큰과 마스터 키를 서로 독립적인 방법으로 생성하여 서로 간의 관련성이 발생하지 않도록 함으로써 마스터 키와 인증 토큰 중 어느 하나가 노출되더라도 나머지 하나가 유출되지 않도록 할 수 있다.

[0120] 제2 장치(803)는 임시 키를 생성할 수 있다(835). 제2 장치(803)는 제조 시점에 제1 장치(801)에 주입한 이니셜 키와 동일한 키 및 단계(820)에서 생성한 랜덤 정보를 이용하여 임시 키를 생성할 수 있다. 이때, 임시 키를 생성하는 알고리즘은 제2 장치(803)와 제1 장치(801) 간에 사전에 공유될 수 있다.

[0121] 제2 장치(803)는 단계(830)에서 생성한 마스터 키, 및 단계(825)에서 생성한 인증 토큰을 임시 키로 암호화하여 단계(820)에서 생성한 랜덤 정보와 함께 제1 장치(801)에게 전송할 수 있다(840). 이때, 임시 키로 암호화되는 정보들(마스터 키, 및 인증 토큰)을 암호학적 정보라고 부를 수 있다.

[0122] 제1 장치(801)는 제조 시점에 제1 장치(801)에 주입된 이니셜 키와 단계(840)에서 전송된 랜덤 정보를 이용하여 임시 키를 생성할 수 있다(845).

[0123] 제1 장치(801)는 단계(845)에서 생성한 임시 키를 이용하여 단계(840)에서 수신한 암호화된 암호학적 정보를 복호화하여 인증 토큰 및 마스터 키를 추출할 수 있다(850). 이와 같이, 제1 장치(801)와 제2 장치(803)는 임시 키를 이용하여 안전한 방식으로 동일한 마스터 키와 인증 토큰을 공유할 수 있다. 임시 키는 마스터 키 및 인증 토큰의 전송을 위해 1번만 사용되고 폐기될 수 있다.

[0124] 제1 장치(801)는 단계(850)에서 추출한 인증 토큰 및 마스터 키를 제1 장치(801)의 안정한 영역에 저장할 수 있다(855).

[0125] 제1 장치(801)는 암호학적 정보의 공유가 완료되었음을 나타내는 신호를 제2 장치(803)에게 전송할 수 있다(860). 제1 장치(801)로부터 암호학적 정보의 공유가 완료되었음을 나타내는 신호를 수신한 제2 장치(803)는 제1 장치(801)를 등록할 수 있다(865).

[0126] 제1 장치(801) 및 제2 장치(803)는 상술한 기기 등록 절차를 통해 마스터 키와 인증 토큰을 서로 공유할 수 있다.

[0128] 도 9는 일 실시예에 따른 제1 장치와 제2 장치 간의 상호 인증 절차를 설명하기 한 도면이다.

[0129] 도 9를 참조하면, 도 8을 통한 기기 등록 절차를 완료한 제1 장치(901)와 제2 장치(903) 간에 수행되는 상호 인증 절차가 도시된다.

[0130] 제1 장치(901)는 제2 장치(903)에게 상호 인증을 요청할 수 있다(910). 제1 장치(901)는 상호 인증 요청과 함께, 예를 들어, 제1 장치(901)의 MAC 정보 및 제1 장치(901)의 칩 시리얼 정보 등을 포함하는 식별 정보를 전송할 수 있다.

[0131] 제2 장치(903)는 단계(910)에서 전송된 식별 정보를 이용하여 제1 장치(901)를 검증할 수 있다(915).

[0132] 제2 장치(903)는 세션 키 생성을 위한 랜덤 정보를 생성할 수 있다(920).

[0133] 제2 장치(903)는 미리 공유된 마스터 키 및 단계(920)에서 생성한 랜덤 정보를 이용하여 세션 키(제1 세션 키)를 생성할 수 있다(925).

[0134] 제2 장치(903)는 미리 공유된 인증 토큰을 특정 알고리즘(제1 변조 알고리즘)에 의해 제1 변조한 다음 제1 세션 키를 이용하여 암호화(제1 암호화)할 수 있다(930).

[0135] 제2 장치(903)는 단계(930)에서 제1 암호화된 인증 토큰을, 단계(920)에서 생성한 랜덤 정보와 함께 제1 장치(901)에게 전송할 수 있다(935).

[0136] 제1 장치(901)는 단계(935)를 통해 수신한 랜덤 정보와 사전에 공유된 마스터 키를 이용하여 세션 키(제2 세션 키)를 생성할 수 있다(940).

[0137] 제1 장치(901)는 단계(935)에서 수신한 제1 암호화된 인증 토큰을, 제2 세션 키를 이용하여 복호화할 수 있다(945).

[0138] 제1 장치(901)는 단계(945)에서 복호화한 인증 토큰을 검증할 수 있다(950). 제1 장치(901)는 미리 공유된 인증 토큰을 제2 장치(903)가 단계(930)에서 한 것과 동일한 방식으로 변조할 수 있다. 그리고, 변조된 인증 토큰이 단계(945)에서 복호화 한 인증 토큰과 동일한 지 비교함으로써 복호화한 인증 토큰을 검증할 수 있다. 다시 말해, 제1 장치(901)는 미리 공유된 인증 토큰을 제1 변조 알고리즘을 이용하여 제1 변조하고, 제1 변조된 인증 토큰과 단계(945)에서 복호화한 인증 토큰을 비교하여 복호화한 인증 토큰을 검증할 수 있다. 이때, 제1 장치(901)는 제2 장치(903)에서 사용한 제1 변조 알고리즘을 미리 알고 있어야 한다.

[0139] 제2 장치(903)로부터 수신한 인증 토큰에 대한 검증을 마친 제1 장치(901)는 제2 장치(903)의 검증을 위한 인증 토큰을 제2 장치(903)와는 다른 방식으로 변조 및 암호화하여 제2 장치(903)에게 전송할 수 있다. 제1 장치(901)는 제1 장치를 위한 특정 알고리즘(제2 변조 알고리즘)에 기초하여 미리 공유된 인증 토큰을 변조(제2 변조)하고, 제2 변조된 인증 토큰을 단계(940)에서 생성된 제2 세션 키를 이용하여 암호화(제2 암호화)할 수 있다(955).

