(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년07월16일
(11) 등록번호 10-0970552
(24) 등록일자 2010년07월08일

(51) Int. Cl.
H04L 9/30 (2006.01) *H04L 9/28* (2006.01)
(21) 출원번호 10-2008-0062320
(22) 출원일자 2008년06월30일
심사청구일자 2008년06월30일
(65) 공개번호 10-2010-0002424
(43) 공개일자 2010년01월07일
(56) 선행기술조사문헌
WO2006051517 A1
WO2004032416 A1
KR1020060134775 A

(73) 특허권자
경희대학교 산학협력단
경기도 용인시 기흥구 서천동 1 경희대학교 국제캠퍼스내
(72) 발명자
홍충선
경기 용인시 수지구 상현동 성원3차상떼빌아파트 233-101
허준
경기도 군포시 궁내동 우륵주공아파트 711-1601
조응준
경기도 수원시 영통구 영통1동 1029-12번지 103호
(74) 대리인
서재승

전체 청구항 수 : 총 6 항 심사관 : 정은선

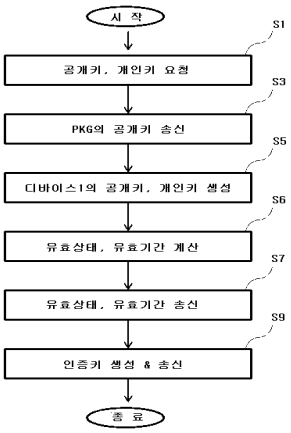
(54) 비인증서 공개키를 사용하는 보안키 생성 방법

(57) 요 약

본 발명에 보안키 생성 방법에 관한 것으로, IP 네트워크에 기반하지 않고도 단위 유효 기간별로 구분된 공개키 기반의 보안 메커니즘을 이용하여 안전하게 데이터 통신을 수행할 수 있는 보안키 생성 방법에 관한 것이다.

본 발명에 따른 보안키 생성 방법은 IP 네트워크로 접속되는 인증기관이나 인증 기관에 의해 발행된 인증서가 없이도 공개키 기반으로 데이터를 보안할 수 있으므로, 간단하게 보안키를 생성할 수 있으며 보안 시스템의 관리 및 보안을 저렴한 비용으로 용이하게 수행할 수 있다. 또한 본 발명에 따른 보안키 생성 방법은 유효 기간에만 사용되는 유효 공개키와 유효 개인키를 사용하여 송수신되는 데이터를 암호화/복호화함으로써, 보다 안전하게 데이터를 송수신할 수 있다.

대 표 도 - 도4



특허청구의 범위

청구항 1

다수의 디바이스와 공개키 발생 장치를 구비하는 통신 네트워크에서, 상기 디바이스로 제공되는 보안키를 생성하는 방법에 있어서,

(a) 상기 공개키 발생 장치는 상기 다수의 디바이스들 중 제1 디바이스로 상기 공개키 발생 장치의 공개키를 송신하는 단계;

(b) 상기 공개키 발생 장치는 상기 제1 디바이스로부터 상기 공개키 발생 장치의 공개키로 암호화된 상기 제1 디바이스의 인증 정보를 수신하고, 상기 수신한 인증 정보로부터 상기 제1 디바이스의 공개키(K_A)와 개인키(K_A^{-1})를 생성하여 상기 제1 디바이스로 송신하는 단계; 및

(c) 상기 공개키 발생 장치는 유효기간 동안만 사용되는 상기 제1 디바이스의 유효 공개키와 유효 개인키를 생성하기 위하여 필요한 유효 상태와 유효 기간에 대한 정보를 상기 제1 디바이스의 공개키로 암호화하여 상기 제1 디바이스로 송신하는 단계를 포함하는 보안키 생성 방법.

청구항 2

제 1 항에 있어서, 상기 (b) 단계는

(b1) 상기 제1 디바이스로부터 상기 공개키 발생 장치의 공개키로 암호화된 상기 제1 디바이스의 인증 정보를 수신하는 단계;

(b2) 상기 수신한 인증 정보에 기초하여 상기 제1 디바이스를 인증하는 단계;

(b3) 상기 수신한 제1 디바이스의 인증 정보를 이용하여 상기 제1 디바이스의 개인키(K_A)와 공개키(K_A^{-1})를 생성하는 단계; 및

(b4) 상기 생성한 제1 디바이스의 개인키(K_A)와 공개키(K_A^{-1})를 상기 공개키 발생 장치의 시스템 파라미터와 함께 상기 제1 디바이스로 송신하는 단계를 포함하는 것을 특징으로 하는 보안키 생성 방법.

청구항 3

제 2 항에 있어서, 상기 제1 디바이스의 인증 정보는

상기 제1 디바이스의 신원기반 식별 정보 또는 랜덤 값과 상기 제1 디바이스의 신원기반 식별 정보로부터 생성되는 인증값인 것을 특징으로 하는 보안키 생성 방법.

청구항 4

제 2 항에 있어서, 상기 (c) 단계는

(c1) 유효 기간 동안만 사용되는 상기 제1 디바이스의 유효 공개키와 유효 개인키를 생성하기 위하여 필요한 유효 상태와 유효 기간에 대한 정보의 요청 메시지를 상기 제1 디바이스로부터 수신하는 단계;

(c2) 상기 제1 디바이스가 사용할 상기 유효 공개키와 유효 개인키의 유효 기간을 계산하는 단계; 및

(c3) 상기 계산한 유효 기간과 상기 유효 상태를 상기 제1 디바이스의 공개키로 암호화하여 상기 제1 디바이스로 송신하는 단계를 포함하는 것을 특징으로 하는 보안키 생성 방법.

청구항 5

제 1 항에 있어서, 상기 보안키 생성 방법은

(d) 상기 유효 기간동안 상기 디바이스를 인증하기 위하여 사용되는 인증키를 상기 제1 디바이스로 송신하는 단계를 더 포함하며,

상기 제1 디바이스는 상기 유효 상태에 대한 정보, 상기 공개키 발생 장치의 식별 정보, 상기 제1 디바이스의 식별 정보로 구성된, 상기 인증키로 암호화된 인증 티켓을 사용하여 디바이스 인증을 수행하는 것을 특징으로 하는 보안키 생성 방법.

