(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
H04L 9/32 (2006.01)

(45) 공고일자 2006년08월09일
(11) 등록번호 10-0610317
(24) 등록일자 2006년08월01일

(21) 출원번호 10-2004-0000551
(22) 출원일자 2004년01월06일

(65) 공개번호 10-2005-0072508
(43) 공개일자 2005년07월12일

(73) 특허권자 삼성전자주식회사
경기도 수원시 영통구 매탄동 416

(72) 발명자 박성준
서울특별시동작구사당동57-18호14통7반

(74) 대리인 정홍식

(56) 선행기술조사문헌
JP10013945 A
JP2001103078 A
KR1020020079044 A
1020030012764
1020030034680
* 심사관에 의하여 인용된 문헌

심사관 : 전용해

(54) 홈 네트워크를 구성하는 기기들에 대한 인증 장치 및 방법

요약

본 발명은 통신이 가능한 적어도 하나의 기기들과 상기 기기들을 제어하는 홈 서버로 구성된 홈 네트워크에서, 홈 서버가 홈 네트워크를 구성하고 있는 기기들에 대해 인증절차를 수행하는 방안을 제안한다. 이를 위해 상기 홈 서버는 저장하고 있는 기기의 고유 정보를 이용하여 인증키를 생성하고, 생성된 인증키와 고유 정보와 함께 기기로 전달한다. 또한 상기 홈 서버는 설정된 연산을 이용하여 생성한 인증키와 고유정보에 대한 연산 값과 기기로부터 전달받은 값을 비교하고, 일치할 경우 기기에 대한 인증 절차를 완료하게 된다.

대표도

도 3

색인어

홈 네트워크, 인증, 기기 비밀키, 기기 인증키, 주소 정보, 해쉬 함수

명세서

도면의 간단한 설명

도 1은 종래 다이제스트 인증 방식에 의해 클라이언트와 서버간의 수행되는 인증수행 과정을 도시한 도면;

도 2는 본 발명에 따른 홈 네트워크를 구성하고 있는 기기들을 도시하고 있는 도면;

도 3은 본 발명에 따른 홈 서버의 구성을 도시한 도면;

도 4는 본 발명에 따른 인증키 메시지의 생성과정과 구조를 도시한 도면; 및

도 5는 본 발명에 따른 홈 서버와 홈 네트워크를 구성하고 있는 기기간에 수행되는 인증 과정을 도시한 도면.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 네트워크를 구성하고 있는 기기의 인증 방안에 관한 것으로서 특히, 해쉬 함수(hash function)를 이용하여 네트워크를 구성하고 있는 기기에 대한 인증 방안에 관한 것이다.

현대사회는 여러 개의 기기들을 하나의 네트워크로 구성하여 하나의 서버가 상기 여러 개의 기기들을 제어한다. 그러나 현재 우리가 사용하는 네트워크는 보안 문제 해결이라는 과제를 안고있다. 즉 개인의 정보가 그대로 타인에게 유출될 수 있으므로 이에 대한 해결책을 필요하게 되었다. 이에 대해 현재까지 여러 가지 암호 알고리즘들이 제안되었고, 상기 암호 알고리즘들은 각기 다른 특성을 갖는다. 하지만 상기 암호 알고리즘들은 일정한 특성을 가지고 있어야 한다. 이하 상기 암호 알고리즘들이 가지고 있어야 할 특성에 대해 알아본다.

기밀성(confidentiality): 기밀성은 메시지를 볼 수 있는 자격을 제한하도록 하는 성질을 말한다. 암호 알고리즘을 이용함으로써 데이터를 암호화하는데 사용된 키(key)를 알고 있는 사람만이 데이터를 볼 수 있도록 한다.

무결성(integrity): 무결성은 전달받은 메시지가 전달되는 과정에서 제 3자에 의해 변조되지 않았는가를 확인 할 수 있게 하는 성질이다. 이는 해쉬 알고리즘과 암호 시스템을 이용함으로써 수신측에서 이 메시지가 변조되었는지 아니면 무결한지를 확인 할 수 있다.

인증(authentication): 인증은 메시지의 생성자를 확인하는 것을 말한다. 즉, 송수신자가 상대방의 신원을 확인/ 식별하는 서비스를 말한다. 이는 암호 시스템에 기초한 인증 프로토콜을 사용함으로서 구현할 수 있다.

부인봉쇄(non-repudiation): 송수신 당사자가 각각 전송된 송수신 사실을 추후 부인하는 것을 방지하는 서비스를 말한다. 즉, 송신자가 특정 메시지를 수신자에게 전송하였을 경우 그 메시지의 송신 사실을 부인할 수 없도록 하거나, 수신자가 송신자가 전송하지 않은 메시지를 수신하였다고 주장하는 것을 방지한다.

현재까지 제안된 암호 알고리즘들은 충분한 안정성을 갖으며 상기 특성들을 모두 만족한다. 따라서 상기 암호 알고리즘들을 적절히 사용할 경우, 네트워크 상에서의 문제점을 상당부분 해결할 수 있다. 이하, 상기 특성들을 만족할 수 있는 암호 알고리즘의 종류에 대해 알아본다.

비밀키 암호 알고리즘은 데이터를 암호화하는 암호화키와 암호문을 원래의 데이터로 바꾸어주는 복호화 키가 같은 알고리즘을 의미한다. 따라서 상기 비밀키 암호 알고리즘은 대칭키 암호 알고리즘이라고도 부른다. 통신을 수행하는 송수신단이 하나의 키를 공유하고 이 키를 이용하여 암호 연산을 수행한다.

공개키 암호 알고리즘은 데이터를 암호화하는 암호화키와 암호문을 원래의 데이터로 바꾸어주는 복호화키가 다른 알고리즘에 의해 동작한다. 따라서, 상기 공개키 암호 알고리즘은 비대칭키 암호 알고리즘이라고도 한다. 상기 공개키 암호 알고리즘의 특징은 암호화키가 공개되어도 복호화키가 공개되지 않기 때문에 암호문을 원래의 데이터로 바꿀 수 없게 된다. 이와 같은 특성으로 인하여 상기 암호화키를 공개키(public key), 복호화키를 개인키(private key)라고 부른다. 공개키 암호 알고리즘을 사용할 경우, 공개키는 여러 사람들에게 알리는 방법을 이용한다.

