(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0059912
(43) 공개일자 2014년05월19일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/30* (2006.01)
(21) 출원번호 10-2012-0126168
(22) 출원일자 2012년11월08일
심사청구일자 없음

(71) 출원인
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
이현숙
경기도 수원시 장안구 조원동 수원광교스위첸아파트 102-603
(74) 대리인
리앤목특허법인

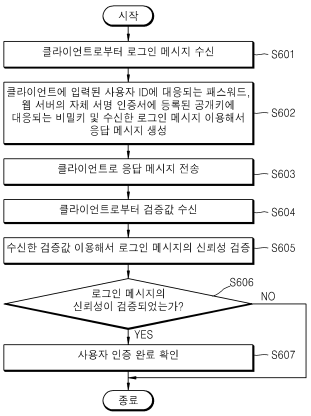
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **웹 서버의 자체 서명 인증서를 이용한 사용자 인증 방법, 이를 수행하기 위한 클라이언트 장치 및 웹 서버를 포함하는 전자 장치**

(57) 요 약

본 발명에 의한 웹 서버의 자체 서명 인증서를 이용한 사용자 인증 방법은, 클라이언트로부터 웹 서버의 자체 서명 인증서에 등록된 공개키를 이용하여 생성된 로그인 메시지를 수신하는 단계; 상기 로그인 메시지 및 상기 공개키에 대응되는 비밀키를 이용해서 응답 메시지를 생성하는 단계; 상기 클라이언트로 상기 생성된 응답 메시지를 전송하는 단계; 상기 클라이언트에서 상기 응답 메시지의 신뢰성이 검증되면 상기 클라이언트로부터 상기 자체 서명 인증서를 이용하여 연결된 SSL 채널을 통해 검증값을 수신하는 단계; 상기 수신한 검증값을 이용하여 상기 로그인 메시지의 신뢰성을 검증하는 단계; 및 상기 로그인 메시지의 신뢰성이 검증되면 사용자 인증 완료를 확인하는 단계를 포함한다.

대 표 도 - 도6



특허청구의 범위

청구항 1

웹 서버의 자체 서명 인증서를 이용한 사용자 인증 방법에 있어서,

클라이언트 장치로부터 웹 서버의 자체 서명 인증서에 등록된 공개키를 이용하여 생성된 로그인 메시지를 수신하는 단계;

상기 로그인 메시지 및 상기 공개키에 대응되는 비밀키를 이용하여 응답 메시지를 생성하는 단계;

상기 클라이언트 장치로 상기 생성된 응답 메시지를 전송하는 단계;

상기 클라이언트 장치에서 상기 응답 메시지의 신뢰성이 검증되면 상기 클라이언트 장치로부터 상기 자체 서명 인증서를 이용하여 연결된 SSL 채널을 통해 검증값을 수신하는 단계;

상기 수신한 검증값을 이용하여 상기 로그인 메시지의 신뢰성을 검증하는 단계; 및

상기 로그인 메시지의 신뢰성이 검증되면 사용자 인증 완료를 확인하는 단계를 포함하는 방법.

청구항 2

제1항에 있어서,

상기 로그인 메시지는 상기 공개키와 상기 클라이언트 장치에서 입력받은 사용자 ID 및 패스워드를 이용하여 생성되는 것을 특징으로 하는 방법.

청구항 3

제2항에 있어서,

상기 응답 메시지를 생성하는 단계는,

상기 사용자 ID에 대응되도록 상기 웹 서버에 등록된 패스워드를 추출하는 단계;

임의의 비밀값을 선택하는 단계; 및

상기 추출된 패스워드, 상기 비밀값, 상기 비밀키 및 상기 로그인 메시지를 이용하여 상기 응답 메시지를 생성하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 4

제1항에 있어서,

상기 응답 메시지를 전송하는 단계는 HTTP 리퀘스트를 통해서 상기 응답 메시지를 전송하는 것을 특징으로 하는 방법.

청구항 5

웹 서버의 자체 서명 인증서를 이용한 사용자 인증 방법에 있어서,

사용자 ID 및 패스워드를 입력받는 단계;

웹 서버의 자체 서명 인증서에 등록된 공개키와 상기 사용자 ID 및 패스워드를 이용하여 로그인 메시지 및 검증값을 생성하는 단계;

상기 웹 서버로 상기 생성된 로그인 메시지를 전송하는 단계;

상기 웹 서버로부터 응답 메시지를 수신하는 단계;

상기 공개키 및 검증값을 이용하여 상기 수신한 응답 메시지의 신뢰성을 검증하는 단계; 및

상기 응답 메시지의 신뢰성이 검증되면 상기 자체 서명 인증서를 이용하여 연결된 SSL 채널을 통해 상기 검증값

을 상기 웹 서버로 전송하는 단계를 포함하는 방법.

청구항 6

제5항에 있어서,

상기 응답 메시지는 상기 로그인 메시지 및 상기 공개키에 대응되는 비밀키를 이용해서 생성되는 것을 특징으로 하는 방법.

청구항 7

제6항에 있어서,

상기 로그인 메시지를 생성하는 단계는,

상기 자체 서명 인증서에 등록된 공개키를 획득하는 단계;

임의의 비밀값을 선택하는 단계;

임의의 RSA(Rivest Shamir Adleman) 키쌍(key pair)을 선택하는 단계; 및

상기 공개키, 상기 비밀값, 상기 RSA 키쌍, 상기 사용자 ID 및 패스워드를 이용하여 상기 로그인 메시지를 생성하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 8

제5항에 있어서,

상기 로그인 메시지를 전송하는 단계는 HTTP 리퀘스트를 통해서 상기 로그인 메시지를 전송하는 것을 특징으로 하는 방법.

청구항 9

웹 서버의 자체 서명 인증서를 이용한 사용자 인증 방법에 있어서,

클라이언트 장치에서 사용자 ID 및 패스워드를 입력받는 단계;

웹 서버의 자체 서명 인증서에 등록된 공개키와 상기 사용자 ID 및 패스워드를 이용하여 상기 클라이언트 장치가 로그인 메시지 및 검증값을 생성하는 단계;

상기 클라이언트 장치가 상기 웹 서버로 상기 생성된 로그인 메시지를 전송하는 단계;

상기 로그인 메시지 및 상기 공개키에 대응되는 비밀키를 이용해서 상기 웹 서버가 응답 메시지를 생성하는 단계;

상기 웹 서버가 상기 클라이언트 장치로 상기 생성된 응답 메시지를 전송하는 단계;

상기 클라이언트 장치가 상기 공개키 및 검증값을 이용하여 상기 응답 메시지의 신뢰성을 검증하는 단계;

상기 응답 메시지의 신뢰성이 검증되면 상기 자체 서명 인증서를 이용하여 연결된 SSL 채널을 통해 상기 클라이언트 장치가 상기 검증값을 상기 웹 서버로 전송하는 단계;

상기 웹 서버가 상기 검증값을 이용하여 상기 로그인 메시지의 신뢰성을 검증하는 단계; 및

상기 로그인 메시지의 신뢰성이 검증되면 상기 웹 서버가 사용자 인증 완료를 확인하는 단계를 포함하는 방법.