청구항 6

다수의 디바이스와 공개키 발생 장치를 구비하는 통신 네트워크에서, 상기 디바이스로 제공되는 보안키를 생성하는 방법에 있어서,

(a) 상기 공개키 발생 장치는 상기 다수의 디바이스들 중 제1 디바이스의 공개키(K_A)와 개인키(K_A^{-1})를 생성하여 상기 제1 디바이스로 송신하는 단계;

(b) 상기 공개키 발생 장치는 유효 기간 동안만 사용되는 상기 제1 디바이스의 유효 공개키와 유효 개인키를 생성하기 위하여 필요한 상기 유효 공개키와 유효 개인키의 유효 기간을 계산하는 단계; 및

(c) 상기 공개키 발생 장치는 상기 계산한 유효 기간과 상기 유효 상태를 상기 제1 디바이스의 공개키로 암호화하여 상기 제1 디바이스로 송신하는 단계를 포함하는 것을 특징으로 하는 보안키 생성 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명에 보안키 생성 방법에 관한 것으로, IP 네트워크에 기반하지 않고도 단위 유효 기간별로 구분된 공개키 기반의 보안 메커니즘을 이용하여 안전하게 데이터 통신을 수행할 수 있는 보안키 생성 방법에 관한 것이다.

배 경 기 술

[0002] 인터넷은 기업 업무 환경의 정보화와 전자상거래 서비스를 드라이브하는 20세기말의 대표적인 패러다임이다. 인터넷의 특성인 개방성과 표준성은 그 사용 주체가 기업이건 개인이든 간에 정보 교환과 정보 공유의 벽을 허물어 버렸다. 반면에 정보의 보호와 안전한 커뮤니케이션 측면에서 인터넷의 특성인 개방성은 인터넷이 가지고 있는 근본적인 취약점으로 산업 발전에 걸림돌이 되고 있다.

[0003] 정보를 다루는 주체들이 서로 신뢰할 수 있는 관계라고 하더라도 인터넷이라는 신뢰할 수 없는 공간을 통해 커뮤니케이션이 이루어지는 한 각각의 서비스 형태나 어플리케이션에 따라 적절한 정보 보호 체계를 구축해야 한다. 전자상거래, 인터넷 뱅킹, 사용자의 인증, 기밀 데이터의 전송 등 각 분야에서 사용되는 정보의 종류가 다양해지고 있으며, 다양한 분야에서 사용하는 정보의 중요성도 증가함에 따라 보안 기술의 적용을 통해 안전한 통신망을 구축하는 것이 네트워크 운용에 있어 기본적인 요구사항이 되고 있다.

[0004] 정보 보호 기술은 여러 가지 형태와 목적을 지니고 있다. 방화벽, 침입탐지, 접근제어, 취약성 분석부터 바이러스 백신에 이르기까지 각각의 독특한 시스템과 시장을 창조해 내었다. 그런데, 전자상거래, 인터넷 뱅킹 서비스 등을 IP 네트워크 기반 환경에서 구축할 때 필수적으로 요구되는 정보보호 기술은 공개키 기반 구조(Public Key Infrastructure,약칭 PKI)라고 할 수가 있다.

[0005] 공개키 기반 구조(Public Key Infrastructure)는 기본적으로 IP 네트워크와 같이 안전이 보장되지 않은 공중망 사용자들이, 신뢰할 수 있는 기관에서 부여된 한 쌍의 공개키와 개인키를 사용함으로써, 안전하고 은밀하게 데이터나 자금을 교환할 수 있게 해주는 방식이다. 지정된 인증기관에 의해 제공되는 공개키로부터 생성된 개인키와 함께 결합되어, 메시지 및 전자서명의 암호화와 복호화에 효과적으로 사용될 수 있다. 공개키와 개인키를 결합하는 방식은 비대칭 암호작성법으로 알려져 있으며, 공개키를 사용하는 시스템을 공개키 기반구조(PKI)라고 부른다.

[0006] 공개키 기반 시스템을 도시하고 있는 도 1을 참고로 공개키 기반 시스템에서 사용하는 보안 기술에 대해 보다 구체적으로 살펴보면, 공개키 기반 시스템은 등록기관(2), 인증기관(3), 저장부(5), 다수의 사용자들이 IP 네트워크(1)를 통해 서로 접속되어 있다. 사용자 1(7)은 IP 네트워크(1)를 통해 인증기관(3)으로 공인 인증서를 요

청한다. 인증기관(3)은 사용자 1(7)로부터 공인 인증서의 발급을 요청받는 경우, 사용자 1(7)의 사용자 정보를 수신하고 수신한 사용자 정보를 등록기관(2)으로 전송하여 사용자 1(7)의 검증을 요청한다. 등록기관(2)은 수신한 사용자 1(7)의 사용자 정보와 저장된 사용자 1(7)의 사용자 정보를 비교하여 사용자를 검증한다. 인증 기관(3)은 등록 기관(2)에서 사용자를 검증한 경우, 사용자 1(7)로 공인 인증서를 발급하고, 발급한 공인 인증서를 저장부(5)에 저장한다. 도 2는 X.509 기반에서 생성되는 공인 인증서의 포맷에 대한 일 예를 도시하고 있다.

[0007] 사용자 2(9)가 사용자 1(7)로 데이터를 송신하고자 하는 경우, 사용자 2(9)는 저장소(5)에 저장된 사용자 1(7)의 공인 인증서에서 사용자 1(7)에 발급된 공개키를 수신받으며, 수신한 사용자 1(7)의 공개키를 이용하여 데이터를 암호화하여 사용자 1(7)로 송신한다. 사용자 1(7)의 개인키는 사용자 1(7)만이 알고 있으므로 사용자는 수신한 데이터를 사용자 1(7)의 개인키를 이용하여 복호화할 수 있다. 한편, 사용자 1(7)은 송신하고자 하는 데이터에 개인키를 이용하여 전자 서명을 하며, 사용자 2(9)는 사용자 1(7)의 공개키를 이용하여 전자 서명을 복호화함으로써, 사용자 1(7)에서 송신된 데이터가 다른 사용자로부터 송신되지 않았음을 검증하게 된다.

