(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년04월15일
(11) 등록번호 10-1029030
(24) 등록일자 2011년04월06일

(51) Int. Cl.
G06Q 50/00 (2006.01) *H04L 29/06* (2006.01)
(21) 출원번호 10-2004-7013043
(22) 출원일자(국제출원일자) 2003년02월21일
심사청구일자 2008년02월21일
(85) 번역문제출일자 2004년08월20일
(65) 공개번호 10-2004-0091656
(43) 공개일자 2004년10월28일
(86) 국제출원번호 PCT/US2003/004964
(87) 국제공개번호 WO 2003/073711
국제공개일자 2003년09월04일
(30) 우선권주장
09/991,201 2002년02월22일 미국(US)
(56) 선행기술조사문헌
US06314454 B1
WO2002011025 A2
전체 청구항 수 : 총 15 항

(73) 특허권자
알포스트 인터내셔널 리미티드
버뮤다 헤밀톤 팔리아먼트 스트리트 20 코너 하우스 3층
(72) 발명자
톰코우터렌스,에이.
미국, 캘리포니아 90019, 로스앤젤리스, 카르모나 애비뉴 1301
(74) 대리인
장훈, 손영태

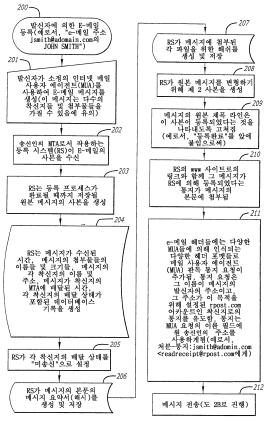
심사관 : 최석규

(54) 전자 메시지들의 전달 및 완전성을 검증하기 위한 시스템및 방법

(57) 요 약

송신인으로부터 메시지를 수신하고 이 메시지를 인터넷을 통해 수신인에게 송신하는 서버를 개시한다. 서버는 통상 제 1 경로에서 통상 인터넷을 통해 메시지를 수신인에게 송신한다. 송신인이 메시지 내의 특정 위치에서 메시지가 등록됨을 나타낼 때, 서버는 제 2 경로에서 인터넷을 통해 수신인에게 메시지를 송신한다. 송신인은 서버에 의해 제공되는 통상적이 아닌 다른 특별한 방법들로 메시지를 서버가 다루어야 하는 메시지 내의 부가적인 표시들(indications)을 제공할 수도 있다. 수신 또는 수신인의 에이전트로부터 인터넷을 통해 메시지가 성공적으로 수신되었는지를 학습한 이후에, 서버는 전자 수신을 작성하여 송신인에게 전달한다. 수신은 메시지 및 어떤 첨부물들(attachments), 수신들을 리스팅하는 전달 성공/실패 테이블 및, 수신인의 특별한 에이전트들에 의해 메시지의 수신 회수, 메시지를 수신하기 위해 수신인의 다른 에이전트들의 실패 및, 메시지의 디지털 시그니쳐와 이에 따른 첨부물 중 적어도 하나를 포함하거나 바람직하게는 모두를 포함한다. 송신인의 수신에 대한 디지털 시그니쳐가 서버에서 디지털 수신을 매칭하는지를 검증함으로써, 서버는, 메시지를 보유하지 않고, 수신이 진짜로 이루어졌는지와 메시지가 정확한지를 검증할 수 있다.

대 표 도 - 도2A



특허청구의 범위

청구항 1

삭제

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

삭제

청구항 7

삭제

청구항 8

삭제

청구항 9

삭제

청구항 10

수신인으로부터 변위된 서버를 통하여 송신인으로부터 상기 수신인으로 인터넷을 통해 메시지를 송신하는 방법에 있어서, 상기 서버에서:

상기 송신인으로부터 상기 메시지를 상기 서버에서 수신하는 단계;

상기 서버에서, 상기 송신인으로부터의 상기 메시지와 함께, 메시지들의 송신 시에 상기 서버에 의해 이용된 일상적인 네트워크 루트와 상이한 네트워크 루트를 통해 상기 서버에 의해 상기 메시지가 송신된다는 표시를 수신하는 단계;

상기 메시지 및 상기 서버의 식별(identification)과 인터넷 어드레스 및 상기 송신인의 아이덴티티를 나타내는 표시를, 상기 송신인에 의해 상기 서버에 표시된 바와 같은 상기 일상적인 네트워크 루트와 상이한 네트워크 루트를 통하여 상기 서버로부터 상기 수신인의 에이전트로 상기 인터넷을 통해 송신하는 단계;

상기 서버에서, 상기 서버로부터 상기 수신인의 상기 에이전트로의 상기 메시지의 상기 송신의 핸드쉐이킹(handshaking) 및 전달 이력(delivery history)을 상기 에이전트로부터 수신하는 단계; 및

상기 메시지, 디지털 핑거프린트를 포함하는 상기 메시지의 디지털 시그니쳐, 및 상기 수신인의 상기 에이전트로부터 상기 서버에 의해 수신된 상기 메시지의 상기 핸드쉐이킹 및 전달 이력을 인터넷을 통해 상기 서버로부터 상기 송신인에게 송신하는 단계를 포함하는, 메시지 송신 방법.

청구항 11

제 10 항에 있어서,

상기 서버에서, 상기 송신인으로부터의 상기 메시지와 함께, 상기 서버로부터 상기 수신인의 상기 에이전트로 상기 메시지를 송신할 시에 실행될 부가적인 기능을 나타내는 코딩을 수신하는 단계,

상기 송신인에 의해 상기 서버에 제공된 상기 코딩에 따라서, 상기 서버로부터 상기 수신인의 상기 에이전트로 상기 메시지를 송신할 시에 상기 부가적인 기능을 제공하는 단계를 포함하는, 메시지 송신 방법.

청구항 12

제 11 항에 있어서,

상기 메시지는, 상기 서버가 상기 서버로부터 상기 수신인의 상기 에이전트로의 상기 메시지 송신의 상기 핸드쉐이킹 및 상기 전달 이력을 상기 수신인의 상기 에이전트로부터 수신한 후에 상기 서버에 의해 상기 송신인에게 송신되고,

상기 서버는 상기 송신인에게 상기 메시지를 송신한 후에 상기 메시지를 보유하지 않는, 메시지 송신 방법.

청구항 13

제 11 항에 있어서,

상기 코딩은 상기 메시지 송신의 기록을 위해 제공되고,

상기 메시지의 송신은 상기 코딩에 따라서 기록되는, 메시지 송신 방법.

청구항 14

제 11 항에 있어서,

상기 코딩은 상기 메시지의 보관을 위해 제공되고,

상기 메시지는 상기 코딩에 따라서 보관되는, 메시지 송신 방법.

청구항 15

삭제

청구항 16

삭제

청구항 17

제 11 항에 있어서,

상기 코딩은 상기 서버로부터 상기 수신인의 상기 에이전트로의 우선순위를 갖는 상기 메시지의 송신에 대해 제공되고,

상기 메시지는 상기 코딩에 따라서 우선순위로 상기 서버로부터 상기 수신인의 상기 에이전트로 송신되는, 메시지 송신 방법.

청구항 18

제 11 항에 있어서,

상기 서버가 상기 메시지, 상기 메시지의 디지털 시그니쳐 및 상기 메시지의 핸드쉐이킹 및 전달 이력을 인터넷을 통해 상기 송신인에게 송신한 후에, 상기 송신인에 의해 보유하도록 요청받지 않는다면, 상기 서버는 상기 메시지의 디지털 시그니쳐 및 상기 메시지의 상기 핸드쉐이킹 및 전달 이력의 카피(copy)를 보유하지만, 상기 메시지를 보유하지 않는, 메시지 송신 방법.

청구항 19

제 10 항에 있어서,

상기 서버는 상기 메시지를 제외한, 상기 수신인의 상기 에이전트로부터 상기 서버에 의해 수신되고 상기 송신

인에게 송신되는 정보의 카피를 보유하고,

상기 메시지가 상기 서버에 의해 상기 수신인의 상기 에이전트에게 송신되었음을 상기 송신인이 인증하고자 할 때, 상기 서버는 상기 메시지를 제외한, 상기 서버에 의해 상기 송신인에게 송신된 상기 메시지에 관련되는 정보와 상기 서버에 의해 보유된 상기 메시지에 관련되는 정보를 매칭(match)시키는, 메시지 송신 방법.

청구항 20

제 10 항에 있어서,

상기 서버는, 상기 메시지를 상기 에이전트에 송신하는 때 상기 메시지에 관련되는 상기 수신인의 상기 에이전트로부터 전달 상태 통지(delivery status notification)를 요청하고,

상기 서버는, 상기 에이전트로부터 상기 메시지의 디지털 시그니쳐를 수신할 때 상기 수신인의 상기 에이전트로부터 상기 전달 상태 통지를 수신하는, 메시지 송신 방법.

청구항 21

제 10 항에 있어서, 수신인으로부터 변위된 서버를 통하여 상기 수신인으로 인터넷을 통해 메시지를 송신하는 방법에서, 상기 서버에서, 상기 송신인으로부터 상기 메시지를 상기 서버에서 수신하는 단계는,

코딩된 형태로 상기 메시지의 개요(synopsis)를 구성하는 해시(hash)를 생성하는 단계,

상기 메시지의 디지털 핑거프린트를 생성하기 위해 암호 코드로 상기 해시를 암호화하는 단계를 포함하는, 메시지 송신 방법.

청구항 22

제 21 항에 있어서,

상기 메시지에 대한 임의의 첨부물(attachment)에 대해, 코딩된 형태로 상기 첨부물의 개요를 구성하는 해시를 생성하는 단계;

상기 첨부물의 디지털 핑거프린트를 생성하기 위해 암호 코드로 상기 첨부물로부터 상기 해시를 암호화하는 단계; 및

상기 메시지 및 상기 메시지의 디지털 핑거프린트가 상기 서버로부터 인터넷을 통해 상기 수신인에게 송신되는 동일한 시점 및 동일한 네트워크 루트를 통해 상기 첨부물 및 상기 첨부물의 상기 디지털 핑거프린트를 상기 송신인에게 인터넷을 통해 송신하는 단계를 더 포함하는, 메시지 송신 방법.

청구항 23

제 21 항에 있어서,

상기 메시지는, 상기 표시가 상기 메시지와 함께 상기 송신인에 의해 상기 서버에 제공되지 않을 때 상기 일상적인 네트워크 루트를 통해 상기 서버에 의해 송신되고,

상기 메시지는, 상기 표시가 상기 메시지와 함께 상기 송신인에 의해 상기 서버에 제공될 때 상기 일상적인 네트워크 루트와 상이한 네트워크 루트를 통해 상기 서버에 의해 송신되는, 메시지 송신 방법.

청구항 24

삭제

청구항 25

제 23 항에 있어서,

상기 메시지의 디지털 핑거프린트, 상기 송신인의 이름, 상기 서버의 아이덴티티와 인터넷 어드레스, 및 상기 수신인의 아이덴티티와 인터넷 어드레스를 상기 서버에서 저장하는 단계, 및

상기 메시지, 상기 메시지의 디지털 핑거프린트, 상기 송신인의 이름, 상기 서버의 상기 아이덴티티와 인터넷 어드레스, 및 상기 수신인의 상기 아이덴티티와 인터넷 어드레스를, 상기 송신인에 의한 저장을 위해 상기 송신

인에게 송신하는 단계를 더 포함하는, 메시지 송신 방법.

청구항 26

제 22 항에 있어서,

상기 메시지의 디지털 핑거프린트, 상기 송신인의 이름, 상기 서버의 아이덴티티와 인터넷 어드레스, 및 상기 수신인의 아이덴티티와 인터넷 어드레스는 상기 서버에서 저장되고,

상기 메시지, 상기 메시지의 디지털 핑거프린트, 상기 송신인의 이름, 상기 서버의 아이덴티티와 인터넷 어드레스, 및 상기 수신인의 아이덴티티와 인터넷 어드레스는 상기 송신인에 의한 저장을 위해 상기 송신인에게 송신되는, 메시지 송신 방법.

청구항 27

삭제

청구항 28

제 21 항에 있어서,

상기 메시지의 디지털 핑거프린트는 상기 메시지의 디지털 다이제스트 및 상기 디지털 다이제스트의 암호를 포함하고,

상기 메시지, 상기 메시지의 디지털 핑거프린트, 상기 송신인의 상기 아이덴티티, 상기 서버의 상기 아이덴티티와 인터넷 어드레스, 상기 수신인의 상기 에이전트의 상기 아이덴티티와 인터넷 어드레스, 및 상기 에이전트에서의 상기 메시지의 수신 상태는 상기 서버에 의해 상기 송신인에게 송신되는, 메시지 송신 방법.

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

청구항 32

삭제

청구항 33

삭제

청구항 34

삭제

청구항 35

삭제

청구항 36

삭제

명 세 서

기 술 분 야

[0001] 본 발명은 전자 메시지의 전달(delivery) 및 내용(content)을 검증하기 위한 시스템 및 방법에 관한 것으로, 특히, e-메일 메시지의 전달 및 내용에 관한 증거를 차후 제공하는 시스템 및 방법에 관한 것이다. 특히, 본 발명은 전자 메시지의 전달 및 내용을 검증하는 동안 인터넷을 통해 등록된 메일을 송신하고 차후에 등록된 e-메일 메시지의 전달 및 내용에 관한 검증을 제공하기 위한 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 최근, e-메일이 필수적인 사업 도구가 되었다. e-메일은 다수의 사업 업무들을 위해 "우편 메일(snail mail)"을 대신하고 있으며, 그 이유는 보다 신속하고, 저렴하며, 일반적으로 보다 신뢰성이 있기 때문이다. 그러나, 등기 및 내용증명 메일 같은 하드 카피(hard copy)가 여전히 우세한 일부 메일 분야들이 남아있다. 예로서, 서신이 내용증명 메일로 보내질 때, 송신인은 그 서신이 운송되었다는 것을 증명하는 영수증을 받게 된다. 반환된 등기 메일 영수증은 수신인 또는 수신인의 허가된 대리인에게 그 서신이 성공적으로 전달되었다는 우체국의 확인을 추가한다. 부가적으로, Federal Express® 및 United Parcel Service®(UPS) 같은 사설 우편사들(private couriers)은 소정 유형의 전달 확인을 제공한다. 커리어(courier) 메일의 모든 단편(piece)이 실제로 등기되어 있기 때문에, 고객들은 그들이 전달 증명을 원할 때 이들 서비스들을 받는 것은 자연스러운 것이다.

[0003] 다수의 현존하는 e-메일 시스템들 및 e-메일 프로그램들은 이미 일부 형태의 전달 증명을 제공한다. 예로서, 오늘날의 일부 e-메일 시스템들은 송신인이 "통지 요청" 태그들(tags)을 메시지에 표시할 수 있게 한다. 이런 태그들은 메시지의 전달 및/또는 메시지 열람 시기에 대한 통지를 송신인이 요청할 수 있게 한다. 송신인이 전달 통지를 요청하였을 때, 인터넷 e-메일 시스템은 메시지가 수신인의 메일 서버 또는 전자 편지함에 전달되었다는 e-메일 영수증을 송신인에게 제공할 수 있다. 영수증 메시지는 메시지의 이름, 착신 어드레스 및 전달 시간을 포함할 수 있다. 또한, 이는 메시지가 그 착신지까지의 경로 도중에 통과한 모든 인터넷 "스테이션들"의 리스트를 포함할 수도 있다(메일링 소프트웨어 내에 제공되어 그 내부에서 작동되는 "플래그들(flags)"의 유형들에 따라서). 이 보고 형태는 e-메일을 구현하는 룰들(rules) 및 프로토콜들 중 일부에 내장된다. 또한, 메시지가 "판독 통지" 요청과 함께 보내지게 될 때, 수신인의 e-메일 프로그램은 수신인이 그 메시지를 읽기 위해 열람하였다는 e-메일 통지를 송신인에게 보낼 수 있다. 다수의 전자 메일 클라이언트들은 이런 종류의 보고가 가능하며 지원하고 있지만, 그러나, 인터넷 프로토콜들은 이를 필수적으로 수행하지 않는다.

[0004] 그러나, 이는 통지 요청이 첨부된 e-메일이 모든 관점에서 등기 메일로서 유효하다는 것을 의미하지는 않는다. 사람들은 그들이 전달 증명, 예로서, 공적 또는 범죄 행위에 사용될 수 있는 증명, 또는, 관리자나, 그 메시지가 전달되는 클라이언트 또는 정부기관에게 작업이 이루어졌다는 것, 주문이 들어갔다는 것 또는 계약 조건이 충족되었다는 것을 확신시키는 증명을 원하기 때문에 서신들을 내용증명 또는 등기한다.

[0005] 미우편국(Unite States Postal Service: USPS)으로부터의 등기 영수증은 전달의 증명을 제공하며, 그 이유는 USPS가 이를 지원하기 때문이다. 이 영수증은 논제의 서신 또는 소포가 수신인 또는 그 허가된 대리자에게 실제로 전달되었다는 우체국의 확인을 나타낸다. 한편, e-메일 영수증에서는, e-메일 영수증이 그 메시지가 전달되었다는 증명으로서 법원에서 설득력 있는 증거로서 허용 및 신뢰되기에는 다양한 장애물들이 존재한다. 결국, 영수증은 소정인에 의해 소정의 시기에 변경 또는 생성될 수 있는 또 다른 e-메일 메시지일 뿐이다.

[0006] e-메일을 경유한 통신의 편리성 및 저렴한 비용의 보다 완전히 취하기 위해서, e-메일 메시지의 내용 및 전달의 신뢰성 있는 증명을 제공할 수 있는 e-메일 시스템 및/또는 방법에 대한 필요성이 존재한다.

[0007] 이 필요성을 충족시키기 위해서, 송신인들이 서비스들에 등록함으로써 전달의 제 3 자 증명을 받을 수 있는 몇몇 시스템들이 설립되었으며, 여기서는,

[0008] a) 송신인이 전자 메시지를 그 문서의 의도된 수신인의 리스트와 함께 제 3 자에게 전송한다.

[0009] b) 제 3 자는 그 메시지를 볼 수 있는 제 3 자의 웹 사이트를 방문하도록 그들을 초대하는 통지를 그 메시지의 의도된 수신인들 각각에게 보낸다.

[0010] c) 의도된 수신인이 제 3 자의 웹 사이트를 방문하여 메시지를 보는 경우에, 제 3 자는 송신인이 이 메시지가 수신인에 의해 읽혀졌다는 것을 알 수 있도록 이 방문을 기록한다.

[0011] 이런 시스템들의 단점들은 다수이다. 첫 번째로, 이들은 제 3 자의 서비스로부터 그 메시지들을 수집하기 위해 e-메일 수신인의 협력에 주로 의존한다. 그러나, 송신인이 메시지의 전달의 증명을 원할 수 있는 상황들은 의도된 수신인이 메시지 수신에 협력할 것으로 생각되지 않는 경우들이 빈번하다. 이런 경우들에 있어서, 예로서, 메시지의 수신확인 영수증이 수신인에게 재정적 또는 법적 부담을 부여하는 경우에, 수신인은 메일이 그가 수신할 수 있는 상태라는 통지를 간단히 무시할 수 있다. 이런 시스템에는 의도된 수신인이 대기 메일 통지를 수신하는 것을 보증하기 위한 수단이 존재하지 않는다는 것을 주목하여야 한다. 두 번째로, 이런 시스템들은 송신인 및/또는 수신인이 각 메시지를 송신하고, 각 메시지를 인수하고, 각 메시지의 전달을 확인하기 위해 월드 와이드 웹 사이트에 접속하는 것을 필요로할 수 있는 한 정규 e-메일에 비해 사용이 느리고 성가시다. 또한, 이런 방법들에 의한 문서들의 전송은 송신인과 수신인 양자 모두가 웹 사이트에 파일들을 업로드 및 다운로드 하는 것을 필요로할 수 있다. 마지막으로, 이들 방법들이 그들이 인수되거나 소멸되는 시간까지 각 메시지 전체의 카피를 제 3 자가 보유하는 것을 필요로 하기 때문에, 이 방법들은 그 제공자가 연장된 시간 기간에 걸쳐 데이터 저장 및 데이터 추적을 위해 현저한 연산 자원들을 투자하는 것을 필요로 한다. 전달 증명을 제공하는 대안적인 방법으로서, 일부 시스템들은 동일 e-메일 클라이언트를 사용하는 수신인에게서 제공된, 메시지가 수신된 시기를 송신인들에게 통지하는 전용 e-메일 클라이언트들 또는 웹 브라우저 플러그인들을 제공한다. 이런 시스템들의 명백한 단점은 이들이 송신인 및 수신인 양자 모두가 동일 e-메일 클라이언트를 사용하는 것을 필요로 한다는 것이다.