청구항 10

제9항에 있어서,

상기 로그인 메시지를 생성하는 단계는,

상기 자체 서명 인증서에 등록된 공개키를 획득하는 단계;

임의의 비밀값을 선택하는 단계;

임의의 RSA(Rivest Shamir Adleman) 키쌍(key pair)을 선택하는 단계; 및

상기 공개키, 상기 비밀값, 상기 RSA 키쌍, 상기 사용자 ID 및 패스워드를 이용하여 상기 로그인 메시지를 생성하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 11

제9항에 있어서,

상기 응답 메시지를 생성하는 단계는,

상기 클라이언트 장치에서 입력받은 사용자 ID에 대응되도록 상기 웹 서버에 등록된 패스워드를 추출하는 단계;

임의의 비밀값을 선택하는 단계; 및

상기 추출된 패스워드, 상기 비밀값, 상기 비밀키 및 상기 로그인 메시지를 이용하여 상기 응답 메시지를 생성하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 12

제9항에 있어서,

상기 로그인 메시지를 전송하는 단계는 HTTP 리퀘스트를 통해서 상기 로그인 메시지를 전송하고,

상기 응답 메시지를 전송하는 단계는 상기 HTTP 리퀘스트를 통해서 상기 응답 메시지를 전송하는 것을 특징으로 하는 방법.

청구항 13

웹 서버를 포함하는 전자 장치에 있어서,

클라이언트 장치와 통신을 수행하기 위한 통신 인터페이스부;

자체 서명 인증서를 생성하는 인증서 생성부;

상기 클라이언트 장치로부터 수신한 로그인 메시지에 대응하여 상기 자체 서명 인증서에 등록된 공개키에 대응되는 비밀키를 이용하여 응답 메시지를 생성하는 응답 메시지 생성부;

상기 자체 서명 인증서를 이용하여 연결된 SSL 채널을 통해서 상기 클라이언트 장치로부터 수신한 검증값을 이용하여 상기 로그인 메시지의 신뢰성을 검증하는 사용자 인증부;

사용자 인증 정보가 저장되는 저장부; 및

사용자 인증 절차를 제어하는 제어부를 포함하며,

상기 제어부는 상기 통신 인터페이스부를 통해 상기 클라이언트 장치로부터 로그인 메시지를 수신하면 상기 응답 메시지 생성부에서 생성된 응답 메시지를 상기 클라이언트 장치로 전송하도록 하는 전자 장치.

청구항 14

제13항에 있어서,

상기 로그인 메시지는 상기 웹 서버의 자체 서명 인증서에 등록된 공개키와 상기 클라이언트 장치에서 입력받은 사용자 ID 및 패스워드를 이용하여 생성되는 것을 특징으로 하는 전자 장치.

청구항 15

제14항에 있어서,

상기 응답 메시지 생성부는 상기 클라이언트 장치에서 입력받은 사용자 ID에 대응되는 패스워드를 상기 저장부로부터 추출하고, 임의의 비밀값을 선택한 후 상기 추출된 패스워드, 상기 선택된 비밀값, 상기 비밀키 및 상기 로그인 메시지를 이용하여 상기 응답 메시지를 생성하는 것을 특징으로 하는 전자 장치.

청구항 16

제13항에 있어서,

상기 제어부는 HTTP 리퀘스트를 통해서 상기 응답 메시지를 상기 클라이언트 장치로 전송하는 것을 특징으로 하는 전자 장치.

청구항 17

클라이언트 장치에 있어서,

웹 서버와 통신을 수행하기 위한 통신 인터페이스부;

사용자로부터 사용자 ID 및 패스워드를 입력받기 위한 사용자 인증 정보 입력부;

상기 웹 서버의 자체 서명 인증서에 등록된 공개키를 획득하기 위한 보안부;

상기 보안부에서 획득한 공개키와 상기 사용자 인증 정보 입력부에서 입력받은 사용자 ID 및 패스워드를 이용하여 로그인 메시지를 생성하는 로그인 메시지 생성부;

상기 보안부에서 획득한 공개키와 상기 사용자 인증 정보 입력부에서 입력받은 사용자 ID 및 패스워드를 이용하여 검증값을 생성하는 검증값 생성부;

상기 웹 서버로부터 수신한 응답 메시지의 신뢰성을 검증하는 응답 메시지 검증부; 및

사용자 인증 절차를 제어하는 제어부를 포함하며,

상기 제어부는 상기 통신 인터페이스부를 통해 상기 로그인 메시지를 상기 웹 서버로 전송하며, 상기 응답 메시지의 신뢰성이 검증되면 상기 검증값 생성부에서 생성된 검증값을 상기 자체 서명 인증서를 이용하여 연결된 SSL 채널을 통해서 상기 웹 서버로 전송하도록 하는 클라이언트 장치.

청구항 18

제17항에 있어서,

상기 응답 메시지는 상기 로그인 메시지 및 상기 공개키에 대응되는 비밀키를 이용해서 생성되는 것을 특징으로 하는 클라이언트 장치.

청구항 19

제18항에 있어서,

상기 로그인 메시지 생성부는 상기 웹 서버의 자체 서명 인증서로부터 공개키를 획득하고, 임의의 비밀값 및 임의의 RSA 키쌍을 선택한 후 상기 공개키, 상기 비밀값, 상기 RSA 키쌍, 상기 사용자 ID 및 패스워드를 이용하여 상기 로그인 메시지를 생성하는 것을 특징으로 하는 클라이언트 장치.

청구항 20

제17항에 있어서,

상기 제어부는 HTTP 리퀘스트를 통해서 상기 로그인 메시지를 상기 웹 서버로 전송하는 것을 특징으로 하는 클라이언트 장치.

명 세 서

기 술 분 야

[0001] 본 발명은 웹 서버의 자체 서명 인증서를 이용한 사용자 인증 방법에 관한 것이다.

배 경 기 술

[0002] 클라우드 컴퓨팅(cloud computing) 환경에서는 네트워크에 연결된 여러 자원을 동일한 네트워크에 연결된 클라이언트 장치에서 활용할 수 있는 특성을 갖는다.

