(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2008년09월26일
(11) 등록번호 10-0860404
(24) 등록일자 2008년09월19일

(51) Int. Cl.
H04L 9/00 (2006.01) *H04L 12/66* (2006.01)
(21) 출원번호 10-2006-0095009
(22) 출원일자 2006년09월28일
심사청구일자 2006년09월28일
(65) 공개번호 10-2008-0001574
(43) 공개일자 2008년01월03일
(30) 우선권주장
1020060059844 2006년06월29일 대한민국(KR)
(56) 선행기술조사문헌
KR1020050084822 A
(뒷면에 계속)
전체 청구항 수 : 총 21 항

(73) 특허권자
한국전자통신연구원
대전 유성구 가정동 161번지
(72) 발명자
이윤경
대전 유성구 송강동 한마을아파트 114동 702호
황진범
대전 유성구 가정동 236-1번지 한국전자통신연구원 기숙사
(뒷면에 계속)
(74) 대리인
특허법인 씨엔에스 · 로고스

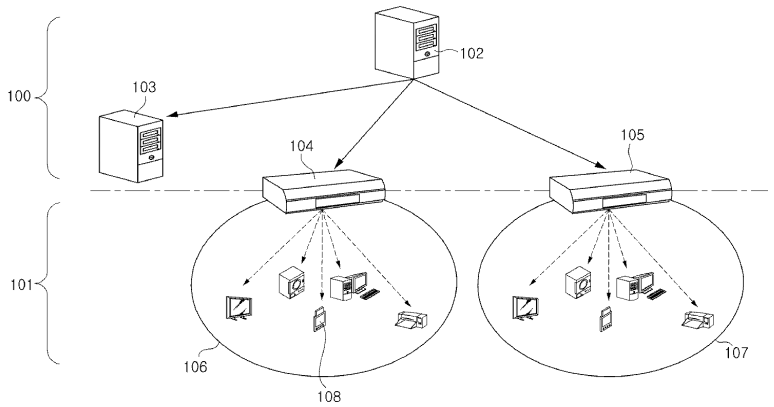
심사관 : 양종필

(54) 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법 및장치

(57) 요 약

본 발명은 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법 및 장치에 관한 것으로서, 각 로컬 도메인별로 해당 로컬 도메인의 홈 게이트웨이가 루트 CA로서 동작하여 디바이스별로 로컬 도메인 인증서를 발급하고, 다른 로컬 도메인에 등록된 디바이스를 인증할 수 있도록 로컬 도메인간에 협약을 수행하여 공개키 및 크로스 도메인 인증서를 발급하며, 디바이스로부터 서비스 요청시 해당 홈게이트웨이가 상기 로컬 도메인 인증서 및 크로스 도메인 인증서를 이용하여 로컬 도메인 내부의 통신만으로 상기 디바이스를 인증하도록 하여, 사용자의 개입을 최소화하여 비전문가도 쉽게 사용할 수 있도록 하고, 성능이 낮은 디바이스를 고려하여 인증을 위한 디바이스 연산을 최소화하며, 쉽게 확장가능하도록 한다.

대 표 도



(72) 발명자

이형규

대전 유성구 송강동 한마을아파트 110-1407

김건우

대전 유성구 지족동 열매마을 201동 1402호

김도우

대전 유성구 가정동 236-1번지

한종욱

대전 서구 월평2동 무지개아파트 105동 603호

정교일

대전 유성구 신성동 삼성한울아파트 107-1102

(56) 선행기술조사문헌

US20020120844 A1

KR1020050032324 A

KR1020060092558 A

이만영 외 2명, 인터넷 보안 기술, pp.159-162, 생능출판사 (2002.08.25.)*

*는 심사관에 의하여 인용된 문헌

특허청구의 범위

청구항 1

다수의 로컬 도메인으로 이루어지는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법에 있어서, 각 로컬 도메인에 속하는 제1 홈 게이트웨이가

다른 로컬 도메인에 속하는 제2 홈게이트웨이에 등록된 제2 디바이스의 인증을 위하여, 제3의 인증기관이 홈게이트웨이들의 글로벌 인증서를 발급 및 검증하는 제1 공개키 기반 인증 계층을 통해 상기 제2 홈게이트웨이와 상호 인증한 후, 상기 인증된 제2 홈게이트웨이로부터 연동협약을 증명하는 크로스 도메인 인증서를 발급받아, 상기 제2 홈게이트웨이의 공개키와 함께 저장하는 연동협약단계;

등록을 요청한 제1 디바이스에 대하여, 상기 제1 홈게이트웨이가 최상위 인증기관(root CA)으로 동작하여 디바이스를 인증하는 제2 공개키 기반 인증 계층에서 상기 제1 디바이스를 인증할 로컬 도메인 인증서를 발급하여, 상기 제1 홈게이트웨이의 공개키와 함께 상기 제1 디바이스로 제공하는 디바이스등록단계;

상기 디바이스 등록단계를 통해 등록된 상기 제1 디바이스로부터 서비스 요청이 수신되면, 상기 제1 디바이스의 로컬 도메인 인증서를 검증하고, 검증결과 유효하면 상기 제1 디바이스의 세션키를 발급하여 상기 제1 홈게이트웨이의 서명과 함께 상기 제1 디바이스로 제공하는 제1 디바이스 인증단계; 및

상기 제2 디바이스로부터 서비스 요청이 수신되면, 상기 제2 디바이스의 로컬 도메인 인증서를 상기 저장된 제2 홈게이트웨이의 공개키로 검증하고, 상기 검증 결과가 유효하면, 상기 제2 디바이스의 세션키를 발급하여, 상기 제1 홈게이트웨이의 서명 및 상기 제2 홈게이트웨이로부터 발급받은 크로스 도메인 인증서와 함께 상기 제2 디바이스로 제공하는 제2 디바이스 인증단계를 포함하는 것을 특징으로 하는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법.

청구항 2

삭제

청구항 3

삭제

청구항 4

제1항에 있어서,

상기 연동 협약 단계는, 상기 제2 디바이스로부터 서비스 요청을 받은 경우에 수행되도록 하는 것을 특징으로 하는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법.

청구항 5

제1항에 있어서, 상기 디바이스 등록 단계는

상기 제1 디바이스가 정상적인 디바이스인지를 검증하는 과정을 더 포함하고,

검증된 디바이스에 대해서만 로컬 도메인 인증서를 발급하는 것을 특징으로 하는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법.

청구항 6

제5항에 있어서, 상기 정상적인 디바이스인지를 검증하는 과정은

상기 제1 디바이스로 제1의 랜덤값을 생성하여 전달하는 과정과,

상기 제1 디바이스로부터 상기 제1의 랜덤값과, 디바이스 식별정보와, 디바이스에서 생성된 제2의 랜덤값과, 상

기 제1 디바이스의 비대칭키쌍중 공개키를 상기 제1 디바이스의 대칭키 방식의 제1비밀키로 해쉬연산한 해쉬값을 수신하는 과정과,

상기 제1 디바이스로부터 수신한 해쉬값을 상기 제1 디바이스의 제1비밀키를 공유하는 서버로 전송하여, 검증결과를 제공받는 과정을 포함하는 것을 특징으로 하는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법.

청구항 7

제6항에 있어서, 상기 정상적인 디바이스인지를 검증하는 과정은

상기 제1 디바이스에 대하여 제공되어 상기 서버와 공유하고 있는 비밀정보를 사용자로부터 입력받는 과정과,

상기 비밀정보와 상기 제1,2 랜덤값을 함께 해쉬하여 상기 제1홈게이트웨이의 비밀키로 서명한 메시지를 상기 서버로 더 전송하는 과정을 더 포함하는 것을 특징으로 하는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법.

청구항 8

제6항 또는 제7항에 있어서, 상기 정상적인 디바이스인지를 검증하는 과정은,

상기 서버로부터 검증 결과로서, 상기 제1 홈게이트웨이의 공개키와 상기 제2 랜덤값을 상기 제1 디바이스의 제1 비밀키로 해쉬한 메시지와, 디바이스 정보와, 상기 디바이스 정보와 상기 제1 랜덤값을 서버의 비밀키로 서명한 메시지와, 상기 서버의 글로벌 인증서를 수신하는 과정을 더 포함하는 것을 특징으로 하는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법.

청구항 9

제8항에 있어서, 상기 디바이스 등록 단계는

제1 공개키 기반 인증 계층을 통해 상기 서버의 글로벌 인증서 및 서명을 검증하여, 유효한 경우, 상기 로컬 도메인 인증서를 발급하고, 상기 서버로부터 수신한 상기 제1 홈게이트웨이의 공개키와 상기 제2 랜덤값을 상기 제1 디바이스의 제1 비밀키로 해쉬한 메시지와, 디바이스 정보와, 상기 발급된 로컬 도메인 인증서를 상기 제1 디바이스로 전송하는 과정을 더 포함하는 것을 특징으로 하는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법.

청구항 10

제1항에 있어서, 상기 제1 디바이스 인증 단계는

상기 제1 디바이스로 제1 랜덤값을 전송하는 과정과,

상기 제1 디바이스에서 생성된 제2의 랜덤값과, 상기 제1 디바이스의 로컬 도메인 인증서와, 상기 제1 랜덤값을 상기 제1 디바이스의 비대칭키쌍중 하나인 제2 비밀키로 서명한 값을 상기 제1 디바이스로부터 수신하는 과정과,

상기 로컬 도메인 인증서를 검증하여 유효하면, 상기 로컬 도메인 인증서에서 획득한 상기 제1 디바이스의 공개키로 상기 서명을 검증하는 과정과,

상기 서명이 유효한 경우, 상기 제1 디바이스와 공유할 세션키를 생성하고, 상기 세션키를 상기 제1 디바이스의 공개키로 암호화한 메시지와, 상기 세션키와 상기 제2 랜덤값을 상기 제1 홈 게이트웨이의 비밀키로 서명한 메시지를 상기 제1 디바이스로 전송하는 과정을 포함하는 것을 특징으로 하는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법.

청구항 11

제1항에 있어서, 상기 제2 디바이스 인증 단계는

상기 제2 디바이스로 제1 랜덤값을 전송하는 과정과,

상기 제2 디바이스에서 생성된 제2의 랜덤값과, 상기 제2 디바이스의 로컬 도메인 인증서와, 상기 제1 랜덤값을 상기 제2 디바이스의 비대칭키쌍중 하나인 제2 비밀키로 서명한 값을 상기 제2 디바이스로부터 수신하는 과정과,

상기 제2 홈게이트웨이의 공개키를 이용하여 상기 제2 디바이스의 로컬 도메인 인증서를 검증하고, 상기 제2 디바이스의 서명을 검증하는 과정과,

상기 검증 결과 유효한 경우, 상기 제2 디바이스와 공유한 세션 키를 생성하고, 상기 세션키를 상기 제2 디바이스의 공개키로 암호화한 메시지와, 상기 세션키와 상기 제2 랜덤값을 상기 제1 홈게이트웨이의 비밀키로 서명한 메시지와, 상기 제2 홈게이트웨이로부터 발급받은 상기 크로스 도메인 인증서를 상기 제2 디바이스로 전송하는 과정을 더 포함하는 것을 특징으로 하는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법.