[0140] 제1 장치(901)는 제2 암호화된 인증 토큰을 제2 장치(903)에게 전송할 수 있다(960).

[0141] 제2 장치(903)는 단계(960)에서 수신한 제2 암호화된 인증 토큰을 단계(925)에서 생성한 제1 세션 키를 이용하여 복호화할 수 있다(965).

[0142] 제2 장치(903)는 미리 공유된 인증 토큰을 단계(955)에서 제1 장치(901)가 수행한 것과 동일한 방식으로 변조한 다음, 단계(965)에서의 복호화 결과와 같은지를 비교함으로써 단계(965)에서 복호화 된 인증 토큰을 검증할 수 있다(970). 보다 구체적으로, 제2 장치(903)는 제2 변조 알고리즘에 기초하여 미리 공유된 인증 토큰을 제2 변조하고, 제2 변조된 인증 토큰과 단계(965)에서 복호화된 인증 토큰이 같다면 상호 인증이 성공한 것으로 판단할 수 있다. 이때, 제2 장치(903)는 제1 장치(901)에서 사용한 제2 변조 알고리즘을 미리 알고 있어야 한다.

[0143] 일 실시예에서는 상호 인증을 수행하는 객체 간에 마스터 키와 인증 토큰을 모두 알고 있어야 인증이 성공적으로 수행될 수 있다. 마스터 키와 인증 토큰 중 어느 하나의 정보가 노출되더라도 상호 인증을 수행할 수 없으므로 높은 수준의 보안성을 확보할 수 있다. 또한, 일 실시예에서는 제2 장치와 제1 장치에서 각각 한 번씩 인증 토큰을 검증하기 때문에, 제2 장치가 제1 장치를 검증하고, 제1 장치가 제2 장치를 검증하는 문자 그대로의 상호 인증을 수행할 수 있다.

[0144] 또한, 일 실시예에서는 인증 토큰을 상호 검증할 때 단순히 인증 토큰의 암호화 방식 및 복호화 방식뿐만 아니라, 인증 토큰의 변조 알고리즘까지 알고 있어야 한다. 다시 말해, 외부 침입자가 일 실시예에 따른 상호 인증 보안을 공격하기 위해서는 마스터 키, 세션 키의 생성 알고리즘뿐만 아니라, 인증 토큰, 제2 장치에서의 인증 토큰의 변조 알고리즘(제1 변조 알고리즘), 및 제1 장치에서의 인증 토큰의 변조 알고리즘(제2 변조 알고리즘)의 총 5 개의 정보를 모두 알아야 하므로, 보다 높은 수준의 보안성을 확보할 수 있다.

[0145] 사물 인터넷(IoT) 서비스의 특성상 IoT 객체(예를 들어, 디바이스, 게이트웨이, 제2 장치 플랫폼 등)는 다양한 서비스를 제공하게 된다. 이로 인해, IoT 객체 간의 권한 관리 방안은 사물 인터넷 보안의 주요 요소라 할 수 있다. 일 실시예에 따른 토큰 정보는 각 제1 장치의 식별 정보 및 권한 정보를 조합하여 생성되므로 권한 관리 정보로도 활용될 수 있다. 다시 말해, 토큰 정보가 각 제1 장치의 권한 정보를 포함하고 있으므로 제1 장치는 별도의 권한 확인 절차 없이 상호 인증을 수행하는 것만으로도 권한 확인을 함께 수행할 수 있다.

[0147] 도 10은 일 실시예에 따른 제2 장치의 블록도이다.

[0148] 도 10을 참조하면, 일 실시예에 따른 제2 장치(1000)는 프로세서(1010), 송수신부(1020), 및 메모리(1030)를 포함할 수 있다. 프로세서(1010), 송수신부(1020), 및 메모리(1030)는 버스(1040)를 통해 서로 통신할 수 있다.

[0149] 프로세서(1010)는 미리 공유된 마스터 키에 기초한 제1 세션 키를 이용하여 미리 공유된 인증 토큰을 제1 암호화한다. 프로세서(1010)는 제1 장치가 전송한 제2 암호화된 인증 토큰을 제1 세션 키에 의해 복호화하여 검증한다.

[0150] 송수신부(1020)는 프로세서(1010)에서 제1 암호화된 인증 토큰을 제1 장치에게 전송하고, 제1 장치로부터 제2 암호화된 인증 토큰을 수신한다. 이때, 제2 암호화된 인증 토큰은 제1 암호화된 인증 토큰에 대한 제1 장치의 검증 결과에 따라 전송된 것일 수 있다.

[0151] 메모리(1030)는 미리 공유된 마스터 키 및 미리 공유된 인증 토큰을 저장할 수 있다. 메모리(1030)는 미리 공유된 마스터 키에 기초한 생성한 제1 세션 키를 저장할 수 있다. 이 밖에도, 메모리(1030)는 세션 키의 생성 알고리즘, 제2 장치에서의 인증 토큰의 변조 알고리즘(제1 변조 알고리즘), 및 제1 장치에서의 인증 토큰의 변조 알고리즘(제2 변조 알고리즘) 등을 저장할 수 있다.

[0152] 이 밖에도, 프로세서(1010)는 도 2 내지 도 9를 통하여 전술한 적어도 하나의 방법을 수행할 수 있다.

[0153] 프로세서(1010)는 프로그램을 실행하고, 제2 장치(1000)를 제어할 수 있다. 프로세서(1010)에 의하여 실행되는 프로그램 코드는 메모리(1030)에 저장될 수 있다. 제2 장치(1000)는 입출력 장치(도면 미 표시)를 통하여 외부 장치(예를 들어, 제1 장치 또는 네트워크)에 연결되고, 데이터를 교환할 수 있다.