마지막으로 해쉬 알고리즘은 일방향 함수(one-way functions)는 변수를 통해 함수 값을 구하는 연산 즉, 주어진 x에 대하여 f(x)를 구하는 것은 쉽지만, f(x)= 0에서 x를 구하는 것은 매우 어려운 함수를 말한다. 상기 일방향 함수는 공개키 암호화에 있어서 핵심적인 개념이다. 그 자체가 프로토콜은 아니지만 일방향 함수는 대부분의 보안 프로토콜 구축, 특히 전자서명 프로토콜 구축에 있어서 기초가 된다. 따라서 해쉬 알고리즘은 대칭키 암호 시스템, 공개키 암호 시스템과 함께 암호 시스템에 꼭 필요한 요소기술로 자리잡고 있다. 상기 해쉬 알고리즘은 임의의 유한 길이의 입력 값을 고정된 크기의 출력 값으로 바꾸는 함수이다. 상기 출력 값을 해쉬 값(hash value), 혹은 메시지 다이제스트(message digest)라 부른다. 상기 해쉬 알고리즘은 다음과 같은 세 가지 조건을 만족하여야 한다.

① 해쉬 값을 이용해 원래의 입력값을 추정하는 것은 계산상으로 불가능하여야 한다.

② 입력 값과 해당 해쉬 값이 있을 때, 이 해쉬 값에 해당하는 또 다른 입력값을 구하는 것은 계산상으로 불가능하여야 한다.

③ 같은 해쉬 값을 갖는 두 개의 다른 입력 값을 발견하는 것은 계산상으로 불가능하여야 한다.

이하 상기 암호 알고리즘의 특성들 중 인증에 대해 알아본다. 상기 암호 알고리즘에서 사용하는 인증 방식에는 본인만이 알고 있는 사실을 확인하는 방식과 본인만이 소유한 소유물을 확인하는 방식, 그리고 본인만이 가지고 있는 특징을 확인하는 방식이 있다. 상기 본인만이 알고 있는 사실을 확인하는 방식에는 패스워드를 사용하는 방법이 있다. 상기 본인만이 소유한 소유물을 확인하는 방식에는 인증서와 스마트 카드가 있다. 상기 본인만이 가지고 있는 특징을 확인하는 방식에는 생체인식(지문, 홍체 인식)이 있다. 상기 패스워드를 이용하는 인증 방식에는 기본(basic) 인증 방식과 다이제스트 인증 방식이 있다. 상기 기본 인증 방식은 사용자 식별자와 패스워드만을 가지고 클라이언트를 인증하는 방식이다. 상기 다이제스트 인증 방식은 패스워드가 전송되는 상기 기본 인증의 문제점을 해결하면서 사용자의 인증이 필요한 경우에 사용할 수 있다.

도 1은 상기 다이제스트 인증 방식에 의해 클라이언트와 서버간의 수행되는 인증수행 과정을 도시하고 있다. S100에서 상기 클라이언트는 상기 서버로 인증을 요청한다. S102단계에서 상기 서버는 상기 클라이언트의 요청에 따라 랜덤값을 생성하고, S104단계에서 상기 생성된 랜덤값을 상기 클라이언트로 전달한다. S106단계에서 상기 클라이언트는 전달받은 랜덤값과 패스워드를 이용하여 인증값을 생성한다. S108단계에서 상기 클라이언트는 상기 생성한 인증값을 상기 서버로 전달한다. S110단계에서 상기 서버는 전달받은 인증값과 자신이 생성한 인증값을 비교함으로서 클라이언트 인증 과정을 수행한다. 일반적으로 상기 인증값은 해쉬 함수를 이용하여 생성한다.

상기한 바와 같이 네트워크에 대한 신뢰성을 제공하기 위해서는 서버와 여러 기기들(devices)간의 인증 과정을 수행한다. 홈 네트워크를 구성하고 있는 기기들 역시 서버와 인증 과정을 수행할 필요가 있다. 하지만 현재 홈 네트워크 환경에서는 적합한 인증 방식이 결여되어 있다. 일반적으로 홈 네트워크를 구성하고 있는 기기들에 대해 고유한 인증 및 서버 공인 인증서를 제공받기 위해서는 별도의 비용을 부담하여야 한다. 즉, 인증서를 홈 네트워크에 적용하기 위해서는 제조업체에는 공인 인증을 위한 별도의 비용과 기기별로 고유한 인증서를 제공받기 위한 별도의 비용을 부담하여야 한다. 따라서 별도의 비용 없이 서버와 기기들간에 인증 과정을 수행할 수 있는 방안이 논의된다.

발명이 이루고자 하는 기술적 과제

상기 문제점을 해결하기 위한 본 발명의 목적은 홈 네트워크 환경에 적합한 인증 방식을 제안함에 있다.

본 발명의 다른 목적은 홈 네트워크를 구성하고 있는 기기들에 대해 최소한의 안전성과 효율적인 인증 방식을 제안함에 있다.

본 발명의 또 다른 목적은 상기 홈 네트워크를 구성하고 있는 기기들의 성능을 고려하여 최소한의 인증 연산으로 인증 과정을 수행할 수 있는 방안을 제안함에 있다.

본 발명의 또 다른 목적은 복수 개의 기기들을 효율적으로 관리하는 방안을 제안함에 있다.

발명의 구성 및 작용

본원 발명은 홈 네트워크 환경에서 사용할 수 있는 인증 방식을 제안한다. 이를 위해 홈 네트워크를 구성하고 있는 서버가 각 기기들에 인증키를 생성하는 방안을 제안한다.

따라서 본 발명의 목적들을 이루기 위해 통신이 가능한 적어도 하나의 기기들과 상기 기기들을 제어하는 홈 서버로 구성된 홈 네트워크에서, 상기 홈 서버가 홈 네트워크를 구성하고 있는 기기들에 대해 인증절차를 수행하는 방법에 있어서, 저장하고 있는 상기 기기의 고유 정보를 이용하여 인증키를 생성하고, 상기 생성된 인증키를 상기 고유 정보와 함께 상기 기기로 전달하는 단계; 설정된 연산을 이용하여 생성한 상기 인증키와 고유정보에 대한 연산 값과 상기 기기로부터 전달받은 값을 비교하는 단계; 및 상기 생성한 연산값과 상기 기기로부터 전달받은 값이 일치할 경우 기기에 대한 인증 절차를 완료하는 단계;로 구성됨을 특징으로 한다.