청구항 12

다수의 로컬 도메인으로 이루어지는 다중 도메인 홈네트워크 환경에서, 각 로컬 도메인에 속한 제1 홈게이트웨이에 구비되는 디바이스 인증 장치에 있어서,

다른 로컬 도메인에 등록된 방문 디바이스의 인증을 위하여 상기 다른 로컬 도메인에 속한 제2 홈게이트웨이와 제1 공개키 기반 인증 계층을 통해 상호 인증한 후, 인증이 성공하면 공개키 및 협약사실을 증명하기 위한 크로스 도메인 인증서를 교환하는 크로스 도메인 인증 수단;

등록을 요청한 디바이스에 대하여 상기 디바이스를 검증하여 상기 제1 홈 게이트웨이가 최상위 인증기관이 되는 제2 공개키 기반 인증 계층에서 디바이스 인증을 위해 사용할 로컬 도메인 인증서를 발급하는 디바이스 등록 수단; 및

서비스 요청한 디바이스로부터 로컬 도메인 인증서를 수신받아, 상기 수신된 로컬 도메인 인증서를 상기 제1 홈게이트웨이의 공개키 또는 상기 크로스 도메인 인증 수단에서 획득한 상기 제2 홈게이트웨이의 공개키로 검증하여, 상기 로컬 도메인 인증서가 유효하면 상기 서비스 요청한 디바이스와 공유할 세션키를 생성하여 상기 서비스 요청한 디바이스에 제공하는 디바이스 검증 수단을 포함하는 것을 특징으로 하는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 장치.

청구항 13

제12항에 있어서, 상기 크로스 도메인 인증 수단은

제1 공개키 기반 인증 계층에 의해 제3 인증 기관으로부터 상기 제1,2홈게이트웨이에 대해 발급된 글로벌 인증서로 상호 인증을 수행하고, 상기 상호 인증이 성공하면 연동 협약을 증명할 상기 크로스 도메인 인증서를 상기 제2 홈게이트웨이로 발급하거나, 상기 제2 홈게이트웨이로부터 발급된 크로스 도메인 인증서를 전달받아 저장하는 것을 특징으로 하는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 장치.

청구항 14

제13항에 있어서,

상기 크로스 도메인 인증 수단은, 상기 디바이스 검증 수단에서 서비스 요청된 디바이스의 로컬 도메인 인증서가 상기 제1 홈게이트웨이의 공개키로 검증할 수 없는 경우, 상기 디바이스 검증 수단의 요청에 의해 상기 로컬 도메인 인증서에 기록된 홈 로컬 도메인의 제2 홈게이트웨이를 확인하여, 상기 제2 홈게이트웨이로 연동 협약을 요청하는 것을 특징으로 하는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 장치.

청구항 15

제12항에 있어서,

상기 디바이스 등록 수단은,

등록 요청한 디바이스로 제1의 랜덤값을 생성하여 전달하고, 상기 등록 요청한 디바이스로부터 검증 정보로서, 상기 제1의 랜덤값과, 디바이스 식별정보와, 디바이스에서 생성된 제2의 랜덤값과, 디바이스의 공개키중에서 하나 이상을 대칭키인 디바이스의 제1 비밀키로 해쉬한 값을 수신하여, 상기 수신한 해쉬값을 상기 등록 요청한 디바이스와 상기 제1 비밀키를 공유하는 서버로 전송하여 검증받는 것을 특징으로 하는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 장치.

청구항 16

제15항에 있어서, 상기 디바이스 등록 수단은,

등록할 디바이스에 대하여 제공되어 상기 서버와 공유하고 있는 비밀정보가 입력되면, 상기 비밀정보와 상기 제1,2 랜덤값을 함께 제1 홈게이트웨이의 비밀키로 서명한 메시지를 상기 서버로 더 전송하여 검증받는 것을 특징으로 하는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 장치.

청구항 17

다수의 로컬 도메인으로 이루어지는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법에 있어서, 서버가

디바이스별로 부여된 대칭키방식의 제1비밀키 및 비밀정보를 공유하여 보관하는 단계;

홈게이트웨이로부터 등록할 디바이스에 대한 검증을 요청받는 단계;

제1 공개키 기반 인증 계층에 의해 제3 인증기관으로부터 발급된 글로벌 인증서를 이용하여 상기 홈게이트웨이를 검증하는 단계;

상기 홈게이트웨이의 글로벌 인증서가 유효하면, 상기 보관하고 있는 제1 비밀키 및 비밀 정보를 이용하여 상기 디바이스를 검증하는 단계; 및

상기 디바이스의 검증 결과를 상기 홈게이트웨이로 전송하는 단계를 포함하는 것을 특징으로 하는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법.

청구항 18

제17항에 있어서,

상기 홈게이트웨이로부터 등록할 디바이스에 대한 검증을 요청받는 단계는,

상기 디바이스의 식별정보와, 상기 디바이스의 공개키와, 홈게이트웨이에 의해 생성된 제1 랜덤값과, 상기 디바이스에서 생성된 제2 랜덤값중에서 하나 이상을 상기 디바이스의 제1 비밀키로 해쉬한 메시지와, 홈게이트웨이가 획득한 디바이스의 비밀정보와 상기 제1,2랜덤값을 함께 상기 홈게이트웨이의 비밀키로 서명한 메시지와, 상기 홈게이트웨이의 글로벌 인증서를 함께 전달받는 것을 특징으로 하는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법.

청구항 19

제18항에 있어서, 상기 보관하고 있는 제1 비밀키 및 비밀 정보를 이용하여 상기 디바이스를 검증하는 단계는,

상기 제1 비밀키를 이용하여, 상기 해쉬한 메시지를 검증하는 과정과,

상기 홈게이트웨이의 글로벌 인증서를 검증한 후, 글로벌 인증서에서 확인된 홈게이트웨이의 공개키로 상기 서명한 메시지를 검증하는 과정과,

상기 해쉬한 메시지 및 상기 서명의 검증 결과가 모두 유효하면, 해당 디바이스가 유효함을 나타내는 검증 결과를 전송하는 과정을 포함하는 것을 특징으로 하는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법.

청구항 20

제19항에 있어서,

상기 검증 결과는, 상기 홈게이트웨이의 공개키와 제2 랜덤값을 상기 디바이스의 제1 비밀키로 해쉬연산한 메시지와, 상기 디바이스 정보와, 상기 디바이스 정보와 제1랜덤값을 서버의 공개키로 암호화한 메시지와, 제1 공개키 기반 인증 계층에서 발급된 상기 서버의 글로벌 인증서 중에서 하나 이상을 포함하는 것을 특징으로 하는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법.

청구항 21

다수의 로컬 도메인으로 이루어지는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법에 있어서, 상기 디바이스가

디바이스별로 제조단계에서 부여된 대칭키방식의 제1 비밀키를 보유하는 단계;

홈 로컬 도메인에 속하는 제1 홈게이트웨이로 등록을 요청하는 단계;

상기 제1 홈 게이트웨이로부터 재전송 공격 방지를 위한 제1 랜덤값을 수신하는 단계;

상기 제1 랜덤값과, 디바이스의 식별정보와, 상기 디바이스가 생성한 제2 랜덤값과, 공개키 중에서 하나 이상을 상기 제1 비밀키로 해쉬한 값을 상기 제1 홈게이트웨이로 제공하는 단계;

상기 제1 홈 게이트웨이로부터, 상기 제1 홈 게이트웨이의 공개키와 제2 랜덤값을 상기 제1 비밀키로 해쉬한 메시지와, 제1 홈 게이트웨이에서 발급된 상기 홈 로컬 도메인에서 사용가능한 로컬 도메인 인증서를 포함한 검증결과를 수신하는 단계; 및

상기 수신된 해쉬 메시지를 상기 보유한 제1 비밀키로 검증하여, 유효한 경우 상기 제1 홈게이트웨이의 공개키를 자신의 최상위 인증 기관의 공개키로 설정하고, 상기 로컬 도메인 인증서를 저장하는 단계를 포함하는 것을 특징으로 하는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법.

청구항 22

제21항에 있어서,

상기 제1 홈 게이트웨이로 서비스 요청 메시지를 전송하는 단계;

상기 제1 홈게이트웨이로부터 제3 랜덤값을 수신하는 단계;

서비스 요청을 위한 디바이스의 인증 정보로서, 상기 제1 홈게이트웨이에서 생성된 제3의 랜덤값을 상기 디바이스의 비대칭키방식의 제2 비밀키로 서명한 메시지와, 상기 저장한 로컬 도메인 인증서와, 상기 디바이스에서 생성한 제4의 랜덤값을 제1 홈 게이트웨이에 제공하는 단계;

상기 디바이스의 인증 정보를 통해 상기 디바이스를 인증한 제1 홈 게이트웨이로부터 생성된 디바이스와 제1 홈게이트웨이간의 세션키를 상기 디바이스의 공개키로 암호화한 메시지와, 상기 세션키와 상기 제4의 랜덤값을 제1 홈게이트웨이의 비밀키로 서명한 메시지를 수신하는 단계; 및

상기 제1 홈게이트웨이의 비밀키로 서명한 메시지를 상기 제1 홈게이트웨이의 공개키로 검증하여 유효하면, 상기 암호화한 메시지를 상기 디바이스의 제2 비밀키로 복호화하여, 세션키를 획득하는 단계를 더 포함하는 것을 특징으로 하는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법.

