(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년11월12일
(11) 등록번호 10-1458034
(24) 등록일자 2014년10월29일

(51) 국제특허분류(Int. Cl.)
H04L 9/30 (2006.01)
(21) 출원번호 10-2012-0137591
(22) 출원일자 2012년11월30일
심사청구일자 2012년11월30일
(65) 공개번호 10-2014-0069828
(43) 공개일자 2014년06월10일
(56) 선행기술조사문헌
JP2002358274 A
JP2003143194 A
KR1020030083857 A
KR1020040050456 A
전체 청구항 수 : 총 9 항

(73) 특허권자
한국과학기술정보연구원
대전광역시 유성구 대학로 245 (어은동)
(72) 발명자
박상배
인천 연수구 비류대로278번길 18-14, 다동 301호 (청학동, 청학파크맨션)
(74) 대리인
박영복, 지관영, 김용인

심사관 : 이병수

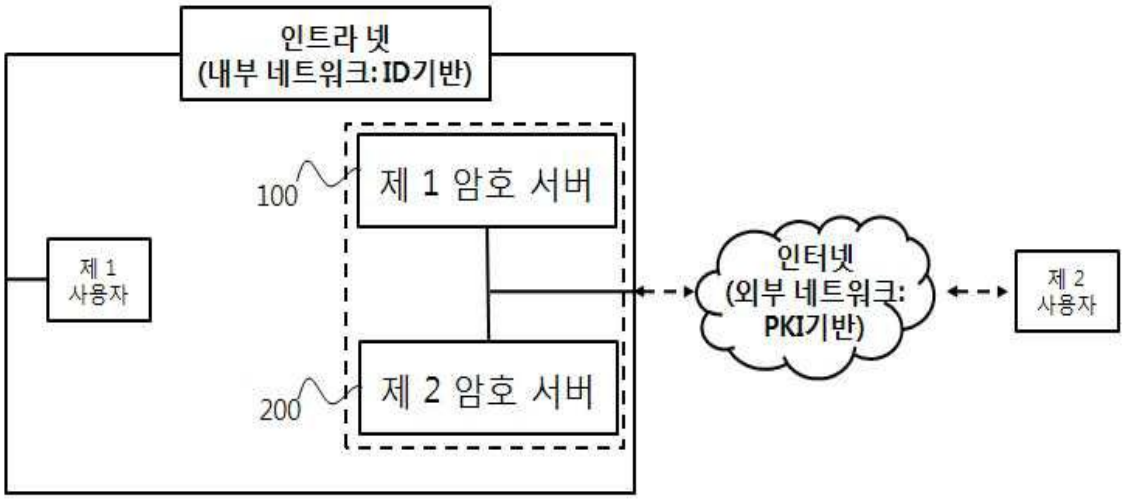
(54) 발명의 명칭 **암호화 메세지 전송 방법, 암호화 메세지 전송 장치, 암호화 메세지를 전송하는 암호화 모듈 프로그램을 저장하는 저장매체**

(57) 요 약

본 발명은, 암호화 메세지 전송 방법, 암호화 메세지 전송 장치, 암호화 메세지를 전송하는 암호화 모듈 프로그램을 저장하는 저장매체에 관한 것이다. 본 발명의 일 실시예는, 내부 인트라 넷의 제 1 사용자가 외부 인터넷의 제 2 사용자에게 전송하려는 메세지를 수신하는 단계; 상기 제 2 사용자가 상기 내부 인트라 넷의 미등록 사용자

(뒷면에 계속)

대 표 도 - 도1



인 경우 상기 제 2 사용자의 가상의 ID (identifier)를 생성하고, 상기 제 1 사용자의 메세지를 상기 생성한 가상의 ID 에 기반하여 암호화하고, 상기 암호화된 메세지를 상기 제 2 사용자에게 전송하는 단계; 상기 제 2 사용자의 PKI (public key infrastructure) 기반의 개인키와 공개키를 생성하고, 상기 공개키를 인증하는 공개키 인증서를 상기 제 2 사용자에게 발급하고, 상기 제 2 사용자의 ID에 대응하는 상기 공개키와 상기 개인키를 보관하고, 상기 개인키를 이용하여 상기 제 1 사용자의 메세지를 전송하는 세션의 세션키를 복구하는 단계; 및 상기 복구된 세션키를 이용하여 PKI 기반의 공개키로 암호화된 상기 제 1 사용자의 메세지를 상기 제 2 사용자에게 전송하는 단계;를 포함하는 암호화 메세지 전송 방법을 제공한다.