발명의 내용

해결 하고자하는 과제

[0008] 최근 들어, 센서 네트워크, 전력선 통신 네트워크, 무선 메쉬 네트워크 등 데이터 전달 매체의 특징과 사용자 환경을 고려한 새로운 네트워크 기술들이 개발되고 있으며, 이들 새로운 네트워크 기술을 상용화하기 위한 노력들이 진행되고 있다. 새롭게 개발된 네트워크에서도 네트워크의 확장에 따른 관리 개체의 증가에도 효율적으로 디바이스를 관리할 수 있고, 안전한 통신망 구축을 위하여 필수적인 보안키 관리 매커니즘의 개발이 요구된다.

[0009] 그러나 위에서 설명한 기존의 공개키 기반의 보안 기술은 기본적으로 IP 네트워크를 기반으로 하기 때문에, IP 네트워크에 기반하지 않은 새로운 네트워크나 이종 네트워크 사이에서 기존의 공개키 기반의 보안 기술을 그대로 적용하지 못한다는 문제점을 가진다.

[0010] 따라서 본 발명이 이루고자 하는 목적은 상기 문제점을 극복하기 위한 것으로, 본 발명은 IP 네트워크에 기반하지 않은 새로운 네트워크나 이종 네트워크에서도 사용할 수 있는 보안키 생성 방법을 제공하는 것이다.

[0011] 본 발명이 이루고자 하는 다른 목적은 인증기관이나 인증서가 없이도 공개키 기반으로 데이터를 보안할 수 있는 간단하고 관리가 용이한 보안키 생성 방법을 제공하는 것이다.

과제 해결수단

[0012] 위에서 설명한 본 발명의 목적을 달성하기 위한 보안키 생성 방법은, 다수의 디바이스와 공개키 발생 장치를 구비하는 통신 네트워크에서 다수의 디바이스들 중 제1 디바이스로 공개키 발생 장치의 공개키를 송신하는 단계와, 제1 디바이스로부터 공개키 발생 장치의 공개키로 암호화된 제1 디바이스의 인증 정보를 수신하고 수신한 인증 정보로부터 제1 디바이스의 공개키(K_A)와 개인키(K_A^{-1})를 생성하여 제1 디바이스로 송신하는 단계 및 유효기간 동안만 사용되는 제1 디바이스의 유효 공개키와 유효 개인키를 생성하기 위하여 필요한 유효 상태와 유효 기간에 대한 정보를 제1 디바이스의 공개키로 암호화하여 제1 디바이스로 송신하는 단계를 포함한다.

[0013] 본 발명의 목적을 달성하기 위한 보안키 생성 방법은, 다수의 디바이스와 공개키 발생 장치를 구비하는 통신 네트워크에서 다수의 디바이스들 중 제1 디바이스의 공개키(K_A)와 개인키(K_A^{-1})를 생성하여 제1 디바이스로 송신하는 단계와, 유효 기간 동안만 사용되는 제1 디바이스의 유효 공개키와 유효 개인키를 생성하기 위한 상기 유효 공개키와 유효 개인키의 유효 기간을 계산하는 단계 및 계산한 유효 기간과 유효 상태를 상기 제1 디바이스의 공개키로 암호화하여 상기 제1 디바이스로 송신하는 단계를 포함하는 것을 특징으로 한다.

효 과

[0014] 본 발명에 따른 보안키 생성 방법은 종래 공개키 기반의 보안 방법에 비해 다음과 같은 다양한 효과들을 가진다.

[0015] 첫째, 본 발명에 따른 보안키 생성 방법은 IP 네트워크를 기반으로 하지 않기 때문에, IP 네트워크에 기반하지

않는 새로운 네트워크나 이종 네트워크에서도 사용할 수 있다.

[0016] 둘째, 본 발명에 따른 보안키 생성 방법은 IP 네트워크로 접속되는 인증기관이나 인증 기관에 의해 발행된 인증서가 없이도 공개키 기반으로 데이터를 보안할 수 있으므로, 간단하게 보안키를 생성할 수 있으며 보안 시스템의 관리 및 보안을 저렴한 비용으로 용이하게 수행할 수 있다.

[0017] 셋째, 본 발명에 따른 보안키 생성 방법은 유효 기간에만 사용되는 유효 공개키와 유효 개인키를 사용하여 송수신되는 데이터를 암호화/복호화함으로써, 보다 안전하게 데이터를 송수신할 수 있다.

발명의 실시를 위한 구체적인 내용

[0018] 이하 첨부한 도면을 참고로 본 발명에 따른 보안키 생성 방법에 대해 보다 구체적으로 살펴본다.

[0019] 도 3은 본 발명의 일 실시예에 따른 보안키 생성 시스템의 기능 블록도를 도시하고 있다.

[0020] 도 3을 참고로 살펴보면, 데이터 통신을 수행하는 다수의 디바이스들(13-1, 13-2,..., 13-n)이 서로 접속되어 있으며, 다수의 디바이스들(13-1, 13-2,..., 13-n)은 공개키 발생 장치(Public Key Generator(PKG), 11)에 접속되어 있다. 다수의 디바이스들(13-1, 13-2,..., 13-n)과 공개키 발생 장치(11)는 안전한 통신 채널로 서로 접속되어 있다. 안전한 통신 채널이란 허가받지 못한 제3자가 공개키 발생 장치(11)와 디바이스 사이의 통신 채널에 접속하지 못하도록 보안된 채널을 의미하며, 유선의 통신 채널 또는 초기에 인증화 단계를 통해 접속되어 있는 통신 채널이 안전한 통신 채널의 일 예이다.