[0012] 따라서, 수신인의 승낙이나 협력을 필요로 하지 않고, 송신인이나 수신인 측에 어떠한 특별한 소프트웨어도 필요로 하지 않으며, 종래의 e-메일을 사용하는 것과 동일 또는 거의 동일한 편리함 및 속도로 동작하며, 서비스 공급자에 의해 경제적으로 운영될 수 있는 전자 메시지들의 내용 및 전달의 신뢰성 있는 증명을 제공할 수 있는 e-메일 시스템/방법에 대한 필요성이 존재한다.

발명의 상세한 설명

[0013] 발명의 요약

[0014] 2000년 7월 27일의 톰코우 터렌시 에이(Terrance A. Tomkow)에 의해 출원된, 계류중인 비예비 출원 제09/626,577호(대리인 파일 RPOST-57228)에 개시되고 청구된, 본 출원의 양수인에게 양도된 본 발명의 일반적인 목적은 보증 및 개봉 증명 증서를 경유하여 e-메일 같은 전자 메시지의 내용 및 전달을 신뢰성 있게 검증하기 위한 시스템 및 방법을 제공하는 것이다. 이상적으로, 계류중인 출원 제09/626,577호(대리인 파일 RPOST-57228)에 개시되고 청구된 본 발명은 등기된 미국 메일의 법적 지위 보다 우월하지는 않더라도 동등한 수준의 법적 지위를 e-메일 및 다른 전자 메시지들에게 줄 것이다. 그러나, 소정의 특정 법적 지위가 여기서 구상된 방법들에 따라 보내진 메시지들에 주어지는 것을 본 발명이 필요로 하는 것은 아니며, 어쨌건 본 발명은 유용한 정보 및 검증을 제공한다.

[0015] 계류중인 비예비 출원 제09/626,577호에 개시되고 청구된 본 발명은 그 시스템을 통해 보내지는 각 전자 메시지의 디지털 시그니쳐를 생성 및 기록하는 전자 메시지 시스템을 포함한다. 발신자는 시스템에 그 전자 메시지의 카피를 보내거나, 시스템 그 자체 내에서 전자 메시지를 생성할 수 있다. 그후, 시스템은 "수신(to)" 어드레스들 및 "참조(cc)" 어드레스들을 포함하는 모든 수신인들(또는, 수신인들과 연관된 착신 메시지 헤더들)에게 이 전자 메시지를 포워딩 및 전달한다. 그후, 시스템은 전자 메시지의 발신자에게 전달 영수증을 반환한다. 이 영수증은 무엇보다도 원본 메시지, 메시지의 디지털 시그니쳐, 및 수신인들에게로의 전달 시간들을 포함하는 핸드쉐이킹(handshaking) 및 전달 이력을 포함한다. 영수증에 포함된 정보의 추후 검증 및 인증을 위해서, 발신자 또는 사용자는 영수증의 카피를 시스템에 송신한다. 그후, 시스템은 그 디지털 시그니쳐가 원본 메시지 및 영수증의 나머지와 일치하는 지를 검증한다. 두 가지가 일치하는 경우에, 이때, 시스템은 서신을 전송하거나, 전자 메시지가 변경되지 않았다는 것을 검증하는 상이한 인증 확인을 제공한다.

[0016] 계류중인 비예비 출원 제09/626,577호에 개시되고 청구된 시스템은 다수의 방식들로 활용될 수 있는 인터넷에 연결된 e-메일 서버의 형태일 수 있다. 예로서, 개인 사용자들은 "카본 카피(carbon copy)"(cc:)를 시스템에 전송함으로써, 또는, 시스템 그자체내에서 메시지를 작성함으로써 e-메일 같은 그 전자 메시지를 등록할 수 있다. 법인 또는 전자 상거래 사용자들을 위하여, 이들 사용자들은 그 서버를 본 발명을 채용하는 서버로 변경할 수 있고, 시스템이 영수증들을 보유 및 보관하게 하는 옵션으로, 그 외부적 전자 메시지들 모두를 등록할 수 있다. 본 시스템은 암호화된 전자 메시지들을 받아들이고 확인할 수 있으며, "방화벽(fire wall)" 내부 및/또는 외부

의 전자 메시지들을 관리할 수 있다. 웹 기반 사용자들, 즉, MSN Hotmail(R) 또는 Yahoo Mail(R) 같은 웹 기반 e-메일들을 사용하는 개인들 또는 법인들을 위하여, 이런 사용자들은 계류중인 비예비 출원 제09/626,577호에 개시되고 청구된 본 발명의 시스템을 사용하여 e-메일들을 기록 및/또는 메시지들을 보관할 것인지 여부를 각 경우마다(case-by-case basis) 선택하기 위해, 그 e-메일 프로그램내의 선택란(box) 또는 기타 설정 플래그를 체크할 수 있다.

[0017] 디지털 시그니쳐는 메시지 다이제스트(message digest)를 생성하고, 그후, 이 메시지 다이제스트를 암호화하도록 메시지 상에 해시 펑션(hash function)을 수행하는 것 같은 공지된 디지털 시그니쳐 기술들을 사용하여 생성될 수 있다. 메시지의 본문, 소정의 첨부물들, 본문과, 첨부물들과, 개별 메시지 다이제스트들을 포함하는 전체 메시지들에 대하여 별개의 디지털 시그니쳐들이 생성될 수 있다. 암호화된 메시지 다이제스트는 일 유형의 메시지 인증 또는 검증 코드나 보증 증서를 제공한다. 다른 메시지 인증 및/또는 검증 코드들도 생성 및 사용될 수 있다.

[0018] 일 특징에서, 계류중인 출원 제09/626,577호에 개시되고 청구된 본 발명은 전자 메시지의 내용 및 전달에 관한 증명을 제공하는 방법이며, 이는 컴퓨터 네트워크를 통해 송신인으로부터 전자 메시지를 수신하는 단계로서, 상기 메시지는 그와 관련된 전달 어드레스를 가지는, 상기 전자 메시지 수신 단계; 상기 메시지에 따른 메시지 다이제스트를 연산하는 단계; 상기 메시지 다이제스트를 암호화하는 단계; 상기 전달 어드레스에 대응하는 착신지로 상기 메시지를 전자적으로 송신하는 단계; 상기 메시지의 전달을 실행하는 단순 메일 전송 프로토콜(Simple Mail Transport Protocol: SMTP) 또는 확장 SMTP(ESMTP) 대화를 기록하는 단계; 메시지 및 전달 어드레스와 관련된 전달 상태 통지 정보를 수신하는 단계; 상기 송신인에게 전자 영수증을 제공하는 단계로서, 상기 영수증은 메시지의 카피, 암호화된 메시지 다이제스트, (E)SMTP 트랜스크립트들 및 적어도 하나의 전달 상태 통지 정보의 서브셋을 포함하는, 상기 전자 영수증 제공 단계, 후일, 상기 송신인으로부터 상기 전자 영수증을 전자적으로 수신하는 단계, 상기 암호화된 메시지 다이제스트가 상기 메시지에 대응한다는 것을 검증하고 상기 메시지가 상기 전달 어드레스와 관련된 전자 메시지 취급자에 의해 수신되었다는 것를 검증하는 단계를 포함한다.

[0019] 다른 특징에서, 계류중인 비예비 출원 제09/626,577호에 개시되고 청구된 본 발명은 전자 메시지의 전달을 검증하는 방법이며, 이는 광역 네트워크 컴퓨터 시스템에서 착신지 어드레스로의 라우팅(routing)을 위해 메시지 송신인으로부터 전자 메시지를 수신하는 단계; 상기 착신지 어드레스와 관련된 전자 메시지 서버와 통신을 형성하는 단계로서, 상기 서버는 착신지 서버를 정의하는, 사익 통신 형성 단계; 상기 착신지 서버가 전달 상태 통지(DSN) 기능을 지원하는지 여부를 판정하도록 상기 착신지 서버에 문의하는 단계; 문의에 대한 응답을 수신하는 단계로서, 상기 문의와 응답은 함께 SMTP 대화를 정의하는, 상기 응답 수신 단계; 상기 SMTP 대화의 결과에 따라 상기 착신지 서버로부터 전달 상태 통지 정보를 요청하는 단계; 상기 착신지 어드레스로 상기 전자 메시지를 전송하는 단계; 상기 전자 메시지의 전달에 관하여 상기 착신지 서버로부터 DSN 정보를 수신하는 단계; 및 상기 SMTP 대화의 적어도 일부와, 상기 DSN 정보의 적어도 일부를 상기 메시지 송신인에게 제공하는 단계를 포함한다.

[0020] 또 다른 특징에서, 계류중인 비예비 출원 제09/626,577호에 개시되고 청구된 본 발명은 수신된 전자 메시지의 내용을 검증하는 방법이며, 이는 전자 메시지를 수신하는 단계; 상기 수신된 메시지의 내용에 대응하는 디지털 시그니쳐를 생성하는 단계; 상기 메시지와 상기 디지털 시그니쳐를 착신 수신인에게 제공하는 단계; 및 추후에, 상기 디지털 시그니쳐가 상기 메시지에 대응한다는 것을 검증하는 단계를 포함한다.

[0021] 계류중인 비예비 출원 제09/626,577호에 개시되고 청구된 본 발명의 또 다른 특징에 따라서, 상기 방법은 메시지가 수신인에 의해 전자적으로 수신되었는지 여부를 설정하는 단계를 포함하고, 이는 송신인으로부터 수신인의 어드레스와 함께 전자적으로 발송될 메시지를 제공하는 단계; 상기 메시지와 관련된 시그니쳐를 생성하는 단계; 상기 메시지를 상기 수신인의 어드레스로 전자적으로 발송하는 단계; 상기 수신인의 어드레스로 발송된 상기 메시지의 최종 전달 상태를 판정하기 위해서 상기 메시지를 추적하는 단계; 상기 메시지의 최종 전달 상태 수신시, 상기 메시지의 카피와, 상기 시그니쳐와, 상기 메시지를 위한 상기 최종 전달 상태를 포함하는 영수증을 생성하는 단계; 및, 상기 메시지가 상기 수신인에 의해 전자적으로 수신되었음을 추후 설정하기 위해 상기 송신인에게 상기 영수증을 제공하는 단계를 포함한다.

[0022] 계류중인 비예비 출원 제09/626,577호에 개시되고 청구된 본 발명의 또 다른 특징에 따라서, 수신인에게 송신된 전자 메시지가 판독되었는지를 증명하기 위한 방법이 제공되고, 이는 수신인의 어드레스와 함께 전자 메시지를 제공하는 단계; 상기 전자 메시지에 대응하는 디지털 시그니쳐를 계산하는 단계; 상기 전자 메시지를 전자적으로 상기 수신인의 어드레스로 발송하는 단계; 상기 수신인으로부터 메일 사용자 에이전트(e-메일 클라이언트 "

판독") 통지를 요청하는 단계; 상기 판독 통지의 수신시, 상기 메시지의 카피와, 상기 대응 전자 메시지를 위한 상기 디지털 시그니쳐와, 상기 수신인으로부터의 판독 영수증을 위한 제 2 디지털 시그니쳐를 포함하는 판독 영수증을 생성하는 단계; 및, 상기 메시지가 상기 수신인에 의해 수신되었음을 추후 검증하기 위해 상기 판독 영수증을 제공하는 단계를 포함한다.

[0023] 계류중인 비예비 출원 제09/626,577호에 개시되고 청구된 본 발명의 다른 특징에 따라서, 전자 메시지의 요지 카피(purported copy)의 완전성(integrity)을 검증하는 방법이 제공되고, 이는 요지 전자 메시지 카피를 수신하는 단계로서, 상기 요지 카피는 그와 관련된 암호화된 메시지 다이제스트를 포함하는, 상기 요지 전자 메시지 카피 수신 단계; 상기 메시지 다이제스트를 해독하는 단계; 상기 요지 카피의 내용에 기초하여 제 2 메시지 다이제스트를 생성하는 단계; 및, 상기 두 메시지 다이제스트들이 일치하는지를 판정하기 위해 상기 해독된 메시지 다이제스트와 상기 제 2 메시지 다이제스트를 비교함으로써 상기 요지 카피를 검증하는 단계를 포함한다.

[0024] 계류중인 비예비 출원 제09/626,577호에 개시되고 청구된 본 발명의 또 다른 특징에 따라서, 수신된 등록된 e-메일을 검증하기 위한 방법이 제공되고, 이는 전자 영수증을 수신하는 단계로서, 상기 영수증은 기초 메시지 및 암호화된 메시지 다이제스트를 포함하는, 상기 전자 영수증 수신 단계; 상기 암호화된 메시지 다이제스트를 해독하는 단계; 상기 기초 메시지로부터 제 2 메시지 다이제스트를 생성하는 것; 및 상기 해독된 메시지 다이제스트가 상기 제 2 메시지 다이제스트와 일치하는 경우에, 상기 e-메일을 검증하는 단계를 포함한다.

[0025] 또 다른 특징에서, 계류중인 비예비 출원 제09/626,577호에 개시되고 청구된 본 발명은 사용자들이 보증 메시지들을 송신 및 수신하기 위해 들어갈 수 있는 웹 사이트로 이루어지며, 이는 상기 메시지들을 송신 및 수신하고 상기 메시지의 상기 내용 및 전달에 관한 보증 증서를 제공하는 독립 제 3 자로서 작용하는 웹 사이트 호스트를 구비한다.

[0026] 본 기술 분야의 숙련자들은 유사 참조 번호들이 유사 부품들을 지시하고 있는 첨부 도면과 연관하여 보면서 하기의 양호한 예시적 실시예의 상세한 설명과, 첨부된 청구범위를 읽음으로써, 계류중인 비예비 출원 제09/626,577호에 개시되고 청구된 본 발명의 상술한 목적들 및 본 발명의 다른 특징들과 장점들을 명백히 알 수 있을 것이다.

[0027] 바람직한 실시예의 간단한 설명

[0028] 송신인으로부터 메시지를 수신하고 이 메시지를 인터넷을 통해 수신인에게 전송하는 서버를 개시한다. 서버는 통상 제 1 경로에서 통상 인터넷을 통해 메시지를 수신인에게 전송한다. 송신인이 메시지내의 특정 위치에서 메시지가 등록됨을 나타낼 때, 서버는 제 2 경로에서 인터넷을 통해 수신인에게 메시지를 전송한다. 송신인은 서버에 의해 제공되는 통상적이 아닌 다른 특별한 방법들로 메시지를 서버가 다루어야 하는 메시지 내의 부가적인 표시들(indications)을 제공할 수도 있다.

수신 또는 수신인의 에이전트로부터 인터넷을 통해 메시지가 성공적으로 수신되었는지를 학습한 이후에, 서버는 전자 수신을 작성하여 송신인에게 전달한다. 수신은 메시지 및 어떤 첨부물들(attachments), 수신들을 리스팅하는 전달 성공/실패 테이블 및, 수신인의 특별한 에이전트들에 의해 메시지의 수신 회수, 메시지를 수신하기 위해 수신인의 다른 에이전트들의 실패 및, 메시지의 디지털 시그니쳐와 이에 따른 첨부물 중 적어도 하나를 포함하거나 바람직하게는 모두를 포함한다. 송신인의 수신에 대한 디지털 시그니쳐가 서버에서 디지털 수신을 매칭하는지를 검증함으로써, 서버는, 메시지를 보유하지 않고, 수신이 진짜로 이루어 졌는지와 메시지가 정확한지를 검증할 수 있다.

[0029] 첨부 도면을 참조로 본 발명의 양호한 실시예에 대하여 상세히 설명한다.

실 시 예

[0044] (발명의 상세한 설명)

[0045] 본 설명은 단지 본 발명의 일반적 원리들을 예시하기 위한 것일 뿐, 제한적인 의미를 가지는 것은 아니다. 본 섹션의 타이틀들 및 본 상세한 설명의 전체 구성은 단지 편의상 취해진 것이며, 본 발명을 제한하기 위한 것은 아니다. 따라서, 본 발명은 인터넷 네트워크 아키텍쳐 및 인프라구조를 사용하는 e-메일 메시징 시스템들에 관하여 설명된다. 여기에 기술된 특정 메시지 유형 및 네트워크 아키텍쳐는 단지 예시를 위한 것이며, 본 발명은 유선 및 무선 네트워크들을 포함하는 상이한 컴퓨터 네트워크 아키텍쳐들을 사용하는 상이한 전자 메시지 프로

토콜들 및 메시지 유형들에도 적용될 수 있다는 것을 이해하여야 한다. 설명의 편의를 위해, 계류중인 출원 제 09/626,577호에 개시되고 청구된 본 발명에 따라 처리되는 메시지들은 여기에서 "등록" 메시지들이라 지칭할 수 있다. 하기의 설명에서, 용어 "RPost"는 본 발명을 구현하는 소프트웨어 및/또는 하드웨어를 생성 및/또는 운영하고, 및/또는 이해관계가 없는 제 3 자 메시지 검증자로서 기능하는 제 3 자 엔티티에 대한 일반적 용어들을 지칭한다. 이 용어는 단지 예시적 설명의 편의를 위해 사용되는 것이며, 본 발명을 제한하는 것으로 이해하여서는 안된다.

[0046] Ⅰ. 유출 메일 서버(OUTGOING MAIL SERVER) 실시예로서의 RPOST

[0047] 도 1은 유출 e-메일들이 계류중인 비예비 출원 제09/626,577호에 개시되고 청구된 본 발명에 따라 기록되는 본 발명의 제 1 실시예의 시스템 다이어그램이다. 본 실시예에서, RPost 등록 서버(14)는 메시지 송신인의 메일 사용자 에이전트(MUA)(13)를 위한 주 유출 메일 전송 에이전트(MTA)로서 기능한다. 비록, 설명의 간이화를 위해, 메시지 수신인(18)이 기술적으로 수신인이며, 따라서, 단지 의도된 수신인 또는 의도된 착신지이지만, 이 엔티티는 여기에서, 수신인, 수신인 또는 착신지로서 지칭될 수 있다. 단일 메시지가 다수의 상이한 착신지들을 가질 수 있으며, 이들 각각이 상이한 MTA를 통해 도달될 수 있다는 것을 주목하여야 한다. 등록된 메시지들을 송신하는 방법은 세 부분들로 나누어질 수 있다.

[0048] 1) 전처리 : 메시지가 전송되기 이전에 취해지는 단계들.

[0049] 2) 전송 : 메시지들을 수신인들에게 전달하는 방법.

[0050] 3) 후처리 : 전달 이후에 메시지들에 대한 정보를 수집하기 위한 절차들, 영수증들의 생성 및 영수증들의 검증.

[0051] 1.1 전처리

[0052] 전송을 위한 메시지를 수신하였을 때, RPost 서버(14)는 하기와 같은 정보를 저장하기 위해 사용되는, 각 메시지를 위한 데이터베이스에 기록들을 생성한다.

[0053] a) 메시지가 수신된 시간;

[0054] b) 메시지의 첨부물들의 명칭들;

[0055] c) 메시지의 어드레스들의 수;

[0056] 메시지의 각 착신지를 위하여, 데이터베이스는 하기의 것들을 기록한다.

[0057] a) 착신지 명(이용가능하면);

[0058] b) 착신지의 인터넷 어드레스;

[0059] c) 착신지의 메일 서버에 메시지가 전달된 시간;

[0060] d) 이 착신지의 전달 상태

[0061] 시스템에 의해 사용되는 수신인 전달 상태들은 하기의 것들을 포함한다.