특허청구의 범위

청구항 1

외부 인터넷의 제 2 사용자에게 전송하려는 제 1 사용자의 메세지를 생성하는 단계;

상기 제 2 사용자가 내부 인트라 넷의 미등록 사용자인 경우 상기 제 2 사용자의 가상의 ID (identifier)를 생성하여 상기 제 1 사용자의 메세지를 상기 생성된 가상의 ID 에 기반하여 암호화하고, 상기 암호화된 제1 사용자 메세지의 알림 메세지를 상기 제 2 사용자에게 전송하는 단계;

상기 제 2 사용자가 상기 내부 인트라 넷에 접속하면, 상기 제 2 사용자의 PKI (public key infrastructure) 기반의 공개키 및 ID에 대응하는 개인키를 생성하고, 상기 PKI 기반의 공개키를 인증하는 공개키 인증서를 상기 제 2 사용자에게 발급하고, 상기 PKI 기반의 공개키 및 상기 ID에 대응하는 개인키를 저장하며, 상기 가상의 ID에 기반하여 암호화된 제 1 사용자의 메세지를 상기 PKI 기반의 공개키로 암호화하고, 상기 ID에 대응하는 개인키를 이용하여 상기 제 1 사용자의 메세지를 전송하는 세션의 세션키를 복구하는 단계; 및

상기 복구된 세션키를 이용하여 상기 PKI 기반의 공개키로 암호화된 상기 가상의 ID에 기반하여 암호화된 제 1 사용자의 메세지를 상기 제 2 사용자에게 전송하는 단계;를 포함하는 암호화 메세지 전송 방법.

청구항 2

제 1항에 있어서,

상기 가상 ID는, 상기 제 2 사용자의 이메일 주소 또는 IP(internet address) 주소인 암호화 메세지 전송 방법.

청구항 3

제 1 항에 있어서,

상기 암호화 메세지 전송 방법은,

상기 저장된 ID에 대응하는 개인키를 이용하여 상기 제 2 사용자에게 전송되는 상기 제 1 사용자의 메세지를 복호하는 단계;를 더 포함하는 암호화 메세지 전송 방법.

청구항 4

외부 인터넷의 제 2 사용자에게 전송하려는 제 1 사용자의 메세지를 생성하고, 상기 제 2 사용자가 내부 인트라 넷의 미등록 사용자인 경우 상기 제 2 사용자의 가상의 ID (identifier)를 생성하여 상기 제 1 사용자의 메세지를 상기 생성된 가상의 ID 에 기반하여 암호화하고, 상기 암호화된 제1 사용자 메세지의 알림 메세지를 상기 제 2 사용자에게 전송하는 제 1 암호 서버; 및

상기 제 2 사용자가 상기 내부 인트라 넷에 접속하면, 상기 제 2 사용자의 PKI (public key infrastructure) 기반의 공개키 및 ID에 대응하는 개인키를 생성하고, 상기 PKI 기반의 공개키를 인증하는 공개키 인증서를 상기 제 2 사용자에게 발급하고, 상기 PKI 기반의 공개키 및 상기 ID에 대응하는 개인키를 저장하며, 상기 가상의 ID에 기반하여 암호화된 제 1 사용자의 메세지를 상기 PKI 기반의 공개키로 암호화하고, 상기 ID에 대응하는 개인키를 이용하여 상기 제 1 사용자의 메세지를 전송하는 세션의 세션키를 복구하고, 상기 복구된 세션키를 이용하여 상기 PKI (public key infrastructure)기반의 공개키로 암호화된 상기 가상의 ID에 기반하여 암호화된 제 1 사용자의 메세지를 상기 제 2사용자에게 전송하는 제 2 암호서버;를 포함하는 암호화 메세지 전송 장치.

청구항 5

제 4 항에 있어서,

상기 가상 ID는, 상기 제 2 사용자의 이메일 주소 또는 IP(internet address) 주소인 암호화 메세지 전송 장치.

청구항 6

제 4 항에 있어서,

상기 제 2 암호서버는,

상기 저장된 ID에 대응하는 개인키를 이용하여 상기 제 2 사용자에게 전송되는 상기 제 1 사용자의 메세지를 복호하는 암호화 메세지 전송 장치.