[0021] 다수의 디바이스들(13-1, 13-2,..., 13-n)들은 공개키 발생 장치(11)로 인증 정보를 송신하고, 공개키 발생 장치(11)는 수신한 디바이스들(13-1, 13-2,..., 13-n)의 인증 정보에 기초하여 각 디바이스(13-1, 13-2,..., 13-n)에 대한 개인키와 공개키를 생성하여 각 디바이스(13-1, 13-2,..., 13-n)로 송신한다.

[0022] 도 4는 본 발명의 일 실시예에 따른 보안키 생성 방법을 설명하는 흐름도이다.

[0023] 도 4를 참고로 보다 구체적으로 살펴보면, 공개키 발생 장치(11)는 다수의 디바이스들(13-1, 13-2,..., 13-n) 중 디바이스 1(13-1)로부터 개인키와 공개키의 요청 메시지를 수신한다(S1). 요청 메시지에 응답하여 공개키 발생 장치(11)는 디바이스 1(13-1)로 공개키 발생 장치(11)의 공개키를 송신한다(S3). 공개키 발생 장치(11)는 디바이스 1(13-1)의 인증 정보를 이용하여 디바이스 1(13-1)의 공개키와 개인키를 생성하여 디바이스 1(13-1)로 송신한다(S5).

[0024] 한편, 공개키 발생 장치(11)는 단위 유효 기간동안 구별하여 사용되는 디바이스 1(13-1)의 유효 공개키와 유효 개인키를 생성하는데 사용되는 유효 상태와 유효 기간에 대한 정보를 계산하고(S6), 상기 계산한 유효 상태와 유효 기간에 대한 정보를 디바이스 1(13-1)의 공개키로 암호화하여 디바이스 1(13-1)로 송신한다(S7). 또한, 공개키 발생 장치(11)는 공개키 발생 장치(11)에 접속되어 있는 다수의 디바이스(13-1, 13-2,..., 13-n)들이 서로 인증을 하는데 사용되는 인증 키를 생성하고 생성한 인증 키를 디바이스 1(13-1)로 송신한다(S9).

[0025] 도 5는 단위 유효 기간을 설명하기 위한 도면이다. 도 5를 참고로 보다 구체적으로 살펴보면, 디바이스 1(13-1)가 일정한 공개키와 개인키를 사용하여 데이터를 송수신하는 경우 제3자의 해킹 가능성이 있으며 이는 통신 시스템에 심각한 위협 요소로 작용할 수 있다.

[0026] 따라서 디바이스 1(13-1)은 단위 유효 기간별로 생성되는 유효 개인키와 유효 공개키를 이용하여 데이터를 송수신함으로써, 허락받지 않은 제3자로부터 데이터가 해킹되는 것을 방지한다. 유효 개인키와 유효 공개키는 단위 유효 기간(i-1, i, i+1)에서 남은 유효 기간과 유효 상태를 통해 생성된다.

[0027] 유효 기간(v)은 전체 단위 유효 기간 중 유효 개인키과 유효 공개키를 생성할 때의 시점에서 지나간 유효 기간(tc)를 빼서 계산한다. 유효 상태는 단위 유효 시간의 길이, 유효 개인키와 유효 공캐키를 사용할 수 있는 해당 유효 시간, 유효 개인키와 유효 공개키를 생성한 날짜 정보 등이 사용될 수 있다.

[0028] 도 6은 공개키 발생 장치와 디바이스 1에서 디바이스 1의 공개키와 개인키를 생성하는 과정을 설명하기 위한 흐름도이다.

[0029] 도 6을 참고로 보다 구체적으로 살펴보면, 디바이스 1(13-1)은 랜덤 값을 발생하고 발생한 랜덤 값과 디바이스 1(13-1)의 식별 정보를 이용하여 인증 값을 생성한다(S11). 인증 값을 생성하기 위하여 랜덤 값과 디바이스 1(13-1)의 식별 정보를 인자로 사용하는 인증 값 발생 함수를 사용한다. 생성한 랜덤 값과 인증 값을 수신한 공개키 발생 장치(11)의 공개키로 암호화하고(S13), 디바이스 1(13-1)의 식별 정보와 암호화한 랜덤 값, 인증

값을 공개키 발생 장치(11)로 송신한다(S15).

[0030] 공개키 발생 장치(11)는 자신의 개인키로 디바이스 1(13-1)로부터 수신한 암호화된 랜덤 값, 인증 값을 복호화하고(S16), 복호화한 인증 값에 기초하여 디바이스 1(13-1)을 인증한다(S17). 공개키 발생 장치(11)는 복호화된 랜덤 값과 디바이스 1(13-1)의 식별 정보로부터 인증 값을 생성한다. 공개키 발생 장치(11)는 인증 값을 생성하기 위하여 디바이스 1(13-1)이 인증 값을 생성하는데 사용하는 인증 값 발생 함수와 동일한 인증 값 발생 함수를 사용한다. 공개키 발생 장치(11)는 공개키 발생 장치(11)에서 생성한 인증 값과 복호화한 인증 값이 서로 동일한지 여부에 따라 디바이스 1(13-1)를 인증한다.

[0031] 디바이스 1(13-1)가 인증된 경우, 공개키 발생 장치(11)는 디바이스 1(13-1)의 식별 정보와 마스터 보안 정보를 이용하여 디바이스 1(13-1)의 개인키과 공개키를 생성한다(S18). 마스터 보안 정보란 공개키 발생 장치만 가지고 있는 키 생성을 위한 인자 값이며 공격자는 유추할 수 없는 값이다. 바람직하게, 공개키 발생 장치(11)는 디바이스 1(13-1)의 개인키와 공개키를 생성하기 위하여 디바이스 1(13-1)의 식별 정보를 인자로 사용하는 해쉬 함수를 사용한다.

[0032] 공개키 발생 장치(11)는 생성한 디바이스 1(13-1)의 공개키와 개인키를 안전한 채널을 통해 디바이스 1(13-1)로 송신한다(S19).