[0003] 네트워크에 연결되는 전자장치들의 내부에 웹 서버를 구축함으로써 동일한 네트워크에 연결된 클라이언트 장치

상의 웹 브라우저를 통해 전자장치들에 접근하고 사용하는 것이 가능하다. 즉, 사용자는 자신이 원하는 전자장치에 접속하기 위해 클라이언트 장치의 웹 브라우저에 해당 전자장치의 IP 주소를 입력하면 해당 전자장치를 제어하기 위한 웹 페이지에 접속할 수 있다.

[0004] 이와 같은 웹 브라우저를 통한 전자장치로의 접속은 정당한 사용자에게만 서비스를 제공하기 위해 안전한 사용자 인증 방법이 요구된다. 그런데, HTTP(hypertext transfer protocol) 통신을 기반으로 하여 안전한 사용자 인증 방법을 구현하는 것을 쉽지 않다. 또한, HTTP에 SSL(Secure Sorket Layer)로 신뢰성 있는 채널인 HTTPs를 생성하여 인증 정보를 전송하는 방식은 전자장치마다 인증기관(Certificate Authority)이 발급한 인증서를 저장하여야 하므로 인증서 발급 비용이 발생하는 단점이 있다. 또한, 챌린지-리스폰스(Challenge-Response) 프로토콜을 이용한 HTTP 인증 기법도 있지만 이는 MD5(Message-Digest algorithm 5)와 같이 안전하지 않은 해쉬함수를 이용하여 설계된 단점이 있다.

발명의 내용

해결하려는 과제

[0005] 웹 서버의 자체 서명 인증서를 이용하여 안전한 패스워드 기반의 사용자 인증 방법을 제공하고자 한다.

과제의 해결 수단

[0006] 상기 기술적 과제를 해결하기 위한 본 발명의 실시예에 따른 웹 서버의 자체 서명 인증서를 이용한 사용자 인증 방법은, 웹 서버의 자체 서명 인증서를 이용한 사용자 인증 방법에 있어서, 클라이언트 장치로부터 웹 서버의 자체 서명 인증서에 등록된 공개키를 이용하여 생성된 로그인 메시지를 수신하는 단계; 상기 로그인 메시지 및 상기 공개키에 대응되는 비밀키를 이용하여 응답 메시지를 생성하는 단계; 상기 클라이언트 장치로 상기 생성된 응답 메시지를 전송하는 단계; 상기 클라이언트 장치에서 상기 응답 메시지의 신뢰성이 검증되면 상기 클라이언트 장치로부터 상기 자체 서명 인증서를 이용하여 연결된 SSL 채널을 통해 검증값을 수신하는 단계; 상기 수신한 검증값을 이용하여 상기 로그인 메시지의 신뢰성을 검증하는 단계; 및 상기 로그인 메시지의 신뢰성이 검증되면 사용자 인증 완료를 확인하는 단계를 포함할 수 있다.

[0007] 이때, 상기 로그인 메시지는 상기 공개키와 상기 클라이언트 장치에서 입력받은 사용자 ID 및 패스워드를 이용하여 생성될 수 있다.

[0008] 또한 이때, 상기 응답 메시지를 생성하는 단계는, 상기 사용자 ID에 대응되도록 상기 웹 서버에 등록된 패스워드를 추출하는 단계; 임의의 비밀값을 선택하는 단계; 및 상기 추출된 패스워드, 상기 비밀값, 상기 비밀키 및 상기 로그인 메시지를 이용하여 상기 응답 메시지를 생성하는 단계를 포함할 수 있다.

[0009] 한편, 상기 응답 메시지를 전송하는 단계는 HTTP 리퀘스트를 통해서 상기 응답 메시지를 전송할 수 있다.

[0010] 상기 기술적 과제를 해결하기 위한 본 발명의 다른 실시예에 따른 웹 서버를 포함하는 전자 장치는, 클라이언트 장치와 통신을 수행하기 위한 통신 인터페이스부; 자체 서명 인증서를 생성하는 인증서 생성부; 상기 클라이언트 장치로부터 수신한 로그인 메시지에 대응하여 상기 자체 서명 인증서에 등록된 공개키에 대응되는 비밀키를 이용하여 응답 메시지를 생성하는 응답 메시지 생성부; 상기 자체 서명 인증서를 이용하여 연결된 SSL 채널을 통해서 상기 클라이언트 장치로부터 수신한 검증값을 이용하여 상기 로그인 메시지의 신뢰성을 검증하는 사용자 인증부; 사용자 인증 정보가 저장되는 저장부; 및 사용자 인증 절차를 제어하는 제어부를 포함하며, 상기 제어부는 상기 통신 인터페이스부를 통해 상기 클라이언트 장치로부터 로그인 메시지를 수신하면 상기 응답 메시지 생성부에서 생성된 응답 메시지를 상기 클라이언트 장치로 전송하도록 할 수 있다.

[0011] 이때, 상기 로그인 메시지는 상기 웹 서버의 자체 서명 인증서에 등록된 공개키와 상기 클라이언트 장치에서 입력받은 사용자 ID 및 패스워드를 이용하여 생성될 수 있다.

[0012] 또한 이때, 상기 응답 메시지 생성부는 상기 클라이언트 장치에서 입력받은 사용자 ID에 대응되는 패스워드를 상기 저장부로부터 추출하고, 임의의 비밀값을 선택한 후 상기 추출된 패스워드, 상기 선택된 비밀값, 상기 비밀키 및 상기 로그인 메시지를 이용하여 상기 응답 메시지를 생성할 수 있다.

[0013] 한편, 상기 제어부는 HTTP 리퀘스트를 통해서 상기 응답 메시지를 상기 클라이언트 장치로 전송할 수 있다.

발명의 효과

[0014] 상기된 바에 따르면, 웹 서버의 자체 서명 인증서를 이용하여 로그인 메시지 및 이에 대응되는 응답 메시지를 생성하고, 응답 메시지의 신뢰성이 검증되면 자체 서명 인증서를 이용하여 연결된 SSL 채널을 통해 검증값을 전송함으로써 클라이언트 장치와 웹 서버가 키를 공유하지 않고도 안전하게 사용자 인증을 수행할 수 있는 장점이 있다.

[0015] 또한, 인증기관에서 발급된 인증서의 사용 없이 웹 서버의 자체 서명 인증서를 이용하여 HTTP 프로토콜 상에서 사용자 ID 및 패스워드만을 이용하여 안전하게 사용자 인증을 수행할 수 있는 장점이 있다.

도면의 간단한 설명

[0016] 도 1은 본 발명의 실시예에 따른 웹 서버의 자체 서명 인증서(self-signed certificate)를 이용한 사용자 인증 방법을 실시하기 위한 환경을 도시한 도면이다.

도 2는 본 발명의 실시예에 따른 웹 서버의 자체 서명 인증서를 이용한 사용자 인증 방법을 수행하기 위한 클라이언트 장치의 구성을 도시한 도면이다.