청구항 23

제21항에 있어서,

디바이스가 등록한 홈 로컬 도메인이 아닌 다른 로컬 도메인에 속하는 제2 홈 게이트웨이로 서비스 요청 메시지를 전송하는 단계;

상기 제2 홈게이트웨이로부터 제3 랜덤값을 수신하는 단계;

서비스 요청을 위한 디바이스의 인증 정보로서, 상기 제3의 랜덤값을 상기 디바이스의 비대칭키방식의 제2 비밀키로 서명한 메시지와, 상기 저장한 로컬 도메인 인증서와, 상기 디바이스가 생성한 제4의 랜덤값을 상기 제2 홈 게이트웨이에 제공하는 단계;

상기 디바이스의 인증 정보를 통해 디바이스를 인증한 제2 홈 게이트웨이로부터 세션키를 상기 디바이스의 공개키로 암호화한 메시지와, 상기 세션키와 상기 제4의 랜덤값을 제2 홈게이트웨이의 비밀키로 서명한 메시지와,

상기 제2 홈게이트웨이가 상기 제1 홈게이트웨이로부터 받은 크로스 도메인 인증서를 수신하는 단계; 및

상기 크로스 도메인 인증서와 서명을 검증하고, 상기 크로스 도메인 인증서와 서명이 유효하면, 상기 암호화한 메시지를 상기 제2 비밀키로 복호화하여, 세션키를 획득하는 단계를 더 포함하는 것을 특징으로 하는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<15> 본 발명은 다중 도메인 홈 네트워크 환경에서의 디바이스 인증 방법 및 장치에 관한 것으로서, 특히 사용자의 개입을 최소화하고 디바이스 내 연산을 최소화할 수 있는 다중 도메인 홈 네트워크 환경에서의 디바이스 인증 방법 및 장치에 관한 것이다.

<16> 일반적인 디바이스 인증 방법으로는, 크게 대칭키를 사용하는 방법과, 공개키 기반 구조(PKI: Public Key Infrastructure)를 사용하는 방법, 두 가지가 알려져 있다.

<17> 대칭키를 사용하는 방법은, 두 디바이스가 동일한 키를 나눠 가진 후에 각각이 상대방의 공유키를 가지고 있다는 것을 확인하여 서로를 인증하는 방법이다. 이 경우, 통신하고자 하는 디바이스 간에 키를 공유하는 데에 많은 관리적 어려움이 있으며, 디바이스의 수가 늘어날수록 공유해야 하는 키의 수가 많아지므로 확장에 어려움이 있다.

<18> PKI를 사용하는 방법은 키의 관리가 쉽고 전역적인 구조로 로컬 도메인의 구별 없이 사용이 가능하지만, 소유자가 자신의 디바이스에 대한 인증서 발급을 제 3 자에게 위임하여야 하고, 모든 인증서 발급 권한이 최상위 인증기관(root certification authority, 이하 루트 CA라 한다)에 집중되므로 디바이스의 숫자가 늘어날수록 하위 CA를 늘려야 하고, 인증서 효력 정지 및 폐지 목록 (Certificate Revocation List, CRL)의 크기가 커지기 때문에 이에 대한 관리비용이 늘어나게 된다. 또한, 컴퓨팅 능력이 낮은 디바이스 간에 인증을 수행할 경우에는 인증서의 패스를 구축하고 검증하는 무거운 방식을 수용할 수 없는 경우가 있다. 이러한 PKI의 문제점을 해결하기 위해 제안된 사설 인증 방식이나 SPKI와 같은 로컬인증 방식의 경우 PKI의 단점을 보완할 수는 있지만, 그 반면에 디바이스마다 각 로컬 도메인의 인증서를 발급받아야 하므로 디바이스를 관리하는 사용자에게 많은 불편을 주게 된다.

발명이 이루고자 하는 기술적 과제

<19> 이에 본 발명은 상기와 같은 종래의 문제점을 해결하기 위하여 제안된 것으로서, 제1 목적은 사용자의 개입을 최소화하여 비전문가도 쉽게 사용할 수 있는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법 및 장치를 제공하는 것이다.

<20> 또한, 본 발명의 제2 목적은, 성능이 낮은 디바이스를 고려하여 인증을 위한 디바이스 연산을 최소화한 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법 및 장치를 제공하는 것이다.

<21> 또한, 본 발명의 제3 목적은, 디바이스의 수가 늘어나도 쉽게 확장가능한 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법 및 장치를 제공하는 것이다.

발명의 구성 및 작용

<22> 상술한 본 발명의 목적을 달성하기 위한 기술적인 수단으로서, 다수의 로컬 도메인으로 이루어지는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법에 있어서, 각 로컬 도메인에 속하는 제1 홈 게이트웨이가

<23> 다른 로컬 도메인에 속하는 제2 홈게이트웨이에 등록된 제2 디바이스의 인증을 위하여, 제3의 인증기관이 홈게이트웨이들의 글로벌 인증서를 발급 및 검증하는 제1 공개키 기반 인증 계층을 통해 상기 제2 홈게이트웨이와 상호 인증한 후, 상기 인증된 제2 홈게이트웨이로부터 연동협약을 증명하는 크로스 도메인 인증서를 발급받아, 상기 제2 홈게이트웨이의 공개키와 함께 저장하는 연동협약단계;

<24> 등록을 요청한 제1 디바이스에 대하여, 상기 제1 홈게이트웨이가 최상위 인증기관(root CA)으로 동작하여 디바이스를 인증하는 제2 공개키 기반 인증 계층에서 상기 제1 디바이스를 인증할 로컬 도메인 인증서를 발급하여, 상기 제1 홈게이트웨이의 공개키와 함께 상기 제1 디바이스로 제공하는 디바이스등록단계;

<25> 상기 디바이스 등록단계를 통해 등록된 상기 제1 디바이스로부터 서비스 요청이 수신되면, 상기 제1 디바이스의 로컬 도메인 인증서를 검증하고, 검증결과 유효하면 상기 제1 디바이스의 세션키를 발급하여 상기 제1 홈게이트웨이의 서명과 함께 상기 제1 디바이스로 제공하는 제1 디바이스 인증단계; 및

상기 제2 디바이스로부터 서비스 요청이 수신되면, 상기 제2 디바이스의 로컬 도메인 인증서를 상기 저장된 제2 홈게이트웨이의 공개키로 검증하고, 상기 검증 결과가 유효하면, 상기 제2 디바이스의 세션키를 발급하여, 상기 제1 홈게이트웨이의 서명 및 상기 제2 홈게이트웨이로부터 발급받은 크로스 도메인 인증서와 함께 상기 제2 디바이스로 제공하는 제2 디바이스 인증단계를 포함하는 것을 특징으로 한다.

<26> 삭제

<27> 바람직하게, 상기 정상적인 디바이스인지를 검증하는 과정은, 상기 제1 디바이스로 제1의 랜덤값을 생성하여 전달하는 과정과, 상기 제1 디바이스로부터 상기 제1의 랜덤값과, 디바이스 식별정보와, 디바이스에서 생성된 제2의 랜덤값과, 상기 제1 디바이스의 비대칭키쌍중 공개키를 상기 제1 디바이스의 대칭키 방식의 제1비밀키로 해쉬연산한 해쉬값을 수신하는 과정과, 상기 제1 디바이스로부터 수신한 해쉬값을 상기 제1 디바이스의 제1비밀키를 공유하는 서버로 전송하여, 검증결과를 제공받는 과정을 포함하는 것을 특징으로 한다.

<28> 바람직하게, 상기 제1 디바이스 인증 단계는, 상기 제1 디바이스로 제1 랜덤값을 전송하는 과정과, 상기 제1 디바이스에서 생성된 제2의 랜덤값과, 상기 제1 디바이스의 로컬 도메인 인증서와, 상기 제1 랜덤값을 상기 제1 디바이스의 비대칭키쌍중 하나인 제2 비밀키로 서명한 값을 상기 제1 디바이스로부터 수신하는 과정과, 상기 로컬 도메인 인증서를 검증하여 유효하면, 상기 로컬 도메인 인증서에서 획득한 상기 제1 디바이스의 공개키로 상기 서명을 검증하는 과정과, 상기 서명이 유효한 경우, 상기 제1 디바이스와 공유할 세션키를 생성하고, 상기 세션키를 상기 제1 디바이스의 공개키로 암호화한 메시지와, 상기 세션키와 상기 제2 랜덤값을 상기 제1 홈 게이트웨이의 비밀키로 서명한 메시지를 상기 제1 디바이스로 전송하는 과정을 포함하는 것을 특징으로 한다.

<29> 더하여, 상기 제2 디바이스 인증 단계는, 상기 제2 디바이스로 제1 랜덤값을 전송하는 과정과, 상기 제2 디바이스에서 생성된 제2의 랜덤값과, 상기 제2 디바이스의 로컬 도메인 인증서와, 상기 제1 랜덤값을 상기 제2 디바이스의 비대칭키쌍중 하나인 제2 비밀키로 서명한 값을 상기 제2 디바이스로부터 수신하는 과정과, 상기 제2 홈게이트웨이의 공개키를 이용하여 상기 제2 디바이스의 로컬 도메인 인증서를 검증하고, 상기 제2 디바이스의 서명을 검증하는 과정과, 상기 검증 결과 유효한 경우, 상기 제2 디바이스와 공유한 세션 키를 생성하고, 상기 세션키를 상기 제2 디바이스의 공개키로 암호화한 메시지와, 상기 세션키와 상기 제2 랜덤값을 상기 제1 홈게이트웨이의 비밀키로 서명한 메시지와, 상기 제2 홈게이트웨이로부터 발급받은 상기 크로스 도메인 인증서를 상기 제2 디바이스로 전송하는 과정을 더 포함한다.

<30> 더하여, 본 발명은 상기 목적을 달성하기 위한 다른 구성 수단으로서, 다수의 로컬 도메인으로 이루어지는 다중 도메인 홈네트워크 환경에서, 각 로컬 도메인에 속한 제1 홈게이트웨이에 구비되는 디바이스 인증 장치에 있어서, 다른 로컬 도메인에 등록된 방문 디바이스의 인증을 위하여 상기 다른 로컬 도메인에 속한 제2 홈게이트웨이와 제1 공개키 기반 인증 계층을 통해 상호 인증한 후, 인증이 성공하면 공개키 및 협약사실을 증명하기 위한 크로스 도메인 인증서를 교환하는 크로스 도메인 인증 수단; 등록을 요청한 디바이스에 대하여 상기 디바이스를 검증하여 상기 제1 홈 게이트웨이가 최상위 인증기관이 되는 제2 공개키 기반 인증 계층에서 디바이스 인증을 위해 사용할 로컬 도메인 인증서를 발급하는 디바이스 등록 수단; 및 서비스 요청한 디바이스로부터 로컬 도메인 인증서를 수신받아, 상기 수신된 로컬 도메인 인증서를 상기 제1 홈게이트웨이의 공개키 또는 상기 크로스 도메인 인증 수단에서 획득한 상기 제2 홈게이트웨이의 공개키로 검증하여, 상기 로컬 도메인 인증서가 유효하면 상기 서비스 요청한 디바이스와 공유할 세션키를 생성하여 상기 서비스 요청한 디바이스에 제공하는 디바이스 검증 수단을 포함하는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 장치를 제공한다.