[0062] 미전송(UNSENT)

[0063] 이 상태는 메시지가 보내지지 않았다는 것을 나타낸다.

[0064] 전달 완료 및 DSN 대기(DELIVERED-AND-WAITING-FOR-DSN)

[0065] 이 상태는 이 메시지가 성공/실패 통지가 기대될 수 있도록 전달 상태 통지(DSN)를 지원하는 ESMTP 호환 MTA에 전달되었다는 것을 나타낸다.

[0066] 전달 완료(DELIVERED)

[0067] 이 상태는 이 수신인에게 송신된 메시지의 카피가 ESMTP DSN을 지원하지 않는 서버에 성공적으로 전달되었다는 것을 표시한다.

[0068] 편지함으로 전달 완료(DELIVERED-TO-MAILBOX)

[0069] 이 상태는 이 수신인에게 송신된 메시지의 카피가 수신인의 편지함에 전달되었다는 것을 나타내는 DSN 메시지가 수신되었다는 것을 표시한다.

[0070] 중계 완료(RELAYED)

[0071] 이 상태는 그 수신인에게 송신된 메시지의 카피가 다른 서버로 중계되었다는 것을 나타내는 MTA DSN이 수신되었다는 것을 표시한다.

[0072] 전달 불가(UNDELIVERABLE)

[0073] 이 상태는 반복된 시도들 이후에, RPost가 이 수신인에게 메시지들을 전달하기 위해 MTA에 접속하는 것이 불가능하다는 것을 나타낸다.

[0074] 실패(FAILED)

[0075] 이 상태는 이 수신인에게 메시지의 카피를 전달하는 것에 대한 실패를 나타내는 MTA DSN이 수신되었다는 것을 표시한다.

[0076] 이때, 시스템은 또한 메시지의 내용들에 해싱 펑션들(hashing functions)을 수행한다.

[0077] RPost 서버(14)는 해시 펑션 및 암호화 알고리즘을 채용한다. 해시 펑션은 MD2, MD5, 보안 해싱 알고리즘(secure hashing algorithm: SHA) 또는 미래에 개발될 수 있는 상이한 해시 펑션들 같은 소정의 널리 공지된 해시 펑션들 중 하나일 수 있다. 브루스 쉬나이더(Bruce Schneider)의 "해시 알고리즘들 및 방법들은 응용 암호작성법 : 프로토콜들, 알고리즘들 및 C의 소스 코드(John Wiley & Sons, Inc.; New York; 1993)", 연방 정보 처리 표준 공보 180-1(FIPS PUB 180-1)의 "보안 해시 표준(National Institute of Standards and Technology)" 및 발명의 명칭이 "정보 완전성 검증을 위한 분포 핑거프린트들"인 크라우크지크(Krawczyk)에게 허여된 미국 특허 제 5,530,757호에 기술되어 있으며, 이들은 그 해시 펑션들, 암호화 및 이들 펑션들을 실행하기 위한 방법 및 시스템들에 대한 그 교시들을 본 명세서에서 참조하고 있는 것들이다. 메시지의 내용들이 변경되었는지 여부를 검출하기 위한 다른 공지된 방법들 또는 신규한 방법들이 사용될 수 있다.

[0078] 양호한 해시 펑션(H)은 일방적(one-way), 즉, 이는 역변환이 곤란하며, 여기서, "역변환이 곤란하다"는 것은 해시값(h)이 주어질 때, H(x)=h 같은 소정의 입력 x를 발견하는 것이 연산적으로 불가능하다는 것을 의미한다. 또한, 해시 펑션은 적어도 약하게 충돌이 없어야만 하며, 이는 메시지 x가 주어질 때, H(x) = H(y)가 되는 소정의 입력 y를 찾는 것이 연산적으로 불가능하다는 것을 의미한다. 이 결과는 사용된 알고리즘과 결과 해시값 또는 메시지 다이제스트를 알고있는 위조 가능자가 그럼에도 불구하고, 동일 수로 해시하는 위조 메시지를 생성할 수 없다는 것이다. 해시 펑션에 의해 반환된 해시값(h)은 일반적으로 메시지 다이제스트라 지칭된다. 메시지 다이제스트는 때때로, 메시지(x)의 "디지털 핑거프린트"라고 지칭된다. 현재, 결과들이 보안되고, 위조할 수 없게 되는 것을 보증하기 위해서, 일방 해시 펑션들이 적어도 128 비트 길이인 출력들을 생성하는 것이 권장된다. 기술 진보의 현 상태로서, 해시 펑션들을 보안하기 위한 권장 길이는 증가될 수 있다.

[0079] RPost 서버(14)는 메시지 본문을 위해 메시지 다이제스트를 연산하고, 메시지의 첨부물들 각각에 대하여 별개의 메시지 다이제스트를 연산하며, 그들이 추후 메시지의 영수증에 포함될 수 있는 방식으로 이들을 저장한다.

[0080] 등록이 필요한 방식으로 메시지가 변경되기 이전에, 원본 메시지와 그 첨부물들의 카피가 이들이 추후 시스템에 의해 검색될 수 있는 방식으로 저장된다.

[0081] RPost 서버는 수신인의 MTA로의 전송 이전에 다수의 방식으로 메시지를 변경할 수 있다.

[0082] 비록 이것이 본 발명을 실시하는 데 필수적이지는 않지만, 메시지는 메시지의 "제목" 라인의 시작부에 단어 "등록완료"를 삽입하거나, 원본 메시지 또는 상이한 태깅의 단부에

[0083] "이 메시지는 RPost에 기록되었습니다. 부가 정보를 원하신다면 웹사이트 www.RPost.com을 방문하여 주시기 바랍니다"

[0084] 등의 태그를 첨부함으로써 이 메시지가 등록되었다는 사실을 나타내도록 태그첨부될 수 있다. 부가적으로, 태그는 명령들, 월드와이드웹 어드레스들 또는 등록된 메시지를 작성 및 송신할 수 있는 웹 페이지로의 링크연결에 의해 수신인을 초대하여 그 메시지에 대한 등록된 답신을 보낼 수 있게 하는 링크들을 포함할 수 있다.

[0085] 비록, 태깅은 선택적이지만, 전달된 메시지는 일반적으로 여기서 태그 첨부 메시지라 지칭된다.

[0086] 인터넷 프로토콜들은 e-메일 메시지들을 위한 영수증의 두 가지 형태들을 제공한다.

[0087] MTA 통지들

[0088] 이들은 다양한 사건들이 발생하였다는 것을 메시지의 명목상 송신인에게 통지하는, 수신인의 MTA에 의해 송신되는 e-메일이다. SMTP 프로토콜에 부합하는 MTA들은 통상적으로, 수신인의 우편함에 메시지를 전달할 수 없는 경우(어드레스가 유효하지 않거나, 수신인의 우편함이 그 할당된 저장 분량을 초과한 경우에 발생할 수 있는 바와 같이)에만 통지를 보낸다.

[0089] 확장 SMTP 표준의 도입과 함께, 송신 MTA들이 메시지들의 전달의 성공 및 실패에 대한 통지들을 요청하는 것이 가능해졌다. 이들 전달 상태 통지들(DSN들)은 예로서, 메시지가 수신인의 우편함에 성공적으로 투입된 것, 메시지가 소정의 사유로 수신인의 우편함에 전달될 수 없는 것, 수신인의 메시지가 DSN 영수증들을 제공하지 않는 상이한 서버상으로 중계되는 것 같은 특정 사건들이 발생할 때, 수신 MTA에 의해 메시지의 명목상 송신인에게 보내지는 e-메일들이다.

[0090] 확장 SMTP(ESMTP) 프로토콜을 지원하는 e-메일 서버들만이 이런 형태의 DSN을 지원하며, 이런 기능에 대한 지원은 ESMTP 서버들에게 선택적인 것이고, 서버의 관리자들에 의해 선택된 구조에 따른다는 것을 인지하여야 한다.

[0091] 비록, DSN이 ESMTP의 출현과 함께 사용될 수 있는 용어이지만, 하기에서, "DAN"을 ESMTP 프로토콜을 따르던 그렇지 않던 수신된 메시지의 상태에 관련한 소정의 MTA 생성 메시지를 지칭하기 위해 사용할 것이다.

[0092] MUA 통지들(판독 통지들)

[0093] 이들은 예로서, 메시지가 판독을 위해 열람된 것 또는 판독되지 않고 시스템으로부터 삭제된 것 같은 특정 사건들이 발생하였을 때, 수신인의 메일 사용자 에이전트(MUA)(e-메일 프로그램)에 의해 메시지의 작성자(명목상)에게 보내지는 e-메일들이다. 인터넷 협정(RFC 1891)에 의해, 어떠한 MUA 프로그램도 이런 통지들을 생성할 것을 강요받지 않는다. MUA가 이들 영수증들을 생성하는지 여부는 그 사용자에 의해 선택된 구조에 따른다.

[0094] RPost 서버(14)는 호환 MTA들 및 MUA들로부터 MTA DNS들 및 MUA 통지들 양자 모두를 유도하는 것을 시도하는 방식으로 메시지들을 형성 및 전송한다. 호환 MUA들로부터 판독 영수증을 유도하기 위해서, 특정 헤더들이 e-메일 메시지의 헤더부에 포함되어야만 한다. 서로 다른 MUA들은 서로 다른 헤더들에 응답하며, 그래서, 서버(14)는 다양한 MUA들에 의해 인식되는 형태로 판독 통지를 요청하는 각 메시지에 다수의 서로 다른 헤더들을 추가한다. 이들 헤더들은 모두 하기의 형태를 취한다.

[0095] 헤더 라벨 : 사용자명 <사용자 어드레스>

[0096] 예로서 :

[0097] 처분-통지:John smith<jsmith@adomain.com>에게

[0098] 판독-통지:John smith<jsmith@adomain.com>에게

[0099] 여기서, "John smith"는 MUA 통지가 보내지게 되는 사용자의 이름이며, <jsmith@adomain.com>은 그 사용자의 인터넷 어드레스이다. 통상적으로, 이런 헤더들은 그 메시지의 작성자를 지칭하지만, 본 방법의 경우에는 통지가 RPost에 의해 처리될 수 있도록 이 통지가 RPost에게 반환되어야할 필요가 있다. 이렇게 되는 것을 보증하기 위해서, 서버(14)는 MUA 영수증들을 그들이 RPost 서버에 의해 처리될 수 있는 어드레스, 예로서, "readreceipt@RPost.com"으로 보내질 것을 요청하는 헤더들을 삽입한다. 이는 소정의 호환 수신 MUA들이 그 통지들을 처리를 위해 RPost 어드레스로 보내도록 지시한다.

[0100] 반환된 MUA 통지들을 처리하는 임무는 이 단계에서 다루어져야만 하는 상이한 문제점을 유발한다. MUA 통지들의 포맷 및 내용을 통제하는 표준들은 존재하지 않는다. 이들은 그들이 보고하는 사건(예로서, "판독을 위한 열람")의 시기와 원본 메시지의 제목을 인용하는 경우가 많다. 그러나, 이 정보가 통지내에 포함되어 있는 경우에도, 그 메시지의 작성자를 식별하거나, 이를 촉발시키는 메시지를 고유하게 식별하기에 불충분하다. 시스템이 MUA 통지를 수신하였을 때, RPost가 송신인을 위해 생성한 영수증에 이 통지 정보를 포함시키도록 그것을 촉발시킨 메시지를 식별할 수 있어야만 한다. 대안적으로, 통지 정보가 RPost 판독 영수증(하기 참조)의 형태로 송신인에게 전달되도록 시스템은 적어도 MUA 통지가 지칭하는 메시지의 송신인을 신뢰성있게 식별할 수 있어야만 한다.

[0101] 후자의 목적을 달성하기 위해서, 시스템은 인터넷 어드레스들이 두 성분들 : 이름 필드와 어드레스 필드를 가지며, 여기서 어드레스 필드는 꺽쇠 괄호들 "<>"로 묶여져 있다는 사실을 이용할 수 있다. 대부분의 MUA들은 그 MUA 통지들의 착신지 어드레스에 양자 모두의 필드들을 포함한다. MUA 영수증들을 위한 그 요청들을 작성시, RPost 시스템은 서버(14) 판독 영수증-취급 어드레스를 통지를 위한 어드레스로서 포함하지만, 헤더의 이름 필

드내의 원본 송신인의 어드레스를 사용한다. 예로서, 메시지의 원본 송신인은 인터넷 어드레스 jsmith@adomain.com을 가지는 사용자 존 스미스인 경우에, RPost 서버는 하기의 형태의 헤더들을 포함한다.

[0102] 처분-통지: jsmith@adomain.com<readreceipts@RPost.com>에게

[0103] 이는 jsmith@adomin.com<readreceipts@RPost.com>으로 어드레스를 기재하여, readreceipts@RPost.com으로 호환 MUA 송신 통지가 이루어지게 한다.

[0104] 이 어드레스 "readreceipts@RPost.com"에서 이런 통지를 수신시, 서버는 통지의 내용의 검사에 의해 결정할 수는 없지만, 수신인의 필드를 해석함으로써, 통지가 원래 jsmith@adomain.com에 의해 송신된 메시지에 관련한 것이라는 것을 판정한다. 이 정보를 가지고, 서버는 그후 디지털적으로 서명된 RPost 판독 영수증 내에 이 통지의 내용들을 집어넣고 이 영수증을 어드레스 jsmith@adomain.com으로 송신한다.

[0105] 또한, RPost 시스템은 수신 MTA들에 의해 생성된 MTA DSN 통지들을 유도 및 수집하기 위해 노력한다. 이런 통지들이 항상 메시지 헤더의 "FROM :" 필드내에 기재된 어드레스로 보내지기 때문에, 서버(14)는 그 메시지가 수신될 수 있도록 각 메시지 헤드를 DSN들이 처리되는 RPost 어드레스를 "FROM:"으로서 변경한다.

[0106] 그러나, DSN들의 처리의 문제점은 다른 논점을 유발하며, 이는 본 단계에서 반드시 다루어져야만 한다. DSN들은 소정의 표준 내용 또는 포맷을 가지고 있지 않으며, 단지 이들 e-메일들의 내용들을 검사함으로써 어떤 메시지의 내용이 그 통지를 제공한 것인지를 판정하는 것이 불가능한 경우가 빈번하다. 이 문제점은 DSN 인벨로프 식별 번호들(RFC 1869 참조)의 사용에 의해 ESMTP 프로토콜에 따라 생성된 DSN들에 대하여 부여되는 것으로 생각된다. 이 프로토콜에 따라서, 이 번호는 소정의 반환 DSN에서 응용되어 송신인이 DSN의 제목 메시지를 식별할 수 있게 한다. 그러나, 사실상, 그 자신들을 지원 ESMTP DSN으로 보고하는 다수의 MTA들은 DSN 인벨로프 식별이나 그 제목 메시지를 신뢰성 있게 식별하기에 충분한 소정의 다른 정보를 반환하지 않는다. 마지막으로, DSN이 통지를 제공하게 만든 메시지를 식별하기에 충분한 정보를 반환하는 경우에도, 그 통지를 촉발시킨 메시지의 특정 수신인을 식별하기에 충분한 정보를 포함하지 않는 경우가 많다. 따라서, 하나의 도메인에서 단일 메시지가 두 수신인들에게 보내질 수 있고, 하나는 수신인의 우편함에 성공적으로 전달될 수 있고, 나머지는 그렇지 않을 수 있다. 그 도메인을 위한 MTA는 DSN의 수신인에 대하여 어떤 수신인이 성공적으로 전달되었고, 어떤 수신인이 그렇지 못한지를 판정할 수 있게 하기 위한 어떠한 수단도 제공하지 않는 방식(예로서, DSN이 원본 메시지에 포함된 어드레스들이 아닌 그 별칭들로서 수신인의 어드레스를 보고하는 경우에 발생할 수 있는 바와 같이)으로 DSN내에서 이들 이벤트들을 보고할 수 있다.

[0107] 본 발명은 네 단계들에서 이 문제점을 해결한다.

[0108] 1) 각 유출 메시지를 위해 고유 식별 번호가 생성되게 한다(예로서, 시간 소인에 기초하여). 이 번호는 데이터베이스내에 저장된다.

[0109] 2) 각 메시지의 수신인들이 하나하나 세어지고, 식별 번호들이 데이터베이스내에 저장된다.

[0110] 3) 메시지는 각 의도된 수신인의 MTA에 개별적으로 송신된다(두 수신인들이 공통 도메인 명 및 MTA를 가지고 있는 경우에도, 서버(14)는 이 메시지를 두 개의 별개의 SMTP 텔레넷 세션들(telenet sessions))에서 그 MTA에게 전송한다).

[0111] 4) 서버(14)가 그 메시지를 수신인의 MTA에 전송할 때, 이는 그 메시지가 송신인의 식별 번호와 메시지의 고유 식별를 통합하는 어드레스로부터 송신된 것으로 보여지도록 그 메시지의 "FROM" 필드를 확대시킨다. 또한, 이 어드레스는 서버가 반환 메시지들을 DSN들로서 식별할 수 있게 하는 서브스트링(예로서, "rcpt")도 포함한다.

[0112] 따라서, John Smith라는 이름의 송신인으로부터 서버(14)에 의해 "mmyyddss"라 명명된 단일 메시지가 그 제 1 의도된 수신인(시스템에 의해 "a"라 명명되는)에게 하기와 같은 헤더로 송신될 수 있다.

[0113] From : John Smith <rcptmmddyyssa@RPost.com>

[0114] 동일 메시지는 제 2 수신인에게 하기와 같은 헤더로 송신될 수 있다.

[0115] From : John Smith <rcptmmddyyssb@RPost.com>

[0116] 다수의 e-메일 MUA들은 메시지의 송신인의 이름만을 표시하며, 따라서, 특정 어드레스는 대부분의 수신인들에게 보여지지 않는다.

[0117] 이 형태의 어드레스부여의 결과는 수신 MTA들이 DSN들을 발행할 때(ESMTP를 따르던 그렇지 않던), 이들은 이들

DSN들을 상이한 RPost 수신인들에게 보내게 된다. 이들 DSN들을 수신하였을 때, 서버(14)는 이들을 그 "RCPT" 접두사에 의해 DSN 메시지들로서 식별할 수 있고, 수신인들을 해석함으로써, 어떤 메시지와 어떤 수신인이 DSN의 제목인지를 판정할 수 있다.

[0118] 서버(14)는 각 메시지의 "FROM" 필드를 그것이 그 메시지를 그 수신인의 MTA에 전송하기를 시도할 때마다 변경한다.

[0119] 수신인이 전송된 메시지들에 답신하는 것을 보증하는 것은 시스템(14)이 명시적인 "reply-to:" 메시지 헤더를 원 송신인의 이름과 인터넷 어드레스가 기재되어 있는 메시지내에 추가함으로써 적절히 달성된다. 본 실시예의 경우에, 이는 하기와 같을 수 있다.

[0120] Reply-to : john smith <jsmith@adomain.com>

[0121] 이는 수신 MUA들이 구축된 RPost 어드레스가 아닌 실제 송신인의 어드레스로 수신된 메시지에 대한 답신들을 보내게 한다.

[0122] I.2 전송

[0123] 상술한 바와 같이, RPost 서버가 그 메시지의 각 수신인에게 별개의 유출 메시지의 카피를 전송하는 것은 본 방법의 일부이다. 또한, RPost는 각 착신지를 위한 기록의 메일 교환기(MX)를 사용한 직접 SMTP 접속을 통해 이런 전달 각각을 수행하기를 시도한다.

[0124] 주의: 각 유효 인터넷 e-메일 어드레스는 인터넷 도메인명 또는 IP 어드레스를 포함한다. 각 도메인 명/어드레스는 그 도메인내의 어드레스들을 위한 메일을 수신하도록 허가된 e-메일 서버(들)를 이와 연계시킨다. 소정 도메인들은 하나 이상의 서버를 가진다. 각 도메인을 책임지는 도메인명 서버는 인터넷을 거쳐 그 메일 서버들의 신분을 방송한다. 이 정보는 공개적으로 입수할 수 있으며, 인터넷 e-메일 및 도메인명 서비스를 통제하는 규칙들 및 협약들을 따르는 방식으로 관리 및 전송된다.