도 3은 본 발명의 실시예에 따른 웹 서버의 자체 서명 인증서를 이용한 사용자 인증 방법을 수행하기 위한 웹 서버를 포함하는 복합기의 구성을 도시한 도면이다.

도 4는 본 발명의 실시예에 따른 웹 서버의 자체 서명 인증서를 이용한 사용자 인증 방법을 수행할 때 클라이언트 장치 및 복합기에서 수행되는 동작을 도시한 도면이다.

도 5 내지 도 7은 본 발명의 실시예에 따른 웹 서버의 자체 서명 인증서를 이용한 사용자 인증 방법을 설명하기 위한 순서도들이다.

발명을 실시하기 위한 구체적인 내용

[0017] 이하에서는 도면을 참조하여 본 발명의 실시예들을 상세히 설명한다. 본 실시예들의 특징을 보다 명확히 설명하기 위하여 이하의 실시예들이 속하는 기술분야에서 통상의 지식을 가진 자에게 널리 알려져 있는 사항들에 관해서는 자세한 설명은 생략하기로 한다.

[0018] 도 1은 본 발명의 실시예에 따른 웹 서버의 자체 서명 인증서(self-signed certificate)를 이용한 사용자 인증 방법을 실시하기 위한 환경을 도시한 도면이다.

[0019] 도 1을 참조하면, 클라이언트 장치(100)와 웹 서버가 포함된 복합기(200)는 동일한 네트워크(300)에 연결되어 있다. 이때, 도 1에서는 웹 서버가 포함된 전자장치의 일 예로 복합기(200)를 들었으나 이 외에 라우터 등 다양한 종류의 전자장치로 구현될 수 있다. 사용자는 클라이언트 장치(100)에서 네트워크(300)를 통해 복합기(200)에 접속하고 이를 제어할 수 있다. 그런데, 정당한 사용자만이 복합기(200)에 접속할 수 있도록 하기 위해서 사용자 인증 과정이 필요하다. 사용자 인증을 위해 사용자가 클라이언트 장치(100)상의 웹 브라우저에 사용자 인증 정보, 즉 사용자 ID 및 패스워드를 입력하면, 클라이언트 장치(100)는 네트워크(300)를 통해 복합기(200)와 통신을 함으로써 사용자 인증 과정을 수행할 수 있다. 자세한 사용자 인증 방법은 아래에서 자세히 설명하도록 한다.

[0020] 도 2는 본 발명의 실시예에 따른 웹 서버의 자체 서명 인증서를 이용한 사용자 인증 방법을 수행하기 위한 클라이언트 장치의 구성을 도시한 도면이다. 도 2를 참조하면, 클라이언트 장치(100)는 통신 인터페이스부(110), 제어부(120), 사용자 인증 정보 입력부(130), 보안부(140), 로그인 메시지 생성부(150), 응답 메시지 검증부(160) 및 검증값 생성부(170)를 포함할 수 있다. 각 구성의 구체적인 동작은 아래에서 도 4를 참조하여 자세하게 설명하도록 한다.

[0021] 도 3은 본 발명의 실시예에 따른 웹 서버의 자체 서명 인증서를 이용한 사용자 인증 방법을 수행하기 위한 웹 서버를 포함하는 복합기의 구성을 도시한 도면이다. 도 3을 참조하면, 웹 서버를 포함하는 복합기(200)는 통신 인터페이스부(210), 제어부(220), 인증서 생성부(230), 응답 메시지 생성부(240), 사용자 인증부(250) 및 저장부(260)를 포함할 수 있다. 각 구성의 구체적인 동작은 아래에서 도 4를 참조하여 자세하게 설명하도록 한다.

[0022] 도 4는 본 발명의 실시예에 따른 웹 서버의 자체 서명 인증서를 이용한 사용자 인증 방법을 수행할 때 클라이언트 장치 및 복합기에서 수행되는 동작을 도시한 도면이다.

[0023] 이하에서는 도 2 내지 도 4를 참조하여 본 발명의 실시예에 따른 웹 서버의 자체 서명 인증서를 이용한 사용자

인증 방법을 상세하게 설명한다.

[0024] S401 단계에서 클라이언트 장치(100)의 사용자 인증 정보 입력부(130)는 사용자로부터 사용자 인증 정보, 즉 사용자 ID 및 패스워드를 입력받는다. 사용자 인증 정보가 입력되면 사용자 인증 절차가 개시되고, 클라이언트 장치(100)의 보안부(140)는 복합기(200)의 인증서 생성부(230)에서 생성된 자체 서명 인증서(self-signed certificate)로부터 공개키를 획득한다.

[0025] S402 단계에서 클라이언트 장치(100)의 로그인 메시지 생성부(150) 및 검증값 생성부는 보안부(140)에서 획득한 공개키와 사용자 인증 정보 입력부(130)에서 입력받은 사용자 ID 및 패스워드를 이용하여 로그인 메시지 및 검증값을 각각 생성한다.

[0026] 로그인 메시지 "LoginMsg" 및 검증값 "Verifier"를 생성하는 구체적인 방법을 설명하면 다음과 같다. 보안부(140)에서 획득한 공개키가 "PK=e_s"이고 패스워드를 "PW"라고 가정한다. 로그인 메시지 생성부(150)는 임의의 비밀값 "u"를 선택하고, 임의의 RSA(Rivest Shamir Adleman) 키쌍(key pair) "(PK', SK')=(e_c, d_c)"을 생성한다. 그리고 "LoginMsg=[u H(PW)^{d_c}, u^{e_s} H(PW)]=[R_1, R_2]"와 같이 로그인 메시지를 생성한다. 이때, H는 복합기(200)에 포함된 웹 서버가 웹 브라우저를 통해 클라이언트 장치(100)와 공유한 해쉬함수이다. 또한, "Verifier=[verifier_c, verifier_s]=[(u, d_c), e_c]"와 같이 검증값을 생성한다.

[0027] S402 단계에서 로그인 메시지 및 검증값의 생성이 완료되면 S403 단계에서 클라이언트 장치(100)의 제어부(120)는 통신 인터페이스부(110)를 통해 복합기(200)의 웹 서버로 생성된 로그인 메시지를 전송한다. 이때, 로그인 메시지는 HTTP 리퀘스트를 통해서 전송될 수 있다.