청구항 7

외부 인터넷의 제 2 사용자에게 전송하려는 제 1 사용자의 메세지를 생성하고, 상기 제 2 사용자가 내부 인트라넷의 미등록 사용자인 경우 상기 제 2 사용자의 가상의 ID (identifier)를 생성하여 상기 제 1 사용자의 메세지를 상기 생성된 가상의 ID 에 기반하여 암호화하고, 상기 암호화된 제1 사용자 메세지의 알림 메세지를 상기 제 2 사용자에게 전송하고, 상기 제 2 사용자가 상기 내부 인트라 넷에 접속하면, 상기 제 2 사용자의 PKI (public key infrastructure) 기반의 공개키 및 ID에 대응하는 개인키를 생성하고, 상기 PKI 기반의 공개키를 인증하는 공개키 인증서를 상기 제 2 사용자에게 발급하고, 상기 PKI 기반의 공개키 및 상기 ID에 대응하는 개인키를 저장하며, 상기 가상의 ID에 기반하여 암호화된 제 1 사용자의 메세지를 상기 PKI 기반의 공개키로 암호화하고, 상기 ID에 대응하는 개인키를 이용하여 상기 제 1 사용자의 메세지를 전송하는 세션의 세션키를 복구하고, 상기 복구된 세션키를 이용하여 상기 PKI 기반의 공개키로 암호화된 상기 가상의 ID에 기반하여 암호화된 제 1 사용자의 메세지를 상기 제 2 사용자에게 전송하는, 암호화 모듈 프로그램을 저장하는 저장매체.

청구항 8

제 7 항에 있어서,

상기 가상 ID는, 상기 제 2 사용자의 이메일 주소 또는 IP(internet address) 주소인, 암호화 모듈 프로그램을 저장하는 저장매체.

청구항 9

제 7 항에 있어서,

암호화 모듈 프로그램을 저장하는 저장매체는,

상기 저장된 ID에 대응하는 개인키를 이용하여 상기 제 2 사용자에게 전송되는 상기 제 1 사용자의 메세지를 복호하는 암호화 모듈 프로그램을 저장하는 저장매체.

명 세 서

기 술 분 야

[0001] 본 발명은, 암호화 메세지 전송 방법, 암호화 메세지 전송 장치, 암호화 메세지를 전송하는 암호화 모듈 프로그램을 저장하는 저장매체에 관한 것이다.

배 경 기 술

[0002] 최근 네트워크를 통해 정보를 교환하면서 정보 보안에 대한 중요성이 커지고 있다. 조직 내 기업 비밀이나 정보가 이메일 등으로 누출되는 사례가 빈번하게 발생하고 있다. 이메일을 통해 회사 내의 기밀문서 유출과 같은 정보 유출의 경우가 증가하고 있다.

[0003] 이메일은 보안은 S/MIME(Secure Multipurpose Internet Mail Extensions)과 같은 방식을 많이 사용한다. 이메일은 MTA (Mail transfer agent), MUA (Mail user agent), MDA (Mail delivery agent) 등의 에이전트를 이용하여 송수신될 수 있고, POP3/IMAP4 과 같은 프로토콜을 사용하여 송수신될 수 있다. S/MIME과 같이 공개키 기반의 이메일을 사용할 경우 사용자가 자신의 개인키를 제공하지 않는 한 복호화가 불가능하여 메일 내용의 감시 통제가 불가능한 문제점이 있었다.

[0004] 예를 들어 PKI(public key infrastructure) 기반의 S/MIME 방식의 암호화 메일의 경우, 사용자의 개인키 없이 복호화가 불가능하여 통제할 수 없으므로 전체적인 메세지 내용의 통제가 힘든 문제점이 있다. 그리고, 사용자의 ID(identifier) 기반 암호를 이용하면 중앙에서 통제가 가능한 폐쇄적 네트워크 구성이 가능하나, 외부망과 연동하는데 문제점이 있다.

발명의 내용

해결하려는 과제

[0005] 본 발명의 목적은 내부의 네트워크와 외부 네트워크의 사용자 간의 메세지를 암호화하여 송수신하여도 해당 메세지의 내용을 감시하고 통제할 수 있는, 암호화 메세지 전송 방법, 암호화 메세지 전송 장치, 암호화 메세지를 전송하는 암호화 모듈 프로그램을 저장하는 저장매체를 제공하는 것이다.

[0006] 본 발명의 다른 목적은 내부의 네트워크와 외부 네트워크의 상호 운용성을 확보할 수 있는 암호화 메세지 전송 방법, 암호화 메세지 전송 장치, 암호화 메세지를 전송하는 암호화 모듈 프로그램을 저장하는 저장매체를 제공하는 것이다.

[0007] 본 발명의 다른 목적은 외부 네트워크로 전송되는 메세지에 대해 수신자의 신원을 알 수 있고 메세지의 내용을 조사할 수 있는 암호화 메세지 전송 방법, 암호화 메세지 전송 장치, 암호화 메세지를 전송하는 암호화 모듈 프로그램을 저장하는 저장매체를 제공하는 것이다.