[0125] 메시지의 카피를 소정의 착신지로 전송하기 이전에, RPost 서버는 착신지의 도메인과 관련된 MTA를 식별하기 위해 인터넷명 서버 참조를 수행한다. 착신지 어드레스의 메일 수신을 담당하는 식별된 MTA로, 시스템은 착신지의 로컬 MTA와의 텔레넷 접속을 개시할 것을 시도한다.

[0126] 그들이 최종 착신지에 도달할때까지 MTA로부터 MTA로 인터넷 e-메일이 중계되는 것은 통상적인 관습이다. RPost 서버와 착신지의 MTA 사이의 직접 접속을 필요로하는 주된 목적은 RPost 서버가 메시지의 전달을 기록(이 기록은 수신 도메인 명을 위한 e-메일을 수신하는 것을 담당하는 e-메일 서버와의 SMTP 대화의 형태를 취함)할 수 있도록 하는 것이다.

[0127] 이 기록의 존재는 등록된 메일 영수증이 전달의 증거를 제공하는 것과 동일한 방식으로, 이 메시지가 전달되었다는 유용한 증거를 제공한다. USPS 등기 메일은 수신인의 허가된 대리인(예로서, 서기, 또는 우편소 관리자)에 전달되었다는 것을 증명할 수 있는 경우에, 확실히 전달된 것으로 취급된다. RPost 전달 영수증의 증거 구성 장점에 대한 소정의 법적 도전이 있는 경우에, 인터넷 e-메일 서비스 공급자를 선택시, 수신인이 그 공급자가 그 대신 전자 메시지들을 수집하는 것을 허가하였다는 것이 인정될 수 있다. 순차적으로, 그 서비스 공급자는 이 도메인을 위한 수신 e-메일 서버들로서 그 MTA들의 어드레스를 방송함으로써, 그 도메인명을 위한 e-메일 수신인들을 위한 허가된 대리인으로서 인정된 그 지위를 가진다.

[0128] 따라서, 수신인의 e-메일을 수신하는 것을 담당하는 메일 서버에 직접적으로 메시지를 전달함으로써, RPost는 수신인이 그의 메일을 수신하도록 법적으로 허가한 대리인에게 그 메시지를 전달한다. 전달 트랜잭션을 기록함으로써(이 트랜잭션은 SMTP 대화의 형태를 취함), RPost는 수신인의 허가 대리인에게로의 전달의 증거를 가지는 것을 주장할 수 있다.

[0129] 여기에 기술된 방법이 각 착신지로의 전달의 증거의 다른 형태들을 수집하기를 시도하지만, 이들 시도들이 성공하는지 여부는 RPost의 제어가 아닌 요인(예로서, 수신인의 메일 서버상에 채용된 SMTP 지원의 형태)들에 의존한다는 것을 인지하여야 한다. 한편, 모든 성공적 전달은 수신인의 메일 서버가 항상 SMTP 기록을 생성할 것을 지휘한다. 이 기록을 기록하는 것은 RPost가 인터넷 메일을 위한 최소 프로토콜들(SMTP)에 따른 소정의 유효 인터넷 착신지에 대한 전달의 증명을 제공할 수 있게 한다. 이는 ESMTP DSN에 의존함으로써 전달을 증명하기를 시도할 수 있는 상이한 방법들 보다 우월한 본 방법의 중요한 장점이다.

[0130] 메시지의 착신지를 위한 MTA를 식별함으로써, RPost 서버는 RFC 1869에 준한 "EHLO" 핸드쉐이크를 발행하여 착

신지 MTA와 ESMTP 접속을 개시하기를 시도한다. SEVER(16)가 ESMTP를 지원하는 경우에, 이는 그것이 지원하는 ESMTP 서비스들을 나열하므로써 응답하게 된다.

[0131] SEVER(16)가 ESMTP를 지원하는 경우에, RPost 서버는 가장 먼저 SEVER(16)가 ESMTP 서비스 "검증(VERIFY)"을 지원하는지를 판정한다. 검증(verify) 서비스는 소출 SMTP 서버가 무엇보다도 MTA의 도메인내의 어드레스가 진짜인지 여부를 판정할 수 있게 한다. RPost 서버가 이들 수단에 의해, 그 메시지를 전달하고자하는 어드레스가 유효하지 않다는 것을 판정하게 되는 경우에, 이는 접속을 종결하고, 메시지를 이 수신인에게 전달하려는 시도를 중단하며, 그 데이터 베이스에, 이 메시지 착신지의 상태를 전달 불가(UNDELIVERABLE)로 기록한다.

[0132] 그 결과가 어떻든, RPost 서버는 ESMTP VERIFY 대화를 파일에 기록하며, 이를 저장하여, 이것이 추후 이 메시지를 위한 전달 영수증에 첨부 또는 포함될 수 있게 한다. 보안 관련 분야 이외에는, 소수의 ESMPT 서버들이 VERIFY 기능을 지원한다는 것을 인지하여야 한다.

[0133] 시스템(16)이 VERIFY 방법을 지원하지 않는 경우에, 그럼에도 불구하고, RPost 서버는 메시지를 시스템(16)에 전달하는 것을 시도한다. 통상적으로, MTA는 그 도메인내의 명목적 소정의 어드레스를 위한 메시지들을 수신하고, 이 어드레스가 유효하지 않을 경우에는, 추후 DSN을 송신한다.

[0134] RPost 서버는 이때 착신 서버가 ESTM 서비스 DSN을 지원하는지 여부를 판정하기를 시도한다. 그렇다면, RPost는 이 메시지를 SERVER(16)가 수신인에 대한 전달이 성공 또는 실패한 경우에 ESMTP DSN과 함께 메시지의 송신인에게 통지하는 것에 대한 요청과 함께 이 메시지를 전송한다. 이 착신지에 대한 메시지의 성공적 전송 이후에, 시스템은 이 착신지의 전달 상태를 전달 완료 및 DSN 대기(DELIVERED-WAITING-FOR-DSN)로 기록한다.

[0135] 서버(16)가 ESMTP를 지원하지 않는다는 것을 나타내는 방식인 "EHLO" 핸드쉐이크로 답신하는 경우에, RPost 서버는 SMTP 접속을 개시하기 위해 "HELO" 메시지를 발행한다. 이 접속이 달성되는 경우에, RPost 서버는 이 메시지를 SMTP 프로토콜에 준하여 전송하며, 착신지의 전달 상태를 전달 완료(DELIVERED)로 기록한다.

[0136] 접속이 SMTP이든, ESMTP이든, RPost서버는 두 서버들 사이의 전체 프로토콜 대화를 기록한다. 통상적으로 이 대화는 무엇보다도, 착신지 서버가 그자신을 식별하고, 지정된 영수증을 위한 메시지의 업로드에 대한 허가를 승인하고, 메시지가 수신되었음을 수신통지한 것을 포함한다. RPost는 이 메시지를 위한 RPost 전달 영수증에 포함 또는 첨부되어 추후 검색되는 방식으로 이 트랜잭션의 기록을 저장한다.

[0137] 다양한 사유들 때문에, RPost는 수신인의 MTA와 SMTP 접속을 달성하지 못할 수 있거나, 이런 접속을 달성하지만, 수신인에 의해 이 메시지를 전송하는 것이 불허될 수 있다. 이 경우에, 인터넷 DNS 참조(lookup)가 착신지 어드레스가 다수의 MTA를 갖고 있는 것을 알아내는 경우에, RPost 서버는 그 메시지를 순차적으로 이들 각각에게 전달하는 것을 시도한다. RPost는 시스템 리소스들이 허용하는 한 빈번히 적절한 MTA로의 전달을 시도한다. 소정 길이의 시간 이후에, RPost가 어드레스로 이 메시지를 전달할 수 없는 경우에, 이는 이 메시지의 이 수신인의 상태를 전달 불가(UNDELIVERABLE)"로 표시하고, 이 메시지를 이 착신지 어드레스로 송신하는 시도를 중단한다.

[0138] RPost 서버가 ESMTP DSN을 명백히 지원하는 착신지 서버에 대한 메시지 전송을 성공할 때, RPost는 이 메시지를 위한 이 수신인의 상태를 "전달 완료 및 DSN 대기(DELIVERED-AND-WAITING-FOR-DSN)"로 기록한다.

[0139] RPost 서버가 ESMTP DSN을 명백히 지원하지 않는 접속을 경유하여 착신지 서버에 대한 메시지 전송을 성공할 때, RPost는 이 메시지를 위한 이 수신인의 상태를 "전달 완료(DELIVERED)"로 기록한다.

[0140] I.3 후처리

[0141] DSN 처리

[0142] MTA DSN들은 그 소유 도메인(예로서, "RPost.com")내의 가상 어드레스들을 착신지로하여 RPost 서버로 반환되며, 이들 어드레스들은 상술한 바와 같이 구성되어 있다. RPost 서버는 이 도메인에 보내진 모든 유입 메일을 조사하여, 그 식별 서브스트링(예로서, "rcpt")에 의해 DSN 메시지들을 검출한다. 이들 어드레스들을 상술한 방식으로 해석함으로써, 시스템은 그 DSN 통지를 촉발시킨 메시지 및 수신인을 식별할 수 있다.

[0143] DSN 메시지들에 대해서는 어떠한 표준 포맷도 존재하지 않으며, 그들이 그 결과들을 보고하는 어떠한 표준 어휘집(lexicon)도 존재하지 않는다. 수신된 DSN을 평가하기 위해서, 시스템은 DSN의 의미를 표현하는 단어 및 어구들에 대하여 DSN 메시지들의 본문 및 제목 라인을 반드시 보아야만 한다. 예로서, "성공적 전달" 또는 "우편함으로의 전달 완료"나 "전달 완료" 같은 어구들은 통상적으로 그 DSN이 관련한 메시지가 착신지의 우편함에 투입

되었다는 것을 신호한다. 이런 어구들을 검출할 때, 시스템은 이 메시지의 이 착신지의 전달 상태를 "우편함으로 전달 완료(DELIVERED TO MAILBOX)"로 변경한다.

[0144] "전달 불가", "치명적 오류", "실패" 및 "비성공" 같은 어구들은 MTA에 의해 그 메시지를 착신지로 전달하는데 실패하였다는 것을 보고하는 DSN을 신호한다. DSN내에서 이들 같은 어구들을 검출할 때, 시스템은 그 수신인의 전달 상태의 기록을 "실패(FILED)"로 변경한다.

[0145] 착신지의 도메인을 위해 시스템이 항상 메일을 소유 MTA로 전달하지만, 이들 MTA들은 종종 상이한 서버에 메시지를 답신한다(예로서, 수신 MTA가 방화벽안에서 메일을 송신하는 경우 같은 경우가될 수 있음). 이 경우에, DSN은 "중계 완료" 또는 "전진방향 중계 완료" 같은 어구들을 포함한다. 이런 경우에, 시스템은 수신인의 전달 상태를 "중계 완료(RELAYED)"로 변경한다.

[0146] DSN의 평가 및 이에 따른 수신인의 전달 상태 갱신이 완료되면, 시스템은 DSN과, 소정의 첨부물들을 저장하고, 이 메시지(들)가 RPost 전달 영수증에 포함 및/또는 첨부될 수 있는 방식으로 보관할 수 있다.

[0147] 메시지 관리

[0148] 때때로, 시스템은 각 송신된 메시지를 조사하고, 시스템이 그 착신지의 전달을 완전히 처리하였는지를 판정하기 위해 그 메시지의 각 착신지의 상태를 검사한다. 완료의 기준들은 착신지의 전달 상태에 따른다.

[0149] 전달 완료 : 이 상태는 이 수신인을 위한 메시지의 카피가 ESMTP DSN을 지원하지 않는 MTA에 전달되었다는 것을 나타낸다. 이런 MTA는 그럼에도 불구하고 메시지가 수신인의 우편함에 전달될 수 없는 경우에 소정 형태의 전달 상태 통지를 보낸다(예로서, 착신지 어드레스가 도메인내의 유효 어카운트에 대응하지 않는 경우에 발생할 수 있음). 따라서, 시스템은 수신 MTA에 전달된 이후 소정 시간 기간이 경과될 때까지 이런 수신인을 위한 전달이 완료된 것으로 취급하지 않는다. 이 시간 주기-통상적으로 2 내지 24 시간-는 전달에 대한 실패의 통지를 반환하기 위해 서버들의 대부분을 위해 필요한 최대 시간의 추정치를 나타내고, 특정 착신지 도메인이 원격지이거나, 이런 통지들을 생성하는데 신속하거나 더딘 것으로 공지되어 있는 경우, 조절될 수 있다.

[0150] 중계 완료 : 이 상태는 수신 MTA가 이 메시지를 ESMTP DSN을 지원하지 않는 상이한 MTA에게 포워딩한 것을 나타내는 DSN이 수신되었다는 것을 표시한다. 이 경우에, 그럼에도 불구하고, 메시지가 전달된 MTA가 수행 과정중 전달 실패의 통지를 송신할 수 있다. 따라서, 이 상태를 가진 수신인들은 상태 "전달 완료"를 가지는 수신인들과 동일한 조건들하에서 완료된 것으로 처리된다.

[0151] 전달 완료 및 DSN 대기 : 이 상태는 수신인의 MTA가 ESMTP DSN을 지원하고, DSN이 의뢰되었지만, 아직 수신되지 않은 것을 나타낸다. 비록, MTA가 그 자체가 이 서비스를 지원하는 것으로 나타내지만, 그럼에도 불구하고, 성공적인 전달의 경우에도 DSN들을 제공하지 않는 경우가 종종 있다. 따라서, 시스템은 소정 시간 간격 이후에, 어떠한 DSN도 수신되지 않은 경우에도 이 상태를 가진 착신지에 대한 전달들을 완료된 것으로 간주한다. 이 간격-통상적으로, 6 내지 24 시간-은 호환 MTA가 DSN을 반환하는데 통상적으로 필요한 최대 시간의 추정치를 나타낸다.

[0152] 우편함으로의 전달 완료 : 이 상태는 이 수신인에 대하여 성공적 전달을 나타내는 DSN이 수신되고, 따라서, 이 착신지에 대한 메시지의 전달이 완료된 것을 나타낸다.

[0153] 실패, 전달 불가 : 이 상태를 가진 수신인들에 대한 전달들은 항상 완료된 것으로서 취급된다.

[0154] 시스템이 하나의 메시지의 모든 수신인들에 대한 전달이 완료된 것을 발견하였을 때, 시스템은 그 메시지를 위한 전달 영수증을 작성한다.

[0155] 전달 영수증들의 생성

[0156] 전달 영수증들은 등록된 메시지의 원 송신인에게 보내지는 e-메일이다. 이 영수증(20)은 하기의 것들을 포함할 수 있다.

[0157] 1. 관리 목적을 위한 식별자, 이 식별자는 송신인의 식별 및/또는 시스템에 의해 수신된 송신인의 메시지의 인터넷 메시지 식별의 값이거나, 그에 대한 레퍼런스를 포함할 수 있음;

[0158] 2. 영수증이 생성된 일자 및 시간;

[0159] 3. 그 의도된 수신인들의 e-메일 어드레스들을 포함한 원본 메시지의 인용된 본문;

[0160] 4. RPost 서버가 메시지를 수신한 일자 및 시간;

[0161] 5. 하기의 사항들을 기재하고 있는 각 착신지를 위한 표;

[0162] (ⅰ) 수신인의 MTA가 메시지를 수신한 시간 및/또는 시스템이 수신인의 MTA로부터 DSN 보고를 수신한 시간;

[0163] (ii) 그 착신지를 위한 메시지의 전달 상태, 전달 영수증에 인용된 전달 상태는 착신지의 전달 상태의 시스템 내부적 기록에 기초함, 이들은 하기와 같이 고쳐써질 수 있음.

[0164] - 그 상태가 실패 또는 전달 불가인 착신지들에 대한 전달들은 영수증에 "실패"로서 기록됨.

[0165] - 그 상태가 전달 완료 또는 전달 완료 및 DSN 대기인 착신지들에 대한 전달들은 "메일 서버로의 전달 완료"로 영수증에 기록됨.

[0166] - 그 상태가 우편함에 전달 완료인 수신인들에 대한 전달들은 "우편함에 대한 전달 완료"로서 영수증에 기록된다.

[0167] 이들 보고들의 목적은 시스템이 달성할 수 있는 전달의 검증 형태를 판독자에게 정확하게 알리는 것이다.

[0168] 6. 이들 첨부물들의 별개의 메시지 다이제스트들을 포함한 원본 첨부물들의 리스트;

[0169] 7. 원본 메시지에 대한 첨부물들의 카피들, 각 원본 첨부물은 영수증에 첨부물로서 첨부됨;

[0170] 8. 각 착신지에 대한 메시지의 전달에 수반된 모든 SMTP 대화들의 트랜스트립트들, 요약들 또는 개요들;

[0171] 9. 밝혀질 수 있는 메시지의 착신지 또는 전달의 세부 사항들 모두를 포함하는 모든 수신된 DSN 보고들의 첨부물 및 본문들을 위한 인용문들; 및

[0172] 10. DSN 보고들에 대한 첨부물로서 시스템에 반환된 소정의 파일들.

[0173] 영수증의 이들 별개의 구성요소들 모두는 상기 영수증내에 포함된 디지털 시그니쳐들 또는 그 소유의 메시지 다이제스트들을 가질 수 있다. 부가적으로, 영수증은 단일의 전체적으로 암호화된 메시지 다이제스트나, 영수증의 일부로서 연산 및 첨부된 디지털 시그니쳐를 포함할 수 있으며, 따라서, 영수증내에 포함된 모든 정보를 증명하기 위해 사용될 수 있는 단일 메시지 인증 코드를 제공할 수 있다. 이 영수증 그자체와 영수증내의 SMTP 대화들 및 DSN 보고들이 시간소인들을 포함할 수 있기 때문에, 영수증은 메시지 수신인(들), 메시지 내용 및 전달 시간(들) 및 경로(들)의 위조불가한 기록을 포함한다.

[0174] MUA 통지 처리

[0175] MUA 통지들은 MTA DSN들과 동일한 방식으로 수집되어 RPost 전달 영수증들내에 포함될 수 있다. 그러나, MTA 통지들은 통상적으로 전달의 몇시간 이내에 MTA들을 수신함으로써 발행되지만, MUA 통지들은 수신인이 그 MUA e-메일 클라이언트를 열고, 수신된 메일에 관한 소정의 작용을 취할 때까지 형성되지 않는다. 이 때문에, 본 발명의 본 실시예에서, MUA 통지들은 MTA 통지들과는 별개로 수집되며, RPost 전달 영수증들과는 별개인 "RPost 판독 영수증"내에 보고된다.

[0176] 상술한 방식으로 구성된 메시지 헤더들에 의해 유도되는 MUA 통지들은 공통 RPost 어드레스(예로서, "readreceipts@RPost.com")로 반환되고, 각 통지는 이 메시지의 원 송신인의 어드레스를 -그 어드레스의 이름 필드에-포함한다. 이는 단지 후술된 방식으로 RPost 판독 영수증에만 필요한 정보이기 때문에, 시스템은 그 데이터뱅크들내에 원본 메시지에 대한 소정의 정보를 저장할 필요 없이 이 통지들이 도달할 수 있을 때 마다 MUS 통지들을 다룰 수 있다.

[0177] MUA 통지들은 무엇보다도, 그 메시지가 수신인에 의해 판독되었다는 것, 메시지가 수신인의 단말상에 디스플레이 되었다는 것(읽던 읽지 않던), 메시지가 열람되지 않고 삭제되었다는 것을 보고할 수 있다. MUA 메시지들의 내용 또는 포맷을 위한 어떠한 프로토콜 통제 표준도 존재하지 않는다. 시스템은 MTA DSN들을 위해 시스템이 사용한 것과 동일한 형태로 그 보고들을 해석하기 위해 MUA들의 텍스트를 검사하도록 구성될 수 있다. 그러나, 본 발명의 본 실시예에서, MUA들은 RPost 서버에 의해 평가 또는 해석되지 않고, 대신, RPost에 의해 인증될 수 있는 형태로 그 자체의 평가를 위해 송신인에게 전달된다. 이를 달성하기 위해서, 시스템은 하기의 것들을 포함할 수 있는 "RPost 판독 통지"로서 꾸며진 e-메일 메시지를 생성한다.