<31> 또한, 본 발명은 상기 목적을 이루기 위한 또 다른 구성 수단으로서, 다수의 로컬 도메인으로 이루어지는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법에 있어서, 서버가, 디바이스별로 부여된 대칭키방식의 제1비밀키 및 비밀정보를 공유하여 보관하는 단계; 홈게이트웨이로부터 등록할 디바이스에 대한 검증을 요청받는 단계; 제1 공개키 기반 인증 계층에 의해 제3 인증기관으로부터 발급된 글로벌 인증서를 이용하여 상기 홈게이트

웨이를 검증하는 단계; 상기 홈게이트웨이의 글로벌 인증서가 유효하면, 상기 보관하고 있는 제1 비밀키 및 비밀 정보를 이용하여 상기 디바이스를 검증하는 단계; 및 상기 디바이스의 검증 결과를 상기 홈게이트웨이로 전송하는 단계를 포함하는 것을 특징으로 하는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법을 제공한다.

<32> 또한, 본 발명은 상기 목적을 이루기 위한 또 다른 구성 수단으로서, 다수의 로컬 도메인으로 이루어지는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법에 있어서, 상기 디바이스가, 디바이스별로 제조단계에서 부여된 대칭키방식의 제1 비밀키를 보유하는 단계; 홈 로컬 도메인에 속하는 제1 홈게이트웨이로 등록을 요청하는 단계; 상기 제1 홈 게이트웨이로부터 재전송 공격 방지를 위한 제1 랜덤값을 수신하는 단계; 상기 제1 랜덤값과, 디바이스의 식별정보와, 상기 디바이스가 생성한 제2 랜덤값과, 공개키 중에서 하나 이상을 상기 제1 비밀키로 해쉬한 값을 상기 제1 홈게이트웨이로 제공하는 단계; 상기 제1 홈 게이트웨이로부터, 상기 홈 게이트웨이의 공개키와 제2 랜덤값을 상기 제1 비밀키로 해쉬한 메시지와, 상기 제1 홈게이트웨이에서 발급된 상기 홈 로컬 도메인에서 사용가능한 로컬 도메인 인증서를 포함한 검증 결과를 수신하는 단계; 및 상기 수신된 해쉬 메시지를 상기 보유한 제1 비밀키로 검증하여, 유효한 경우 상기 제1 홈게이트웨이의 공개키를 자신의 최상위 인증 기관의 공개키로 설정하고, 상기 로컬 도메인 인증서를 저장하는 단계를 포함하는 것을 특징으로 하는 다중 도메인 홈네트워크 환경에서의 디바이스 인증 방법을 제공한다.

<33> 더하여, 상기 디바이스 인증 방법은, 상기 제1 홈 게이트웨이로 서비스 요청 메시지를 전송하는 단계; 상기 제1 홈게이트웨이로부터 제3 랜덤값을 수신하는 단계; 서비스 요청을 위한 디바이스의 인증 정보로서, 상기 제1 홈 게이트웨이에서 생성된 제3의 랜덤값을 상기 디바이스의 비대칭키방식의 제2 비밀키로 서명한 메시지와, 상기 저장한 로컬 도메인 인증서와, 상기 디바이스에서 생성한 제4의 랜덤값을 제1 홈 게이트웨이에 제공하는 단계; 상기 디바이스의 인증 정보를 통해 상기 디바이스를 인증한 제1 홈 게이트웨이로부터 생성된 디바이스와 제1 홈 게이트웨이간의 세션키를 상기 디바이스의 공개키로 암호화한 메시지와, 상기 세션키와 상기 제4의 랜덤값을 제1 홈게이트웨이의 비밀키로 서명한 메시지를 수신하는 단계; 및 상기 제1 홈게이트웨이의 비밀키로 서명한 메시지를 상기 제1 홈게이트웨이의 공개키로 검증하여 유효하면, 상기 암호화한 메시지를 상기 디바이스의 제2 비밀키로 복호화하여, 세션키를 획득하는 단계를 더 포함할 수 있다.

<34> 또한, 상기 디바이스 인증 방법은, 디바이스가 등록한 홈 로컬 도메인이 아닌 다른 로컬 도메인에 속하는 제2 홈 게이트웨이로 서비스 요청 메시지를 전송하는 단계; 상기 제2 홈게이트웨이로부터 제3 랜덤값을 수신하는 단계; 서비스 요청을 위한 디바이스의 인증 정보로서, 상기 제3의 랜덤값을 상기 디바이스의 비대칭키 방식의 제2 비밀키로 서명한 메시지와, 상기 저장한 로컬 도메인 인증서와, 상기 디바이스가 생성한 제4의 랜덤값을 상기 제2 홈 게이트웨이에 제공하는 단계; 상기 디바이스의 인증 정보를 통해 디바이스를 인증한 제2 홈 게이트웨이로부터 세션키를 상기 디바이스의 공개키로 암호화한 메시지와, 상기 세션키와 상기 제4의 랜덤값을 제2 홈게이트웨이의 비밀키로 서명한 메시지와, 상기 제2 홈게이트웨이가 상기 제1 홈게이트웨이로부터 받은 크로스 도메인 인증서를 수신하는 단계; 및 상기 크로스 도메인 인증서와 서명을 검증하고, 상기 크로스 도메인 인증서와 서명이 유효하면, 상기 암호화한 메시지를 상기 제2 비밀키로 복호화하여, 세션키를 획득하는 단계를 더 포함할 수 있다.

<35> 이하 첨부된 도면을 참조하여 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명을 용이하게 실시할 수 있는 바람직한 실시예를 상세히 설명한다. 다만, 본 발명의 바람직한 실시 예에 대한 동작 원리를 상세하게 설명함에 있어 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략한다.

<36> 또한, 도면 전체에 걸쳐 유사한 기능 및 작용을 하는 부분에 대해서는 동일한 도면 부호를 사용한다.

<37> 도 1은 본 발명에 의한 다중 도메인 홈네트워크 환경에서의 디바이스 인증 시스템의 구조도이다.

<38> 도 1에 있어서, 102는 제3의 인증 기관의 서버이고, 103은 홈네트워크에 접속하여 사용되는 디바이스를 제조하며 제조된 디바이스에 대하여 인증하는 제조사 서버이고, 104, 105는 댁내에 설치되어 댁내의 디바이스들 및 외부와의 접속을 중계하는 홈게이트웨이이고, 106, 107은 상기 홈게이트웨이(104,105)에 의해 구성되는 상호 독립된 홈네트워크 영역인 로컬 도메인이고, 108은 홈네트워크에 연결된 디바이스를 나타낸다.

<39> 상기 도 1을 참조하면, 본 발명에 의한 인증 시스템은, 기존의 공인 인증 체계에 따른 제1 공개키 기반 인증 계층(100)과, 홈 네트워크의 로컬 도메인 별로 구성되는 제2 공개키 기반 인증 계층(101)으로 나누어진다.

<40> 상기 제1 공개키 기반 인증 계층(100)은 기존의 인증 체계와 마찬가지로 제3의 인증 서버(102)가 루트 CA가 되

어 인증을 수행하는 계층으로서, 디바이스(108)를 홈게이트웨이(104,105)에 등록할 때에 해당 디바이스에 대한 디바이스 제조사의 서버(103)와 홈 게이트웨이(104,105) 간의 인증을 위해 사용되며, 또한 디바이스(108)가 상기 등록된 로컬 도메인(106)에서 다른 로컬 도메인(107)으로 이동하여 서비스를 요청할 때에, 두 로컬 도메인 간의 디바이스 인증 협약을 위하여 두 로컬 도메인의 홈게이트웨이(104,105)를 상호 인증하는데 사용된다. 이때, 로컬 도메인간의 상호 디바이스 인증을 위해서 홈게이트웨이(104,105) 간에 발급되는 인증서를 크로스 도메인 인증서라 한다.

<41> 상기 제2 공개키 기반 인증 계층(101)은 로컬 도메인별로 댁내의 홈게이트웨이(104,105)가 루트 CA가 되어, 댁내에 등록된 디바이스들에게 인증서를 발급하는데 사용된다. 상기 홈게이트웨이(104,105)에서 댁내에 등록된 디바이스들에게 발급되는 인증서를 로컬 도메인 인증서라 한다. 상기 로컬 도메인 인증서는 댁내에서 디바이스의 인증을 위해 사용된다.

<42> 상술한 인증 구조를 기반으로 이루어지는 본 발명에 의한 디바이스 인증 방법은, 크게 새로운 디바이스(108)를 홈 로컬 도메인(106)에 등록하는 디바이스 등록 단계와, 홈 로컬 도메인(106)에 등록된 디바이스(108)를 다른 로컬 도메인(107)으로 이동한 경우 추가적인 등록 과정 없이 해당 디바이스(108)를 인증받을 수 있도록 하기 위한 로컬 도메인간 협약 단계와, 각 로컬 도메인(107)에서 서비스 요청시 해당 디바이스(108)를 인증하기 위한 디바이스 검증 단계로 구분할 수 있다.

<43> 본 발명에 의한 상술한 디바이스 등록, 로컬 도메인간 협약, 디바이스 검증 과정은 댁내의 홈게이트웨이에 의해서 구현된다.

<44> 상기 구분된 각 단계별 흐름을 도 2 내지 도 5를 참조하여 설명한다.

<45> 더하여, 상기 도 2 내지 도 5를 참조한 설명에서 이해가 용이하도록, 재전송 공격을 방지하기 위해서 이용되는 랜덤값에 대하여, 홈게이트웨이측에서 생성된 랜덤값을 제1 랜덤값으로, 디바이스측에서 생성된 랜덤값을 제2 랜덤값으로 구분한다. 또한, 댁내의 홈게이트웨이에 등록되는 디바이스를 제1 디바이스로, 다른 로컬 도메인의 홈게이트웨이에 등록되는 디바이스를 제2 디바이스로 구분한다.

<46> 도 2는 본 발명에 의한 디바이스 인증 방법에 있어서, 사용자가 구입한 디바이스를 댁내의 홈게이트웨이에 등록하는 디바이스 등록 단계의 흐름도이다.

<47> 도 2에서, 부호 200은 등록할 디바이스를 나타내고, 201은 디바이스(200)가 등록하고자 하는 홈네트워크의 홈게이트웨이이고, 202는 상기 등록할 디바이스(200)를 검증해줄 서버로서, 제조사에 의해 관리되는 서버인 것이 바람직하다.