[0155] 도 11은 일 실시예에 따른 제1 장치의 블록도이다.

[0156] 도 11을 참조하면, 일 실시예에 따른 제1 장치(1100)는 프로세서(1110), 송수신부(1120), 및 메모리(1130)를 포함할 수 있다.

[0157] 프로세서(1110)는 미리 공유된 마스터 키에 기초한 제2 세션 키를 이용하여 제1 암호화된 인증 토큰을 복호화한다. 프로세서(1110)는 검증 결과에 따라, 미리 공유된 인증 토큰을 제2 암호화한다.

[0158] 송수신부(1120)는 제1 장치(1100)의 인증 요청에 응답하여 제2 장치로부터 전송된 제1 암호화된 인증 토큰을 수신하고, 프로세서(1110)에서 제2 암호화된 인증 토큰을 제2 장치에게 전송한다.

[0159] 메모리(1130)는 미리 공유된 마스터 키 및 미리 공유된 인증 토큰을 저장할 수 있다. 메모리(1130)는 미리 공유된 마스터 키에 기초한 생성한 제2 세션 키를 저장할 수 있다. 이 밖에도, 메모리(1130)는 세션 키의 생성 알고리즘, 제2 장치에서의 인증 토큰의 변조 알고리즘(제1 변조 알고리즘), 및 제1 장치에서의 인증 토큰의 변조 알고리즘(제2 변조 알고리즘) 등을 저장할 수 있다.

[0160] 이 밖에도, 프로세서(1110)는 도 2 내지 도 9를 통하여 전술한 적어도 하나의 방법을 수행할 수 있다.

[0161] 프로세서(1110)는 프로그램을 실행하고, 제1 장치(1100)를 제어할 수 있다. 프로세서(1110)에 의하여 실행되는 프로그램 코드는 메모리(1130)에 저장될 수 있다. 제1 장치(1100)는 입출력 장치(도면 미 표시)를 통하여 외부 장치(예를 들어, 제2 장치 또는 네트워크)에 연결되고, 데이터를 교환할 수 있다.

[0163] 본 발명의 일 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위

하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0164] 이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[0165] 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐만 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