과제의 해결 수단

[0008] 본 발명의 일 실시예는, 내부 인트라 넷의 제 1 사용자가 외부 인터넷의 제 2 사용자에게 전송하려는 메세지를 수신하는 단계; 상기 제 2 사용자가 상기 내부 인트라 넷의 미등록 사용자인 경우 상기 제 2 사용자의 가상의 ID (identifier)를 생성하고, 상기 제 1 사용자의 메세지를 상기 생성한 가상의 ID 에 기반하여 암호화하고, 상기 암호화된 메세지를 상기 제 2 사용자에게 전송하는 단계; 상기 제 2 사용자의 PKI (public key infrastructure) 기반의 개인키와 공개키를 생성하고, 상기 공개키를 인증하는 공개키 인증서를 상기 제 2 사용자에게 발급하고, 상기 제 2 사용자의 ID에 대응하는 상기 공개키와 상기 개인키를 보관하고, 상기 개인키를 이용하여 상기 제 1 사용자의 메세지를 전송하는 세션의 세션키를 복구하는 단계; 및 상기 복구된 세션키를 이용하여 PKI 기반의 공개키로 암호화된 상기 제 1 사용자의 메세지를 상기 제 2 사용자에게 전송하는 단계;를 포함하는 암호화 메세지 전송 방법을 제공한다.

[0009] 상기 가상 ID는, 상기 제 2 사용자의 이메일 주소 또는 IP(internet address) 주소일 수 있다.

[0010] 상기 암호화 메세지 전송 방법은, 상기 저장한 개인키를 이용하여 상기 제 2 사용자에게 전송되는 상기 제 1 사용자의 메세지를 복호할 수 있다.

[0011] 본 발명의 다른 일 실시예는, 내부 인트라 넷의 제 1 사용자가 외부 인터넷의 제 2 사용자에게 전송하려는 메세지를 수신하고, 상기 제 2 사용자가 상기 내부 인트라 넷의 미등록 사용자인 경우 상기 제 2 사용자의 가상의 ID(identifier)를 생성하고, 상기 제 1 사용자의 메세지를 상기 생성한 가상의 ID 에 기반하여 암호화하고, 상기 암호화된 메세지를 상기 제 2 사용자에게 전송하는 제 1 암호 서버; 및 상기 제 2 사용자의 PKI (public key infrastructure) 기반의 개인키와 공개키를 생성하고, 상기 공개키를 인증하는 공개키 인증서를 상기 제 2 사용자에게 발급하고, 상기 제 2 사용자의 ID에 대응하는 상기 공개키와 상기 개인키를 보관하고, 상기 개인키를 이용하여 상기 제 1 사용자의 메세지를 전송하는 세션의 세션키를 복구하고, 상기 복구된 세션키를 이용하여 PKI (public key infrastructure)기반의 공개키로 암호화된 상기 제 1 사용자의 메세지를 상기 제 2 사용자에게 전송하는 제 2 암호서버;를 포함하는 암호화 메세지 전송 장치를 제공한다.

[0012] 본 발명의 또 다른 실시예는, 내부 인트라 넷의 제 1 사용자가 외부 인터넷의 제 2 사용자에게 전송하려는 메세지를 수신하고, 상기 제 2 사용자가 상기 내부 인트라 넷의 미등록 사용자인지 판단하고, 미등록 사용자인 경우 상기 제 2 사용자의 가상의 ID를 생성하고, 상기 제 1 사용자의 메세지를 상기 생성한 가상의 ID(identifier)에 기반하여 암호화하고, 상기 암호화된 메세지를 상기 제 2 사용자에게 전송하고, 상기 제 2 사용자의 PKI (public key infrastructure) 기반의 개인키와 공개키를 생성하고, 상기 공개키를 인증하는 공개키 인증서를 상기 제 2 사용자에게 발급하고, 상기 제 2 사용자의 ID에 대응하는 상기 공개키와 상기 개인키를 보관하고, 상기 개인키를 이용하여 상기 제 1 사용자의 메세지를 전송하는 세션의 세션키를 복구하고, 상기 복구된 세션키를 이용하여 PKI 기반의 공개키로 암호화된 상기 제 1 사용자의 메세지를 상기 제 2 사용자에게 전송하는, 암호화 모듈 프로그램을 저장하는 저장매체를 제공한다.

발명의 효과

[0013] 본 발명의 실시예에 따르면 내부의 네트워크와 외부 네트워크의 사용자 간의 메세지를 암호화하여 송수신하여도

해당 메세지의 내용을 감시하고 통제할 수 있다.