<48> 본 발명에 의한 디바이스 인증 방법에 있어서, 기본적으로 디바이스 제조사는 제조한 디바이스(200)의 내부에 디바이스별로 부여되는 비밀키(K_{MD})를 안전하게 삽입하고, 상기 서버(202)는 디바이스(200)를 구분하기 위한 식별정보(ID)와, 해당 디바이스(200)에 저장된 비밀키(K_{MD})를 저장한다. 상기 비밀키(K_{MD})는 대칭키이다. 또한, 사용자가 디바이스(200)를 구입할 때에, 사용자와 서버(202)가 공유할 비밀정보(Secret ID)를 알려주고 이 역시 서버(202)에 저장한다. 상기 비밀키와 비밀 정보는 이후 디바이스의 등록시 디바이스를 검증할 수 있는 정보로서 이용된다.

<49> 더하여, 홈게이트웨이(201)는 공개키 기반 구조의 제1 공개키 기반 인증 계층을 통하여 제3의 인증 기관으로부터 자신에 대한 인증서(이하, 이를 글로벌 인증서라 한다)를 발급받아 보유하고 있다.

<50> 이러한 환경에서, 디바이스(200)를 처음 등록하는 경우, 디바이스(200)와, 홈게이트웨이(201)와, 제조사의 서버(202) 간에 다음과 같은 절차에 의해 상기 디바이스(200)를 인증하여 등록한다.

<51> 도 2를 참조하면, 디바이스(200)는 홈 로컬 도메인에서의 등록을 위하여, 홈게이트웨이(201)로 등록 요청 메시지(Registration Request)를 보낸다(203).

<52> 상기 등록 요청 메시지를 수신한 홈게이트웨이(201)는 해당 디바이스(200)로 재전송 공격(replay attack)을 방지하기 위해 임의로 선택된 제1 랜덤값(N_H)을 보낸다(204).

<53> 등록 요청 메시지를 송신한 디바이스(200)는, 상기와 같이 홈 게이트웨이(201)로부터 그 응답으로 제1 랜덤값(N_H)를 수신하고,자신을 인증하기 위해 필요한 정보를 상기 홈 게이트웨이(201)로 제공하는데, 로컬 도메인내에서 사용할 비대칭키 방식의 공개키(K_D)/비밀키(K_D^{-1}) 쌍을 생성한 후, 자신을 식별하기 위한 디바이스 ID(D_{ID})

와, 상기 생성한 공개키(K_D)와, 자신이 새로 생성한 제2 랜덤값(N_D)과, 상기 홈게이트웨이(201)로부터 수신한 제1 랜덤값(N_H)중에서 하나 이상을 제조시 삽입된 디바이스의 비밀키(K_{MD})로 해쉬한 값 $(D_{ID},K_D,N_D,N_H)HMAC(K_{MD})$을 인증에 필요한 정보로서 홈게이트웨이(201)에 제공한다(205).

<54> 더하여, 상기 홈게이트웨이(201)는 상기 디바이스(200)의 구매시에 제조사로부터 제공된 비밀정보를 사용자로부터 획득한다(206).

<55> 그리고, 상기 홈게이트웨이(201)는 디바이스(200)에게서 수신한 해쉬값 $(D_{ID},K_D,N_D,N_H)HMAC(K_{MD})$과, 상기 획득한 비밀정보(Secret)가 유효한 것인지를 검증하는데, 이때 상기 메시지들에 대한 검증을 상기 디바이스(200)의 비밀키(K_{MD})나 비밀정보(Secret)를 보유한 제조사의 서버(202)에 요청한다. 이를 위해서, 상기 홈 게이트웨이(201)는, 상기 획득한 비밀정보와 제1,2 랜덤값을 자신의 비밀키(K_H^{-1})로 서명한 메시지 $(N_H,N_D,Secret)K_H^{-1}$와, 홈게이트웨이(201)가 제1 공개키 기반 인증 계층(100)을 통해 제3의 인증 기관으로부터 발급받은 글로벌 인증서($Gcert_H$)와, 상기 디바이스(200)로부터 수신한 해쉬값 $(D_{ID},K_D,N_D,N_H)HMAC(K_{MD})$을 서버(202)로 전송한다(207).

<56> 상기 서버(202)는 홈게이트웨이(201)로부터 전달된 메시지 중에서, 디바이스(200)가 생성한 해쉬값 $(D_{ID},K_D,N_D,N_H)HMAC(K_{MD})$을 자신이 보유하고 있는 해당 디바이스의 비밀키 K_{MD}를 사용하여 검증하고, 또한 제3의 인증기관을 통해 홈게이트웨이(201)의 글로벌 인증서($Gcert_H$)를 검증한 후, 상기 글로벌 인증서에 포함된 홈게이트웨이(201)의 공개키로 서명한 메시지 $(N_H,N_D,Secret)K_H^{-1}$를 검증한다. 상기 서버(202)는 검증 결과를 홈게이트웨이(201)로 제공하는데, 상기 검증 결과, 디바이스(200)가 생성한 해쉬값 및 홈게이트웨이(201)가 서명한 메시지가 모두 유효하면, 상기 글로벌 인증서($Gcert_H$)에서 획득한 홈게이트웨이(201)의 공개키(K_H)와 디바이스(200)의 제2 랜덤값 N_D을 함께 디바이스(200)의 비밀키 K_{MD}로 해쉬한 값 $(K_H,N_D)HMAC(K_{MD})$이 붙은 메시지와, 상기 디바이스(200)에 관련된 정보 (DevInfo)와, 상기 제1 랜덤값 N_H과 디바이스 정보를 함께 서버(202)의 비밀키로 서명한 메시지 $(N_H,DevInfo)K_M^{-1}$와, 서버(202)가 제3의 인증기관으로부터 발급받은 글로벌 인증서($Gcert_M$)를 홈게이트웨이(201)에 제공한다(208).

<57> 서버(202)로부터 상기와 같은 응답을 수신한 홈게이트웨이(201)는 제3의 인증기관을 통해 상기 수신된 서버(202)의 글로벌 인증서($Gcert_M$)를 검증하고, 상기 검증 결과 획득한 서버(202)의 공개키로 상기 수신된 서명 메시지 $(N_H,DevInfo)K_M^{-1}$를 검증하여, 유효한 경우, 디바이스(200)가 제2 공개키 기반 인증 계층에서 사용할 로컬 도메인 인증서($Lcert_{HD}$)를 발급하고, 상기 서버(202)로부터 수신한 메시지에 포함된 디바이스(200)의 비밀키 K_{MD}를 사용한 해쉬값 $(K_H,N_D)HMAC(K_{MD})$이 붙은 메시지와, 상기 발급한 로컬 도메인 인증서($Lcert_{HD}$)와, 상기 서버(202)로부터 수신된 디바이스정보(DevInfo)를 디바이스(200)로 전달한다(209). 즉, 상기 홈게이트웨이(201)에서 디바이스(200)로 전달되는 해쉬값 $(K_H,N_D)HMAC(K_{MD})$이 붙은 메시지에는 홈게이트웨이(201)의 공개키 K_H 및 제2 랜덤값 N_D에 대한 정보가 포함된다.

<58> 따라서, 상기 디바이스(200)는 제조시 삽입된 비밀키 K_{MD}로 상기 홈게이트웨이(201)로부터 수신한 해쉬값 $(K_H,N_D)HMAC(K_{MD})$을 검증하고, 상기 해쉬값이 유효한 경우 상기 해시값 $(K_H,N_D)HMAC(K_{MD})$이 붙은 메시지로부터 획득된 홈게이트웨이(201)의 공개키 K_H를 자신의 디바이스 인증을 위한 루트 CA의 공개키로 설정하고, 발급받은 로컬 도메인 인증서를 로컬 도메인내에서 자신을 인증하는 인증서로 사용한다.

<59> 도 3은 상기와 같은 등록 과정을 거쳐 홈 로컬 도메인에 등록된 디바이스가 자신의 홈 로컬 도메인에서 서비스를 요청하는 경우의 디바이스 인증 단계를 나타낸 흐름도이다.

<60> 도 3에서, 300은 도 2와 같은 과정을 통해 홈게이트웨이에 등록된 디바이스를 나타내고, 301은 상기 디바이스(300)가 등록된 홈 로컬 도메인의 홈게이트웨이이다.

<61> 상기 등록된 디바이스에 대한 인증 과정은 해당 디바이스(300)와 홈게이트웨이(301)에서 다음과 같은 절차로 이루어진다.

<62> 디바이스(300)가 홈게이트웨이(301)로 서비스 요청 메시지(Service request)를 보내면(302), 상기 홈게이트웨이(301)는 해당 디바이스(300)에게 재전송 공격의 방지를 위한 제1 랜덤값(N_H)을 보낸다(303).

<63> 이에 상기 디바이스(300)는 상기 수신한 홈게이트웨이(301)의 제1 랜덤값 N_H를 자신의 비대칭키방식의 비밀키로 서명한 값 $(N_H)K_D^{-1}$과, 앞서의 등록 과정을 통해 발급받은 자신의 로컬 도메인 인증서($Lcert_D$)와, 새로 생성한 제2 랜덤값(N_D)을 홈게이트웨이(301)에 제공한다(304).

<64> 상기 홈게이트웨이(301)는 상기 로컬 도메인 인증서($Lcert_D$)를 검증하고, 상기 로컬 도메인 인증서가 유효하면, 상기 로컬 도메인 인증서에서 획득한 디바이스(300)의 공개키로 상기 수신된 디바이스(300)의 서명 $(N_H)K_D^{-1}$을 검증한다. 상기 서명이 유효하면, 해당 디바이스(300)가 서비스받을 수 있도록 디바이스(300)의 세션키(K_{HD})를 생성한 후 이를 디바이스(300)의 공개키(K_D)로 암호화하여 홈게이트웨이(301)의 서명과 함께 디바이스(300)에 제공한다(305). 더 구체적으로, 상기 단계(305)에서는, 생성된 세션키를 디바이스의 공개키로 암호화한 메시지 $(K_{HD})K_D$와, 상기 생성된 세션키 K_{HD}와 제2 랜덤값 N_D에 대한 홈 게이트웨이(301)의 서명 $(K_{HD},N_D)K_H^{-1}$을 디바이스(300)로 보낸다.

<65> 이에 상기 디바이스(300)는 홈게이트웨이(301)의 공개키 K_H를 이용하여 수신된 서명 $(K_{HD},N_D)K_H^{-1}$을 검증하여, 상기 서명이 유효한 경우 상기 암호화된 메시지 $(K_{HD})K_D$를 디바이스(300)의 비밀키(K_D^{-1})로 복호화하여 세션키 K_{HD}를 획득한다.