[0166] 1000: 제2 장치

1010: 프로세서

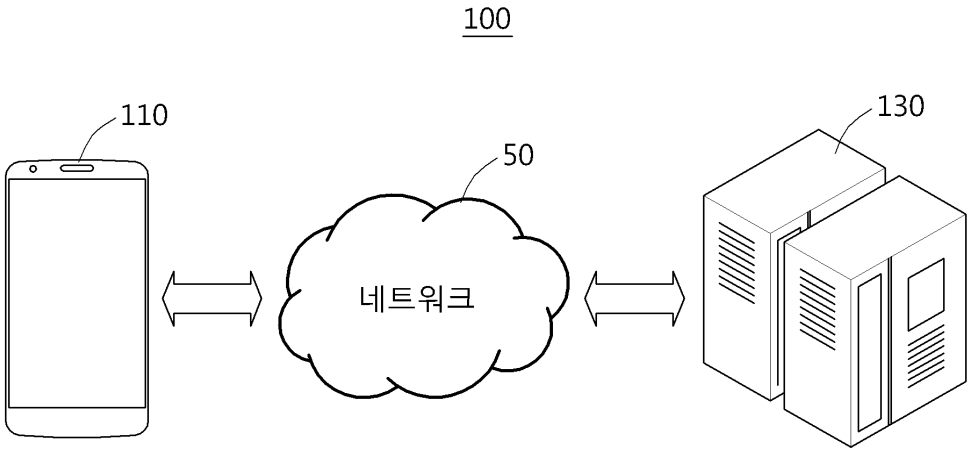
1020: 송수신부

1030: 메모리

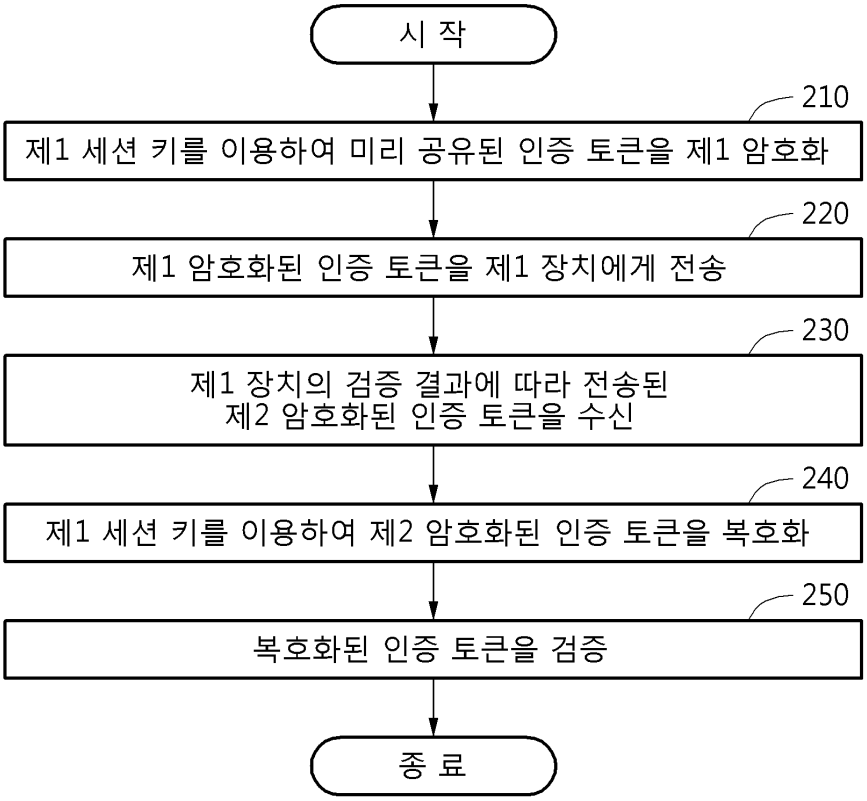
1040: 버스

도면

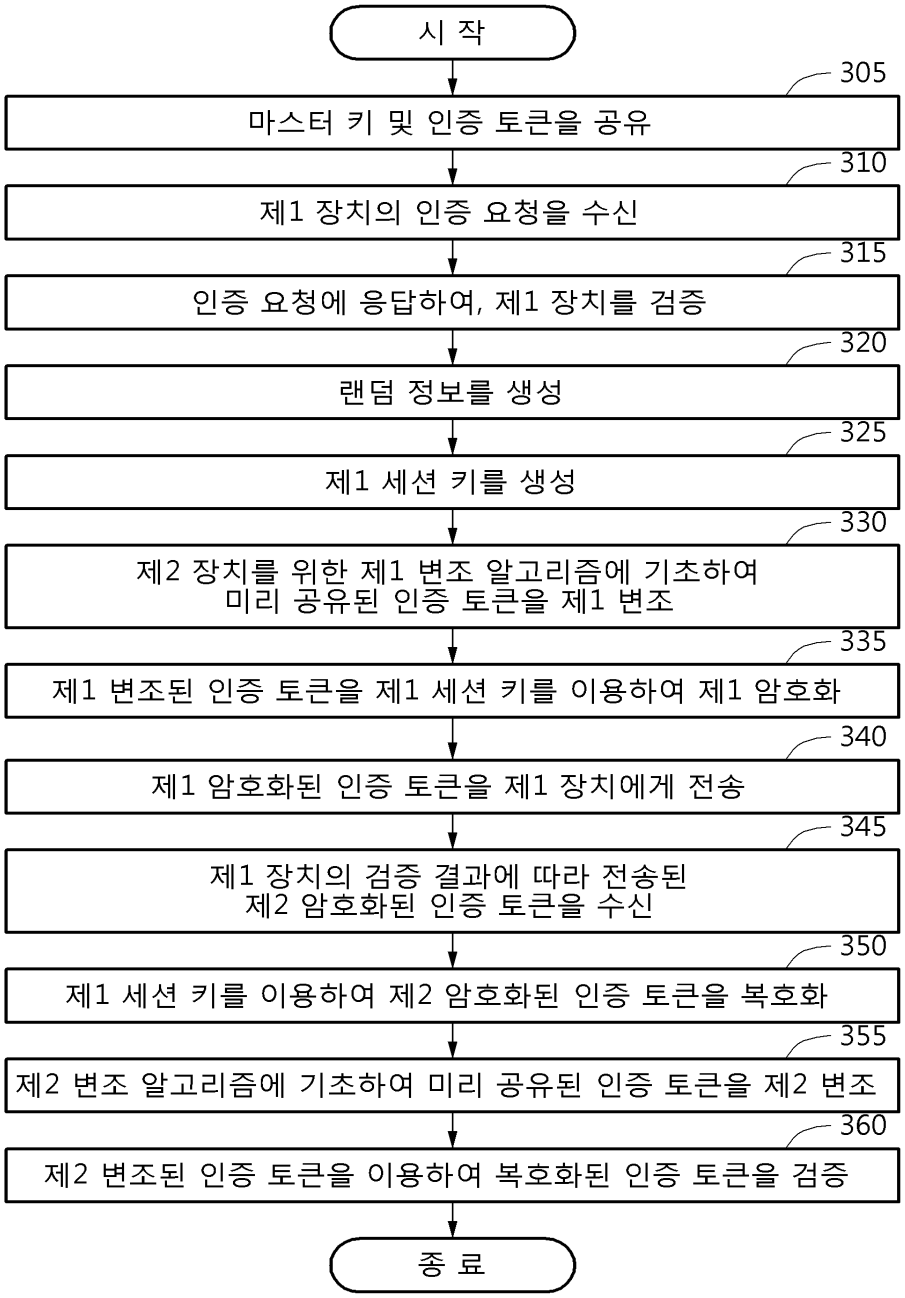
도면1



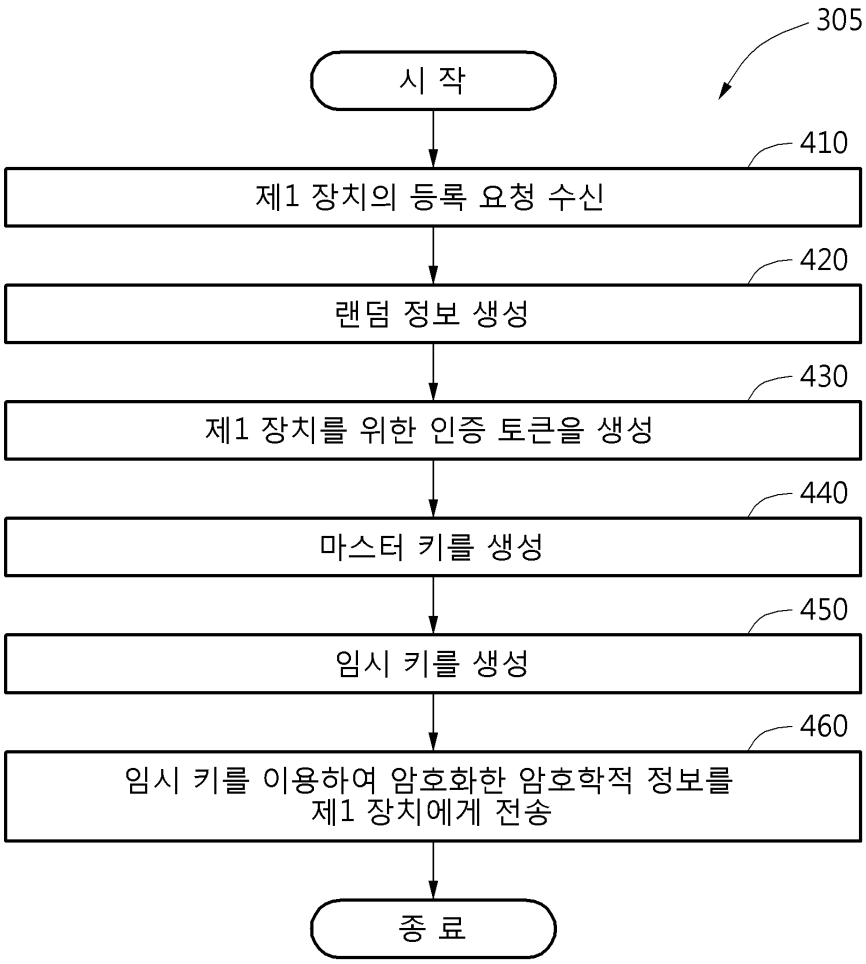
도면2


시 작
210
제1 세션 키를 이용하여 미리 공유된 인증 토큰을 제1 암호화
220
제1 암호화된 인증 토큰을 제1 장치에게 전송
230
제1 장치의 검증 결과에 따라 전송된
제2 암호화된 인증 토큰을 수신
240
제1 세션 키를 이용하여 제2 암호화된 인증 토큰을 복호화
250
복호화된 인증 토큰을 검증
종 료