[0178] 1. 수신된 MUA 통지의 제목 라인;

[0179] 2. 판독 통지의 본문으로서 인용된 수신된 MUA 통지의 본문;

[0180] 3. 첨부물로서 포함된 수신된 MUA 통지;

[0181] 4. 첨부물(들)로서 포함된 수신된 MUA에 대한 소정의 첨부물(들);

[0182] 5. 수신된 MUA 통지와, 그 통지에 대한 소정의 첨부물(들)의 다이제스트;

[0183] 6. 일자 및 시간 소인;

[0184] 7. 문서와, 그 내용들 모두를 위한 인증가능한 일자 소인날인 디지털 시그니쳐를 제공하는 적어도 5번 및 6번 항목의 암호화된 해시.

[0185] 영수증 처분

[0186] 본 발명의 본 실시예의 경우에, RPost 전달 영수증들 및 판독 통지들 양자 모두는 동록된 메시지의 원 송신인에게 보내진다. 이들 영수증들이 암호화된 해시로 디지털적으로 서명되어 있기 때문에, RPost는 후술된 방식으로 소정의 시기에 이들이 인증을 목적으로 RPost에 제출되면, 이들 메시지들내에 포함된 정보를 인증할 수 있다. 이는 그 송신인에게 영수증의 카피가 전송되고 나면(송신인이 그 기록을 위해 영수증을 보관하여야 한다는 지령과 함께), RPost는 더 이상 이 메시지 또는 그 전달에 관련한 소정의 데이터를 보유할 필요가 없으며, 그 시스템으로부터 모든 이런 기록들을 삭제할 수 있다. 따라서, RPost는 원본 메시지 또는 영수증의 어떠한 카피도 유지할 필요가 없다. 이 기록 메모리의 경제성은 서비스 공급자측에서 다량의 데이터 저장소를 필요로 하는 다양한 종래의 메시지 인증 시스템들 보다 우월한 장점을 본 발명에 제공한다.

[0187] 이 경우에, 영수증 데이터를 보관하는 부담이 메시지의 원 송신인에게 부과된다. 대안적으로, 또는 부가적으로, 제 3 자 검증자 RPost는 부가적인 요금을 받고, 일부 또는 모든 영수증 데이터 또는 영수증의 영구적인 카피를 저장할 수 있다. 그 영수증 또는 부분(들)은 자기 테이프, CD ROM 또는 상이한 저장 장치 형태들을 포함하는 소정의 적합한 기록 저장 장치들상에 유지될 수 있다. 부가적으로, 또는 대안적으로, 송신인 또는 송신인의 조직의 제어내에서, 이 목적을 위해 생성된 저장 시스템에 RPost는 영수증들 또는 그 일부를 반환할 수 있다.

[0188] 상술한 바와 같이, RPost 영수증 정보는 원 송신인의 메시지와 그 첨부물들로부터의 모든 데이터를 포함한다. 시스템의 사용자들이 그들의 기록들내에 영수증들을 보관하는 부담을 받게되는 것을 원하지 않는 경우들이 있지만(예로서, 비의도적 데이터 손실의 걱정으로부터 벗어나기 위해), 또한, RPost 제 3자의 손에 그들의 메시지의 내용을 남기지 않기를 원할 수도 있다. 따라서, RPost는 메시지들의 내용들을 버릴 수 있지만, 송신인에 의해 보관된 메시지의 카피를 제출하였을 때, 메시지의 전달을 인증 및 검증하기 위해 RPost에 필요한, 이런 정보(예로서, 송신인, 작성일, 메시지 다이제스트들, 착신지들 및 전달 상태들)만을 그 데이터베이스내에 저장한다.

[0189] 검증

[0190] 후일, 메시지의 발신자가 e-메일이 송신, 전달 및/또는 판독되었다는 증거를 필요로하는 경우에, 발신자는 메시지를 위한 영수증(들)을 시스템의 관리자에게 제출한다.

[0191] 예로서, 특정 메시지가 송신인(10)으로부터 수신인(18)에게 송신되었다는 것을 증명하기 위해서, 송신인(10)은 영수증내에 포함된 정보를 검증해달라는 요청과 함께 영수증의 카피(20)를 RPost에 보낸다. 이는 RPost에 있는 사전규정된 우편함, 예로서, verify@RPost.com으로 이 영수증을 보냄으로써 이루어지게 된다. 그후, RPost는 이 영수증이 유효 영수증인지 여부를 판정한다. 디지털 시그니쳐가 영수증의 나머지와 일치하고, 메시지 다이제스트들이 원본 메시지의 각 대응 부분들에 일치하는 경우에, 영수증은 유효 영수증이다. 특히, RPost는 메시지 본문을 포함하는 메시지의 다양한 부분들, 첨부물 및 SMTP 대화와 DSN 보고들을 포함하는 전체 메시지상에 해시 평션을 수행하여 요지 메시지 카피에 대응하는 하나 이상의 다이제스트들을 생성한다. RPost는 전체 메시지 다이제스트를 포함하는 요지 카피내의 메시지 다이제스트들을 RPost가 요지 메시지 카피로부터 연산하였던 메시지 다이제스트들과 비교한다. 요지 영수증내의 디지털 시그니쳐로서 수신된 전체 메시지 다이제스트를 해독함으로써, 또는, 요지 메시지 카피로부터 산출된 전체 메시지 다이제스트를 암호화함으로써, 전체 메시지 다이제스트가 비교될 수 있다. 디지털 시그니쳐를 포함하는 메시지 다이제스트들이 일치하는 경우에, 이때, 이 영수증은 진정한 RPost 생성 영수증이다. 양호한 해시 펑션이 사용되고, 암호작성 해시 펑션 및 디지털 시그니쳐 암호화 알고리즘에 사용된 키들이 타인들에게 누설되지 않은 것으로 가정하면, 이 영수증이 이 영수증을 제출한 사람에 의해 "위조"되는 것은 실질적으로 불가능하다. 즉, 이 영수증은 RPost에 의해 생성된 영수증이어야만 하며, 따라서, 영수증내에 포함된 메시지, 발신/수신 정보, 전달일자 및 시간, 성공적 전달 사실, 메시지가 운반된 경로 및 영수증내에 포함된 소정의 DSN 정보는 그 정보의 진정한 카피이며 정확하여야만 한다. 이때, RPost는 영수증

내에 포함된 정보에 대한 인증, 검증 및 확인을 제공할 수 있다. 이 확인은 e-메일 확인, RPost에 의해 사용된 방법에 친숙한 RPost 고용인들로부터의 선언 증언, 조서 및 법정에서의 현장 증언 및 다른 형태의 증언의 형태를 취할 수 있다. RPost는 송신인(10), 수신인(18) 또는 소정의 다른 엔티티에게 다양한 각 확인 서비스들에 대하여 과금한다. 또한, RPost는 요지 영수증의 불확실함에 관하여 증언 또는 상이한 확인을 제공할 수도 있다. 증언은 증거에 관한 주법에 대항하는 연방 증거 규정들 901(9), 901(10), 803(6), 803(7), 1001-1004, 1006, 702 - 706 및 다른 적용가능한 규정들에 따라 제공될 수 있다.

[0192] 요약하면, 본 시스템은 특정 내용을 가진 특정 메시지가 보내진 사실, 송신 시기, 송신인, 수신인, 판독을 위한 열람 시기, 및 삭제 시기에 대한, 이해관계가 없는 제 3자의 증언에 기초한 신뢰성있는 증거를 제공한다. 이 증거는 예로서, 계약 체결시, 주식 매수 또는 매도 주문시, 및 소정의 다른 응용분야들에서, 메시지들의 전달 및 내용에 관한 분쟁 발발시 언제든 제공될 수 있다. 시스템의 운영자들은 영수증내에 포함된 정보의 카피 또는 소정의 기록을 보존하기 위한 운영자들을 필요로하지 않고, 영수증 그 자체에 포함된 정보의 정확도에 대하여 확신할 수 있다.

[0193] 본 시스템의 현저한 장점은 어떠한 변경도 필요 없이, 현존하는 MUA들에 의해 사용될 수 있다는 것이다. 모든 연산, 암호화, ESMTP 인터로게이션 및 대화, DSN 보고 수집 및 영수증 편집이 제 3 자 RPost 서버에 의해서 수행되며, 이들 기능들 중 어떠한 것도, 소정의 사용자의 장비내에서 실행되지 않는다. 따라서, 사용자는 쉽고 신속한 시스템의 장점을 취할 수 있다.

[0194] 상술한 본 발명의 실시예에서, RPost 서버는 그를 통과한 모든 메시지들의 전달을 등록한다. 대안적으로, RPost 서버는 특정 착신지들(예로서, 조직 외부)을 가지는 메시지들 또는 특정 송신인들(예로서, 고객 관련 그룹)로부터의 메시지들만을 저장할 수 있다. 대안적으로, 또는 부가적으로, RPost 서버는 메시지의 본문 또는 제목내의 구별되는 문자들 또는 스트링들을 가지는 메시지들만을 등록할 수 있다. 예로서, 서버는 메시지의 제목에 "(R)"이 포함된 송신인의 메시지들만을 등록할 수 있다. 모든 다른 메시지들은 RPost 서버에 의해 전달되거나, 통상적인 인터넷 MTA로서의 소정의 다른 서버 기능을 사용하여 전달될 수 있다.

[0195] 본 실시예에서, RPost는 다양한 방식들로 수입을 증가시킬 수 있다. 예로서, RPost는 메시지 송신인(10) 또는 그녀의 조직에 메시지당 기반, 킬로바이트당 기반, 월납 같은 주기성 기반 균일 요금 또는 이들의 조합으로 과금할 수 있다. 또한, RPost는 검증이 단순 반환 e-메일인지, 작성된 선언서 또는 진술서인지, 법정 또는 조서의 맹세 사실 증언인지, 또는 법정 또는 조서의 맹세 전문가 증언인지 여부에 따른 과금 스케쥴로 영수증 인증 또는 검증에 대하여 과금할 수 있다. 사용자가 RPost가 그 영수증들의 카피들을 보관할 것을 선택하는 경우에, RPost는 항목당 및/또는 킬로바이트당 월납 단위 저장 요금들을 과금할 수 있다.

[0196] Ⅱ. 유출 메시지를 등록하기 위한 흐름도.

[0197] 도 2A 내지 도 2G는 본 시스템의 제 1 실시예의 예시적 동작을 도시하는 흐름도를 구성한다. 이 흐름도를 다른 실시예들에 적용되도록 변형하는 것은 소프트웨어 및 e-메일 프로토콜들과 친숙한 숙련자들의 기술이내에서 가능하다.

[0198] 도 3A의 전처리는 등록 서버(시스템)에 의해 전송되기 이전에 메시지에 취해지는 단계들을 예시한다.

[0199] e-메일 메시지를 등록하기 위해서, 단계 201에서, 발신자/송신인/사용자는 소정의 인터넷 메일 사용자 에이전트(MUA)를 사용하여 e-메일 메시지를 생성한다. 가능한 MUA들은 (1) 클라이언트측 e-메일 프로그램들; (2) 서버 기반 e-메일 프로그램들; (3) 웹 기반 e-메일 프로그램들; 및 (4) 웹 페이지들을 통해 제출된 HTML 폼들을 포함한다. 메시지는 본 명세서에서 참조하고 있는 RFC(Requests for Comments) 822, 2046 및 2047에 기술되어 있는 바와 같은 첨부 파일들을 포함할 수 있다. RFC들은 컴퓨터 통신의 다수의 특징들을 설명하고 있는 인터넷에 관한 일련의 기록들이며, 네트워킹 프로토콜, 프로시져들, 프로그램들 및 개념들을 중점적으로 다루고 있다.

[0200] 본 실시예에서, 본 시스템은 송신인의 유출 메일 서버로서 기능하며, 따라서, 송신인의 메시지가 송진자의 MUA에 의해 RPost 서버로 직접적으로 전달된다(단계 202).

[0201] 단계 203에서, 시스템은 추후 처리를 위해 저장될 원본 메시지의 카피를 생성한다.

[0202] 단계 204에서, 시스템은 메시지가 서버에 의해 수신된 시간, 메시지의 파일 첨부물(들)의 이름들 및 크기(들), 메시지의 각 착신지의 이름(알려져 있을 경우), 각 착신지의 인터넷 어드레스, 메시지가 착신지의 MTA에 전달된 시간(초기에 이 값은 눌이다) 및 각 착신지의 전달 상태(Delivery Status)를 기록하는 단위 같은 정보를 포함할 수 있는 데이터 베이스내의 기록을 생성한다.

[0203] 단계 205에서, 각 착신지의 전달 상태는 "미송신"으로 설정된다.

[0204] 단계 206에서, 시스템은 메시지 본문으로부터 형성된 디지털 핑거프린트 또는 메시지 다이제스트를 생성 및 저장한다.

[0205] 단계 207에서, 시스템은 메시지내에 포함된 각 첨부물을 위한 해시 또는 메시지 다이제스트를 생성한다.

[0206] 단계 208에서, 시스템은 원본 메시지의 변형된 카피를 생성할 수 있다. 이 제 2 카피(단계 209)에서, 메시지의 원본 제목 라인은 이 카피가 등록되었다는 것을 나타내도록 고쳐질 수 있다(예로서, "등록완료"를 앞에 붙임으로써).

[0207] 단계 210에서, 메시지가 시스템의 월드 와이드 웹 사이트에 대한 링크와 함께 시스템에 의해 등록되었다는 통지가 메시지의 본문에 첨부될 수 있다.

[0208] 단계 211에서, e-메일 헤더들은 다양한 MUA들에 의해 인식되는 다양한 헤더 포맷들로 요청 판독 통지가 추가될 수 있다. 농지를 위한 요청들은 시스템과 관련된 어드레스, 예로서, "readrecipt@RPost.com"으로 반환 통지를 향하게 한다. 또한, 이들 헤더들은 MUA 통지가 송신되어야만 하는 어드레스의 이름 필드에 메시지의 원 송신인의 어드레스를 포함할 수도 있다.

[0209] 전처리가 완료된 이후에, 시스템은 메시지의 카피를 도 2B에 예시된 바와 같이 그 착신지들 각각으로 전송한다.

[0210] 도 2B는 등록된 메시지의 전송에 필요한 단계들을 예시한다. 단계 220이 나타내는 바와 같이, 프로세스는 메시지의 각 수신인에 대해 별개의 전송을 필요로한다.

[0211] 단계 221에서, 시스템은 메시지의 그 가공 카피의 헤더 필드를 그 송신인 이름은 메시지의 원 송신인이지만, 그 어드레스는 하기로부터 구성된 "RPost.com" 어드레스인 "FROM:" 이되는 것으로 보여지도록 변경한다.

[0212] a) 반환 MTA 통지들을 식별하기 위해 사용되는 스트링(예로서, "RCPT");

[0213] b) 송신된 메시지를 고유하게 식별하는 스트링;

[0214] c) 메시지의 이 카피가 보내지게되는 착신지를 고유하게 식별하는 태그.

[0215] 단계 222에서, 보내지게 되는 착신지의 도메인명을 사용하여, 시스템은 이 도메인의 어드레스들을 위한 메일 수집을 담당하는 MTA(들)의 어드레스를 착지 위해, 도메인 명 서버 메일 교환 참조를 수행한다.

[0216] 단계 223에서, 시스템은 착신지의 MTA에 대한 직접 텔레넷 접속을 형성하기를 시도한다. 접속이 실패하는 경우에, 시스템은 다시 접속을 형성하기를 시도한다. 이 착신지에 대하여 초과할 수 없는 최대수의 재시도들(227)이 시스템에 제공되며, 시스템은 착신지의 도메인(228)을 위하여 다른 MX 서버를 사용하여 접속 재형성을 시도할 수 있다.

[0217] 최대수의 재시도들 이후에, 시스템이 이 착신지에 대하여 MTA에 대해 접속할 수 없는 경우에, 시스템은 단계 226에서와 같이, 이 착신지의 전달 상태를 "전달 불가"로 기록하고, 이 착신지로의 이 메시지의 전달 시도를 중단한다.

[0218] 착신지의 MTA에 대한 접속시, 시스템은 MTA와의 그 (E)SMTP 대화의 기록을 형성하기 시작한다(225).

[0219] 단계 229에서, 시스템은 "EHLO" 서두를 발행함으로써, 확장 SMTP(ESMTP)가 착신지 MTA와 교환을 시작하기를 시도한다.

[0220] 착신지의 MTS가 ESMTP를 지원하는 경우에, 시스템은 그후 착신지 MTA가 SMTP 함수 VERIFY를 지원하는지를 결정한다(230). MTA가 VERIFY를 지원하는 경우에, 시스템은 착신지 어드레스가 도메인내의 유효 어드레스인지를 판정하는 것을 시도한다(231).

[0221] 그 어드레스가 유효하지 않은 경우에, 그후, 단계 232에서, 시스템은 이 착신지의 전달 상태를 "FAILURE"로 기록하고, 이 착신지로의 이 메시지의 전달 시도를 중단한다.

[0222] 어드레스가 유효한 경우, 또는 ESMTP 서버가 VERIFY를 지원하지 않는 경우에, 시스템은 그후, 수신 MTA가 ESMTP 서비스 DSN(Delivery Status Notification)를 지원하는지 여부를 판정한다(233).

[0223] MTA가 ESMTP DSN을 지원하지 않는 경우에, 시스템은 전달 성공 또는 실패의 메시지의 명목상 소인자에게로의 통지에 대한 ESMTP 요청들과 함께 메시지를 전송한다(234). 메시지가 전송되고 나면, 시스템은 이 착신지의 전달

상태를 "DELIVERED-AND-WAITING-FOR-DSN"으로 기록한다(235).

[0224] 수신 MTA가 확장 SMTP를 지원하지 않는 경우에, 시스템은 SMTP를 사용하여 메시지를 전송하고(236), 착신지의 상태를 "DELIVERED"로 기록한다(237).

[0225] 메시지가 전달되고 나면, 시스템은 그후, (E)SMTP 대화를 저장하고, 추후 복원되어, 이 메시지를 다른 착신지로 송신하기를 시도할 수 있는 방식으로 이 전달을 기록한다(238).

[0226] 그 착신지(들)에 메시지가 전송되고 나면, 시스템은 메시지의 처분에 관한 정보를 수집하기 위해서 몇가지 기능들을 수행하여야만 한다. 도 2C는 수신인 MTA들에 의해 반환된 MTA 통지들을 시스템이 처리하는 프로세스를 예시한다.

[0227] 단계 221에서 도 2B에 예시된 송신된 메시지들의 헤더들내에 사용된 포맷 때문에, MTA 메시지 통지들은 서버에서 가상 로컬 어드레스로 전달된다. 시스템은 그 어드레스들내에 이식된 스트링(예로서, "rcpt")에 의해 이들 통지들을 검출할 수 있다(241). 이 어드레스를 해석함으로써, 242에 예시된 바와 같이, 시스템은 어떤 메시지가, 그리고, 어떤 착신지에 대하여 수신된 통지를 촉발시켰는지를 판정한다.

[0228] 단계 243에서, 시스템은 제목 라인 및 수신된 MTA들의 본문을 조사하여 해석함으로써, MTA가 성공적 전달, 실패한 전달 또는 그 메시지가 다른 서버로 중계되었다는 사실 중 어떠한 것을 나타내는지를 조사한다.

[0229] 단계 243에서의 프로세스가 그 통지가 성공적 전달을 보고하는 것으로 밝혀낸 경우에, 시스템은 단계 245에 예시된 바와 같이, 관련 메시지의 관련 착신지의 전달 상태를 "DELIVERED-TO-MAILBOX"로 변경한다.