<66> 도 4는 상기 도 2와 같이 홈 로컬 도메인에 등록한 디바이스가 다른 로컬 도메인으로 이동하여 서비스를 받고자 할 경우, 새로운 등록 절차없이 디바이스를 인증하기 위한 로컬 도메인 간의 협약 단계를 설명하기 위한 흐름도이다.

<67> 홈 로컬 도메인의 홈게이트웨이에 등록된 디바이스가 다른 로컬 도메인으로 이동한 경우(이하, 이동한 로컬 도메인을 방문 로컬 도메인이라 한다), 상기 방문 로컬 도메인에서 서비스를 받기 위해서는 방문 로컬 도메인의 홈 게이트웨이에서 타 로컬 도메인에서 등록된 디바이스에 대해서도 인증할 수 있어야 한다.

<68> 그런데 상술한 바와 같이, 홈 로컬 도메인의 홈 게이트웨이를 Root CA로 사용하는 경우, 등록된 로컬 도메인이 다른 디바이스들 간에는 공통된 Root CA가 없기 때문에, 다른 로컬 도메인에서 발급된 인증서를 검증할 수 없다.

<69> 본 발명에서는 이를 해결하기 위하여, 각 로컬 도메인에서 루트 CA의 역할을 하는 홈게이트웨이 간의 등록된 로컬 도메인을 상호 인증할 수 있도록 하는 로컬 도메인 협약 단계를 포함한다.

<70> 도 4에서, 400은 등록된 홈 로컬 도메인이 아닌 다른 로컬 도메인에 방문한 디바이스이고, 401은 상기 디바이스(400)가 방문한 방문 로컬 도메인의 Root CA 역할을 하는 홈게이트웨이이고, 402는 상기 디바이스(400)가 등록된 홈 로컬 도메인의 루트 CA 역할을 하는 홈게이트웨이이다.

<71> 도 4를 참조하면, 상기 디바이스(400)가 방문 로컬 도메인의 홈게이트웨이(401)로 서비스를 요청하면(403), 상

기 방문 로컬 도메인의 홈 게이트웨이(401)는 앞서의 디바이스 인증 과정에 따라서 인증을 수행하기 위해 상기 서비스를 요청한 디바이스(400)에게 제1 랜덤값(N_V)을 보낸다(404).

<72> 이에 디바이스(400)는 앞서 도 3에서 설명한 인증 과정과 마찬가지로, 상기 제1 랜덤값 N_V를 자신의 비밀키로 서명한 값 $(N_V)K_D^{-1}$과, 홈 로컬 도메인의 홈 게이트웨이(402)로부터 받은 자신의 로컬 도메인 인증서($Lcert_D$)와, 새로 생성한 제2 랜덤값(N_D)를 방문 로컬 도메인의 홈게이트웨이(401)로 보낸다(405).

<73> 이때, 상기 방문 로컬 도메인의 홈게이트웨이(401)는 상기 도 3의 설명과 마찬가지로, 상기 로컬 도메인 인증서 $Lcert_D$를 검증하는데, 이때, 자신이 발급한 로컬 도메인 인증서가 아니므로, 상기 수신된 디바이스(400)의 로컬 도메인 인증서를 검증할 수 없다. 따라서, 상기 방문 로컬 도메인의 홈 게이트웨이(401)는 상기 수신된 로컬 도메인 인증서 $Lcert_D$에 나타나있는 홈 로컬 도메인의 정보를 획득하여, 상기 획득한 홈 로컬 도메인의 홈 게이트웨이(402)로 자신의 글로벌 인증서($Gcert_V$)를 보내어, 다른 로컬 도메인에서 등록된 디바이스에 대하여 등록 과정을 다시 수행하지 않고, 디바이스를 인증할 수 있도록 하는 연동 협약을 요청한다(406). 상기 글로벌 인증서($Gcert_V$)는 앞서 설명한 제1 공개키 기반 인증 계층(100)을 통하여 제3의 인증 기관의 서버(102)로부터 해당 홈게이트웨이(402)가 발급받은 인증서이다.

<74> 상기 협약 요청을 받은 홈 로컬 도메인의 홈게이트웨이(402)는 수신된 글로벌 인증서를 검증하여, 유효한 글로벌 인증서이면 상기 방문 로컬 도메인의 홈게이트웨이(401)에게 크로스 도메인 인증서($Ccert_{HV}$)를 발급해 주고, 이와 함께 홈게이트웨이(402)가 제1 공개키 기반 인증 계층(100)을 통해 발급받은 글로벌 인증서($Gcert_H$)를 전달한다(407).

<75> 상기 방문 로컬 도메인의 홈게이트웨이(401)는 홈 로컬 도메인의 홈게이트웨이(402)의 글로벌 인증서 $Gcert_H$를 검증하여, 유효한 글로벌 인증서이면, 홈 로컬 도메인의 홈게이트웨이(402)의 로컬 도메인 네임과 홈게이트웨이(402)의 공개키를 저장한다. 이와 같이, 홈 로컬 도메인의 홈게이트웨이(402)의 글로벌 인증서를 검증한 후에는 디바이스(400)의 인증서를 검증할 수 있으므로, 이전 단계(405)에서 디바이스(400)로부터 받은 메시지의 서명을 검증할 수 있다. 즉, 상기 단계(405)에서 수신한 상기 디바이스(400)의 로컬 도메인 인증서와 서명을 검증하고, 상기 검증결과, 상기 서명 및 로컬 도메인 인증서가 유효한 경우 상기 디바이스(400)와 공유할 세션키 K_{VD}를 생성하고, 이를 상기 로컬 도메인 인증서로부터 획득한 디바이스(400)의 공개키로 암호화한 메시지 $(K_{VD})K_D$와, 상기 세션키 K_{VD}와 제2랜덤값 N_D을 홈게이트웨이(401)의 공개키로 서명한 메시지 $(K_{VD},N_D)K_H^{-1}$와, 홈 로컬 도메인으로부터 발급받은 크로스 도메인 인증서 $Ccert_{HV}$를 디바이스(400)에게 보낸다(408).

<76> 이에 상기 디바이스(400)는 홈게이트웨이(401)의 서명 $(K_{VD},N_D)K_H^{-1}$과 크로스 도메인 인증서 $Ccert_{HV}$를 검증하여, 상기 수신된 세션키 K_{VD}가 유효한 홈게이트웨이(401)로부터 얻어진 것인지를 확인할 수 있다. 즉, 상기 디바이스(400)는 상기 검증 결과 서명과 크로스 도메인 인증서가 유효하면, 상기 암호화 메시지 $(K_{VD})K_D$를 디바이스(400)의 비밀키로 복호화하여 세션키 K_{VD}를 획득한다.

<77> 도 5는 상술한 바와 같이, 로컬 도메인간 협약을 맺은 서로 다른 로컬 도메인에 속한 디바이스에 대한 인증과정을 나타낸 흐름도이다.

<78> 도 5에서, 500은 등록된 홈 로컬 도메인과 협약을 맺은 방문 로컬 도메인에서 서비스를 요청하는 디바이스이고, 501은 상기 방문 로컬 도메인의 홈게이트웨이이다.

<79> 디바이스간 상호 인증을 위하여, 클라이언트 디바이스는 서비스 요청과 함께 자신이 속한 로컬 도메인의 홈게이트웨이의 식별정보(identity)를 서비스 디바이스에게 알려준다. 서비스 디바이스는 자신이 속한 홈게이트웨이에 상기 식별정보(identity)에 해당하는 홈게이트웨이의 공개키를 요청하고, 이 공개키로 클라이언트 디바이스의

인증서를 검증할 수 있게 된다. 상호인증이 필요한 경우에는 서비스 로컬 도메인의 홈게이트웨이가 클라이언트에게 인증받기 위해 클라이언트의 홈게이트웨이가 서비스 로컬 도메인의 홈게이트웨이에게 발급한 인증서를 제출한다. 방문 로컬 도메인의 홈게이트웨이에 의한 타 로컬 도메인에서 등록된 디바이스에 대한 인증 단계는 도 5와 같이 이루어진다.

<80> 상기 디바이스(500)가 방문 로컬 도메인의 홈게이트웨이(501)에게 서비스를 요청하면(502), 상기 방문 로컬 도메인의 홈게이트웨이(501)는 디바이스(500)로 제1 랜덤값(N_V)을 보낸다(503).

<81> 상기 디바이스(500)는 자신에 대한 검증이 가능하도록 제1 랜덤값 N_V를 자신의 비밀키로 서명한 값 $(N_V)K_D^{-1}$과, 자신의 로컬 도메인 인증서 $Lcert_D$ 그리고 새로 생성한 제2 랜덤값(N_D)을 홈게이트웨이(501)에게 보낸다(504).

<82> 상기 홈게이트웨이(501)는 상기 수신된 디바이스(500)의 로컬 도메인 인증서를 상술한 협약 단계를 통해 획득한 홈 로컬 도메인의 홈게이트웨이의 공개키 K_H를 사용하여 검증한 후에 상기 로컬 도메인 인증서에서 획득한 디바이스의 공개키로 상기 서명을 검증한다. 서명이 유효한 경우 디바이스(500)와 공유할 세션키(K_{VD})를 생성하고, 상기 생성된 세션키를 상기 디바이스(500)의 공개키로 암호화한 메시지 $(K_{VD})K_D$와, 상기 세션키 K_{VD}와 제2 랜덤값 N_D를 홈게이트웨이(501)의 비밀키로 서명한 메시지 $(K_{VD},N_D)K_V^{-1}$와, 디바이스(500)의 홈 로컬 도메인의 홈게이트웨이로부터 협약 단계를 통해서 발급받은 크로스 도메인 인증서 $Ccert_{HV}$를 서비스 요청에 대한 응답으로서 디바이스(500)로 보낸다(505).

<83> 상기 디바이스(500)는 수신된 메시지에서, 크로스 도메인 인증서를 검증하여, 협약된 홈게이트웨이인지를 확인하고, 상기 수신된 서명을 확인한 후, 유효한 경우 수신된 암호화 메시지 $(K_{VD})K_D$를 복호화하여 세션키 K_{VD}를 획득한다.

<84> 도 6은 상술한 디바이스 인증 방법을 구현한 장치를 도시한 기능블록도이다.

<85> 본 발명에 의한 디바이스 인증 장치는, 다중 도메인 홈네트워크 환경에 있어서, 각 로컬 도메인의 홈 게이트웨이 내에 구현될 수 있다.