[0028] 복합기(200)의 제어부(220)는 통신 인터페이스부(210)를 통해 클라이언트 장치(100)로부터 전송되는 로그인 메시지를 수신하여, 이를 응답 메시지 생성부(240)에 전달하고 저장부(260)에 저장한다. 복합기(200)가 로그인 메시지를 수신하면 이에 대응하여 응답 메시지 생성부(240)는 S404 단계에서 응답 메시지를 생성한다. 응답 메시지 생성부(240)는 사용자 인증 정보 입력부(130)에서 입력받은 사용자 ID에 대응되는 패스워드를 저장부(260)로부터 추출하고, 추출된 패스워드, 자체 서명 인증서에 등록된 공개키에 대응되는 비밀키 및 수신한 로그인 메시지를 이용하여 응답 메시지를 생성한다.

[0029] 응답 메시지 "ReplyMsg"를 생성하는 구체적인 방법을 설명하면 다음과 같다. 사용자 ID에 대응되는 패스워드를 "PW"라고 하고 공개키에 대응되는 비밀키를 "SK=d_s"라고 가정한다. 응답 메시지 생성부(240)는 임의의 비밀값 "v"를 선택한다. 이어서, "u'=R_2^{d_s}/H(PW)^{d_s}"에 따라 "u'"를 획득하고, "ReplyMsg=[v H(PW)^{d_s}, v R_1/{R_2^{d_s}/H(PW)^{d_s}}, H(u', v)]=[R_3, R_4, R_5]"에 따라 응답 메시지를 생성한다.

[0030] S404 단계에서 응답 메시지의 생성이 완료되면 S405 단계에서 복합기(200)의 제어부(220)는 통신 인터페이스부(120)를 통해 클라이언트 장치(100)로 생성된 응답 메시지를 전송한다. 이때, 응답 메시지는 HTTP 리퀘스트를 통해서 전송될 수 있다.

[0031] 클라이언트 장치(100)의 제어부(120)는 통신 인터페이스부(110)를 통해 복합기(200)로부터 전송되는 응답 메시지를 수신하여, 이를 응답 메시지 검증부(160)로 전달한다. S406 단계에서 응답 메시지 검증부(160)는 보안부(140)에서 획득한 공개키 및 검증값 생성부(170)에서 생성된 검증값을 이용하여 수신한 응답 메시지의 신뢰성을 검증한다.

[0032] 응답 메시지의 신뢰성을 검증하는 구체적인 방법을 설명하면 다음과 같다. 응답 메시지 검증부(160)는 "v=R_4/H(PW)^{d_c}"에 따라 "v"를 획득하고, "R_3^{e_s}/H(PW)=(R_4/H(PW)^{d_c})" 및 "R_5=H(u, v)"를 만족하는지 여부를 판단한다. 만약, 이를 만족한다면 응답 메시지의 신뢰성이 인정되는 것으로 판단하고, 만족하지 않는다면 응답 메시지의 신뢰성이 인정되지 않는 것으로 판단한다.

[0033] 응답 메시지의 신뢰성이 인정되지 않으면 사용자 인증 절차는 종료된다. 하지만, 응답 메시지의 신뢰성이 인정되면 S407 단계에서 클라이언트 장치(100)의 제어부(120)는 자체 서명 인증서를 이용하여 연결된 SSL(Secure Sockets Layer) 채널을 통해서 검증값 생성부(170)가 생성한 검증값을 복합기(200)로 전송한다.

[0034] 복합기(200)의 제어부(220)는 통신 인터페이스부(210)를 통해서 클라이언트 장치(100)가 전송한 검증값을 수신하여 사용자 인증부(250)로 전달한다. S408 단계에서 사용자 인증부(250)는 수신한 검증값을 이용하여 로그인 메시지의 신뢰성을 검증한다. 로그인 메시지의 신뢰성이 인정되면 사용자 인증에 성공한 것으로 판단하고, 로그인 메시지의 신뢰성이 인정되지 않으면 사용자 인증에 실패한 것으로 판단한다.

[0035] 로그인 메시지의 신뢰성을 검증하는 구체적인 방법을 설명하면 다음과 같다.

"R_1^{e_c}/H(PW)=(R_2^{d_s}/H(PW)^{d_s})^{d_c}"를 만족하는지 여부를 판단하여 만약, 이를 만족한다면 로그인 메시지의 신뢰성이 인정되는 것으로 판단하고, 만족하지 않는다면 로그인 메시지의 신뢰성이 인정되지 않는 것으로 판단한다.

[0036] 도 5 내지 도 7은 본 발명의 실시예에 따른 웹 서버의 자체 서명 인증서를 이용한 사용자 인증 방법을 설명하기 위한 순서도들이다. 이하에서는 도 5 내지 도 7을 참조하여 본 발명의 실시예에 따른 웹 서버의 자체 서명 인증서를 이용한 사용자 인증 방법을 자세히 설명한다. 다만, 로그인 메시지 및 응답 메시지의 생성 및 검증에 대한 구체적인 방법은 상기의 도 2 내지 도 4에 대한 설명 부분에서 자세하게 설명하였으므로 이하에서는 생략한다.

[0037] 도 5의 순서도는 본 발명의 실시예에 따른 사용자 인증 방법 중 클라이언트 장치와 웹 서버를 포함하는 시스템 전체에서 수행되는 단계들을 포함한다. 도 5를 참조하면, S501 단계에서 클라이언트 장치에서 사용자로부터 사용자 인증 정보, 즉 사용자 ID 및 패스워드를 입력받는다. S502 단계에서는 클라이언트 장치가 웹 서버의 자체 서명 인증서에 등록된 공개키, 사용자 ID 및 패스워드를 이용하여 로그인 메시지 및 검증값을 생성한다. S503 단계에서는 클라이언트 장치가 S502 단계에서 생성된 로그인 메시지를 웹 서버로 전송한다. 이때, 로그인 메시지는 HTTP 리퀘스트를 통해서 전송될 수 있다.

[0038] S504 단계에서 웹 서버는 S501 단계에서 입력받은 사용자 ID에 대응되는 패스워드, 웹 서버의 자체 서명 인증서에 등록된 공개키에 대응되는 비밀키 및 수신한 로그인 메시지를 이용하여 응답 메시지를 생성한다. S505 단계에서 웹 서버는 S504 단계에서 생성된 응답 메시지를 클라이언트 장치로 전송한다. 이때, 응답 메시지는 HTTP 리퀘스트를 통해서 전송될 수 있다.

[0039] S506 단계에서 클라이언트 장치는 웹 서버의 자체 서명 인증서에 등록된 공개키 및 S502 단계에서 생성된 검증값을 이용하여 수신한 응답 메시지의 신뢰성을 검증한다. S507 단계에서 응답 메시지의 신뢰성이 검증되었는지를 판단하여 신뢰성이 검증되었다면 S508 단계로 진행하고, 신뢰성이 검증되지 않았다면 사용자 인증 절차를 종료한다.