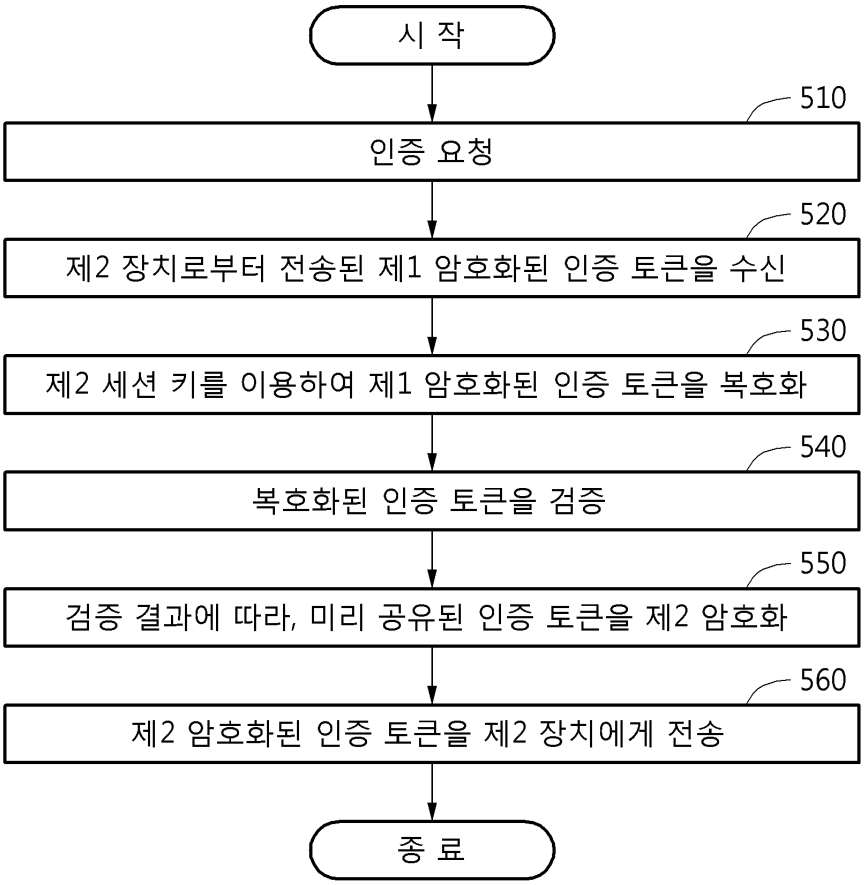
도면3


시 작
305
마스터 키 및 인증 토큰을 공유
310
제1 장치의 인증 요청을 수신
315
인증 요청에 응답하여, 제1 장치를 검증
320
랜덤 정보를 생성
325
제1 세션 키를 생성
330
제2 장치를 위한 제1 변조 알고리즘에 기초하여
미리 공유된 인증 토큰을 제1 변조
335
제1 변조된 인증 토큰을 제1 세션 키를 이용하여 제1 암호화
340
제1 암호화된 인증 토큰을 제1 장치에게 전송
345
제1 장치의 검증 결과에 따라 전송된
제2 암호화된 인증 토큰을 수신
350
제1 세션 키를 이용하여 제2 암호화된 인증 토큰을 복호화
355
제2 변조 알고리즘에 기초하여 미리 공유된 인증 토큰을 제2 변조
360
제2 변조된 인증 토큰을 이용하여 복호화된 인증 토큰을 검증
종 료