<86> 도 6에서, 600은 홈 게이트웨이를 나타내며, 630은 상기 홈 게이트웨이(600)내에 구비된 본 발명에 따른 디바이스 인증 장치를 나타낸다. 더하여, 610은 홈 게이트웨이(600)와 다수 디바이스를 연결하는 홈네트워크 인터페이스를 나타내고, 620은 홈게이트웨이(600)의 외부 네트워크와의 연결을 담당하는 외부 네트워크 인터페이스를 나타낸다. 상기 홈네트워크 인터페이스(610)와 외부 네트워크 인터페이스(620)를 통하여 디바이스 및 다른 홈게이트웨이 및 서버들과 통신이 이루어진다.

<87> 상기 도 6을 참조하면, 본 발명에 의한 디바이스 인증 장치는, 다른 로컬 도메인에 등록된 디바이스의 인증을 위하여 상기 다른 로컬 도메인과 공개키 기반 구조를 통해 로컬 도메인간 상호 연동을 협약하여 공개키 및 협약 사실을 증명하기 위한 크로스 도메인 인증서를 교환하는 크로스 도메인 인증 수단(631)과, 등록을 요청한 디바이스에 대하여 상기 디바이스를 검증하여 로컬 도메인에서 사용되는 로컬 도메인 인증서를 발급하는 디바이스 등록 수단(632)와, 서비스 요청한 디바이스로부터 로컬 도메인 인증서를 수신받아, 상기 수신된 로컬 도메인 인증서를 자신의 공개키 또는 상기 크로스 도메인 인증 수단에서 획득한 공개키로 검증하여, 상기 로컬 도메인 인증서가 유효하면 서비스 요청한 디바이스와 공유할 세션키를 생성하여 디바이스에 제공하는 디바이스 검증 수단(633)을 포함한다.

<88> 상기 크로스 도메인 인증 수단(631)은, 일반적인 공개키 기반 구조(PKI)를 통해 인증 장치, 즉, 홈 게이트웨이 간의 인증을 수행한다.

<89> 더하여, 상기 크로스 도메인 인증 수단(631)은, 상기 디바이스 검증 수단(633)에서 서비스 요청된 디바이스의 로컬 도메인 인증서가 수신되었으나, 상기 로컬 도메인 인증서를 검증할 수 없는 경우에, 동작하여 상기 수신된

로컬 도메인 인증서에 기록된 홈 로컬 도메인의 인증 장치와의 사이에 연동 협약을 수행한다.

<90> 그리고, 상기 디바이스 등록 수단(632)은, 등록 요청한 디바이스로부터 검증을 위한 정보를 수신하여, 상기 수신된 정보에 대한 검증을 상기 디바이스와 검증을 위한 정보를 공유하는 서버를 통해 검증받는다. 더 구체적으로 상기 검증을 위한 정보는 제조단계에서 디바이스내에 삽입된 비밀키와, 상기 디바이스의 구입시 제공되는 비밀정보를 포함한다.

<91> 더하여, 상기 디바이스 등록 수단(632)은, 등록 요청한 디바이스로 재전송 공격의 방지를 위한 제1의 랜덤값을 생성하여 전달하고, 이후 상기 디바이스로부터 검증을 위한 정보로서, 상기 제1의 랜덤값과, 디바이스 식별정보와, 디바이스에서 생성된 제2의 랜덤값과, 디바이스의 공개키중에서 하나 이상을 디바이스의 비밀키로 해쉬한 값을 수신하여, 상기 수신한 해쉬값을 디바이스와 비밀키를 공유하는 서버로 전송하여 검증받는다. 이때 서버와 홈게이트웨이와의 상호 인증은 일반적으로 알려진 공개키 기반 구조를 통해 이루어진다.

<92> 상기 디바이스 검증 수단(633)은 서비스를 요청한 디바이스로부터 검증을 위한 정보로서, 해당 디바이스에 발급된 로컬 도메인 인증서를 수신하여, 상기 로컬 도메인 인증서를 검증하며, 유효한 경우 해당 디바이스에 대한 세션키를 생성하고, 상기 세션키를 암호화하여 서명과 함께 디바이스로 제공한다.

<93> 이때, 다른 로컬 도메인에서 발급되어 인증이 불가능한 경우, 상기 수신된 로컬 도메인 인증서에 기록된 홈 로컬 도메인의 정보를 상기 크로스 도메인 인증 수단(631)으로 제공하여 협약을 요청한다.

<94> 그후, 협약 결과에 의해 홈 로컬 도메인의 공개키 및 크로스 도메인 인증서가 획득되면, 상기 공개키를 통해 수신된 로컬 도메인 인증서를 검증하며, 검증 결과 유효한 경우, 해당 디바이스에 대한 세션키를 생성하고, 상기 세션키를 암호화하여, 서명 및 상기 크로스 도메인 인증서와 함께 디바이스로 전송하여, 자신이 협약된 인증 장치임을 알린다.

<95> 이상에서 설명한 본 발명은 전술한 실시 예 및 첨부된 도면에 의해 한정되는 것이 아니고, 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경할 수 있다는 것은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 당업자에게 있어 명백할 것이다.

발명의 효과

<96> 상술한 바와 같이, 본 발명은 인증 계층을 2단계로 나누고 각 로컬 도메인 간의 협약을 통한 인증을 제공함으로써, 루트 CA를 홈게이트웨이들로 분산시켜 확장성을 보장할 수 있으며, 한 번의 디바이스 등록으로 다른 로컬 도메인의 서비스에도 인증받을 수 있게 연동함으로써 사용자의 개입을 최소화할 수 있고, 인증서 검증 패스를 단 하나의 인증서로 구성되도록 하여 패스 구축 및 검증에 대한 비용을 감소시킬 수 있으며, 로컬 도메인간 협약과정이 끝난 이후에는 모든 인증 프로세스가 로컬 도메인 내부의 커뮤니케이션을 통해서만 일어나므로 외부로의 접속 없이 효율적인 인증을 수행할 수 있는 우수한 효과가 있다.

도면의 간단한 설명

<1> 도 1은 본 발명에 의한 다중 도메인 홈 네트워크 환경에서의 디바이스 인증 시스템의 전체 구조도,

<2> 도 2는 본 발명에 의한 디바이스 인증 방법에 있어서, 초기 디바이스 구입시 등록 절차를 나타낸 흐름도,

<3> 도 3은 본 발명에 의한 디바이스 인증 방법에 있어서, 로컬 도메인 내부에서 서비스 요청시의 디바이스 인증 절차를 나타낸 흐름도,

<4> 도 4는 본 발명에 의한 디바이스 인증 방법에 있어서, 다른 로컬 도메인에서 등록된 디바이스의 서비스 사용을 위한 두 로컬 도메인 간의 협약 절차를 나타낸 흐름도,

<5> 도 5는 본 발명에 의한 디바이스 인증 방법에 있어서, 다른 로컬 도메인에 등록된 디바이스의 서비스 요청시 디바이스 인증 절차를 나타낸 흐름도, 그리고

<6> 도 6은 본 발명에 의한 디바이스 인증 장치의 기능 블록도이다.

<7> * 도면의 주요 부분에 대한 부호의 설명 *

<8> 100: 제1 공개키 기반 인증 계층

<9> 101: 제2 공개키 기반 인증 계층

<10> 102: 최상위 인증 서버

<11> 103: 제조사 서버

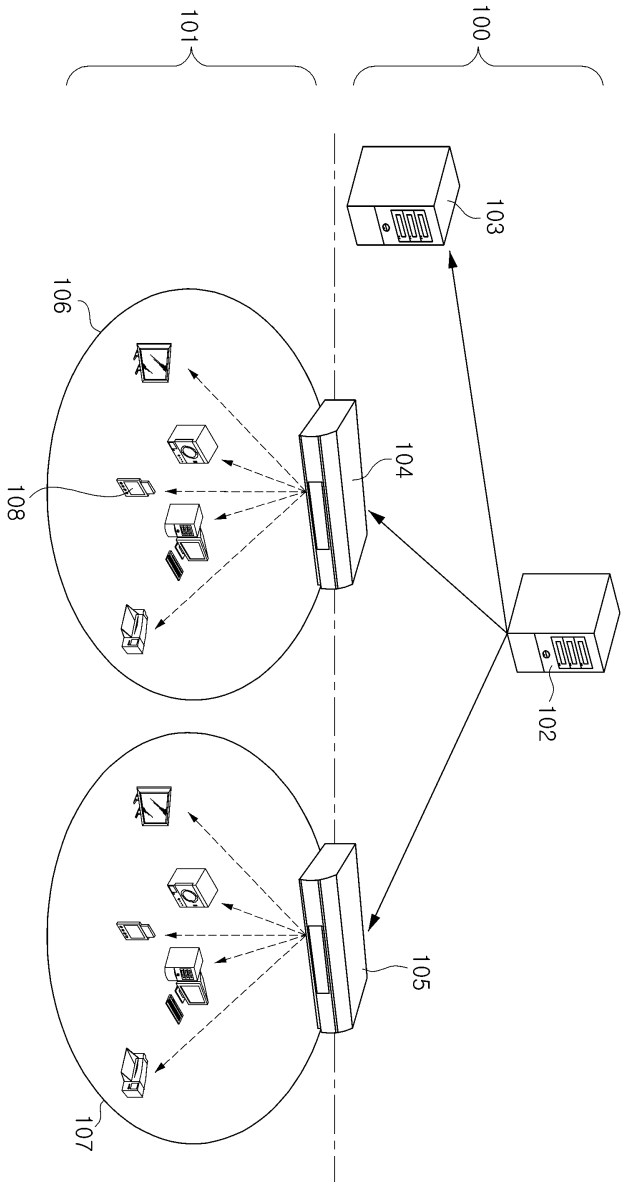
<12> 104, 105: 홈 게이트웨이

<13> 106, 107: 로컬 도메인(domain)