[0230] 시스템이 MTA 통지가 전달 실패를 보고하는 것으로 판정한 경우에, 시스템은 관련 메시지의 관련 착신지의 전달 상태를 "FAILURE"로 변경한다(247).

[0231] 시스템이 MTA 통지가 그 메시지가 다른 서버로 중계되었다는 것을 나타내는 것으로 판정한 경우에, 시스템은 단계 249에 예시된 바와 같이, 관련 메시지의 관련 착신지의 전달 상태를 "RELAYED"로 변경한다.

[0232] MTA 통지가 처리되고 나면, 시스템은 이 메시지와 그 모든 첨부물들을 이들이 추후 재소환되어 이 착신지를 위한 영수증을 구성하는데 사용될 수 있는 방식으로 저장한다(250).

[0233] 때때로, 도 2D에 예시된 바와 같이, 시스템은 메시지의 각 착신지에 대해 수신된 모든 MTA 통지들을 시스템이 복원하였는지 여부를 판정하기 위해 각 메시지의 상태를 검사하고, 이 메시지를 위한 영수증을 구축하기 시작할 수 있다.

[0234] 시스템은 메시지의 각 착신지의 전달 상태를 검사한다.

[0235] 소정의 착신지가 전달 상태 "UNSENT"을 가지는 경우에, 이때, 메시지의 처리는 료되지 않는다(252).

[0236] 착신지의 전달 상태가 "DELIVERED-AND-WAITING-FOR-DSN"인 경우에, 이때, 시스템은 단계 254에 예시된 바와 같이, 메시지의 전달 이후 시스템의 대기 기간(예로서, 24시간)이 경과하지 않았다면, 이 착신지를 위한 처리가 완료된 것으로 간주하지 않는다.

[0237] 착신지의 전달 상태가 "전달 완료"인 경우에(257), 이때, 시스템은 시스템의 운영자들이 착신지의 MTA로부터 전달 실패 통지가 수신되기에 충분한 것으로 취급하는 시간 기간(예로서, 2시간)이 경과한 경우에, 이 착신지의 처리를 완전히 제공된 것으로 간주한다(258).

[0238] 소정의 다른 착신지 전달 상태(예로서, "실패", "전달 불가", "우편함으로 전달")는 완전히 처리된 것으로 취급된다.

[0239] 소정의 메시지의 착신지들의 처리가 완료되지 않은 경우에, 시스템은 어떠한 작용도 취하지 않으며, 시스템내의 다른 메시지들로 이동할 것을 고려한다(단계 255).

[0240] 그러나, 단계 259에 예시된 바와 같이, 메시지의 모든 착신지의 처리가 완료된 경우에, 시스템은 메시지를 위한 전달 영수증을 생성한다.

[0241] 도 2E에 예로서 예시된 바와 같이, 이 영수증은 하기의 것들을 포함한다.

[0242] 블록 271에서와 같은 관리 목적을 위한 식별자, 이 식별자는 송신인의 식별 및/또는 시스템에 의해 수신된 송신인의 메시지의 인터넷 메시지 식별의 값이거나, 그에 대한 레퍼런스를 포함할 수 있음.

[0243] 블록 272에서와 같은, 그 의도된 수신인들의 e-메일 어드레스들을 포함한, 원본 메시지(12)의 인용된 본문이 포함될 수도 있음.

[0244] 블록 273에서와 같은, 하기의 것들을 나열하는 각 수신인을 위한 표.

[0245] a) 수신인의 MTA가 메시지를 수신한 시간 및/또는 시스템이 수신인의 MTA로부터 DSN 보고를 수신한 시간;

[0246] b) 그 착신지에 대한 메시지의 전달 상태 보고, 즉, "메일 서버에 전달 완료", "우편함에 전달 완료", "중계 완료", "전달 실패", "전달 불가".

[0247] 블록 274에서와 같이, 그 별개의 해시값들 또는 메시지 다이제스트들을 포함한 e-메일의 원본 첨부물들의 리스트.

[0248] 블록 275에서와 같이, 각 착신지에 대한 메시지 전달에 수반된 모든 SMTP 대화들의 트랜스크립트들 또는 트랜스크립트들의 개요들.

[0249] 블록 276에서와 같이, 그들이 밝힐 수 있는 메시지의 전달 또는 처분에 대한 세부 사항들을 포함하는 모든 수신된 DSN들의 첨부물들과 본문들로부터의 인용문들.

[0250] 블록 277에서와 같이, 시스템은 영수증에 원본 메시지의 모든 첨부물들의 카피들을 추가할 수 있으며, 블록 278에서와 같이, 시스템은 DSN들에 대한 첨부물들로서 시스템에 반환된 파일들을 추가로 첨부할 수 있음.

[0251] 단계 279에서, 여기까지 영수증의 텍스트를 생성한 이후에, 그후, 시스템은 e-메일 메시지를 위한 제 1 해시와, 영수증의 본문에 대한 소정의 첨부물들을 위한 제 2 해시(들)를 생성하고, 시스템의 운영자들에게만 알려진 암호화 키를 사용하여 이 해시(들) 각각에 대한 전자 시그니쳐를 산출한다. 암호화는 예로서, 본 명세서에서 참조하고 있는, 연방 정보 처리 표준 공보 4-2(FIPS PUB 46-2), 데이터 암호화 표준(National Institute of Standards and Technology)에 기술된 데이터 암호화 표준을 사용할 수 있다. 대안적으로, 해시값을 암호화하는 상이한 공지된 또는 신규한 암호화 방법들도 사용될 수 있다.

[0252] 단계 280에서, 암호화된 해시는 그후 "문서 디지털 시그니쳐"로서 메시지의 단부에 첨부된다.

[0253] 단계 281에서, 이제 완전한 영수증(20)은 송신인의 기록들을 위해 이 영수증이 보관되어야한다는 조언과 함께 송신인에게 e-메일로 보내질 수 있다. 단계 282에서, 시스템은 이제 원본 메시지, 첨부물들 및 DSN들의 모든 카피들을 삭제할 수 있다. 대안적으로, 영수증을 송신인에게 보내는 대신, 시스템이 영수증을 저장하거나, 송신인 및 시스템 양자 모두가 영수증을 저장할 수 있다.

[0254] MUA 통지들이 단지 수신인의 선택으로 반환되며, 수신인이 수신된 메시지에 대한 소정의 행위를 취하였을 때에만 반환되기 때문에, 시스템의 실시예들은 MTA 통지들과는 상이하게 이들 반환 메시지들을 취급하도록 선택될 수 있다.

[0255] 도 2F는 이들 MUA 통지들이 시스템에 의해 처리될 수 있는 방식을 예시한다. MUA 통지들은 단계 211에서, 도 2A의 방식으로 유출 메시지들의 다양한 헤더들을 포함함으로써, 시스템에 의해 요청된다. 이들 헤더들은 호환 MUA들이 이를 위해 따로 설정된 시스템 어드레스(예로서, "readreceipt@RPost.com")로 통지들을 보내도록 지휘한다. 또한, 이 헤더들은 이 반환 어드레스의 "이름" 필드에 메시지의 원 송신인의 e-메일 어드레스를 사용한다. 따라서, 단계 286에서, MUA 통지들이 readreceipt@RPost.com에 반환되었을 때, 시스템은 통지의 어드레스를 검사함으로써, 판독 통지가 보내져야만 하는 어드레스를 결정할 수 있다.

[0256] 착신지의 MUA로부터의 판독 영수증의 도달시, 시스템은 단계 287에서, 수신된 MUA 통지의 제목을 그 제목으로서 포함하는 판독 영수증을 생성하고, 그 메시지 본문에 수신된 MUA 통지의 본문을 통합한다.

[0257] 단계 288에서, 시스템은 이 영수증에 MUA의 영수증을 동반할 수 있는 소정의 파일들을 첨부한다(통상적으로 이들은 원본 e-메일에 대한 식별 레퍼런스들과, 전달 또는 처분의 세부사항들을 포함할 수 있음).

[0258] 단계 289에서, 시스템은 영수증에 첨부된 소정의 파일들을 위한 해시를 생성하고, 영수증의 본문내에 이 해시를 기록한다.

[0259] 단계 290에서, 시스템은 영수증의 본문과 그 첨부물들을 위한 해시를 생성하고, 이 해시를 암호화하며, 그 결과를 이 메시지에 "문서 디지털 시그니쳐"로서 첨부한다.

[0260] 단계 291에서, 시스템은 결과적인 영수증을 메시지의 송신인에게 송신한다. 단계 292에서, 이 영수증을 보낸 이

후에, 시스템은 이 트랜잭션의 모든 내부 기록들을 삭제할 수 있다.

[0261] III. 2차 메일 서버 실시예로서의 RPOST

[0262] 도 3은 RPost가 사용자의 1차 MTA로서 기능하지 않고, 다른 MTA와 협력하여 동작하는 본 발명의 제 2 실시예의 시스템 다이어그램이다. 본 실시예에서, 송신인은 유출 메시지, 메시지 제목, 또는 메시지 어드레스에 소정 유형의 플래그를 포함시킴으로써 특정 유출 메시지를 등록하도록 선택할 수 있다. 예를 들면, 송신인이 메시지의 제목에 부호 "(R)"을 포함시키는 경우 및 포함시키는 경우에만, 송신인의 MTA는 메시지를 RPost 서버를 통해 전송시켜 영수증을 발행하도록 지시한다.

[0263] 본 실시예에서, RPost의 운영자들은 송신인의 MTA의 운영자로부터, 전송된 메시지 당 및/또는 킬로바이트 당의 수입(revenues)을 받는다.

[0264] IV. RPOST 실시예로의 CC

[0265] 도 4는 참조("cc")가 RPost 서버로 송신되는 제 3 실시예의 시스템 다이어그램이다. 본 실시예에서, 사용자 또는 메시지 송신인(10)은 변형이 없는 표준 MUA 및 표준 MTA를 사용할 수 있다. 메시지 송신인(10)은 메시지 본문과 소정의 수의 첨부물을 갖는 e-메일을 작성하고, 이를 임의의 참조들(cc's) 및 원한다면 숨은 참조들(bcc's)과 함께 메시지 수신인(18)에게 보낸다. 부가적으로, 메시지 송신인(10)은 cc를 RPost에 보낸다. RPost 서버(14)는 사전에 메시지에 태그를 첨부하며, 태그 첨부된 메시지를 수신인의 MTA(16) 및 임의의 지정된 cc들에 송신한다. 이러한 카피(copy)를 수신할 때, RPost 서버(14)는 카피의 e-메일 수신 확인 영수증을 송신할 수 있다.

[0266] 메시지의 수신인(18) 및 다른 착신지들은 동일한 메시지의 두 개의 버전들: 즉, 송신인(10)으로부터 직접 수신된 메시지의 제 1 버전, RPost로부터 전송된 제 2의 태그 부착 버전을 수신할 수 있다. RPost가, 메시지의 태그 부착 버전이 수신인 MTA(16)에 의해 성공적으로 수신되었다는 것을 수신인 MTA(16)로부터 확인받으면, RPost 서버(14)는 사전에 메시지 영수증(20)을 작성하며 송신인의 기록들을 위해 영수증을 송신인(10)에게 송신한다.

[0267] 수입은 메시지 발신 도메인들 또는 개별 메시지 송신인들에 대한 계정들을 설정하고 메시지 당, 킬로바이트 당, 또는 이들의 조합으로 사용자들의 계정들에 요금을 과금으로써 생성될 수 있다. 수입은 또한 영수증들상의 광고들의 배치에 대해 및 상술한 바와 같은 인증 및 검증 서비스들로부터 생성될 수 있다.

[0268] V. 웹사이트 실시예

[0269] 도 5는 제 4 실시예의 시스템 다이어그램이다. 본 실시예에서, RPost 서버(14)는 사용자가 메시지들을 작성하는 웹사이트와 관련된다. 메시지 송신인(10)은 RPost 웹사이트를 방문하고 원하는 "본수신", "cc", "bcc", "제목" 및 메시지 원문 정보에 기입함으로써 웹사이트에서 자신의 메시지를 작성한다. 첨부물들은 표준 브라우저들과 웹 서버들에서 가용한 특징들을 사용하여 추가될 수 있다. 본 실시예에서, 송신인은 등록 영수증이 송신될 수 있는 어드레스를 부가적으로 제공해야 한다. RPost 서버(14)는 송신인의 MTA를 통해 송신인(10)에게 영수증을 송신한다.

[0270] 수입은 메시지 발신 도메인들 또는 개별 메시지 송신인들에 대한 계정들을 설정하고 메시지 당, 킬로바이트 당, 또는 이들의 조합으로 사용자들의 계정들에 과금함으로써 생성될 수 있다. 수입은 또한 영수증들 상의 광고들의 배치에 대해 및 상술한 바와 같은 인증 및 검증 서비스들로부터 생성될 수 있다.

[0271] VI. 웹 기반 MUA 실시예

[0272] 도 6은 제 5 실시예의 시스템 다이어그램이다. 본 실시예에서, RPost 서버(14)는 웹 기반 메일 사용자 에이전트와 관련된다. 사용자들이 웹 브라우저를 통해 메일을 작성하는 것을 허용하는 것에 부가하여, 이러한 MUA는 가입자들에게 웹 서버 사이트 상에 저당된 메시지들을 디스플레이하는 브라우저 표시 가능 메일박스들(browser viewable mailbox)을 제공한다. 이러한 서비스의 가입자들은 사용자명들과 패스워드들을 갖는 메일 계정들에 대한 액세스를 얻는다. 본 실시예에서, 메시지 송신인(10)은 RPost 웹사이트를 방문하고, 사용자명과 패스워드를 기입함으로써 웹 기반 e-메일 계정에 액세스하여, RPost 서버(14)로 전달되기 위해 전송되는 자신의 메시지를 작성한다. RPost 서버에 의해 생성된 영수증들은 가입자의 계정과 관련된 웹 기반 메일박스로 반환된다.

[0273] 다른 실시예들에서 가용한 수입원들에 부가하여, 본 실시예에서, 운영자들은 웹 기반 메일박스에 보유된 영수증들에 대한 저장 수수료들을 과금할 수 있다.

[0274] 상기 실시예들 모두에 있어서, 영수증은 하기의 사항에 대한 증거로서 기능할 수 있다.

[0275] (1) 발신자가 e-메일 메시지를 송신한 사실;

[0276] (2) 메시지가 특정 시간에 송신된 사실;

[0277] (3) e-메일이 특정 수신인(들)에게 보내진 사실;

[0278] (4) e-메일이 지정된 수신인(들)의 각각의 e-메일 우편함으로 전달된 사실;

[0279] (5) e-메일이 특정 시간에 송신된 사실;

[0280] (6) e-메일이 특정 네트워크 루트에 의해 전달된 사실; 및

[0281] (7) e-메일 메시지와 그의 첨부물들이 영수증에 기록된 특정 내용을 갖고 있다는 사실.

[0282] 더욱이, 특정 상황들하에서 시스템은

[0283] (1) e-메일이 수신인의 메일 사용자 에이전트(MUA)를 통해 검사되었는지; 및

[0284] (2) 수신인이, 특정 시간에, 예를 들면 e-메일의 판독 또는 삭제와 같은 메시지에 대한 응답 동작을 수행하였는지에 한 증거로서 사용될 수 있는 별도 영수증(separate receipt)을 생성한다.

[0285] 다른 실시예들과 마찬가지로, 본 실시예는 전자 메시지의 전달 및 보전의 시스템의 관련되지 않은 제 3 자의 운영자들에 의해 증명되며 검증될 수 있는 문서화 증거를 제공한다. 달리 말하면, 시스템은, 이후에 특정 e-메일 메시지가 송신되어 언제 어떻게 성공적으로 전달되었는지를 증명하는데 사용될 수 있는 등록 e-메일로의 e-메일의 변환으로서 고려될 수 있다.

[0286] 분쟁이 발생되는 경우, 시스템의 운영자들이 시스템의 생성물로서 영수증의 인증을 결정할 수 있도록 영수증이 암호화되어 있기 때문에 분쟁은 시스템에 의해 생성된 영수증에 의해 해결될 수 있다. 그 후, 시스템의 운영자들은, 운영자들이 영수증에 포함된 임의의 기록 또는 카피를 보존해야 할 필요가 없이, 영수증 자체에 포함된 정보만에 의존하여 인증 영수증에 포함된 정보의 정확성을 증명할 수 있다.

[0287] 이러한 장점들에 부가하여, 시스템에 의해 생성된 영수증들은 또한 시스템을 통해 전송될 때 이러한 자료들의 존재 및 저작권의 증거로서 또한 사용될 수 있다. 더욱이, 시스템은 임의의 인터넷 e-메일 클라이언트 프로그램/MUA로부터 사용될 수 있기 때문에, 시스템은 사용이 용이하며, 따라서 부가의 소프트웨어가 필요하지 않다.

[0288] 영수증을 확인하기 위한 흐름도

[0289] 도 7은 영수증을 확인하기 위한 예시적인 방법을 도시하는 흐름도이다. 메시지의 송신인이, e-메일이 송신되고 전달되었다는(및/또는 판독되었다는) 증거를 요구하는 경우에는, 송신인은 단계 700에서 메시지에 대응하는 영수증(들)을 시스템의 운영자들에게 제출한다. 다음, 시스템의 운영자들은, 단계 702에서, 영수증에 첨부된 문서 디지털 시그니쳐를 분리하여 해독한다. 단계 703에서, 운영자들은 첨부물들을 포함하는 문서의 잔여부의 해시(hash of balance)를 생성한다.

[0290] 단계 704에서, 현재의 해시값이 해독된 해시값과 일치하지 않으면, 시스템은, RPost가 전달의 정확한 기록으로서 영수증 또는 영수증에 기재된 메시지의 내용을 인증할 수 없다고 진술하는 보고서를 생성한다.

[0291] 해독된 해시가 메시지의 현재 해시와 동일하면, 시스템은, 단계 706에서, 영수증이 시스템을 통과하였기 때문에 메시지의 본문에 포함된 정보가 변경되지 않았다는 것을 보증할 수 있다. 원본 메시지가 첨부물들을 포함하지 않으면, 시스템은 영수증이 메시지의 내용들 및 RPost 서버에 의한 그의 전달의 정확한 기록이라는 것을 보증하는 보고서를 생성할 수 있다.

[0292] 영수증이 원본 메시지가 첨부물들을 포함한다고 보고하면, 영수증은 또한 각각의 첨부물의 이름 및 해시값을 기록할 수 있다. 영수증의 생성시에, 원본 메시지의 모든 첨부물들은 변경되지 않고 영수증에 첨부된다. 따라서, 시스템은, 이러한 첨부 파일 각각에 대해 첨부 파일(708)의 해시를 생성하며, 이를 영수증(709)의 본문에 기록된 해시값과 비교한다.

[0293] 파일의 연산된 해시값이 영수증에 포함된 값과 일치하면, 시스템은 영수증에 첨부된 파일이 최초 전달된 바와 같은 메시지에 첨부된 것과 동일하다는 것을 보증할 수 있다. 해시들이 일치되지 않으면, 시스템은 영수증에 첨부된 파일이 원본 메시지에 첨부된 파일과 동일하다는 것을 보증할 수 없다고 보고할 수 있다.

[0294] 원본 메시지에 첨부된 각각의 파일에 대해 이러한 연산을 수행함으로써, 시스템은 영수증과 영수증의 첨부 파일

들 각각의 인증을 보고하거나(710), 확인의 실패를 보고하는 보고서를 준비할 수 있다(712).

[0295] 평가를 완료하면, 시스템은 영수증의 카피와 모든 첨부물들을 생성된 보고서에 첨부하고, 확인을 위한 보고서를 제출한 사용자의 반송 어드레스로 e-메일을 통해 이를 송신할 수 있다.