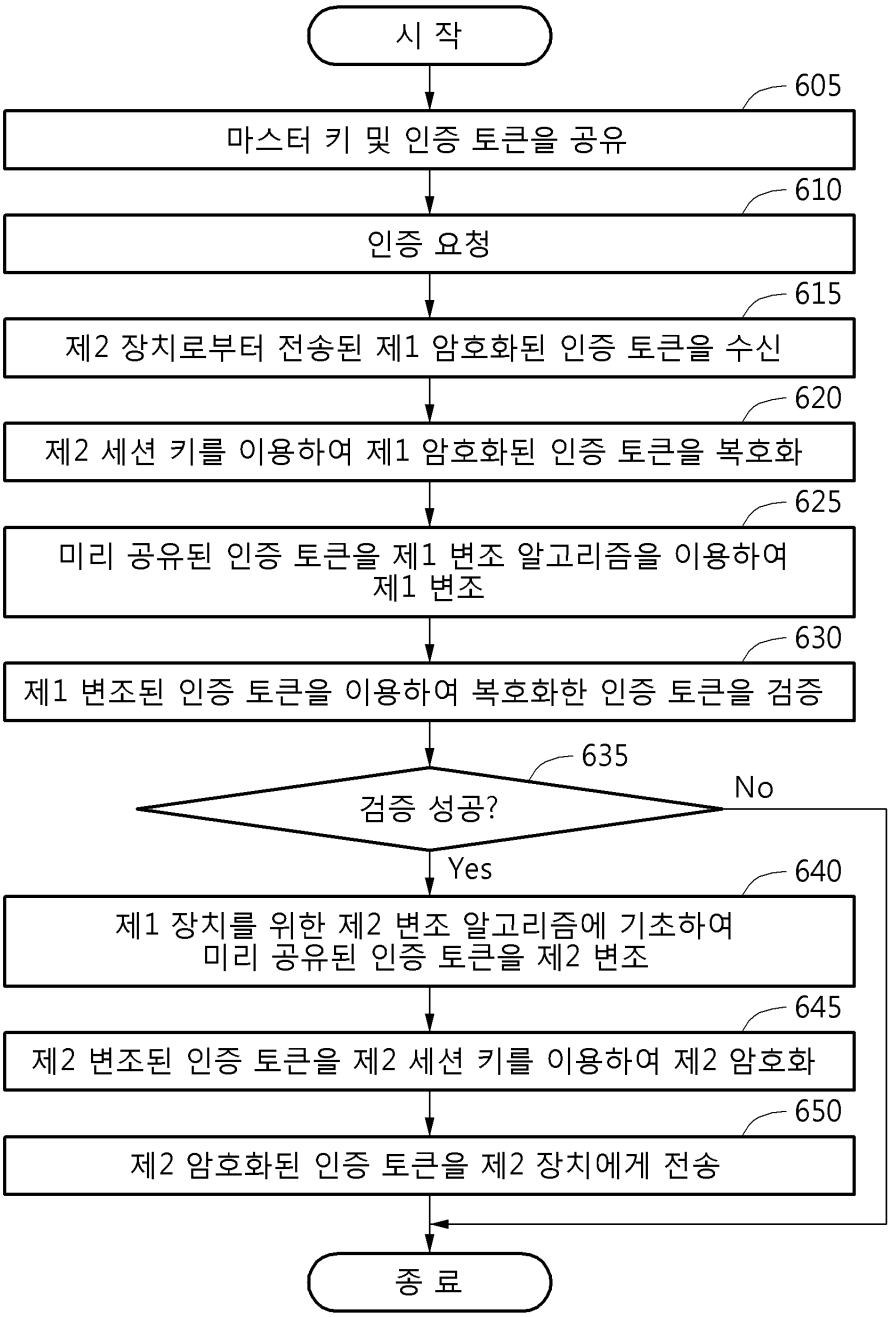
도면4


305
시 작
410
제1 장치의 등록 요청 수신
420
랜덤 정보 생성
430
제1 장치를 위한 인증 토큰을 생성
440
마스터 키를 생성
450
임시 키를 생성
460
임시 키를 이용하여 암호화한 암호학적 정보를
제1 장치에게 전송
종 료

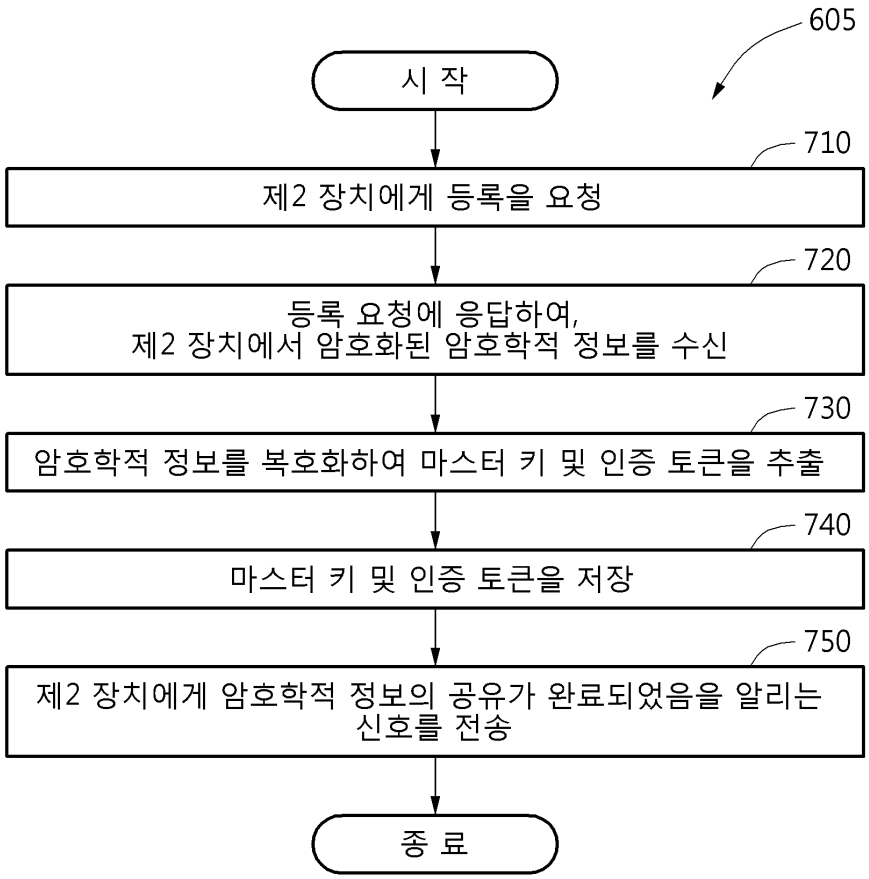
도면5


시 작
510
인증 요청
520
제2 장치로부터 전송된 제1 암호화된 인증 토큰을 수신
530
제2 세션 키를 이용하여 제1 암호화된 인증 토큰을 복호화
540
복호화된 인증 토큰을 검증
550
검증 결과에 따라, 미리 공유된 인증 토큰을 제2 암호화
560
제2 암호화된 인증 토큰을 제2 장치에게 전송
종 료