[0040] S508 단계에서는 웹 서버의 자체 서명 인증서를 이용하여 연결된 SSL 채널을 통해서 클라이언트 장치가 웹 서버로 S502 단계에서 생성된 검증값을 전송한다. S509 단계에서 웹 서버는 수신한 검증값을 이용해서 S503 단계에서 수신한 로그인 메시지의 신뢰성을 검증한다. S510 단계에서는 로그인 메시지의 신뢰성이 검증되었는지를 판단하여 신뢰성이 검증되었다면 S511 단계로 진행하고, 신뢰성이 검증되지 않았다면 사용자 인증 절차를 종료한다. S511 단계에서는 사용자 인증이 완료되었음을 확인하고 사용자 인증 절차를 종료한다.

[0041] 도 6의 순서도는 본 발명의 실시예에 따른 사용자 인증 방법 중 웹 서버에서 수행되는 단계들을 포함한다. 도 6을 참조하면, S601 단계에서 클라이언트 장치로부터 로그인 메시지를 수신한다. 이때, 로그인 메시지는 웹 서버의 자체 서명 인증서에 등록된 공개키를 이용하여 생성된 것이다. 또한 이때, 로그인 메시지는 HTTP 리퀘스트를 통해서 수신될 수 있다.

[0042] 이어서 S602 단계에서 클라이언트 장치에 입력된 사용자 ID에 대응되는 패스워드, 웹 서버의 자체 서명 인증서에 등록된 공개키에 대응되는 비밀키 및 S501 단계에서 수신한 로그인 메시지를 이용하여 응답 메시지를 생성한다. 생성된 응답 메시지는 S603 단계에서 클라이언트 장치로 전송된다. 이때, 응답 메시지는 HTTP 리퀘스트를 통해서 전송될 수 있다.

[0043] 클라이언트 장치에서 응답 메시지의 신뢰성이 검증되면 S604 단계에서 클라이언트 장치로부터 검증값을 수신한다. 이때, 검증값은 웹 서버의 자체 서명 인증서를 이용하여 연결된 SSL 채널을 통해서 수신될 수 있다. 그리고 S605 단계에서는 수신한 검증값을 이용하여 S601 단계에서 수신한 로그인 메시지의 신뢰성을 검증한다. S606 단계에서는 로그인 메시지의 신뢰성이 검증되었는지를 판단하여 신뢰성이 검증되었다면 S607 단계로 진행하고, 신뢰성이 검증되지 않았다면 사용자 인증 절차를 종료한다. S607 단계에선느 사용자 인증이 완료되었음을 확인하고 사용자 인증 절차를 종료한다.

[0044] 도 7의 순서도는 본 발명의 실시예에 따른 사용자 인증 방법 중 클라이언트 장치에서 수행되는 단계들을 포함한다. 도 7을 참조하면, S701 단계에서 사용자로부터 사용자 인증 정보, 즉 사용자 ID 및 패스워드를 입력받음으로써 사용자 인증 절차가 시작된다. S702 단계에서는 웹 서버의 자체 서명 인증서에 등록된 공개키, S701 단계에서 입력받은 사용자 ID 및 패스워드를 이용하여 로그인 메시지 및 검증값을 생성한다.

[0045] 이어서 S703 단계에서는 S702 단계에서 생성된 로그인 메시지를 웹 서버로 전송하고, S704 단계에서 웹 서버로부터 응답 메시지를 수신한다. 이때, 로그인 메시지 및 응답 메시지의 송수신은 HTTP 리퀘스트를 통해서 수행될 수 있다. 또한 이때, 응답 메시지는 S701 단계에서 입력받은 사용자 ID에 대응되는 패스워드, 웹 서버의 자체

서명 인증서에 등록된 공개키에 대응되는 비밀키 및 S702 단계에서 생성된 로그인 메시지를 이용하여 웹 서버에서 생성한 것이다.

[0046] S705 단계에서는 웹 서버의 자체 서명 인증서에 등록된 공개키 및 S702 단계에서 생성된 검증값을 이용하여 수신한 응답 메시지의 신뢰성을 검증한다. S706 단계에서 응답 메시지의 신뢰성이 검증되었는지를 판단하여 신뢰성이 검증되었다면 S707 단계로 진행하고, 신뢰성이 검증되지 않았다면 사용자 인증 절차를 종료한다.

[0047] S707 단계에서는 웹 서버의 자체 서명 인증서를 이용하여 연결된 SSL 채널을 통해서 웹 서버로 S702 단계에서 생성된 검증값을 전송함으로써 절차는 종료된다.

[0048] 이와 같이 웹 서버의 자체 서명 인증서를 이용하여 로그인 메시지 및 이에 대응되는 응답 메시지를 생성하고, 응답 메시지의 신뢰성이 검증되면 자체 서명 인증서를 이용하여 연결된 SSL 채널을 통해 검증값을 전송함으로써 클라이언트 장치와 웹 서버가 키를 공유하지 않고도 안전하게 사용자 인증을 수행할 수 있는 장점이 있다.

[0049] 또한, 인증기관에서 발급된 인증서의 사용 없이 웹 서버의 자체 서명 인증서를 이용하여 HTTP 프로토콜상에서 사용자 ID 및 패스워드만을 이용하여 안전하게 사용자 인증을 수행할 수 있는 장점이 있다.

[0050] 이제까지 본 발명에 대하여 그 바람직한 실시예들을 중심으로 살펴보았다. 본 발명에 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 한다.

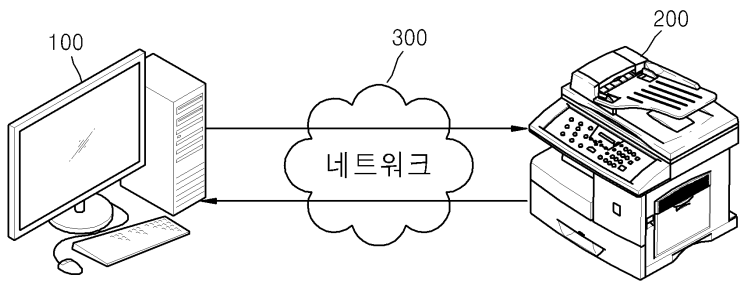
부호의 설명

[0051]