[0033] 도 7은 공개키 발생 장치와 디바이스 1에서 유효 공개키와 유효 개인키를 생성하는 과정을 설명하기 위한 흐름도이다.

[0034] 도 7을 참고로 보다 구체적으로 살펴보면, 디바이스 1(13-1)은 공개키 발생 장치(11)로 단위 유효 기간 동안 사용할 유효 공개키와 유효 개인키를 요청하는 메시지를 송신한다(S21). 공개키 발생 장치(11)는 디바이스 1(13-1)로부터 유효 공개키와 유효 개인키의 요청 메지시를 수신하는 경우, 디바이스 1(13-1)의 유효 공개키와 유효 개인키를 생성하는데 사용되는 유효 상태와 유효 기간에 대한 정보를 계산하고(S23), 계산한 유효 상태와 유효 기간에 대한 정보를 디바이스 1(13-1)의 공개키를 이용하여 암호화하여(S24) 디바이스 1(13-1)로 송신한다.

[0035] 디바이스 1(13-1)은 수신한 유효 상태와 유효 기간에 대한 정보를 디바이스 1(13-1)의 개인키로 복호화하고(S27), 복호화한 유효 상태와 유효 기간에 대한 정보를 이용하여 단위 유효 기간(i) 동안 사용할 디바이스 1(13-1)의 유효 개인키와 유효 공개키를 생성한다(S29). 바람직하게, 디바이스 1(13-1)의 유효 개인키와 유효 공개키는 유효 상태와 유효 기간을 인자로 사용하는 해쉬함수을 이용하여 생성한다.

[0036] 도 8은 공개키 발생 장치로부터 수신한 인증키를 이용하여 디바이스들 사이에서 디바이스 인증 절차를 수행하는 과정을 설명하는 흐름도이다.

[0037] 도 8을 참고로 보다 구체적으로 살펴보면, 디바이스 1(13-1)은 공개키 발생 장치(11)로부터 수신한 유효 상태에 대한 정보, 공개키 발생 장치(11)의 식별 정보, 디바이스 1(13-1)의 식별 정보를 이용하여 디바이스 1(13-1)의 인증 티켓을 생성한다(S31). 생성한 인증 티켓을 공개키 발생 장치(11)로부터 수신한 인증 키로 암호화하고(S32), 암호화한 인증 티켓를 디바이스 1(13-1)의 식별 정보와 함께 데이터 통신을 위해 인증하고자 하는 디바이스 2(13-2)로 송신한다(S33). 디바이스 2(13-2)는 공개키 발생 장치(11)로부터 수신한 인증 키를 이용하여 수신한 디바이스 1(13-1)의 인증 티켓을 복호화하고, 디바이스 1(13-1)로부터 수신한 인증 티켓의 유효성을 검증하여 디바이스 1(13-1)을 인증한다(S35). 인증티켓을 암호화하는데 사용하는 인증키는 공개키 발생장치로부터 인증 받은 디바이스들에게만 안전하게 전달된다. 따라서, 동일한 인증키를 사용한 인증티켓은 신뢰할 수 있다. 또한, 인증티켓을 수신한 디바이스는 인증티켓에 포함되어 있는 유효상태 정보를 현재 사용되고 있는 유효상태 정보와 비교함으로써 인증티켓의 유효성을 검증할 수 있다.

[0038] 한편, 디바이스 2(13-2)는 공개키 발생 장치(11)로부터 수신한 유효 상태에 대한 정보, 공개키 발생 장치(11)의 식별 정보, 디바이스 2(13-2)의 식별 정보를 이용하여 디바이스 2(13-2)의 인증 티켓을 생성한다(S36). 생성한 인증 티켓을 공개키 발생 장치(11)로부터 수신한 인증 키로 암호화하고(S37), 암호화한 인증 티켓를 디바이스 2(13-2)의 식별 정보와 함께 데이터 통신을 위해 인증하고자 하는 디바이스 1(13-1)로 송신한다(S38). 디바이스 1(13-1)는 공개키 발생 장치(11)로부터 수신한 인증 키를 이용하여 수신한 디바이스 2(13-2)의 인증 티켓을 복호화하고, 디바이스 2(13-2)로부터 수신한 인증 티켓의 유효성을 검증하여 디바이스 2(13-2)을 인증한다(S39).

[0039] 따라서 디바이스 1(13-1)과 디바이스 2(13-2)는 IP 네트워크에 접속되어 있는 등록 기관, 인증 기관, 공인 인증서 없이도 데이터 통신을 수행하고자 하는 디바이스들 사이의 디바이스 인증을 수행한다.

[0040] 한편, 상술한 본 발명의 일 실시예들은 컴퓨터에서 실행될 수 있는 프로그램으로 작성 가능하고, 컴퓨터로 읽을 수 있는 기록 매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다.

[0041] 상기 컴퓨터로 읽을 수 있는 기록 매체는 마그네틱 저장 매체(예를 들어, 롬, 플로피 디스크, 하드 디스크 등), 광학적 판독 매체(예를 들어, 시디롬, 디브이디 등) 및 캐리어 웨이브(예를 들어, 인터넷을 통한 전송)와 같은 저장 매체를 포함한다.

[0042] 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야에서 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

도면의 간단한 설명

[0043] 도 1은 종래 공개키 기반 시스템을 설명하기 위한 기능 블록도이다.

[0044] 도 2는 종래 공개키 기반 시스템에서 각 디바이스에 발행되는 공인 인증서 포맷의 일 예이다.

[0045] 도 3은 본 발명의 일 실시예에 따른 보안키 생성 시스템의 기능 블록도를 도시하고 있다.

[0046] 도 4는 본 발명의 일 실시예에 따른 보안키 생성 방법을 설명하는 흐름도이다.

[0047] 도 5는 단위 유효 기간을 설명하기 위한 도면이다.