[0014] 본 발명의 실시예에 따르면 내부의 네트워크와 외부 네트워크의 상호 운용성을 확보할 수 있다.

[0015] 본 발명의 실시예에 따르면 외부 네트워크로 전송되는 메세지에 대해 수신자의 신원을 알 수 있고, 메세지의 내용을 조사할 수 있다.

도면의 간단한 설명

[0016] 도 1은 본 발명에 따른 암호화 메세지 전송 장치의 일 실시예를 예시한 도면

도 2는 본 발명에 따른 암호화 메세지 전송 방법의 일 실시예를 예시한 도면

발명을 실시하기 위한 구체적인 내용

[0017] 이하 본 발명의 실시예를 첨부한 도면을 참조하여 설명한다.

[0018] 본 발명의 실시예에 따른 암호화 시스템은 사용자가 공개키, 개인키의 키 쌍 대신, 사용자의 ID를 자신의 공개키로 사용하여 암호 및 전자서명을 수행하는 암호기법으로 사용할 수 있다.

[0019] 본 발명의 실시예에 따른 암호화 시스템은 사용자가 자신의 키 쌍을 생성하여 인증기관(CA)에 전달하여 공개키 인증서를 발급받아 사용하지만, ID 기반 암호는 신뢰할 수 있는 기관(Trusted Party)에서 사용자 ID에 대한 개인키를 생성할 수 있다.

[0020] 예를 들어, PKI 기반의 암호화 시스템에서는 사용자가 개인키를 생성하고 키 생성 시스템이 공개키를 인증하여 사용자 별로 프라이버시를 보호할 수 있다.

[0021] 반면, ID 기반의 암호화 시스템에서는 ID를 부여하는 기관에서 ID를 부여를 확인하고, 사용자가 개인키를 생성하여 사용하며, 공개키 인증서와 같은 인증서 교환없이 암복호화가 가능하다.

[0022] 공개키 암호화의 경우, 대칭키 암호에 비하여 처리 속도가 매우 느리기 때문에 통신 모델은 다음과 같이 두 암호 시스템을 함께 사용하여 안전성과 효율성을 보장할 수 있다.

[0023] (1) 송신자는 임의의 세션키 (SK)를 생성하고, 세션키 (SK)와 대칭키 암호 알고리즘으로 메시지를 암호화한다.

[0024] (2) 송신자는 수신자의 공개키로 세션키 (SK)를 암호화하고, 암호화된 메시지와 함께 전송할 수 있다.

[0025] (3) 수신자는 자신의 개인키로 SK를 복호화할 수 있다.

[0026] (4) 수신자는 복호화한 SK를 이용하여 메시지를 복호화할 수 있다.

[0027] 이하에서의 메시지 암호화는 이와 같은 데이터 인벨롭핑(data enveloping)을 기본으로 전제하고, 세션키 (SK)에 대한 공개키 암호 연산으로 메세지 송수신을 암호화하는 실시예를 개시하도록 한다.

[0028] 도 1은 본 발명에 따른 암호화 메세지 전송 장치의 일 실시예를 예시한 도면이다. 이 도면을 참고하여 본 발명에 따른 암호화 메세지 전송 장치의 일 실시예를 설명하면 다음과 같다.

[0029] 제 1 암호 서버(100)는 인트라 넷 사용자들에게 ID를 생성하도록 하여 사용자들의 ID를 저장할 수 있다. 인트라 넷 사용자들끼리 이메일을 이용하여 메세지를 전송할 경우, 제 1 암호 서버(100)는 인트라 넷 사용자들에게 자신의 ID에 기반한 개인키를 생성하도록 하고 이를 저장할 수 있고 각자의 ID 기반으로 생성한 개인키를 인트라 넷의 각 사용자에게 배포할 수 있다.

[0030] 인트라 넷 사용자들은 상대방의 ID를 이용하여 메세지를 암호화하여 제 1 암호 서버(100)를 통해 전송하고, 인트라 넷 사용자가 다른 인트라 넷 사용자로부터 메세지를 수신한 경우, 자신의 개인키를 이용하여 메세지를 복호할 수 있다.

[0031] 인트라 넷 사용자가 외부의 인터넷 사용자에게 메세지를 전송할 경우는 다음과 같이 처리할 수 있다.