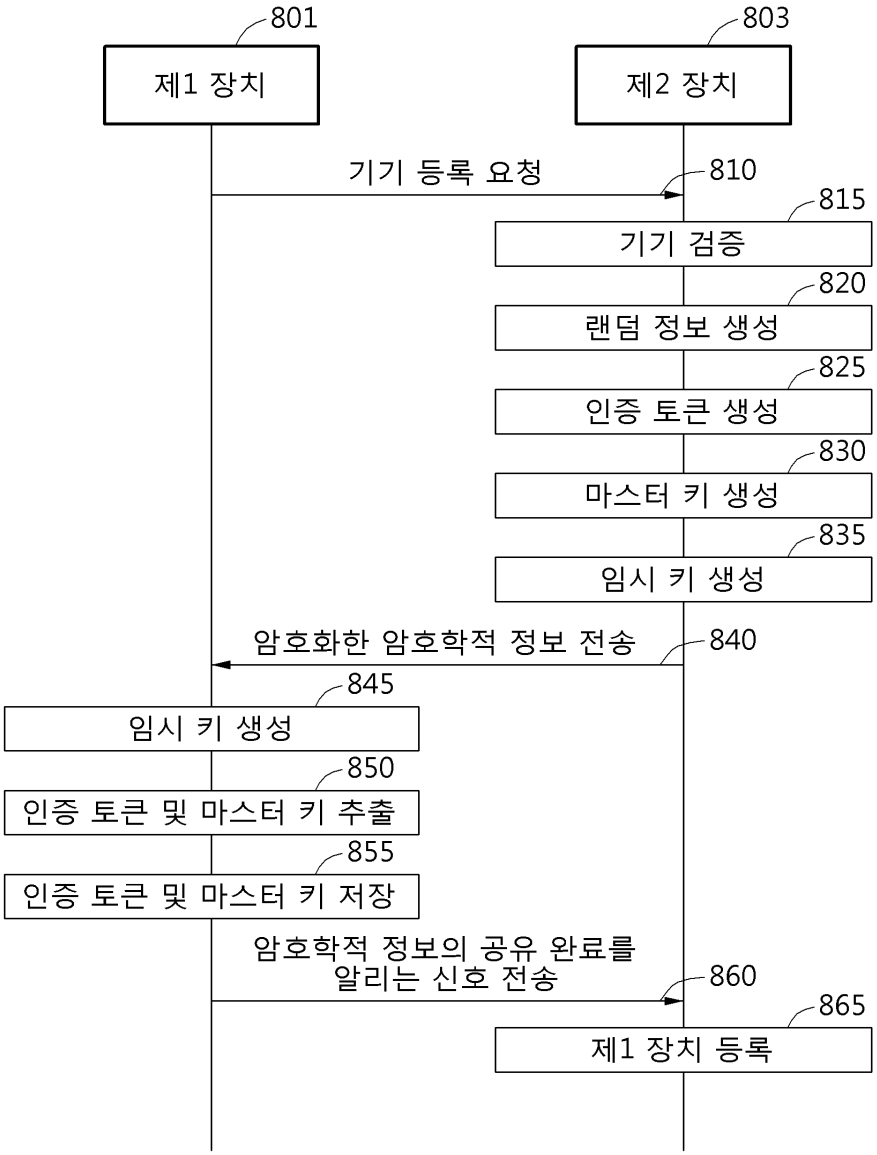
도면6


시 작
605
마스터 키 및 인증 토큰을 공유
610
인증 요청
615
제2 장치로부터 전송된 제1 암호화된 인증 토큰을 수신
620
제2 세션 키를 이용하여 제1 암호화된 인증 토큰을 복호화
625
미리 공유된 인증 토큰을 제1 변조 알고리즘을 이용하여 제1 변조
630
제1 변조된 인증 토큰을 이용하여 복호화한 인증 토큰을 검증
635
검증 성공?
No
Yes
640
제1 장치를 위한 제2 변조 알고리즘에 기초하여 미리 공유된 인증 토큰을 제2 변조
645
제2 변조된 인증 토큰을 제2 세션 키를 이용하여 제2 암호화
650
제2 암호화된 인증 토큰을 제2 장치에게 전송
종 료