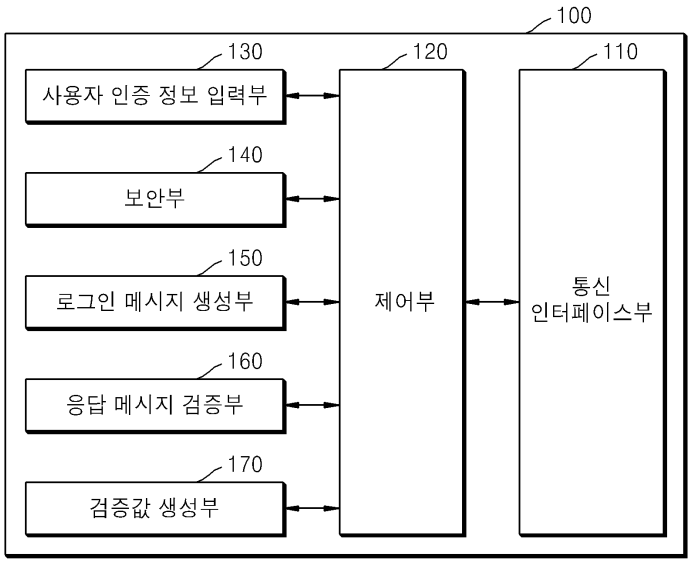
100: 클라이언트 장치	110: 통신 인터페이스부
120: 제어부	130: 사용자 인증 정보 입력부
140: 보안부	150: 로그인 메시지 생성부
160: 응답 메시지 검증부	170: 검증값 생성부
200: 웹 서버가 포함된 복합기	210: 통신 인터페이스부
220: 제어부	230: 인증서 생성부
240: 응답 메시지 생성부	250: 사용자 인증부
260: 저장부	300: 네트워크

도면

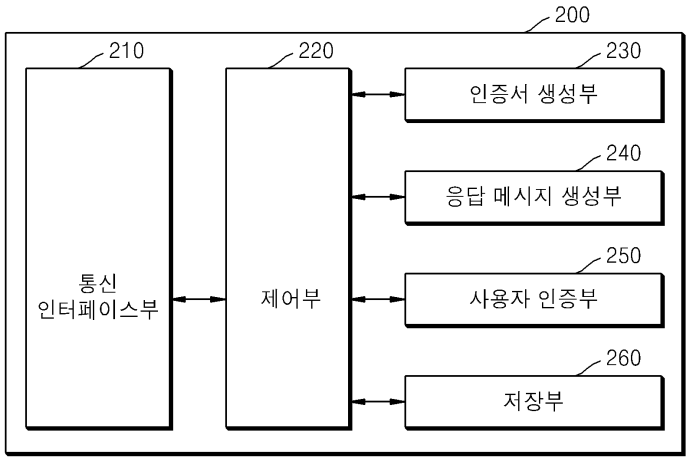
도면1



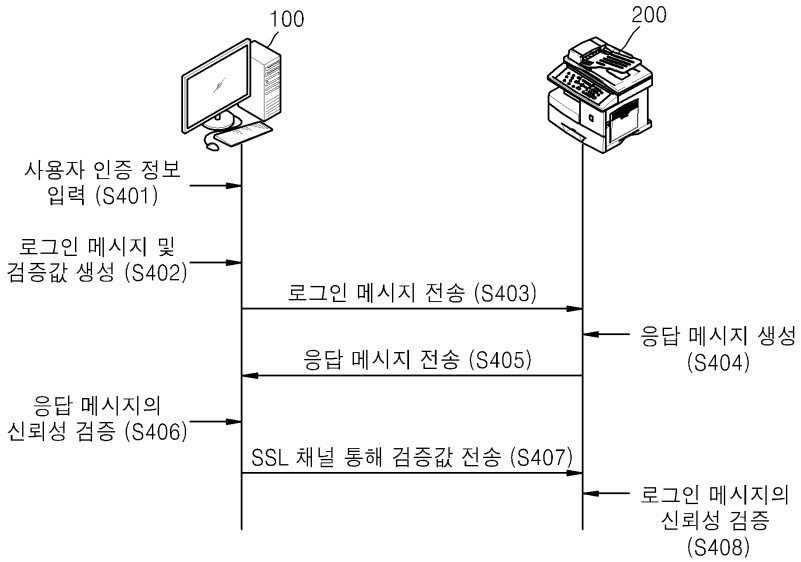
도면2


100
130
사용자 인증 정보 입력부
140
보안부
150
로그인 메시지 생성부
160
응답 메시지 검증부
170
검증값 생성부
120
제어부
110
통신
인터페이스부