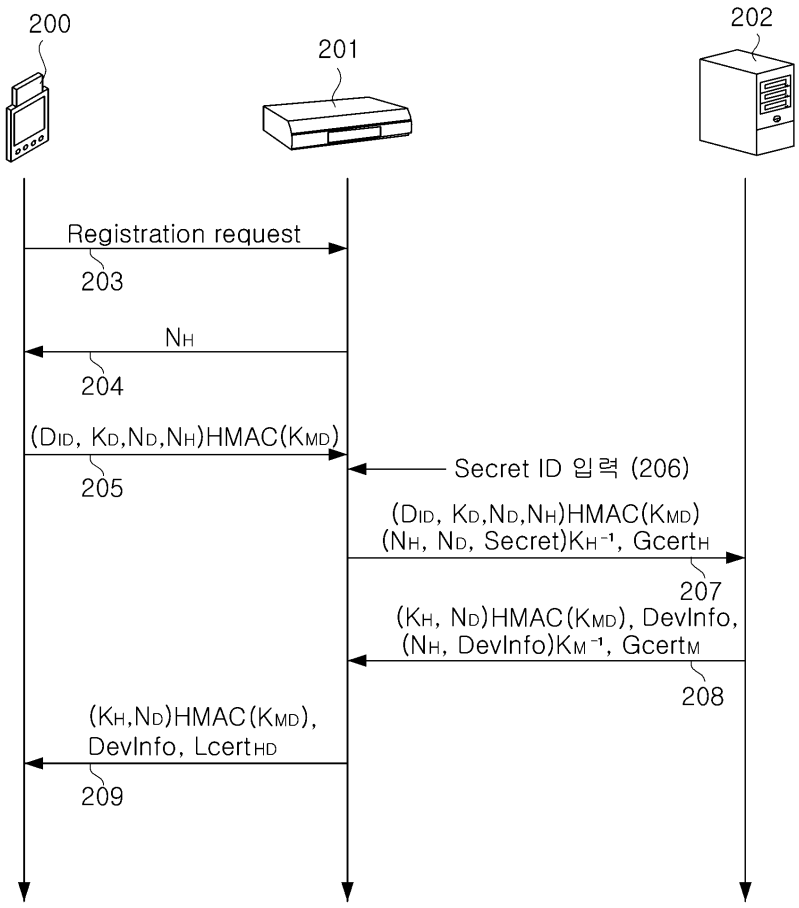
<14> 108: 디바이스

도면

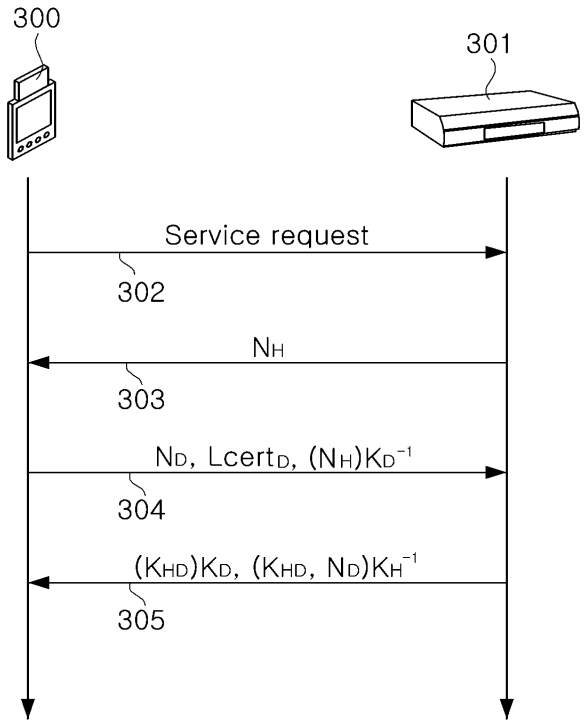
도면1



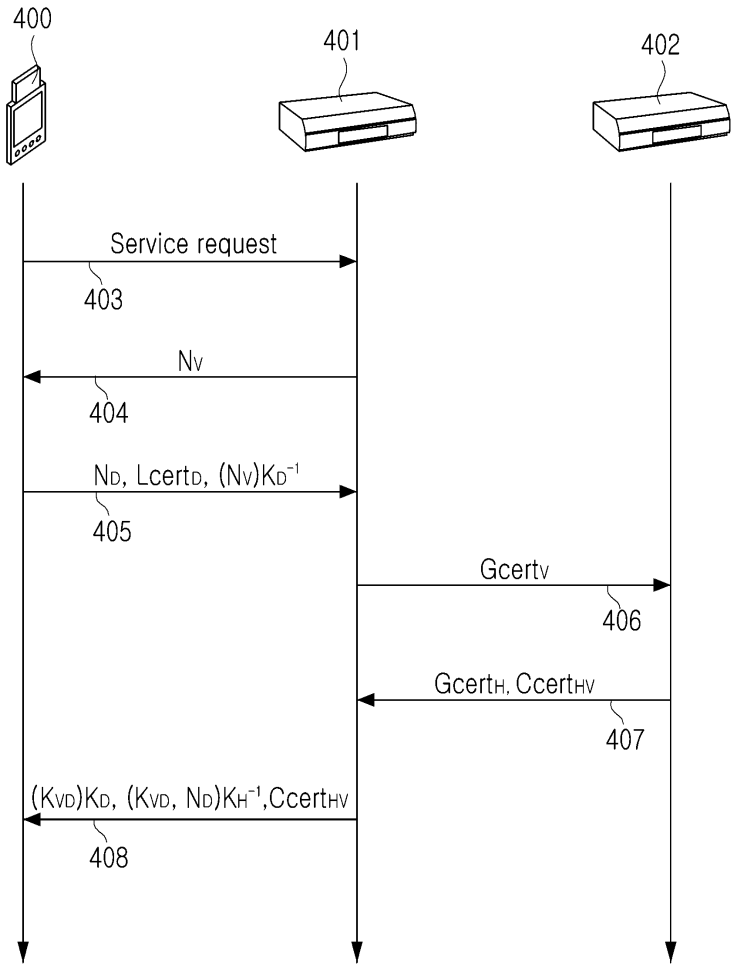
도면2


200
201
202
Registration request
203
N_H
204
$(D_{ID}, K_D, N_D, N_H)HMAC(K_{MD})$
205
Secret ID 입력 (206)
$(D_{ID}, K_D, N_D, N_H)HMAC(K_{MD})$
$(N_H, N_D, Secret)K_H^{-1}$, $Gcert_H$
207
$(K_H, N_D)HMAC(K_{MD})$, DevInfo,
$(N_H, DevInfo)K_M^{-1}$, $Gcert_M$
208
$(K_H, N_D)HMAC(K_{MD})$,
DevInfo, $Lcert_{HD}$
209

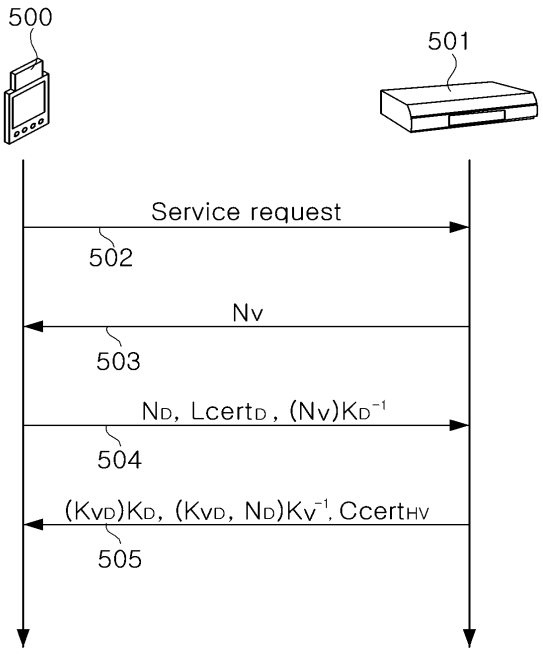
도면3


300
301
Service request
302
N_H
303
N_D, $Lcert_D$, $(N_H)K_D^{-1}$
304
$(K_{HD})K_D$, $(K_{HD}, N_D)K_H^{-1}$
305

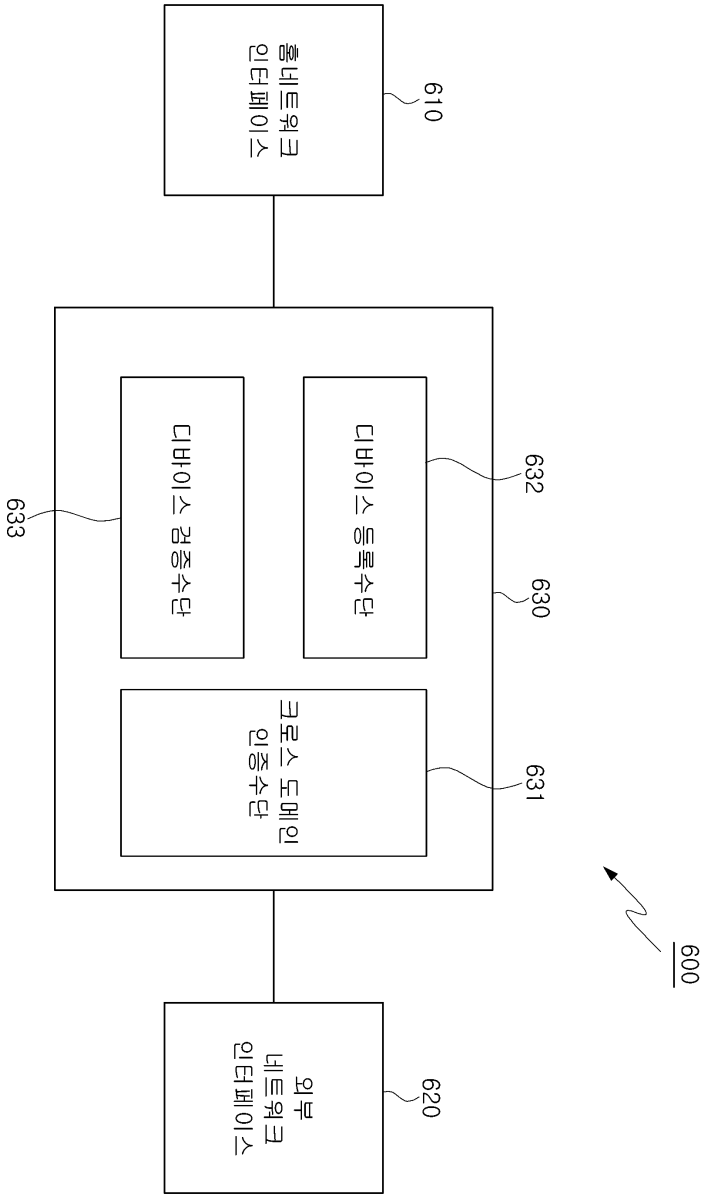
도면4


400
401
402
Service request
403
N_V
404
N_D, $Lcert_D$, $(N_V)K_D^{-1}$
405
$Gcert_V$
406
$Gcert_H$, $Ccert_{HV}$
407
$(K_{VD})K_D$, $(K_{VD}, N_D)K_H^{-1}$, $Ccert_{HV}$
408

도면5


500
501
Service request
502
Nv
503
ND, LcertD, (Nv)KD-1
504
(KvD)KD, (KvD, ND)Kv-1, CcertHV
505

도면6


홈 네트워크
인터페이스
610
디바이스 검증수단
633
디바이스 등록수단
632
630
크로스 도메인
인증수단
631
600
외부
네트워크
인터페이스
620