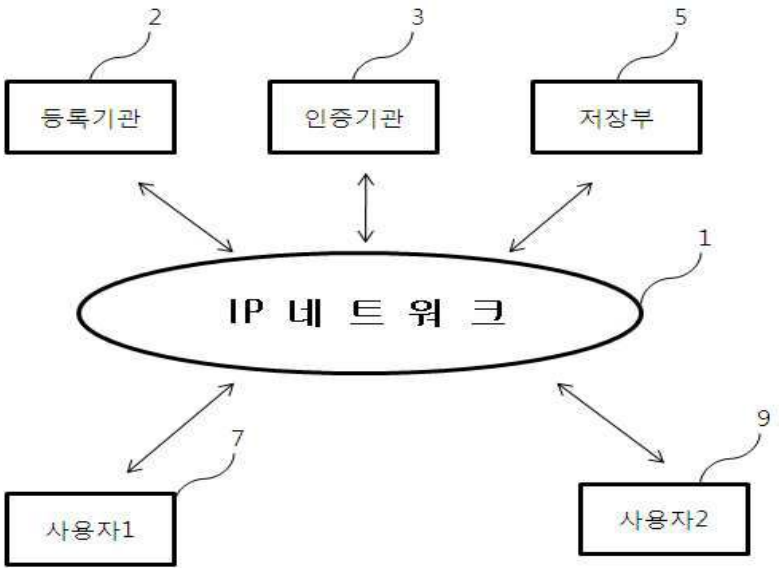
[0048] 도 6은 공개키 발생 장치와 디바이스 1에서 디바이스 1의 공개키와 개인키를 생성하는 과정을 설명하기 위한 흐름도이다.

[0049] 도 7은 공개키 발생 장치와 디바이스 1에서 유효 공개키와 유효 개인키를 생성하는 과정을 설명하기 위한 흐름도이다.

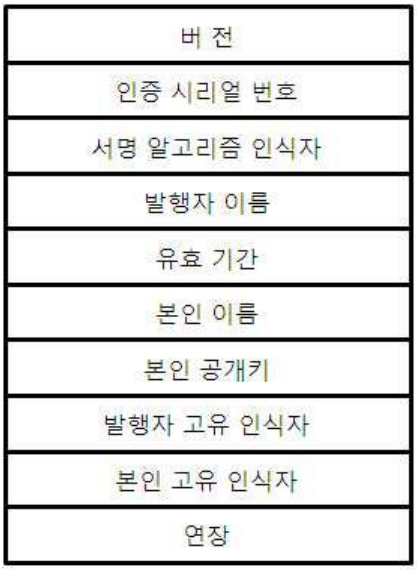
[0050] 도 8은 공개키 발생 장치로부터 수신한 인증키를 이용하여 디바이스들 사이에서 디바이스 인증 절차를 수행하는 과정을 설명하는 흐름도이다.