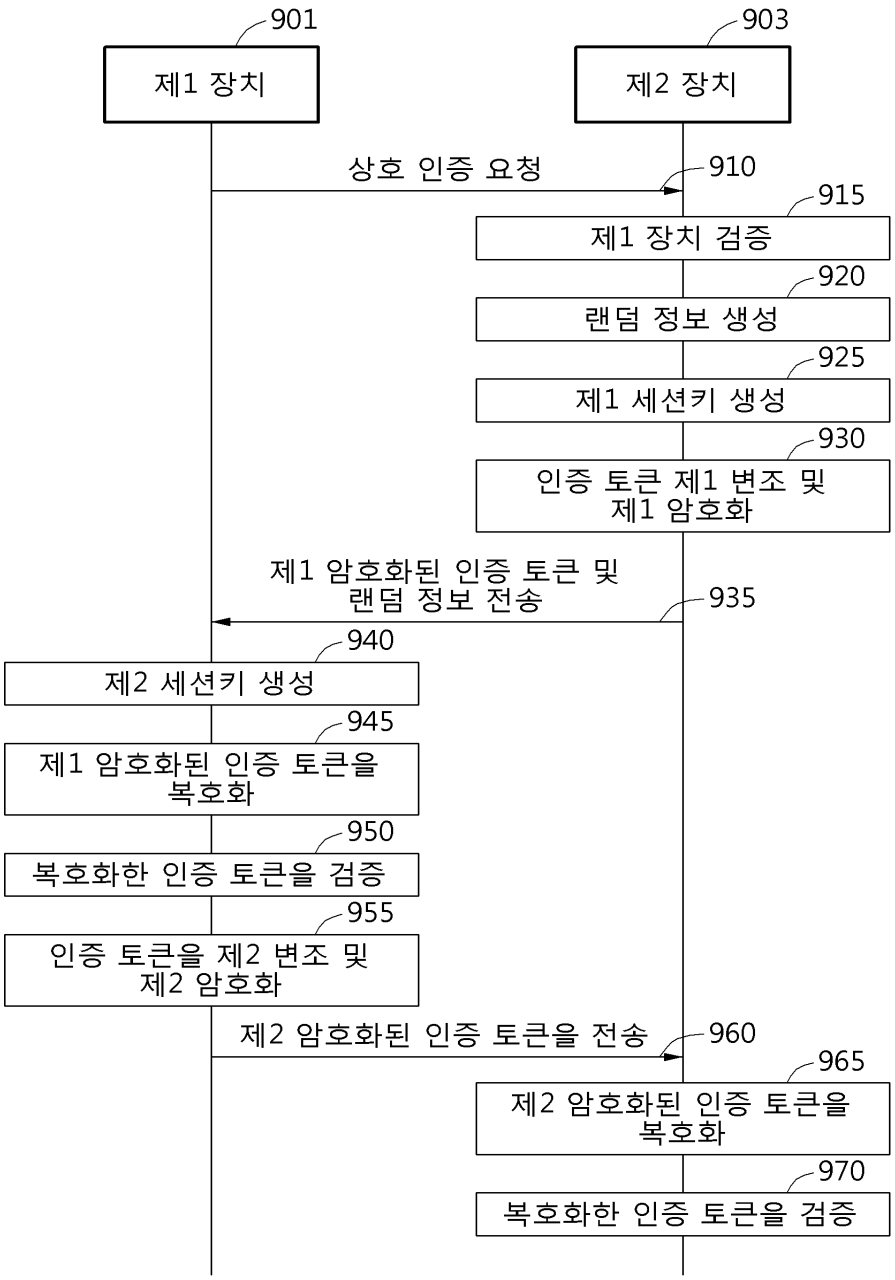
도면7


605
시 작
710
제2 장치에게 등록을 요청
720
등록 요청에 응답하여,
제2 장치에서 암호화된 암호학적 정보를 수신
730
암호학적 정보를 복호화하여 마스터 키 및 인증 토큰을 추출
740
마스터 키 및 인증 토큰을 저장
750
제2 장치에게 암호학적 정보의 공유가 완료되었음을 알리는
신호를 전송
종 료

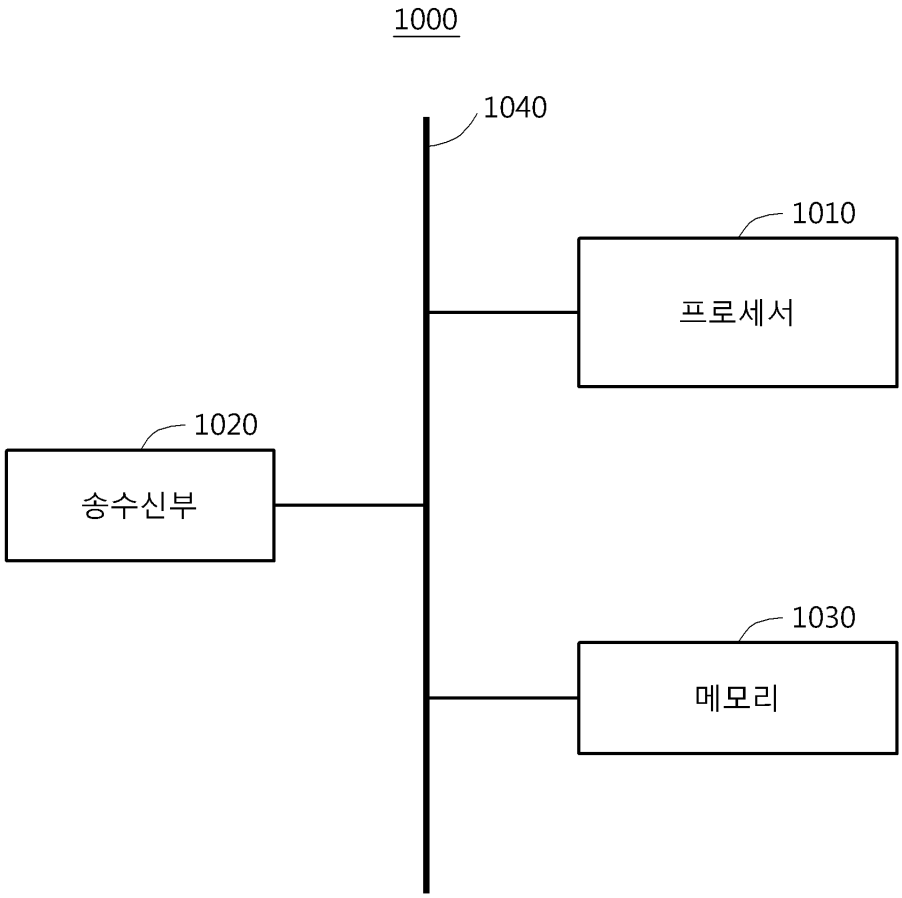
도면8


801
제1 장치
803
제2 장치
기기 등록 요청
810
815
기기 검증
820
랜덤 정보 생성
825
인증 토큰 생성
830
마스터 키 생성
835
임시 키 생성
암호화한 암호학적 정보 전송
840
845
임시 키 생성
850
인증 토큰 및 마스터 키 추출
855
인증 토큰 및 마스터 키 저장
암호학적 정보의 공유 완료를
알리는 신호 전송
860
865
제1 장치 등록

도면9


901
제1 장치
903
제2 장치
상호 인증 요청
910
915
제1 장치 검증
920
랜덤 정보 생성
925
제1 세션키 생성
930
인증 토큰 제1 변조 및
제1 암호화
제1 암호화된 인증 토큰 및
랜덤 정보 전송
935
940
제2 세션키 생성
945
제1 암호화된 인증 토큰을
복호화
950
복호화한 인증 토큰을 검증
955
인증 토큰을 제2 변조 및
제2 암호화
제2 암호화된 인증 토큰을 전송
960
965
제2 암호화된 인증 토큰을
복호화
970
복호화한 인증 토큰을 검증

도면10



도면11