[0032] 제 1 암호 서버(100)는 인트라 넷의 사용자들 중 제 1 사용자의 메세지를, 인트라 넷과 연결된 외부 인터넷의 제 2 사용자에게 전송하기 위해 제 2 사용자의 가상의 ID를 생성할 수 있다. 제 1 암호 서버(100)는 제 1 사용자의 메세지를 가상의 ID 에 기반하여 암호화하고, 상기 암호화된 메세지를 제 2 사용자에게 전송한다(S110). 여기서 가상의 ID는 제 2 사용자의 이메일주소 또는 IP 주소 등이 사용될 수 있다.

[0033] 제 1 암호서버(100)는 생성한 제 2 사용자의 가상의 ID를 기반으로 하여 인트라 넷의 제 1 사용자가 외부 인터넷의 제 2 사용자에게 전송하려는 이메일 메세지를 암호화하여 전송하거나, 그 제 2 사용자에게 전송할 이메일 메세지가 있음을 알리는 메세지를 전송할 수 있다.

[0034] 외부 인터넷의 제 2 사용자는 암호화된 메세지 또는 전송할 메세지가 있음을 알리는 메세지에 안내에 따라 제 2 암호 서버(200)에 접속할 수 있다.

[0035] 제 2 암호 서버(200)는, 제 2 사용자의 ID가 제 1 암호 서버(100)에 등록되지 않은 경우, 제 2 사용자가 상기 제 2 암호 서버(200)에 대해 PKI (public key infrastructure) 기반의 개인키와 공개키를 생성한다.

[0036] 제 2 암호 서버(200)는, 공개키를 인증하는 공개키 인증서를 상기 제 2 사용자에게 발급하고, 제 2 사용자의 ID에 대응하는 공개키와 개인키를 보관할 수 있다. 그리고 제 2 암호서버(200)는, 발급한 공개키 인증서를 이용하여 제 2 사용자를 인증할 수 있다.

[0037] 제 2 암호 서버(200)는 제 2 사용자가 인증된 경우, 해당 사용자의 ID에 대응하여 저장한 제 2 사용자의 ID에 따른 개인키를 이용하여 제 2 사용자와의 세션키를 복구할 수 있다.

[0038] 그리고, 복구된 세션키를 이용하여 PKI 기반의 공개키로 암호화된 제 1 사용자의 메세지를 제 2 사용자에게 전송할 수 있다.

[0039] 제 2 암호서버(200)는, 제 2 사용자의 ID에 대응하는 개인키로 세션키를 복구할 수 있기 때문에, 암호화된 메세지에 포함된 기밀 정보 유출 여부를 언제든지 조사할 수 있다.

[0040] 제 2 사용자는 자신의 개인키로 세션키를 복호할 수 있고, 복호한 세션키를 이용하여 PKI 기반의 공개키로 암호화된 제 1 사용자의 메세지를 복호할 수 있다.

[0041] 이 도면에서 점선은, PKI 기반의 암호화 시스템을 따르고, 실선은 ID 기반의 암호화 시스템을 따른다.

[0042] 도 2는 본 발명에 따른 암호화 메세지 전송 방법의 일 실시예를 예시한 도면이다. 이 도면을 참고하여 본 발명에 따른 암호화 메세지 전송 장치의 일 실시예를 설명하면 다음과 같다.

[0043] 내부 인트라 넷의 제 1 사용자가 외부 인터넷의 제 2 사용자에게 전송하려는 메세지를 수신한다(S100).

[0044] 제 2 사용자가 상기 내부 인트라 넷의 미등록 사용자인 경우, 제 2 사용자의 가상의 ID를 생성하고, 제 1 사용자의 메세지를 생성한 가상의 ID 에 기반하여 암호화하고, 상기 암호화된 메세지를 상기 제 2 사용자에게 전송한다(S110). 여기서 가상의 ID는 제 2 사용자의 이메일주소 또는 IP 주소 등이 사용될 수 있다.

[0045] 생성한 제 2 사용자의 가상의 ID를 기반으로 하여 인트라 넷의 제 1 사용자가 외부 인터넷의 제 2 사용자에게 전송하려는 이메일 메세지를 암호화하여 전송하거나, 그 제 2 사용자에게 전송할 이메일 메세지가 있음을 알리는 메세지를 전송할 수 있다.

[0046] 외부 인터넷 상의 제 2 사용자의 ID가 본 발명의 일 실시예에 따른 암호화 시스템의 미등록 ID이고, 제 2 사용자가 암호화된 메세지 또는 전송할 메세지가 있음을 알리는 메세지에 안내에 따라 암호화 시스템에 접속한 경우, 제 2 사용자가 생성한 PKI 기반의 생성된 개인키와 그에 따른 공개키를 저장하고 공개키를 인증하는 공개키 인증서를 제 2 사용자에게 발급한다(S120).