[0296] VII. 유입 e-메일들의 등록

[0297] 도 8은 유입 e-메일들이 등록되는 본 발명의 다른 실시예를 도시하는 시스템 다이어그램이다. 본 실시예에서, 메시지 송신인(60)은 e-메일 메시지(70)를 송신한다. 송신인의 MTA(62)는 통상적으로 인터넷상으로 메시지(70)를 송신한다. 그러나, 본 실시예에서 RPost는 유입 e-메일들을 등록하기 위해 서비스 가입자/수신인(68)과 계약한다. 협정에 따르면, RPost는 네트워크 솔루션스, 인크.(Network Solutions, Inc.; NSI) 또는 상이한 도메인명 기관에 의해 수신인(68)을 위한 메일 수신인(MX 서버)으로서 지정되어 있다. 이는 송신인의 MTA(62)에 의해 수행된 도메인명 서비스(DNS) 요청이 수신인용 IP 어드레스로서 RPost의 IP 어드레스로 전환시키도록 하며, 송신인의 MTA(62)가 RPost 서버(64)로 e-메일 메시지를 송신하도록 한다. RPost 서버(64)는 수신인(68)을 위한 SMTP, POP, POP3 또는 IMAP MTA("POP 메일 서버"로 총칭함)로서 기능한다. SMTP, POP 및 IMAP MTA들은 RFC(821), SMTP 프로토콜, RFC 1939 포스트 오피스 프로토콜-버전 3(RFC1725를 폐용시킴), 및 RFC 2060 IMAP (인터넷 메시지 액세스 프로토콜) 버전 4 rev 1(RFC 1730을 폐용시킴)에 의해 지배되며, 이들은 본원에 참조로서 합체되어 있다.

[0298] RPost 서버(64)는 원본 메시지(70)의 등록 버전(74)을 준비하고, 원본 메시지(70) 대신에, 또는 원본 메시지에 부가하여 수신인의 수신함(in-box)으로 등록 버전(74)을 배치시킨다. 등록 버전은 e-메일 영수증들과 관련하여 상술한 모든 검증 및 정보 특징들을 가질 수 있다. 상기 정보는 메시지 본문 및 원문 각각에 대한 개별 메시지 요약들, 수신/송신 정보(to/from information), 다른 헤더 정보, 각각의 첨부물, 전체 메시지 요약 및 디지털 시그니쳐 및 메시지 발송 정보 및 태그들을 포함할 수 있지만, 이에 한정되는 것은 아니다. 도 6에 도시한 바와 같은 메시지(70)의 등록 버전(74)은 헤더 정보, 첨부물, 각각의 메시지에 대한 개별 메시지 요약, 및 디지털 시그니쳐 또는 암호화 메시지 요약을 포함하는 메시지 본문을 포함한다. 해시 평션들 및 암호화는 시스템의 운영자들에만 공지된 비밀 어구들(private phrase) 및 비밀 키이들(private keys)을 사용하여 수행된다. 등록 버전(74)은 수신인의 MUA를 통한 검사 또는 다운로딩을 위해 수신인(68)에게 가용된다.

[0299] RPost 서버는 선택적으로 메시지 송신인(60)에게 확인 e-메일(72)을 송신할 수 있다. 확인 메시지(72)는 메시지가 수신되어 등록되었다는 것을 지시하는 단순한 텍스트 메시지일 수 있다. 확인 메시지(72)는, "당신의 e-메일 메시지는 2000년 3월 24일 오후 2:05에 수신되었습니다. 메시지의 디지털 시그니쳐는 [128-비트 디지털 시그니쳐]입니다. 부가의 정보를 위해, 우리의 웹사이트 www.RPost.com을 방문하여 주십시오."와 같은 메시지를 또한 포함할 수 있다. 대안적으로, 또는 부가적으로, 확인 메시지(72)는 등록 버전(74)에 포함된 모든 정보를 포함할 수 있다.

[0300] 따라서, 시스템은 메시지 수신인(68)에게 영수증(74) 또는 하기의 사항에 대한 다른 검증가능한 확인을 제공할 수 있다.

[0301] (1) 수신인이 e-메일 메시지를 수신한 사실;

[0302] (2) 메시지가 특정 시간에 수신된 사실;

[0303] (3) e-메일이 특정 송신인으로부터 보내진 사실;

[0304] (4) 메시지 취지들이 특정 네트워크 루트를 통해 전달된 사실; 및

[0305] (5) e-메일 메시지 및 그 첨부물이 특정 내용을 갖고 있다는 사실.

[0306] 따라서, 시스템은, 특정 전자 메시지들 및 문서들이 특정 송신인들로부터 유입된 바와 동일한 메시지들 및 문서들임을 나타내면서 특정 내용을 갖고 수신인들에게 전달되었다는, 시스템의 운영자들에 의해 증명될 수 있는 증거를 제공한다.

[0307] 도 9는 유입 메일을 등록하는 일례를 도시하는 흐름도이다. 단계 901에서, RPost 서버(64)는 신규 e-메일 메시지를 수신한다. 단계 902에서, 시스템은 메시지의 헤더들 및 첨부물들을 포함하는 메시지의 내용들의 해시/디지털 시그니쳐를 생성한다. 부가적으로, 시스템은 각각의 메시지 첨부물을 위한 개별 해시를 생성시킬 수 있다. 단계 903에서, 시스템은 시스템의 운영자들에게만 공지된 암호화 키이를 사용하여 해시(들)를 암호화한다. 단계 904에서, 최종 암호화된 해시(들)은 메시지의 본문에 첨부된다. 다음, 단계 905에서, 수정된 메시지가 수신인의

MUA를 통해 검사 또는 다운로드를 위해 가용화될 수 있다.

[0308] 도 10은 수신된 등록 e-메일 메시지를 확인하는 일례의 흐름도이다. 단계 1000에서, 메시지의 수신인이, 특정 내용을 갖는 e-메일이 특정 시간에 수신되었다는 증거를 요구해야 하는 경우, 수신인은 e-메일 메시지(70)의 등록 버전(74)(도 8)의 카피를 검증을 위해 시스템의 운영자들에게 제출할 수 있다. 메시지를 검증하기 위해, 단계 1001에서, 시스템은 메시지에 첨부된 문서 전자 시그니쳐를 분리하고 해독한다. 단계 1002에서, 시스템은 문서의 밸런스의 해시 및 메시지에 첨부된 각각의 파일에 대한 해시를 생성한다. 단계 1003 및 1004에서, 해시들이 비교된다. 문서 해시(들)가 해독된 해시(들)와 일치하면, 메시지 및 그 첨부물들은 시스템을 통과하며 수신인에게 전달될 때까지 변경되지 않아야 한다.

[0309] e-메일이 변경되지 않았다고 판정하면, 시스템의 운영자들은 하기의 사항을 보증할 수 있다.

[0310] (1) e-메일이 특정 시간에 시스템에 의해 수신되었다는 사실;

[0311] (2) e-메일이 특정 인터넷 루트를 통해 시스템에 도달하였다는 사실;

[0312] (3) e-메일이 특정 송신인으로부터 도달하였다는 사실;

[0313] (4) e-메일과 그 첨부물들이 그들이 현재 포함하는 특정 내용을 갖고 전달되었다는 사실.

[0314] 한편, 단계 1006에서, 해시값들이 일치하지 않으면, 운영자는 e-메일이 인증되었다고, 즉 e-메일이 시스템에 의해 수신된 e-메일의 정확한 버전이라는 것을 보증할 수 없다.

[0315] 도 11은 전자 도구를 사용하는 비즈니스("e-비즈니스")에 의한 본 발명의 예시적인 사용을 도시한다. E-비즈니스(30)는 그의 고객들(34)로부터의 모든 유입 및 유출 e-메일 메시지들을 등록하도록 시스템을 사용할 수 있다. 이 경우, 시스템은 포스트 오피스 프로토콜(POP) 서버(36)와 단순 메일 전송 프로토콜(SMTP) 서버(38)를 포함한다. 예를 들면, e-비즈니스(30)는 고객들에 대한 e-메일 폼들, 고객들(34)로부터의 전진(forward) 문의들 및 불만들(40)을 그의 웹사이트에 설정할 수 있다. 등록 문의들, 불만들, 주문들, 구매 신청들, 및 다른 정보(46)는 시스템에 의해 e-비즈니스(30)로 송신된다. 다음, 영수증들이 SMTP 서버(38)를 통해 고객들(34)에 제공된다. 이 방법에서는 고객들이 메일을 송신했는지의 여부 및 메일에 포함된 내용에 관해서는 문제삼지 않는다. 더욱이, e-비즈니스는 고객들과의 모든 통신이 등록될 수 있도록 RPost 서버를 통해 웹사이트(32)를 설정할 수 있다. 달리 말하면, 웹사이트 폼을 통해 데이터 주문들(42) 및 자동화 응답들(44)은 시스템 서버를 통해 등록될 수 있으며, 더욱이, e-비즈니스에 의해 고객들(34)에 송신된 임의의 확인, 통지들 수집, 고객 지원, 및 특수 제공들(48)이 등록될 수 있으며, 무엇이, 언제, 또는 누가 주문했는지에 대한 논쟁들을 배제하기 위해 확인서가 고객에게 송신된다. 원한다면, 동일한 영수증들이 고객들(34)과 e-비즈니스(30) 모두에게 제공될 수 있다. 대안적으로, POP 서버(36)와 SMTP 서버(38)의 기능들은 단일 시스템 서버에서 조합될 수 있다.

[0316] POP는 e-메일 서버로부터 e-메일을 검색하는데 사용되는 프로토콜이다. 다수의 e-메일 적용들(종종 e-메일 클라이언트들로 칭함)이 POP 프로토콜을 사용하지만, 몇몇은 보다 신규한 인터넷 메시지 액세스 프로토콜(IMAP)을 사용한다. POP2라 칭하는 POP의 한 버전은 메시지들을 송신하기 위한 SMTP를 필요로 한다. 보다 신규한 버전인, POP3는 SMTP를 갖거나 갖지 않고 사용될 수 있다. SMTP는 서버들 사이에 e-메일 메시지들을 송신하기 위한 프로토콜이다. 인터넷을 통해 e-메일을 송신하는 다수의 e-메일 시스템들은 하나의 서버로부터 다른 서버로 메시지들을 송신하기 위해 SMTP를 사용하며, 다음, 메시지들은 POP 또는 IMAP를 사용하여 e-메일 클라이언트에 의해 검색될 수 있다. 게다가, SMTP는 일반적으로 메일 클라이언트로부터 메일 서버로 메시지들을 송신하는데 사용된다. e-메일 서버들은 인터넷과 통신하기 위해 다양한 프로토콜들을 사용할 수 있다. 통상적으로 사용되는 프로토콜들은 SMTP, POP3 및 IMAP4를 포함한다. 메일 판독자들(readers)은 서버의 대향 단(end)에 위치한다. 메일 서버들은 SMTP를 통해 메시지들을 수신하기 때문에, e-메일 판독자들은 SMTP를 사용하여 메일 서버로 e-메일을 송신한다. 마찬가지로, 메일 서버들은 POP3 및 선택적으로 IMAP4를 사용하여 메시지들을 송신하기 때문에, 메일 판독자들은 POP3 또는 IMAP4 프로토콜을 사용하여 메일 서버들로부터 메시지들을 수신한다.

[0317] 상기에는 일반적으로 e-메일이 송신 및/또는 수신되었는지를 검증하는 시스템 및 방법을 설명하였지만, 계류중인 출원 제09/626,577호에 개시되고 청구된 본 발명은 전자 메시지 네트워크를 통해 또는 임의의 전자 게이트를 통해 전송될 수 있는 임의의 전자 메시지에 적용할 수 있다. 전자 메시지들은 텍스트, 오디오, 비디오, 그래픽들, 데이터, 및 다양한 파일 유형들의 첨부물들을 포함할 수 있다. 본원에 개시된 방법들 및 기술들은 서버들 및 다른 컴퓨터들내로 프로그램될 수 있으며, 본 발명을 실시하는 컴퓨터 프로그램들은 CD ROM들, RAM, 하드 드라이브들, 및 자기 테이프를 포함하지만, 이에 한정되는 것은 아닌 컴퓨터 판독 가능 매체상에 기록될 수 있다. 본 발명에 따른 e-메일 등록 서비스들은 법인체 및 다른 기관 클라이언트들에 대한 단일의 공급자 ISP 해결책을

제공하도록 인터넷 서비스 공급자(ISP) 서비스들과 번들될 수 있다. 상술한 본 발명을 실시하는 것은 소프트웨어 분야의 숙련자들에게는 명백하다.

[0318] 앞에서 나타낸 바와 같이, 도 1-11은 서버가 송신인으로부터 메시지를 수신하여 제 1 경로의 이 메시지를 수신인에게 전송하거나, 수신인의 메일 전송 에이전트(MTA)에 전송한다. 송신인이 서버로 하여금, 제 1 경로보다 더 이동된 경로 또는 보다 적게 이동된 루트 또는 적어도 서로 다른 경로에 의해 수신인 또는 수신인의 메일 전송 에이전트 또는 수신인을 위한 메일 전송 에이전트에 메시지를 송신하고자 하는 시기들이 존재한다. 이를 달성하기 위해, 송신인은 메시지의 "주제" 라인과 같은 특정 위치에 특정한 표시로 메시지 폼(1200)(도 14)을 마킹한다. 이 특정 위치는 도 14에서 메시지 폼(1200)내의 1202에 표시된다. 메시지의 "주제" 라인(1202)에서 마킹하는 단계는 도 12의 1206에 도시된다.

[0319] "주제" 라인 내의 "(R)"를 갖는 메시지는 송신인에 의해, 송신인의 메일 전송 에이전트를 구성하는 서버에 전송된다. 이는 도 12에서 1208에 표시된다. 1210에 표시된 바와 같이, 서버는, "주제" 라인에 "(R)"이 존재하는지를 결정하도록 "주제" 라인을 스캔한다. 답신이 "노(No)"이면(1211 참조), 서버는 메시지를 도 1-11에 도시되고 도 12에 "원래 루트"로서 표시되며 상세한 설명에서 상기 논의된 루트를 통해 수신인 또는 수신인의 메일 전송 에이전트에 전송한다. 이는 도 12의 1212에 표시된다. 답신이 "예스(Yes)"(1213 참조)이면, 메시지는 도 14의 1214에 표시된 바와 같은 특정 네트워크를 통해 전송된다.

[0320] 도 13은 도 12에 대해 여러 면들에 있어서 동일하다. 하지만, 도 13은 도 12에 도시된 것과는 상이한 부가적인 기능들을 수행하기 위해 부가적인 블록들을 포함한다. 이들은 아래의 것을 포함하며 그에 제한되지 않는다.

[0321] (1) 송신인은 메시지의 카피가 달성되기를 원할 수 있다. 이는 코딩이 "R1"이 되도록 "주제" 라인 내의 "(R)" 다음의 번호 "1"과 같은 코딩을 부가함으로써 달성될 수 있다.

[0322] (2) 송신인은 송신인의 메일 전송 에이전트를 구성하는 서버(14)에 의해 기록되기를 바랄 수 있다. 이는 메시지의 "주제" 라인 내의 "(R)"과 같은 코딩을 제공함으로써 달성될 수 있다.

[0323] (3) 송신인은 메시지 전송의 기록이 데이터 베이스에 기록되기를 바랄 수 있다. 이는 메시지의 "주제" 라인 내의 "(R)"과 같은 코딩을 제공함으로써 달성될 수 있다.

[0324] (4) 송신인은 특정 주석(annotation)이나 부가적인 참조(reference)로 데이터베이스에 기록되기를 원할 수 있다. 이는 메시지의 "주제" 라인 내의 "(R)"과 같은 코딩을 제공함으로써 달성될 수 있다.

[0325] 도 13은 송신인의 메일 전송 에이저트를 구성하는 서버가 이 문단에서 특정되는 것들과 같은 선택된 e-메일 메시지들을 처리하는 방법을 제공한다.

[0326] 도 13은 특히 메시지의 "주제"라인 내의 코딩 "(xyz)"에 제한된다. 도 13에서, 송신인은 메시지의 "주제" 라인 내의 "(xyz)"를 포함하는 전자 메시지를 구성하는 것으로서 1300에 도시된다. 도 12 및 도 13의 1210에 표시된 바와 같이, 메일 전송 에이전트를 구성하는 서버(14)는 외부 메시지의 "주제" 라인을 스캔한다. 메시지의 "주제" 라인이 코드 "(R)"를 포함하지 않는다면, 서버는 도 1-11에 도시되고 상술된 루트를 통해 메시지를 전송한다(도 12 및 도 13의 1212 참조). 코드 "(R)"가 서버에 의해 메시지의 "주제" 라인에서 검출되면, 서버는 도 12 및 도 13의 1214에 표시된 바와 같은 특정 네트워크 루트를 통해 메시지를 전송한다.

[0327] 도 13은, 코드 "(xyz)"가 서버에 의해 메시지의 "주제" 라인으로부터 공급된다는 것을 나타낸다. 구획문자 "xyz"가 검출되면, 메시지의 카피는 세이브된다. 이는 도 13의 1308에 표시된다. 구획문자 "xyz"가 식별되지 않으면, 메시지의 카피는 세이브되지 않는다.

[0328] 본 발명이 바람직한 실시예들 및 도면들에 대해 상세히 설명되었지만, 본 기술분야의 당업자들에게는 본 발명의 다양한 적용들 및 변형들이 본 발명의 사상과 범위에서 벗어나지 않고 달성될 수 있음이 명백하다. 따라서, 상술한 상세한 설명 및 첨부된 도면들이 본원 발명의 일정범위에 제한되지 않으며, 첨부된 청구범위 및 적절하게 해석되는 법적 등가물들로부터만 추론되어야 한다는 것을 이해할 수 있을 것이다. 하기의 청구범위에서는, 용어 "~ 수단"을 포함하는 청구항들은 35 U.S.C. §112, 6항에 따라 해석되도록 의도되며, 용어 "~ 수단"을 포함하지 않는 청구항들은 35 U.S.C. §112, 6항에 따라 해석되지 않도록 의도된다.

도면의 간단한 설명

[0030] 도 1은 특수 메일 전송 에이전트(MTA)에 의해 전송됨으로써 유출(outgoing) 메시지들이 등록되는, 본 발명의 제 1 실시예의 시스템 다이어그램.

[0031] 도 2A 내지 도 2F는 도 1의 실시예에 따라 유출 e-메일을 등록하기 위한 대표적인 흐름도.

[0032] 도 3은 별개의 등록 MTA를 통해 선택된 메시지들을 전송하기 위해 송신인이 메일 전송 에이전트를 지휘할 수 있는, 본 발명의 제 2 실시예의 시스템 다이어그램.

[0033] 도 4는 등록된 특수 서버에 유출 메시지들의 카본 카피들(cc들)이 보내지는, 본 발명의 제 3 실시예의 시스템 다이어그램.

[0034] 도 5는 사용자들이 착신 웹사이트에서 등록 대상 유출 메시지들을 작성하는, 본 발명의 제 4 실시예의 시스템 다이어그램.

[0035] 도 6은 사용자들이 등록된 e-메일들을 송신하고, 웹 기반 메일 사용자 에이전트(MUA)내로부터의 영수증들을 저장할 수 있는, 본 발명의 제 5 실시예의 시스템 다이어그램.

[0036] 도 7은 등록된 e-메일 영수증을 확인하기 위한 흐름도.

[0037] 도 8은 유입(incoming) 메시지들을 등록하기 위한 본 발명의 실시예의 시스템 다이어그램.

[0038] 도 9는 유입 메시지들을 등록하기 위한 흐름도.

[0039] 도 10은 수신된 등록된 메시지들을 확인하기 위한 흐름도.

[0040] 도 11은 유입 및 유출 통신들을 등록 및 수신통지하기 위해 전자상거래에 의한 본 발명의 예시적 사용을 도시하는 시스템 다이어그램.