본 발명의 목적들을 이루기 위해 통신이 가능한 적어도 하나의 기기들과 상기 기기들을 제어하는 홈 서버로 구성된 홈 네트워크에서, 상기 홈 네트워크를 구성하고 있는 기기가 상기 홈 서버에 요청한 인증절차를 수행하는 방법에 있어서, 상기 홈 서버로부터 전달받은 정보로부터 추출한 인증키와 기기의 고유정보에 대해 설정된 연산에 의해 수행한 연산값을 생성하는 단계; 및 상기 생성한 연산 값을 상기 전달한 홈 서버로부터 인증 결과 대한 정보를 수신하는 단계;로 구성됨을 특징으로 한다.

본 발명의 목적들을 이루기 위해 통신이 가능한 적어도 하나의 기기들과 상기 기기들을 제어하는 홈 서버로 구성된 홈 네트워크에서, 상기 홈 서버가 홈 네트워크를 구성하고 있는 기기들에 대해 인증절차를 수행하는 장치에 있어서, 저장하고 있는 상기 기기의 고유 정보를 이용하여 인증키를 생성하는 기기 인증키 생성부; 상기 생성된 인증키와 상기 고유 정보를 이용하여 상기 기기로 전달할 인증키 메시지를 생성하는 인증키 메시지 생성부; 및 설정된 연산을 이용하여 생성한 상기 인증키와 고유정보에 대한 연산 값과 상기 기기로부터 전달받은 값을 비교하는 기기 인증부;로 구성됨을 특징으로 한다.

이하 도면을 이용하여 본 발명의 기술적 사상에 대해 상세하게 설명한다. 도 2는 본 발명에 따른 홈 네트워크를 구성하고 있는 기기들을 도시하고 있다. 상기 도 2에서 도시되어 있는 바와 같이 상기 홈 네트워크는 복수 개의 기기들과 상기 기기들을 관리/제어하는 홈 서버(gateway)(200)로 구성된다. 상기 복수 개의 기기들은 각종 Audio/Video, PC, 냉장고와 세탁기가 디지털화되며, 유/무선으로 네트워크를 형성하여 서로 데이터통신이 가능한 차세대 가전제품이라 할 수 있다. 상기 기기들은 IP(Internet Protocol)주소가 각각 할당되고, 그에 따라 인터넷 연결이 가능하다. 또한 상기 기기들은 음성인식 기술과 음성합성기술이 적용되어 음성에 의한 작동을 수행 할 수도 있다.

상기 도 2에 도시되어 상기 홈 네트워크를 구성하고 있는 기기들은 적어도 2 개의 그룹으로 분할하여 관리한다. 즉, 유사한 기능을 수행하는 기기들을 하나의 그룹으로 관리함으로서 사용자의 편의성을 추구할 수 있게 된다. 상기 도 2에는 일 예로 리빙 그룹(living group)(210), AV 그룹(audio/video group)(220), PC 그룹(personal group)(230)을 도시하고 있다. 상기 리빙 그룹(210)에는 냉장고, 세탁기, 에어컨, 전자레인지 등이 포함되며, 상기 AV 그룹(220)에는 디지털 TV, DVD(Digital Video Disc), VCD 등이 포함된다. 상기 PC 그룹(230)에는 PC와 화상전화기 등이 포함된다.

도 3은 본 발명에 따른 홈 서버의 구성을 도시하고 있다. 이하 상기도 3을 이용하여 본 발명에 따른 홈 서버의 구성에 대해 상세하게 알아본다. 상기 홈 서버는 제어부(300)와 처리부(310), 네트워크 I/O부(330)로 구성된다. 상기 제어부(300)는 사용자 인터페이스부(302)와 그룹 관리부(304)로 구성된다. 상기 처리부(310)는 기기 인증부(312)와 기기 검출부(314), 인증키 메시지 생성부(328), 랜덤 정보 생성부(326), 기기 인증키 생성부(324), 인증 요청부(322), 처리 결과부(318), 기기 정보 관리부(320), 암/복호화부(316)로 구성된다. 이하 상기 각 구성들에서 수행되는 동작들에 대해 알아보기로 한다.

상기 사용자 인터페이스부(302)는 기기 관리를 위한 값을 사용자로부터 입력받는 기능을 수행한다. 상기 그룹 관리부(304)는 각 기기들에 대한 식별자(ID) 및 그룹 식별자를 생성하는 기능을 수행한다. 상기 그룹 식별자는 홈 네트워크를 구성하는 기기들을 그룹 단위로 관리하기 위해 사용되는 식별자이다.

상기 기기 검출부(314)는 상기 네트워크 I/O부(330)로부터 입력받은 모든 패킷으로부터 상기 패킷을 전송한 기기 및 인증 확인 값, 인증 정보를 추출하는 기능을 수행한다. 또한, 상기 추출한 정보들은 기기 인증부(312)로 전달하는 기능을 수행한다. 상기 기기 인증부(312)는 기기 검출부(314)로부터 전달받은 정보들(특히 인증 확인 값)과 상기 기기 정보 관리부(320)에 저장되어 있는 인증 정보를 이용하여 생성한 인증 확인 값을 비교한다. 상기 전달받은 인증 확인 값과 생성한 인증확인 값을 비교함으로서 상기 기기에 대한 인증 여부를 확인한다. 또한, 상기 기기에 대한 인증 결과를 결과 처리부(318)로 전달한다.

상기 결과 처리부(318)는 상기 기기에 대한 인증 결과 값을 전달받아 인증이 확인되었을 경우 인증확인 메시지를 생성한다. 상기 생성한 인증확인 메시지를 제어부(300)와 기기정보 관리부(320)로 전달한다. 상기 기기에 대한 인증이 실패하였을 경우 인증 실패 메시지를 생성한다. 상기 생성된 인증실패 메시지는 상기 제어부(300)와 인증 요청부(322)로 전달한다.

상기 인증 요청부(322)는 상기 홈 서버에 새로운 기기가 등록하거나, 인증이 실패하였을 경우 재 인증을 요청하기 위한 메시지를 생성한다. 또한, 상기 그룹 관리부(322)로부터 상기 기기에 대한 기기 식별자/그룹 식별자를 전달받는다. 상기 기기 인증키 생성부(324)는 상기 기기에 대한 인증을 확인하기 위한 값을 생성하며, 상기 기기에서는 이 값이 포함된 인증 확인 값을 생성한다. 상기 랜덤 정보 생성부(326)는 상기 홈 서버에서 상기 기기로 전달하는 랜덤 정보를 생성한다. 상기 랜덤 정보는 재사용 공격을 방지하기 위해 상기 기기에서 이 값을 포함하여 인증 확인 값을 생성한다.