도면

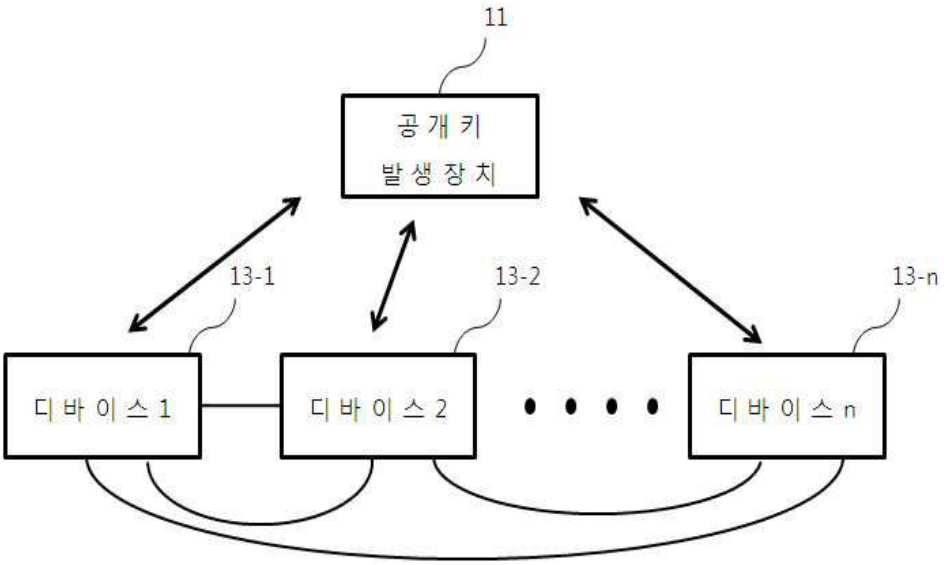
도면1



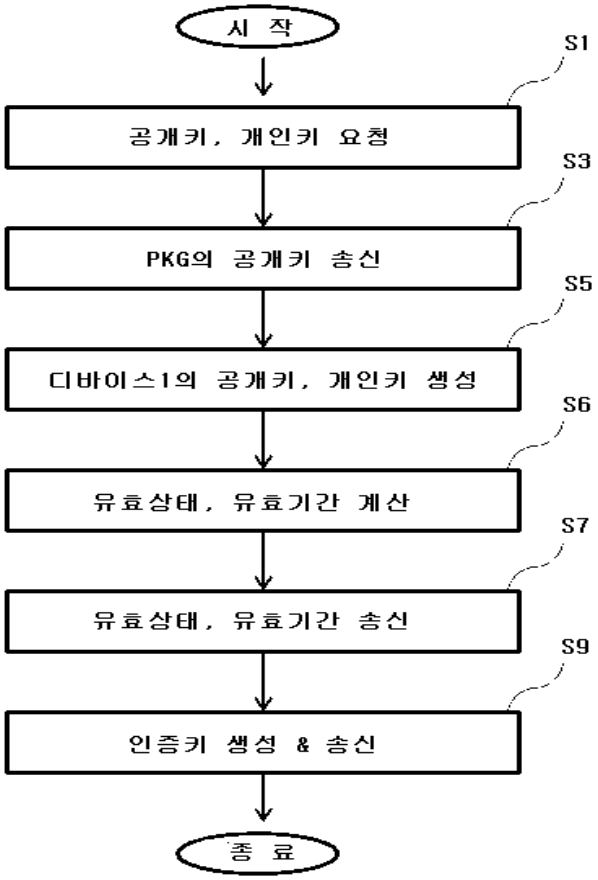
도면2


버 전
인증 시리얼 번호
서명 알고리즘 인식자
발행자 이름
유효 기간
본인 이름
본인 공개키
발행자 고유 인식자
본인 고유 인식자
연장

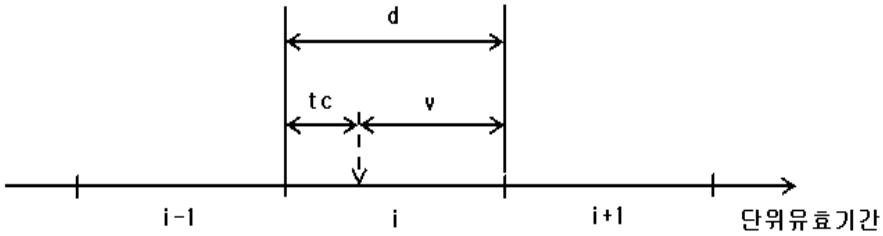
도면3


11
공 개 키
발 생 장 치
13-1
13-2
13-n
디 바 이 스 1
디 바 이 스 2
디 바 이 스 n

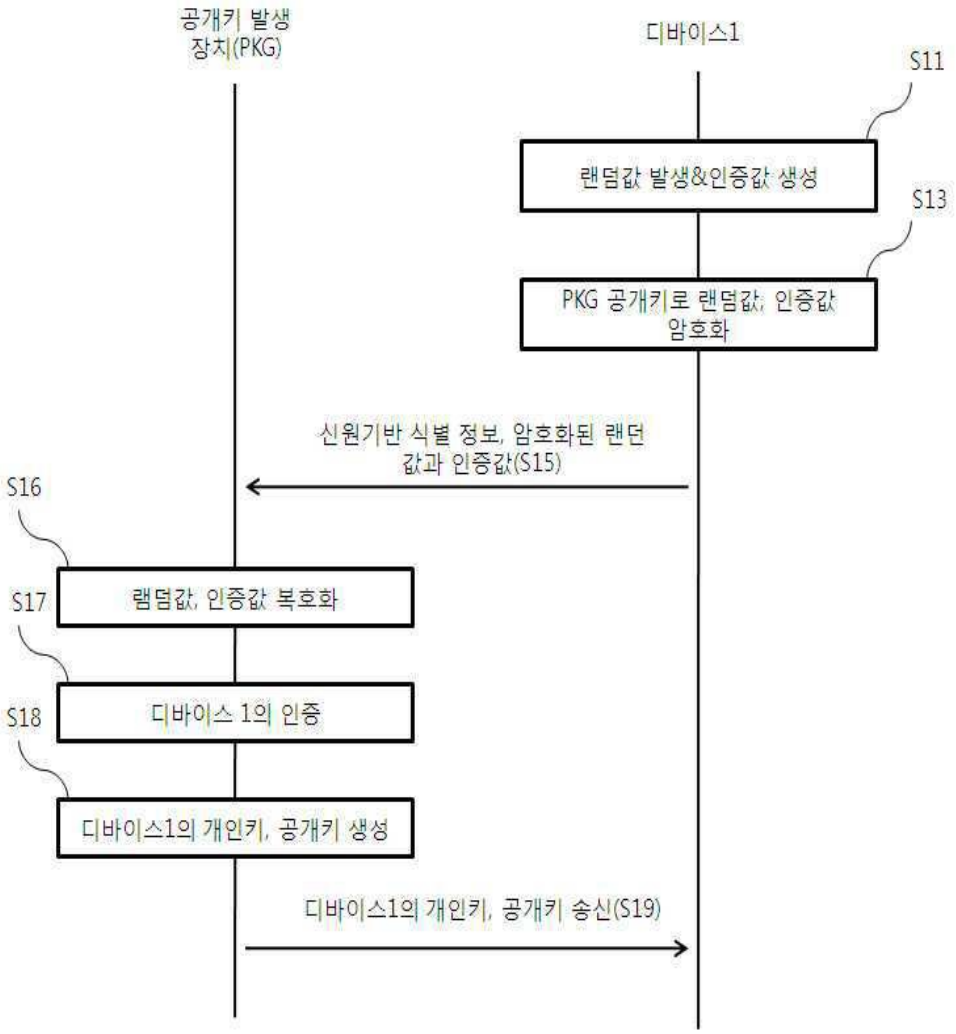
도면4


시 작
S1
공개키, 개인키 요청
S3
PKG의 공개키 송신
S5
디바이스1의 공개키, 개인키 생성
S6
유효상태, 유효기간 계산
S7
유효상태, 유효기간 송신
S9
인증키 생성 & 송신
종 료