[0047] 제 2 사용자의 ID에 대응하는 공개키와 개인키를 보관하고, 보관된 개인키를 이용하여 제 1 사용자의 메세지를 전송하는 세션의 세션키를 복구한다(S130).

[0048] 복구된 세션키를 이용하여 PKI 기반의 공개키로 암호화된 제 1 사용자의 메세지를 제 2 사용자에게 전송한다(S140).

[0049] 본 발명의 일 실시예에 따르면, 외부 인터넷 망의 제 2 사용자는 ID 기반의 개인키로 세션키를 복구할 수 있기 때문에, 암호화된 메세지에 포함된 기밀 정보 유출 여부를 언제든지 조사할 수 있다.

[0050] 외부 인터넷 망의 제 2 사용자는 자신의 개인키로 세션키를 복호할 수 있고, 복호한 세션키를 이용하여 PKI 기반의 공개키로 암호화된 제 1 사용자의 메세지를 복호할 수 있다.

[0051] 한편, 인트라 넷에 연결된 사용자들에게 대해서는 인트라 넷 사용자들에게 ID를 생성하도록 하여 사용자들의 ID를 암호화 시스템에 저장할 수 있다. 인트라 넷 사용자들끼리 이메일을 이용하여 메세지를 전송할 경우, 인트라 넷 사용자들에게 자신의 ID에 기반한 개인키를 생성하도록 하고 이를 저장할 수 있다.

[0052] 그리고, 각자의 ID 기반으로 생성한 개인키를 인트라 넷의 각 사용자에게 배포할 수 있다.

[0053] 인트라 넷 사용자들은 상대방의 ID를 이용하여 메세지를 암호화하여 전송하고, 인트라 넷 사용자가 다른 인트라 넷 사용자로부터 메세지를 수신한 경우, 자신의 개인키를 이용하여 메세지를 복호할 수 있다.

[0054] 한편, 도 1의 제 1 암호 서버 및 제 2 암호 서버는, 암호화시스템의 암호화 모듈로 구현될 수도 있는데, 그러한 경우 본 발명의 실시예는 암호화 모듈에서 구현되는 암호화 메세지를 전송하는 암호화 모듈 프로그램을 저장하는 저장매체가 될 수도 있다.

[0055] 따라서 본 발명의 실시예는, 내부 인트라 넷의 제 1 사용자가 외부 인터넷의 제 2 사용자에게 전송하려는 메세지를 수신하고, 상기 제 2 사용자가 상기 내부 인트라 넷의 미등록 사용자인지 판단하고, 미등록 사용자인 경우 상기 제 2 사용자의 가상의 ID를 생성하고, 상기 제 1 사용자의 메세지를 상기 생성한 가상의 ID(identifier)에 기반하여 암호화하고, 상기 암호화된 메세지를 상기 제 2 사용자에게 전송하고, 상기 제 2 사용자의 PKI (public key infrastructure) 기반의 개인키와 공개키를 생성하고, 상기 공개키를 인증하는 공개키 인증서를 상기 제 2 사용자에게 발급하고, 상기 제 2 사용자의 ID에 대응하는 상기 공개키와 상기 개인키를 보관하고, 상기 개인키를 이용하여 상기 제 1 사용자의 메세지를 전송하는 세션의 세션키를 복구하고, 상기 복구된 세션키를 이용하여 PKI 기반의 공개키로 암호화된 상기 제 1 사용자의 메세지를 상기 제 2 사용자에게 전송하는, 암호화 모듈 프로그램을 저장하는 저장매체를 제공한다.

[0056] 본 발명의 실시예에 따르면, 네트워크의 내부에 일관적인 정보보호 정책을 적용하는 외부에도 적용할 수 있고, 외부에서 내부의 기밀 정보 등을 알 수 없는 폐쇄적인 가상 네트워크를 구성할 수 있다.

[0057] 본 발명의 실시예에 따르면, 외부 통신대상에 대한 내부의 인증절차를 통하여 외부 통신을 지원하여 상호운용성 향상시킬 수 있다. 그리고, 네트워크의 정보보호를 위해 전체 통신 내용에 대해서도 전송 내용을 검사하여 통신을 차단할 수 있다.

[0058] 본 발명의 실시예에 따르면 외부에 대한 통신도 전 구간에 걸쳐 구간별 암호화를 적용하여 기밀성을 향상시킬 수 있고, 외부 시스템의 변경없이도 적용이 가능하다.