상기 인증키 메시지 생성부(328)에서 생성하는 암호 키 메시지에 대해서는 하기에서 알아보기로 한다. 상기 암/복호화부(316)는 상기 기기의 성능에 따라 선택적으로 사용되어질 수 있다. 즉, 홈 기기키를 비밀키로 사용하여 메시지에 대한 암호/복호화를 수행할 수 있다. 상기 기기 정보관리부(320)는 홈 네트워크를 구성하고 있는 기기들에 대한 정보들을 저장하고 있다. 상기 기기 정보관리부(320)에서 저장하고 있는 정보들에는 기기의 종류, 기기의 식별자, 기기의 그룹 식별자, 기기의 주소 정보(device address), 기기 비밀키 등이 포함된다. 상기 기기 비밀키는 상기 기기를 제조한 제조사에서 상기 기기에 부가하는 고유번호일 수 있다. 하기 〈표 1〉은 상기 기기정보 관리부에서 저장하고 있는 기기들에 정보들에 대한 일 예를 나타내고 있다. 상기 〈표 1〉에 의하면 냉장고와 전자레인지는 동일한 그룹 식별자를 가짐을 알 수 있다.

[표 1]

기기의 종류	냉장고	전자레인지	DVD	화상전화기
기기의 식별자	aaa	bbb	ccc	ddd
기기의 그룹 식별자	AAA	AAA	BBB	CCC
기기의 주소 정보	123.234.567	234.234.123	234.56.789	789.035.245
기기의 비밀키	234-345-987	123-563-786	556-432-789	876-783-324

상기 네트워크 I/O부(330)는 상기 홈 서버에서 지원하는 여러 가지 네트워크 인터페이스들을 포함한다.

도 4는 본 발명에 따른 인증 키 메시지를 생성하는 과정을 도시하고 있다. 상기 도 4는 기기정보 관리부(320)와 기기 인증키 생성부(324)를 도시하고 있다. 상기 기기정보 관리부(320)는 저장하고 있는 기기 비밀키와 주소 정보를 출력하고, 상기 기기 인증키 생성부(324)는 생성한 기기 인증키를 출력한다. 상기 기기 인증키 생성부(324)는 홈 네트워크를 구성하고 있는 기기들을 그룹별로 관리하기 위해, 하나의 그룹에 대해 하나의 기기 인증키를 생성한다. 하지만 사용자의 설정에 따라 각 기기에 대해 고유한 기기 인증키를 생성할 수 도 있다.

이하 상기 인증키 메시지 생성부(328)에서 인증키 메시지를 생성하는 과정에 대해 알아본다. 상기 인증키 메시지 생성부(328)에서 인증을 요하는 기기는 기기 1 내지 기기 3이라 가정한다. 상기 인증키 메시지 생성부(328)는 기기 1의 인증을 위해 상기 기기정보 관리부(320)로부터 기기1에 대한 기기 비밀키(410)와 주소 정보(412)를 전달받는다. 또한 상기 기기 인증키 생성부(324)로부터 기기 1의 인증을 위한 기기 인증키(414)를 전달받는다. 상기 전달받은 기기 비밀키(410)와 주소정보(412), 기기 인증키(414)는 연산부(440)로 전달된다. 상기 연산부(440)는 전달받은 기기 비밀키(410)와 주소정보(412), 기기 인증키(414)를 이용하여 배타적 논리합(exclusive OR) 연산을 수행한다. 상기 인증키 메시지 생성부(328)는 기기 2의 인증을 위해 상기 기기정보 관리부(320)로부터 기기2에 대한 기기 비밀키(420)와 주소 정보(422)를 전달받는다. 또한 상기 기기 인증키 생성부(324)가 생성한 기기 2의 인증을 위한 기기 인증키(424)를 전달받는다. 상기 전달받은 기기 비밀키(420)와 주소정보(422), 기기 인증키(424)는 연산부(442)로 전달된다. 상기 연산부(442)는 전달받은 기기 비밀키(420)와 주소정보(422), 기기 인증키(424)를 이용하여 배타적 논리합 연산을 수행한다. 상기 인증키 메시지 생성부(328)는 기기 3의 인증을 위한 상기 기기정보 관리부(320)로부터 기기3에 대한 기기 비밀키(430)와 주소 정보(432)를 전달받는다. 또한 상기 기기 인증키 생성부(324)가 생성한 기기 3의 인증을 위한 기기 인증키(434)를 전달받는다. 상기 전달받은 기기 비밀키(430)와 주소정보(432), 기기 인증키(434)는 연산부(444)로 전달된다. 상기 연산부(444)는 전달받은 기기 비밀키(430)와 주소정보(432), 기기 인증키(434)를 이용하여 배타적 논리합 연산을 수행한다. 하기 〈수학식1〉은 상기 연산부들(440 내지 444)에서 수행되는 동작을 수식으로 표현하고 있다.

수학식 1

$$\text{인증키 생성} = (\text{기기 비밀키}) XOR (\text{기기 인증키}) XOR (\text{주소 정보})$$

상기 각 연산부들(440 내지 444)에서 생성된 인증키들은 인증키 메시지에 포함된다. 상기 인증키 메시지는 상기 기기들의 그룹 식별자와 각 기기들의 식별자, 각 기기들의 인증키가 포함된다. 또한, 랜덤 정보 생성부에서 생성한 랜덤 정보가 포함된다.

도 5는 본 발명에 따른 홈 서버와 홈 네트워크를 구성하고 있는 기기간에 수행되는 인증 과정을 도시하고 있다. 이하 상기 도 5를 이용하여 본 발명에 따른 홈 서버와 기기간에 수행되는 인증 과정에 대해 상세하게 알아보기로 한다.

상기 기기는 제조사가 부여한 기기 비밀키를 가지고 있으며, 상기 부여받은 기기 비밀키는 상기 홈 서버와 공유하고 있다고 가정한다. 또한, 상기 기기와 홈 서버는 해쉬 알고리즘의 종류, 암호화 지원 여부, 암호화를 지원할 경우 암호화 알고리즘에 관한 정보들은 공유하고 있다고 가정한다. 만약 암호화를 지원하지 않는다면 상기 암호화 알고리즘에 관한 정보는 필요 없게 된다.