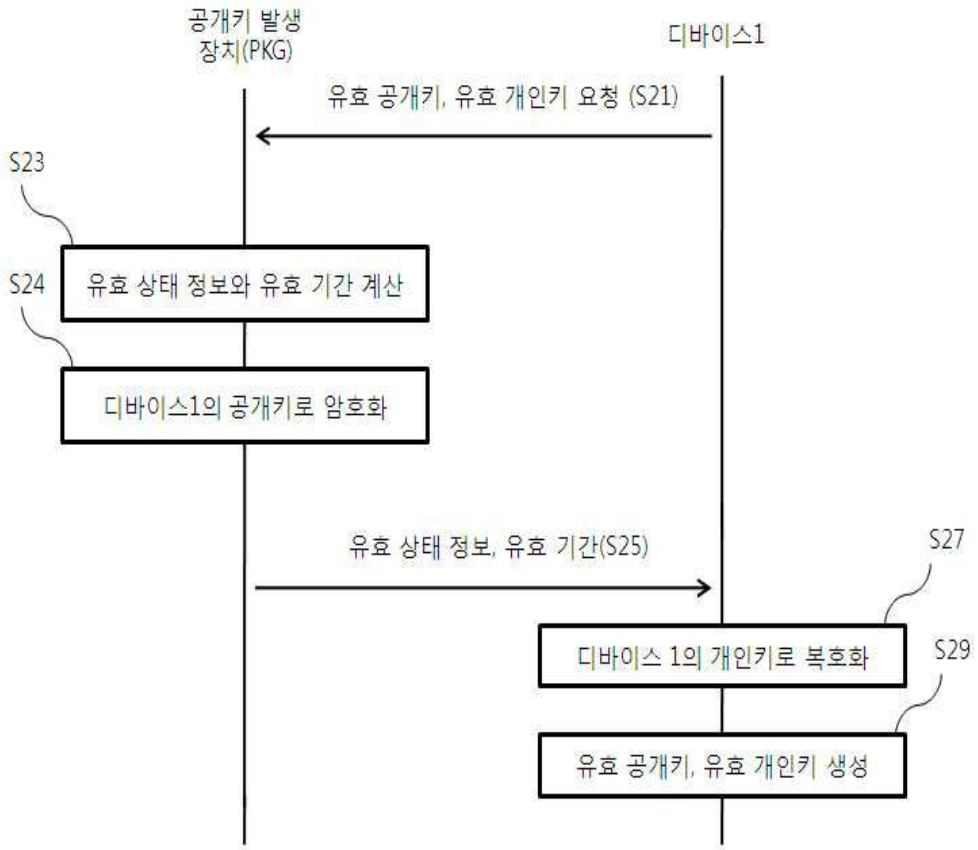
도면5


d
tc
v
i-1
i
i+1
단위유효기간

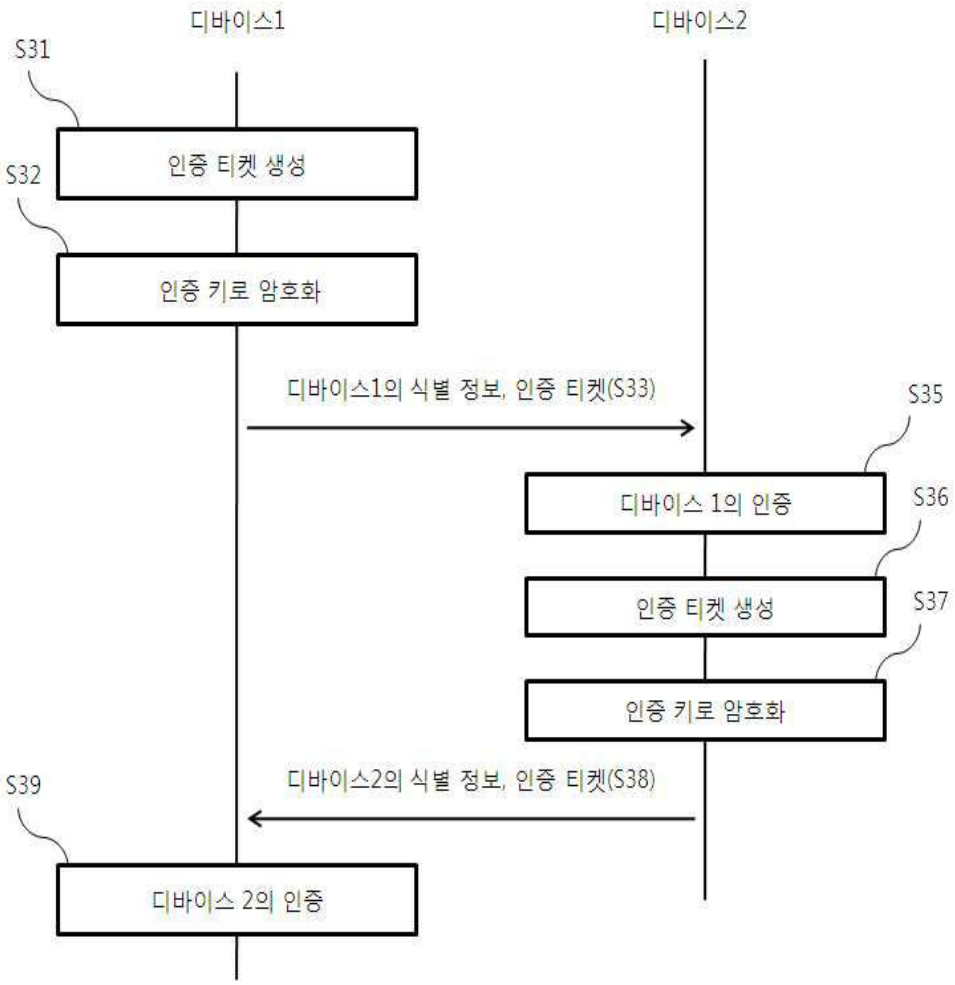
도면6


공개키 발생 장치(PKG)
디바이스1
S11
랜덤값 발생&인증값 생성
S13
PKG 공개키로 랜덤값, 인증값 암호화
신원기반 식별 정보, 암호화된 랜덤 값과 인증값(S15)
S16
램덤값, 인증값 복호화
S17
디바이스 1의 인증
S18
디바이스1의 개인키, 공개키 생성
디바이스1의 개인키, 공개키 송신(S19)

도면7


공개키 발생 장치(PKG)
디바이스1
유효 공개키, 유효 개인키 요청 (S21)
S23
S24
유효 상태 정보와 유효 기간 계산
디바이스1의 공개키로 암호화
유효 상태 정보, 유효 기간(S25)
S27
디바이스 1의 개인키로 복호화
S29
유효 공개키, 유효 개인키 생성

도면8


디바이스1
디바이스2
S31
인증 티켓 생성
S32
인증 키로 암호화
디바이스1의 식별 정보, 인증 티켓(S33)
S35
디바이스 1의 인증
S36
인증 티켓 생성
S37
인증 키로 암호화
디바이스2의 식별 정보, 인증 티켓(S38)
S39
디바이스 2의 인증