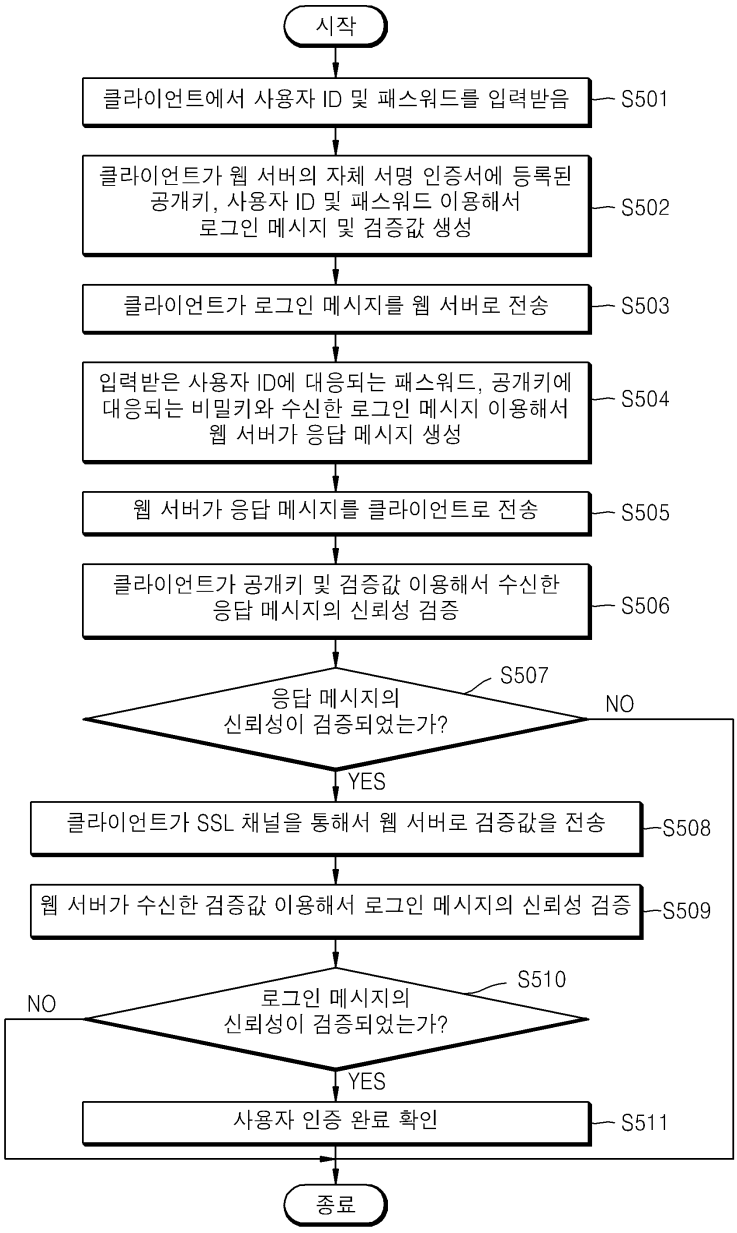
도면3


200
210
통신
인터페이스부
220
제어부
230
인증서 생성부
240
응답 메시지 생성부
250
사용자 인증부
260
저장부

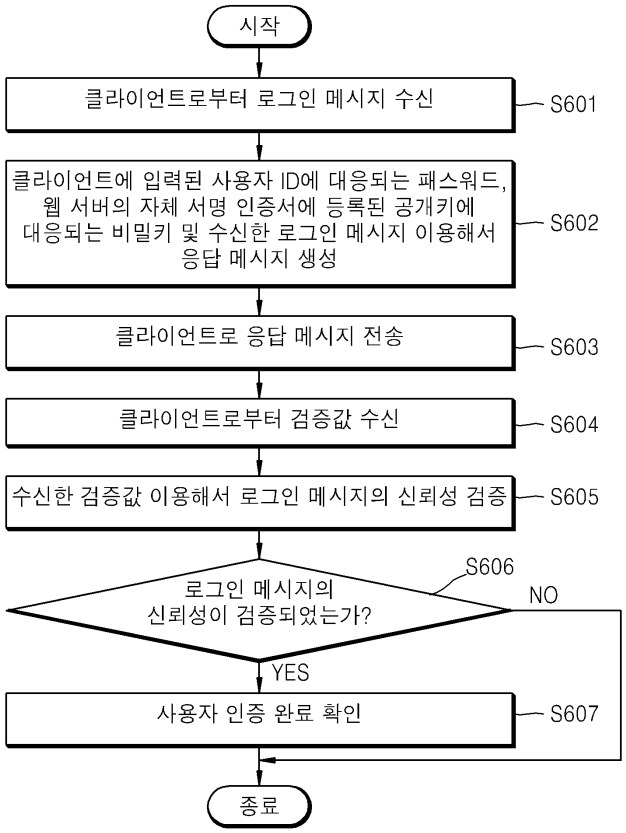
도면4


100
200
사용자 인증 정보 입력 (S401)
로그인 메시지 및 검증값 생성 (S402)
로그인 메시지 전송 (S403)
응답 메시지 생성 (S404)
응답 메시지 전송 (S405)
응답 메시지의 신뢰성 검증 (S406)
SSL 채널 통해 검증값 전송 (S407)
로그인 메시지의 신뢰성 검증 (S408)

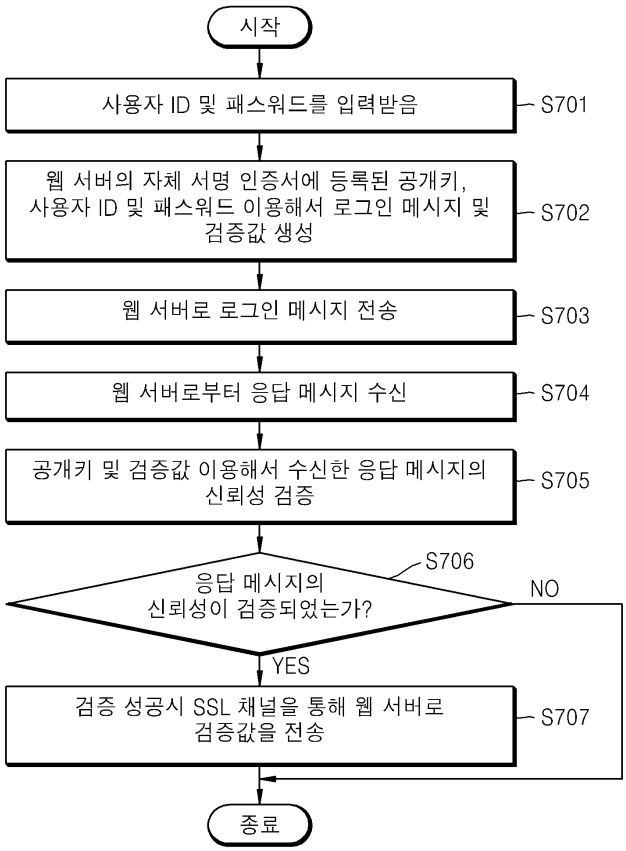
도면5


시작
클라이언트에서 사용자 ID 및 패스워드를 입력받음
S501
클라이언트가 웹 서버의 자체 서명 인증서에 등록된 공개키, 사용자 ID 및 패스워드 이용해서 로그인 메시지 및 검증값 생성
S502
클라이언트가 로그인 메시지를 웹 서버로 전송
S503
입력받은 사용자 ID에 대응되는 패스워드, 공개키에 대응되는 비밀키와 수신한 로그인 메시지 이용해서 웹 서버가 응답 메시지 생성
S504
웹 서버가 응답 메시지를 클라이언트로 전송
S505
클라이언트가 공개키 및 검증값 이용해서 수신한 응답 메시지의 신뢰성 검증
S506
응답 메시지의 신뢰성이 검증되었는가?
S507
NO
YES
클라이언트가 SSL 채널을 통해서 웹 서버로 검증값을 전송
S508
웹 서버가 수신한 검증값 이용해서 로그인 메시지의 신뢰성 검증
S509
로그인 메시지의 신뢰성이 검증되었는가?
S510
NO
YES
사용자 인증 완료 확인
S511
종료

도면6


시작
클라이언트로부터 로그인 메시지 수신
S601
클라이언트에 입력된 사용자 ID에 대응되는 패스워드, 웹 서버의 자체 서명 인증서에 등록된 공개키에 대응되는 비밀키 및 수신한 로그인 메시지 이용해서 응답 메시지 생성
S602
클라이언트로 응답 메시지 전송
S603
클라이언트로부터 검증값 수신
S604
수신한 검증값 이용해서 로그인 메시지의 신뢰성 검증
S605
로그인 메시지의 신뢰성이 검증되었는가?
S606
NO
YES
사용자 인증 완료 확인
S607
종료

도면7


시작
사용자 ID 및 패스워드를 입력받음
S701
웹 서버의 자체 서명 인증서에 등록된 공개키, 사용자 ID 및 패스워드 이용해서 로그인 메시지 및 검증값 생성
S702
웹 서버로 로그인 메시지 전송
S703
웹 서버로부터 응답 메시지 수신
S704
공개키 및 검증값 이용해서 수신한 응답 메시지의 신뢰성 검증
S705
응답 메시지의 신뢰성이 검증되었는가?
S706
NO
YES
검증 성공시 SSL 채널을 통해 웹 서버로 검증값을 전송
S707
종료