S500단계에서 상기 홈 서버는 홈 네트워크를 구성하고 있는 기기들에 대한 정보와 상기 기기에 대한 기기 비밀키, 주소 정보를 공유한다. 상기 홈 서버는 공유한 정보들을 이용하여 해당 기기에 대한 기기 식별자와 그룹 식별자를 생성한다. 상기 그룹 식별자는 상기 기기들의 환경, 위치, 기능 등을 고려하여 설정하게 된다. 상기 도 2에서는 리빙 그룹, AV 그룹, PC 그룹 등으로 상기 홈 네트워크를 구성하는 기기들을 분류하였다.

S502단계에서 상기 홈 서버는 상기 기기 식별자를 이용하여 해당 기기에 대한 기기 인증키를 생성한다. 상기 기기 인증키 생성은 상기 서버의 인증키 생성부에서 수행된다. 상기 기기 인증키는 사용자에 의해 직접 설정될 수 도 있다. S504단계에서 상기 홈 서버는 상기 인증키 메시지를 생성한다. 상기 인증키 메시지는 그룹 식별자, 기기 식별자, 기기 인증키, 랜덤 정보 등으로 구성된다. 상기 기기 인증키는 상술한 바와 같이 기기 비밀키, 기기 인증키, 주소 정보를 이용하여 배타적 논리합 연산을 수행함으로서 생성한다.

S506단계에서 상기 홈 서버는 생성한 인증키 메시지를 기기들로 전송한다. 상기 인증키 메시지는 상기 기기들에 대해 인증을 요구하는 메시지의 역할도 수행하므로 인증요청 메시지(Authentication Request Message)라 칭하기도 한다. S508단계에서 상기 기기는 수신한 인증요청 메시지와 저장하고 있는 기기 비밀키와 주소 정보를 이용하여 자신에게 할당된 기기 인증키를 획득하게 된다.

S510단계에서 상기 기기는 획득한 기기 인증키와 인증에 관련된 정보들을 이용하여 해쉬 연산을 수행함으로서 인증값을 생성한다. 상기 인증에 관련된 정보들은 상기 홈 서버와 기기가 서로 공유함을 상술한 바와 같다. 상기 인증에 관련된 정보들에는 주소 정보, 기기 비밀키, 랜덤 정보 등이 포함될 수 있다. S512단계에서 상기 기기는 생성한 인증값을 인증 메시지(Authentication Message)에 포함시켜 상기 홈 서버로 전달한다. S514단계에서 상기 홈 서버는 전달받은 인증값과 기기 정보 관리부에 저장되어 있는 정보들을 이용하여 생성한 해당 기기에 대한 인증값을 비교한다. 상기 비교 결과 두 값이 일치하면 인증이 성공하였음을 의미하며, 두 값이 일치하지 않으면 인증이 실패하였음을 의미한다. S516단계에서 상기 홈 서버는 인증 결과에 대한 정보를 인증 결과 메시지(Authentication Result Message)에 포함시켜 상기 기기로 전송한다. 상기 도 5에서는 도시되어 있지 않지만 상기 홈 네트워크를 구성하고 있는 기기가 암호화 연산까지 지원 가능할 경우 미리 설정된 인증키 알고리즘을 이용하여 메시지를 송수신할 수 있다.

발명의 효과

상기한 바와 같이 본원 발명은 홈 서버가 홈 네트워크를 구성하고 있는 기기들에 대한 인증키를 할당함으로서 비용 절감을 가져온다. 또한, 최소한의 연산만을 이용하여 홈 네트워크를 구성하고 있는 기기들에 대한 인증 과정을 수행함으로서 메모리 용량이 적은 기기들에 수행할 수 있게 된다. 또한, 사용자의 선택에 따라 기기들을 그룹으로 관리할 수 있으므로 사용자의 편의성을 도모할 수 있게 된다.

(57) 청구의 범위

청구항 1.

통신이 가능한 적어도 하나의 기기들과 상기 기기들을 제어하는 홈 서버로 구성된 홈 네트워크에서, 상기 홈 서버로 홈 네트워크를 구성하고 있는 기기들에 대해 인증절차를 수행하는 방법에 있어서,

저장하고 있는 상기 기기의 고유정보를 이용하여 인증키를 생성하고, 상기 생성된 인증키를 상기 고유정보와 함께 상기 기기로 전달하는 단계;

설정된 연산을 이용하여 생성한 상기 인증키와 상기 고유정보를 배타적 논리 합 연산한 연산 값과 상기 기기에 의해 상기 인증키와 인증 관련 정보가 해쉬연산된 값을 비교하는 단계; 및

상기 연산 값과 상기 해쉬연산된 값이 일치할 경우 상기 기기에 대한 인증 절차를 완료하는 단계;로 구성됨을 특징으로 하는 상기 방법.

청구항 2.

제 1항에 있어서, 상기 기기의 고유 정보는 제작자가 설정한 기기의 고유 번호와 인터넷 프로토콜 주소에 관한 정보임을 특징으로 하는 상기 방법.

청구항 3.

제 1항에 있어서, 상기 설정된 연산을 이용하여 생성한 연산값은 해쉬 연산을 이용하여 생성한 값임을 특징으로 하는 상기 방법.

청구항 4.

제 1항에 있어서, 상기 고유정보를 배타적 논리 합 연산 수행하여 상기 인증키를 생성하고, 상기 생성된 인증키를 상기 기기로 전달함을 특징으로 하는 상기 방법.

청구항 5.

통신이 가능한 적어도 하나의 기기들과 상기 기기들을 제어하는 홈 서버로 구성된 홈 네트워크에서, 상기 홈 네트워크를 구성하고 있는 기기가 상기 홈 서버에 요청한 인증절차를 수행하는 방법에 있어서,

상기 홈 서버로부터 전달받은 정보로부터 추출한 인증키와 기기의 고유정보를 배타적 논리 합 연산한 연산값을 생성하는 단계; 및

상기 연산값을 상기 홈 서버로 전달하고, 상기 홈 서버로부터 인증 결과에 대한 정보를 수신하는 단계;로 구성됨을 특징으로 하는 상기 방법.

청구항 6.

제 5항에 있어서, 상기 기기의 고유 정보는 제작자가 설정한 기기의 고유 번호와 인터넷 프로토콜 주소에 관한 정보임을 특징으로 하는 상기 방법.

청구항 7.

제 5항에 있어서, 상기 설정된 연산을 이용하여 생성한 연산값은 해쉬 연산을 이용하여 생성한 값임을 특징으로 하는 상기 방법.