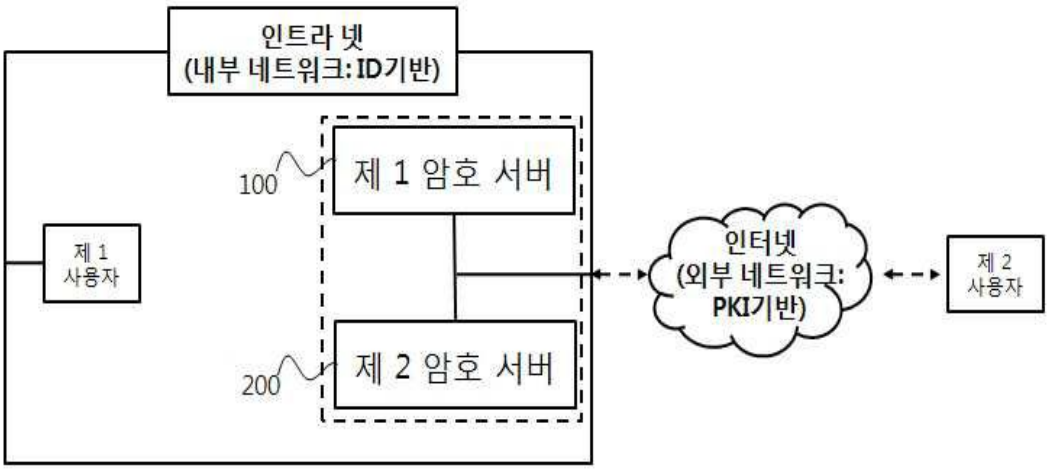
부호의 설명

[0059] 100: 제 1 암호 서버

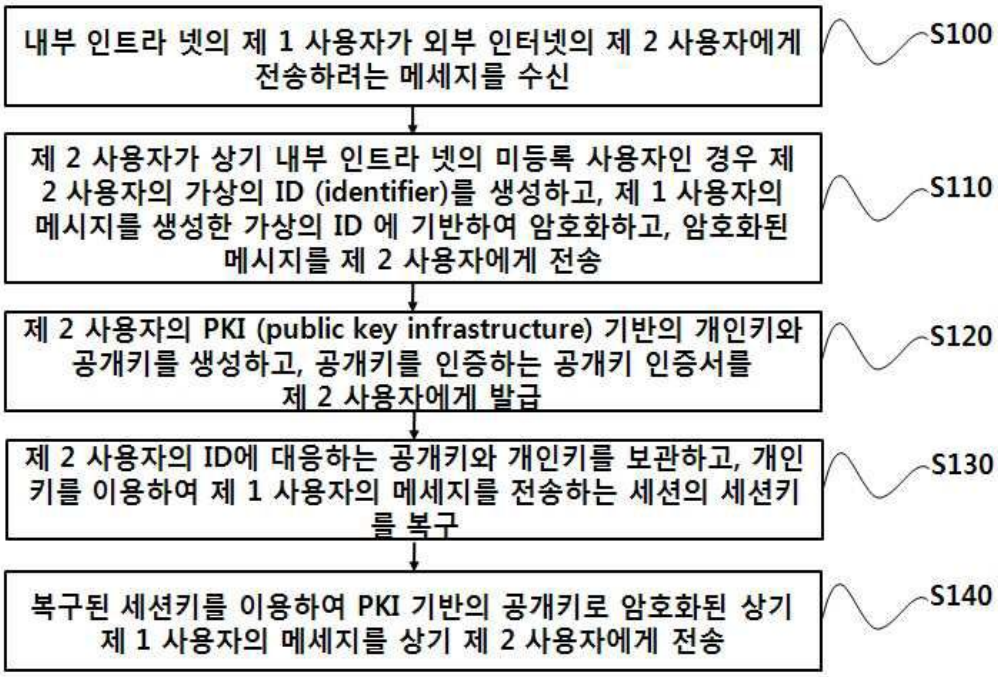
200: 제 2 암호 서버

도면

도면1



도면2



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 1항 5번째줄

【변경전】

상기 암호화된 메세지의

【변경후】

상기 암호화된 제1 사용자 메세지의

【직권보정 2】

【보정항목】 청구범위

【보정세부항목】 청구항 9항 4번째줄

【변경전】

상기 암호화 모듈

【변경후】

암호화 모듈

【직권보정 3】

【보정항목】 청구범위

【보정세부항목】 청구항 7항 4번째줄

【변경전】

상기 암호화된 메세지의

【변경후】

상기 암호화된 제1 사용자 메세지의

【직권보정 4】

【보정항목】 청구범위

【보정세부항목】 청구항 4항 4번째줄

【변경전】

상기 암호화된 메세지의

【변경후】

상기 암호화된 제1 사용자 메세지의