청구항 8.

제 5항에 있어서, 상기 홈 서버로부터 전달받은 정보와 상기 기기의 고유정보에 대한 배타적 논리 합 연산을 수행함으로서 상기 인증키를 추출함을 특징으로 하는 상기 방법.

청구항 9.

통신이 가능한 적어도 하나의 기기들과 상기 기기들을 제어하는 홈 서버로 구성된 홈 네트워크에서, 상기 홈 서버가 홈 네트워크를 구성하고 있는 기기들에 대해 인증절차를 수행하는 장치에 있어서,

저장하고 있는 상기 기기의 고유 정보를 이용하여 인증키를 생성하는 기기 인증키 생성부;

상기 생성된 인증키와 상기 고유 정보를 이용하여 상기 기기로 전달할 인증키 메시지를 생성하는 인증키 메시지 생성부; 및

설정된 연산을 이용하여 생성한 상기 인증키와 상기 고유정보를 배타적 논리 합 연산한 연산 값과 상기 기기에 의해 상기 인증키와 인증 관련 정보가 해쉬연산된 값을 비교하는 기기 인증부;로 구성됨을 특징으로 하는 상기 장치.

청구항 10.

제 9항에 있어서, 상기 홈 서버는, 상기 기기의 고유 정보인 제작자가 설정한 기기의 고유 번호와 인터넷 프로토콜 주소를 저장하고 있는 기기정보 관리부를 부가함을 특징으로 하는 상기 장치.

청구항 11.

제 9항에 있어서, 상기 기기 인증부는,

해쉬 연산을 이용하여 상기 인증키와 고유 정보에 대한 연산 값을 생성함을 특징으로 하는 상기 장치.

청구항 12.

제 9항에 있어서, 상기 인증키 메시지 생성부는,

생성한 인증키와 고유정보에 대한 배타적 논리 합 연산을 수행함으로서 인증키 메시지를 생성함을 특징으로 하는 상기 장치.

청구항 13.

제 9항에 있어서, 상기 홈 서버는,

인증이 필요한 기기가 상기 홈 네트워크로 유입되면 상기 기기로 인증을 요청하기 위한 메시지를 생성하는 인증 요청부를 부가함을 특징으로 하는 상기 장치.

청구항 14.

제 9항에 있어서, 상기 홈 네트워크를 구성하고 있는 각 기기들에 대해 적어도 두 개의 그룹들 중 하나의 그룹에 할당하고, 상기 할당된 그룹의 식별자와 기기 식별자를 저장하고 있는 그룹 관리부를 부가함을 특징으로 하는 상기 장치.

청구항 15.

제 14항에 있어서, 상기 기기 인증키 생성부는,

하나의 그룹에 포함된 기기들에 대해 하나의 인증키를 생성함을 특징으로 하는 상기 장치.

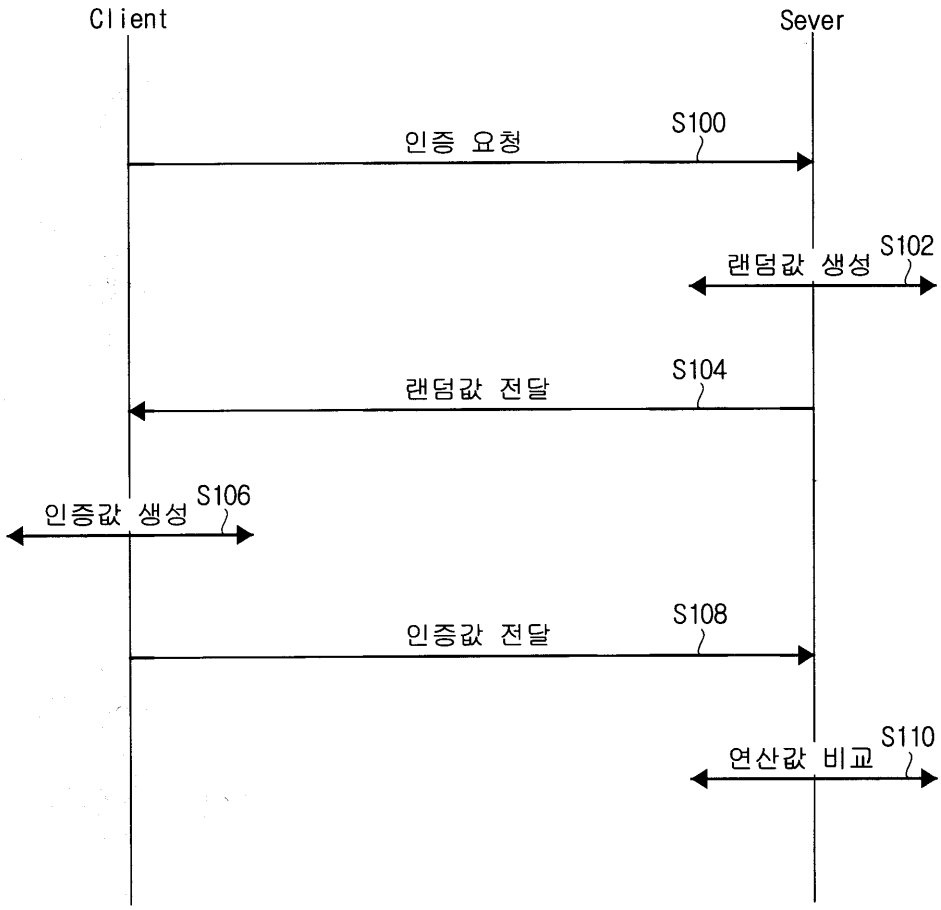
청구항 16.

제 15항에 있어서, 상기 인증키 메시지 생성부는,

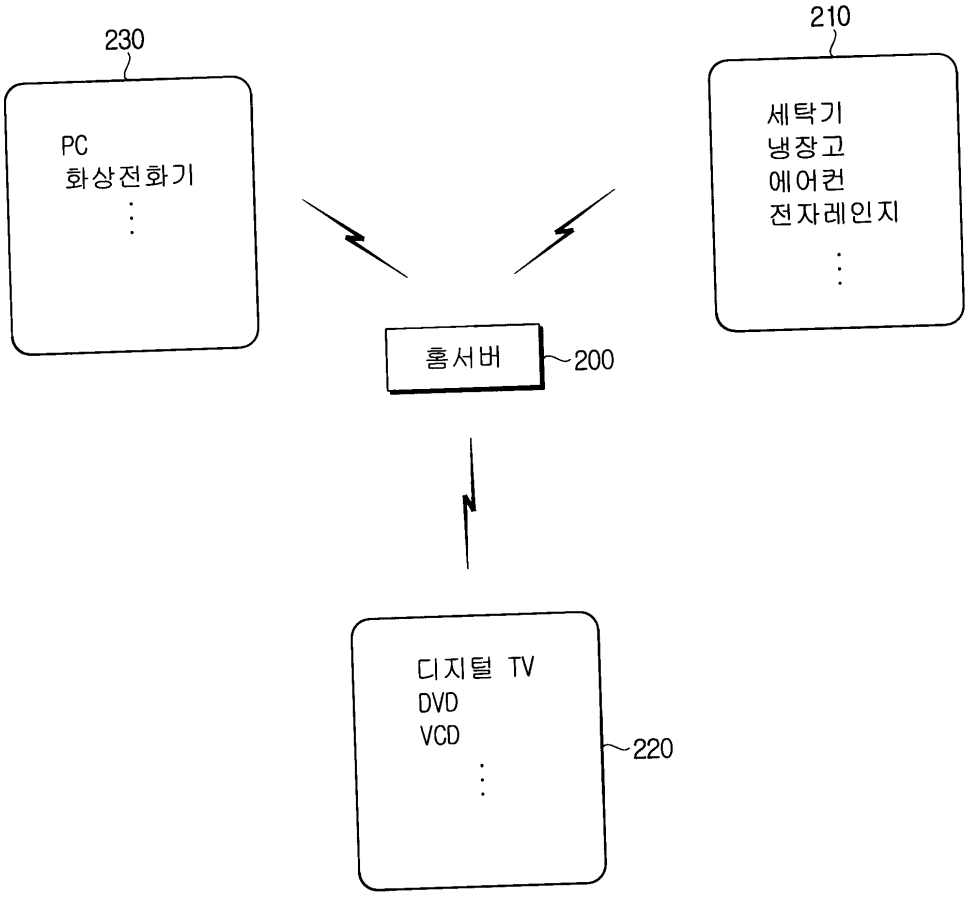
그룹 식별자와 상기 그룹을 구성하고 있는 기기에 대한 기기 식별자들과 기기 각각에 대한 인증키를 포함하는 인증키 메시지를 생성함을 특징으로 하는 상기 장치.

도면

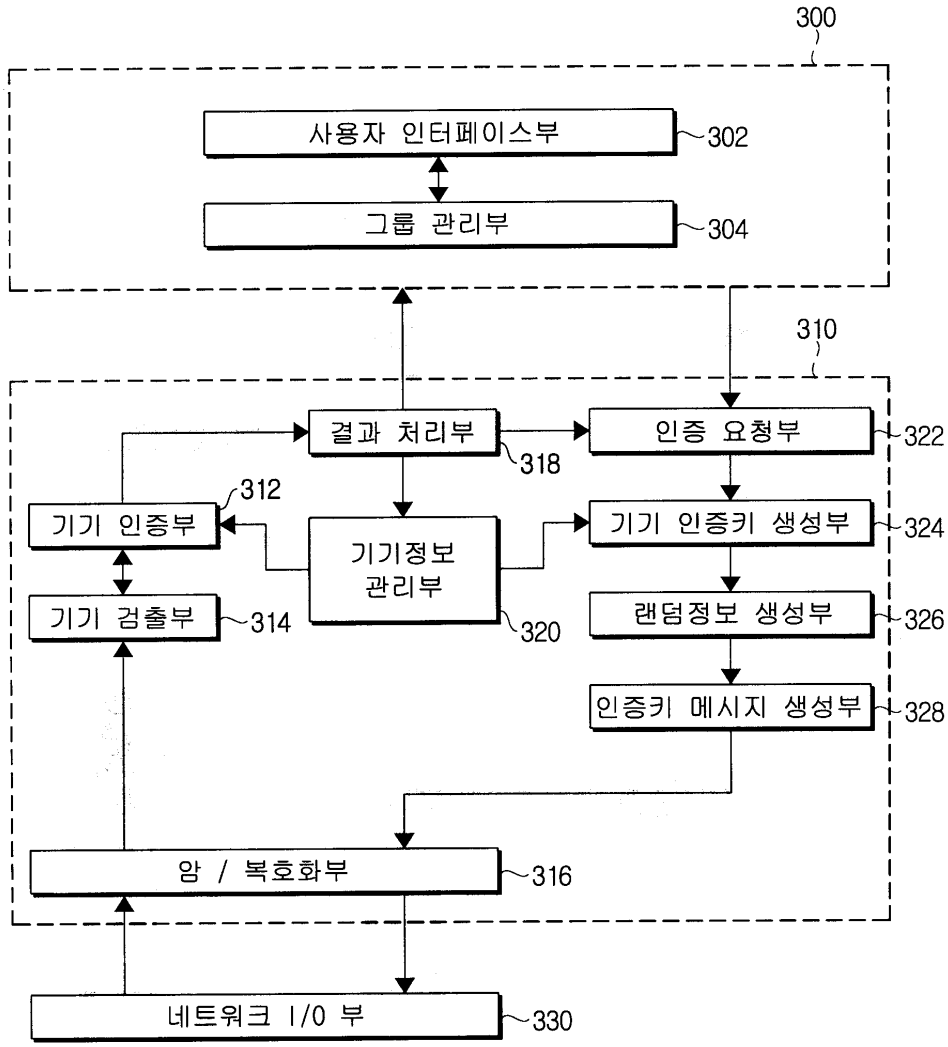
도면1



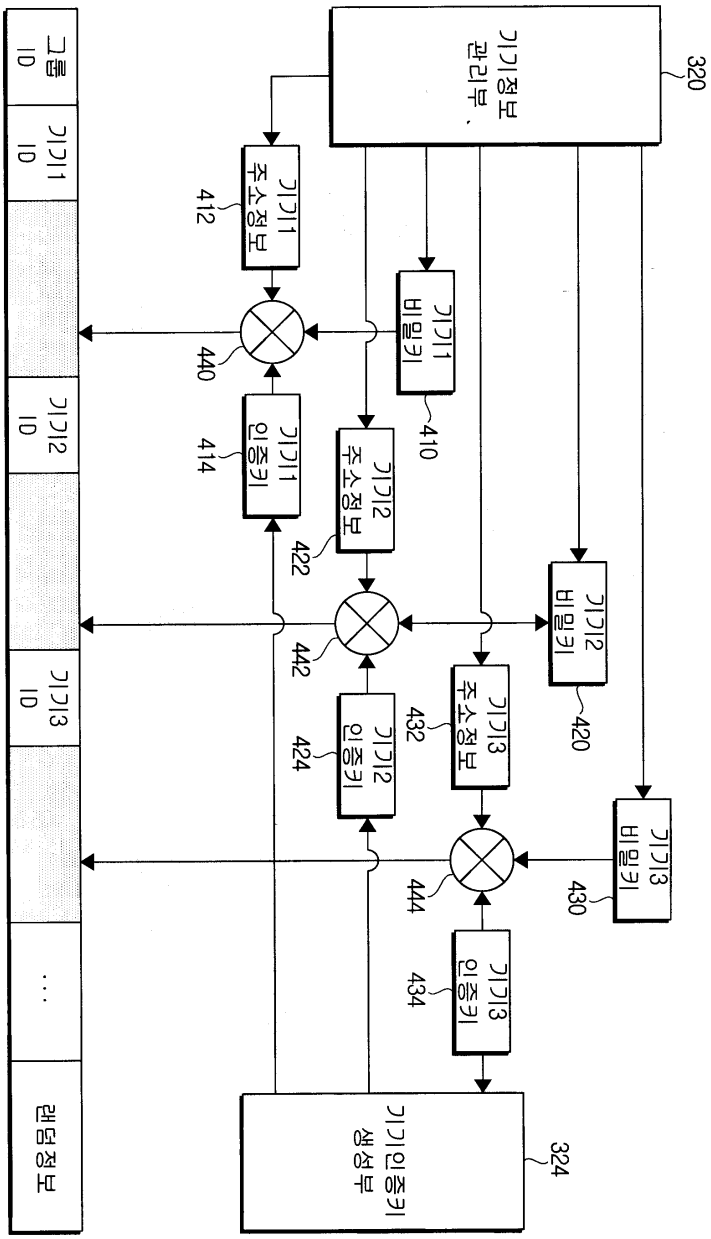
도면2



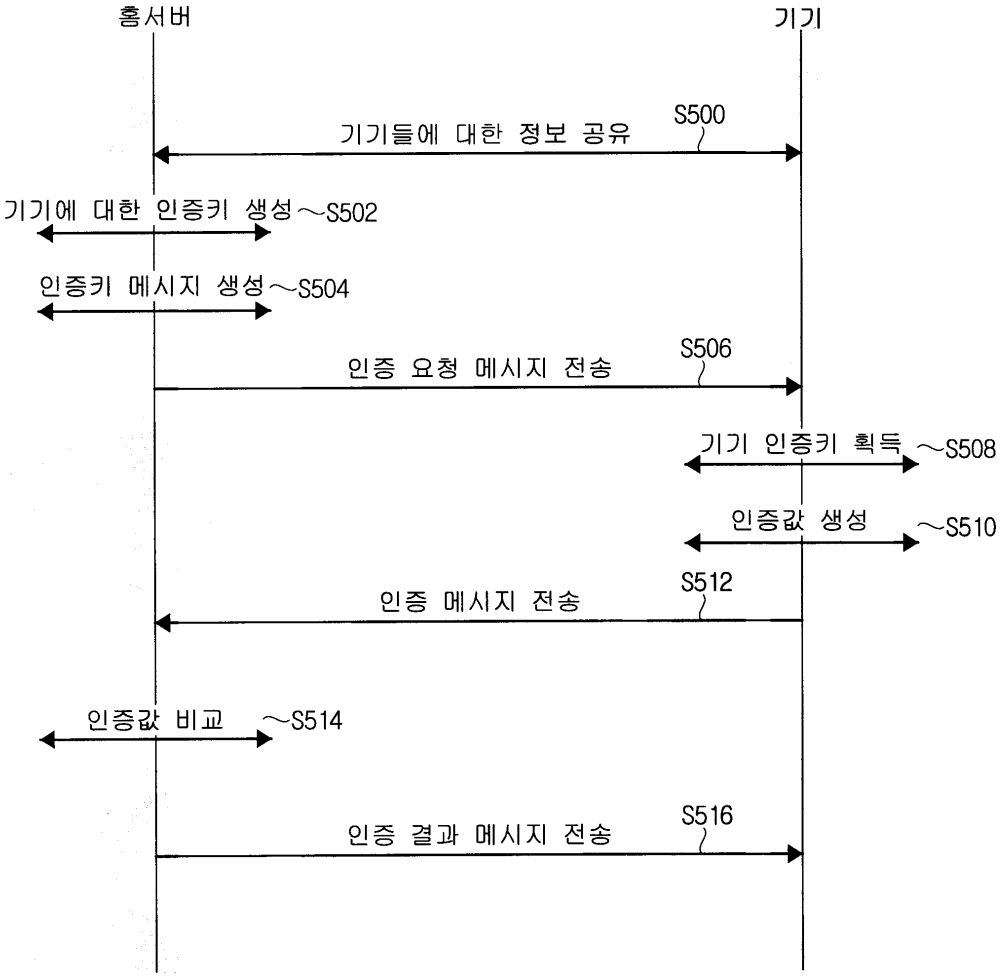
도면3


300
사용자 인터페이스부
302
그룹 관리부
304
310
결과 처리부
318
인증 요청부
322
312
기기 인증부
기기정보 관리부
320
기기 인증키 생성부
324
기기 검출부
314
랜덤정보 생성부
326
인증키 메시지 생성부
328
암 / 복호화부
316
네트워크 I/O 부
330

도면4


그룹 ID
기기1 ID
기기2 ID
기기3 ID
...
랜덤정보
기기정보 관리부
320
기기1 주소정보
412
기기1 비밀키
410
기기1 인증키
414
기기2 주소정보
422
기기2 비밀키
420
기기2 인증키
424
기기3 주소정보
432
기기3 비밀키
430
기기3 인증키
434
440
442
444
기기인증키 생성부
324

도면5


홈서버
기기
S500
기기들에 대한 정보 공유
기기에 대한 인증키 생성
S502
인증키 메시지 생성
S504
S506
인증 요청 메시지 전송
기기 인증키 획득
S508
인증값 생성
S510
S512
인증 메시지 전송
인증값 비교
S514
S516
인증 결과 메시지 전송