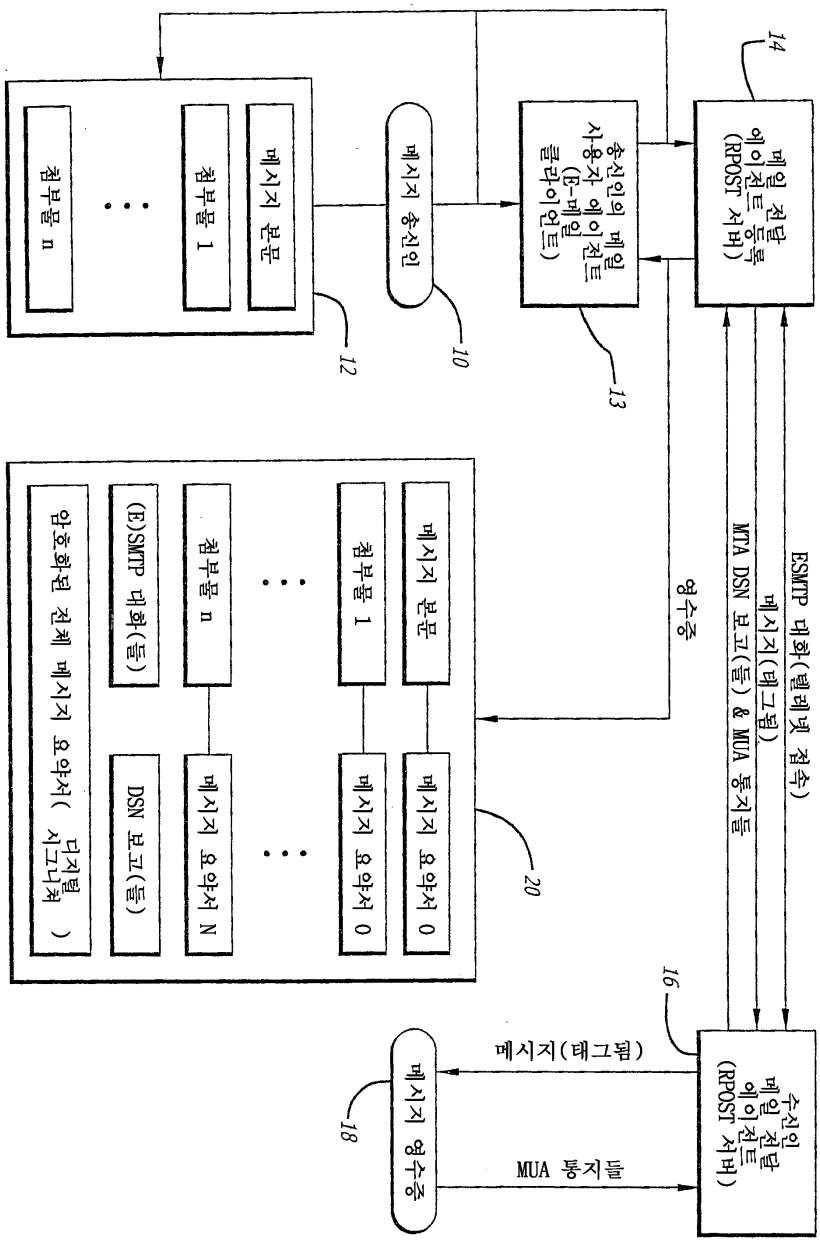
[0041] 도 12는 이전 도면들에 도시된 서로 다른 실시예들의 각 실시예들에 도시된 바와 같은 시스템에서 메일을 기록하는 방법을 위한 흐름도를 보여주고, 메일을 기록하였음을 나타내는 표시와 함께 송신인으로부터 서버로의 메시지가, 상기 메시지가 서버에 의해 수신인에게 전송되는 루트와는 상이한 특정한 루트를 통해 수신인에게 어떻게 서버에 의한 메시지의 전송을 제공하는지를 보여주는 블록도.

[0042] 도 13은 도 12에 도시되는 것과 유사한 흐름도를 보여주지만, 도 12의 흐름도에 의해 제공되는 기능들에 부과하여 특정한 기능들을 제공하기 위한 부가적인 블록들을 갖는 블록도.

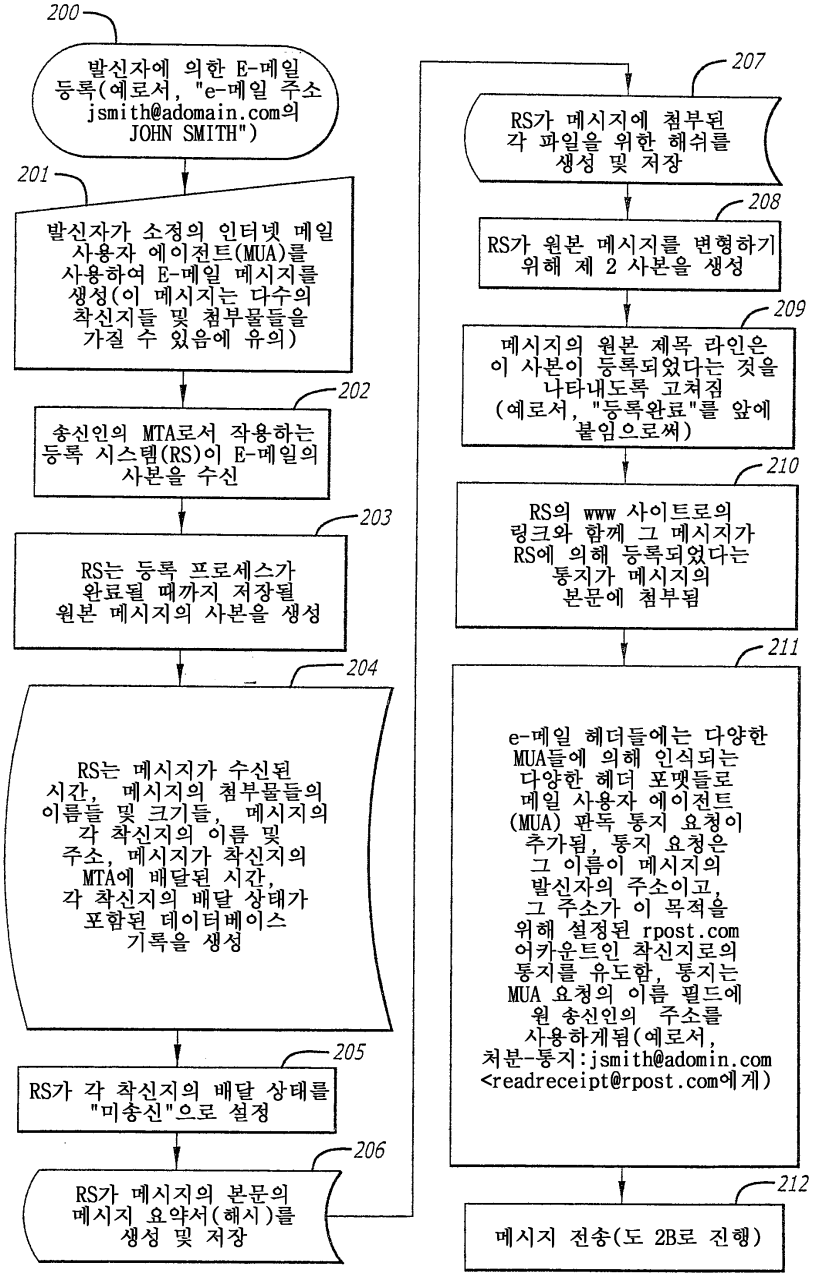
[0043] 도 14는 서버에 의해 수신인에게 송신될 메시지를 기록하기 위해 송신인에 의해 사용되는 형태의 부분도.

도면

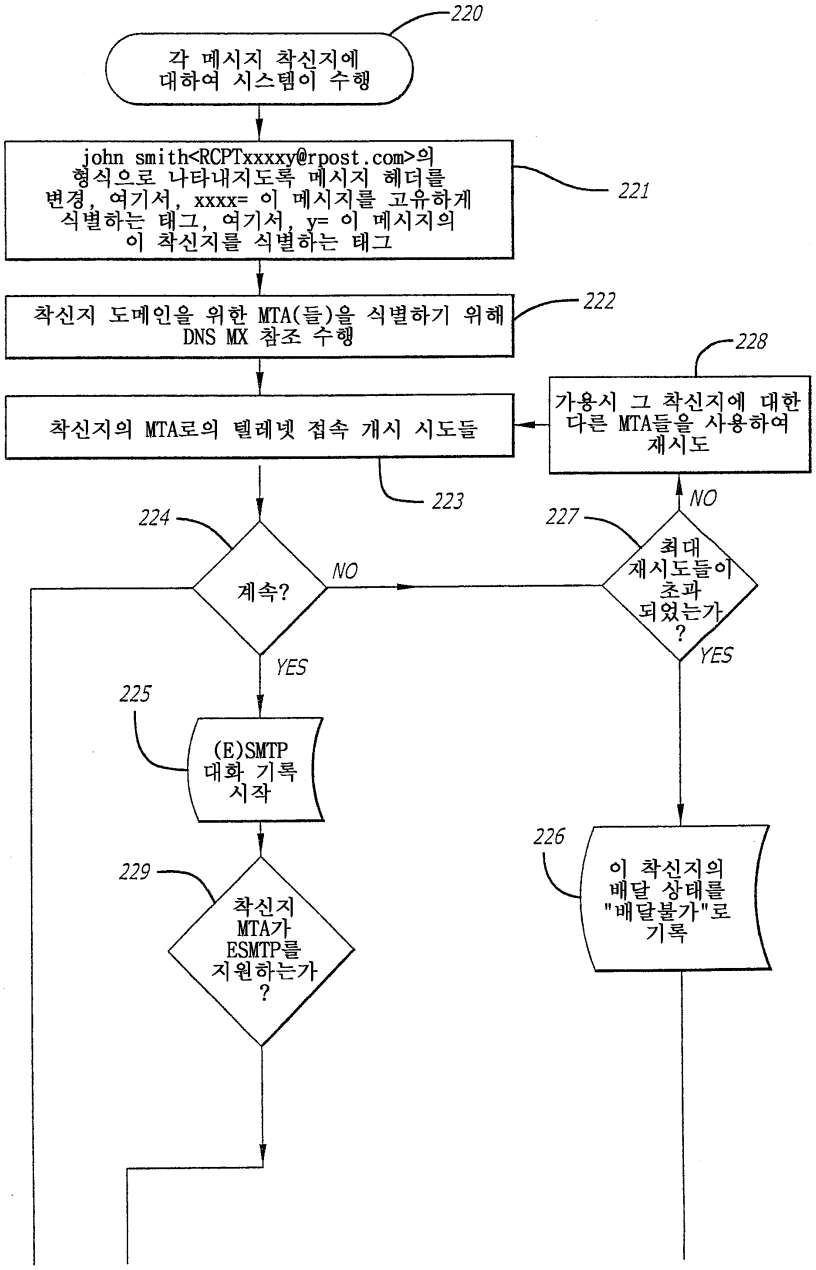
도면1


14
메일 전달 에이전트 등록 (RPOST 서버)
송신인의 메일 사용자 에이전트 (E-메일 클라이언트)
13
메시지 송신인
10
메시지 본문
첨부물 1
첨부물 n
12
영수증
ESMTP 대화(텔레넷 접속)
메시지(테그됨)
MTA DSN 보고(들) & MUA 통지들
메시지 본문
첨부물 1
첨부물 n
메시지 요약서 0
메시지 요약서 0
메시지 요약서 N
(E)SMTP 대화(들)
DSN 보고(들)
암호화된 전체 메시지 요약서(디지털 시그니쳐)
20
16
수신인 메일 전달 에이전트 (RPOST 서버)
메시지(태그됨)
MUA 통지들
메시지 영수증
18

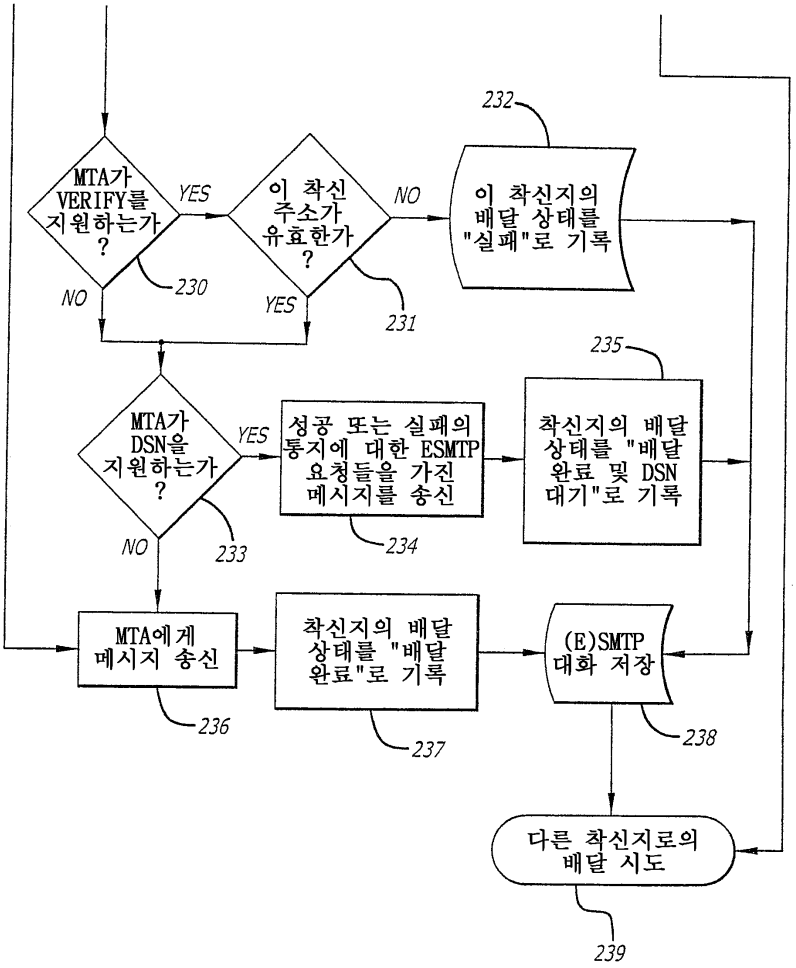
도면2A


200
발신자에 의한 E-메일 등록(예로서, "e-메일 주소 jsmith@adomain.com의 JOHN SMITH")
201
발신자가 소정의 인터넷 메일 사용자 에이전트(MUA)를 사용하여 E-메일 메시지를 생성(이 메시지는 다수의 착신지들 및 첨부물들을 가질 수 있음에 유의)
202
송신인의 MTA로서 작용하는 등록 시스템(RS)이 E-메일의 사본을 수신
203
RS는 등록 프로세스가 완료될 때까지 저장될 원본 메시지의 사본을 생성
204
RS는 메시지가 수신된 시간, 메시지의 첨부물들의 이름들 및 크기들, 메시지의 각 착신지의 이름 및 주소, 메시지가 착신지의 MTA에 배달된 시간, 각 착신지의 배달 상태가 포함된 데이터베이스 기록을 생성
205
RS가 각 착신지의 배달 상태를 "미송신"으로 설정
206
RS가 메시지의 본문의 메시지 요약서(해시)를 생성 및 저장
207
RS가 메시지에 첨부된 각 파일을 위한 해쉬를 생성 및 저장
208
RS가 원본 메시지를 변형하기 위해 제 2 사본을 생성
209
메시지의 원본 제목 라인은 이 사본이 등록되었다는 것을 나타내도록 고쳐짐 (예로서, "등록완료"를 앞에 붙임으로써)
210
RS의 www 사이트로의 링크와 함께 그 메시지가 RS에 의해 등록되었다는 통지가 메시지의 본문에 첨부됨
211
e-메일 헤더들에는 다양한 MUA들에 의해 인식되는 다양한 헤더 포맷들로 메일 사용자 에이전트 (MUA) 판독 통지 요청이 추가됨, 통지 요청은 그 이름이 메시지의 발신자의 주소이고, 그 주소가 이 목적을 위해 설정된 rpost.com 어카운트인 착신지로의 통지를 유도함, 통지는 MUA 요청의 이름 필드에 원 송신인의 주소를 사용하게됨(예로서, 처분-통지:jsmith@adomin.com <readreceipt@rpost.com에게)
212
메시지 전송(도 2B로 진행)

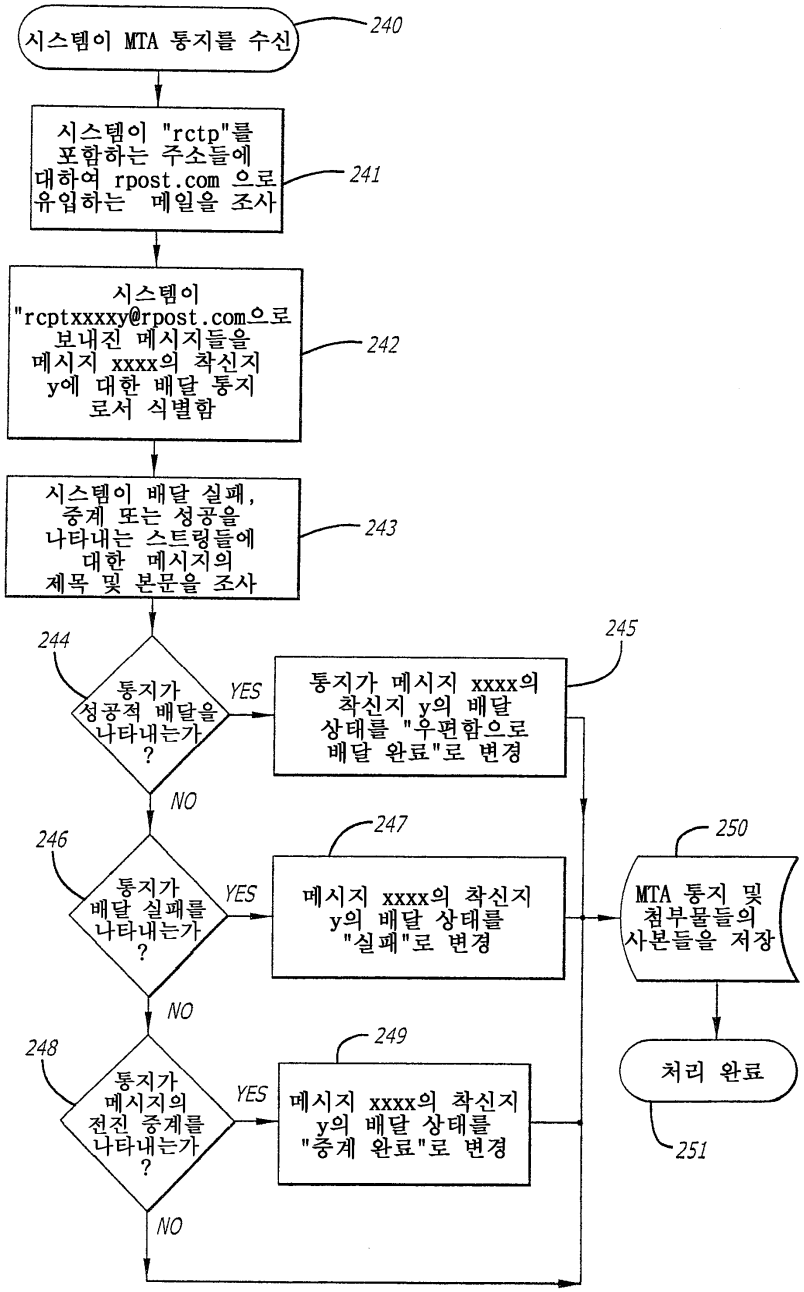
도면2B-1


220
각 메시지 착신지에 대하여 시스템이 수행
john smith<RCPTxxxxy@rpost.com>의 형식으로 나타내지도록 메시지 헤더를 변경, 여기서, xxxx= 이 메시지를 고유하게 식별하는 태그, 여기서, y= 이 메시지의 이 착신지를 식별하는 태그
221
착신지 도메인을 위한 MTA(들)을 식별하기 위해 DNS MX 참조 수행
222
228
가용시 그 착신지에 대한 다른 MTA들을 사용하여 재시도
착신지의 MTA로의 텔레넷 접속 개시 시도들
223
NO
224
계속?
NO
227
최대 재시도들이 초과 되었는가 ?
YES
YES
225
(E)SMTP 대화 기록 시작
226
이 착신지의 배달 상태를 "배달불가"로 기록
229
착신지 MTA가 ESMTP를 지원하는가 ?

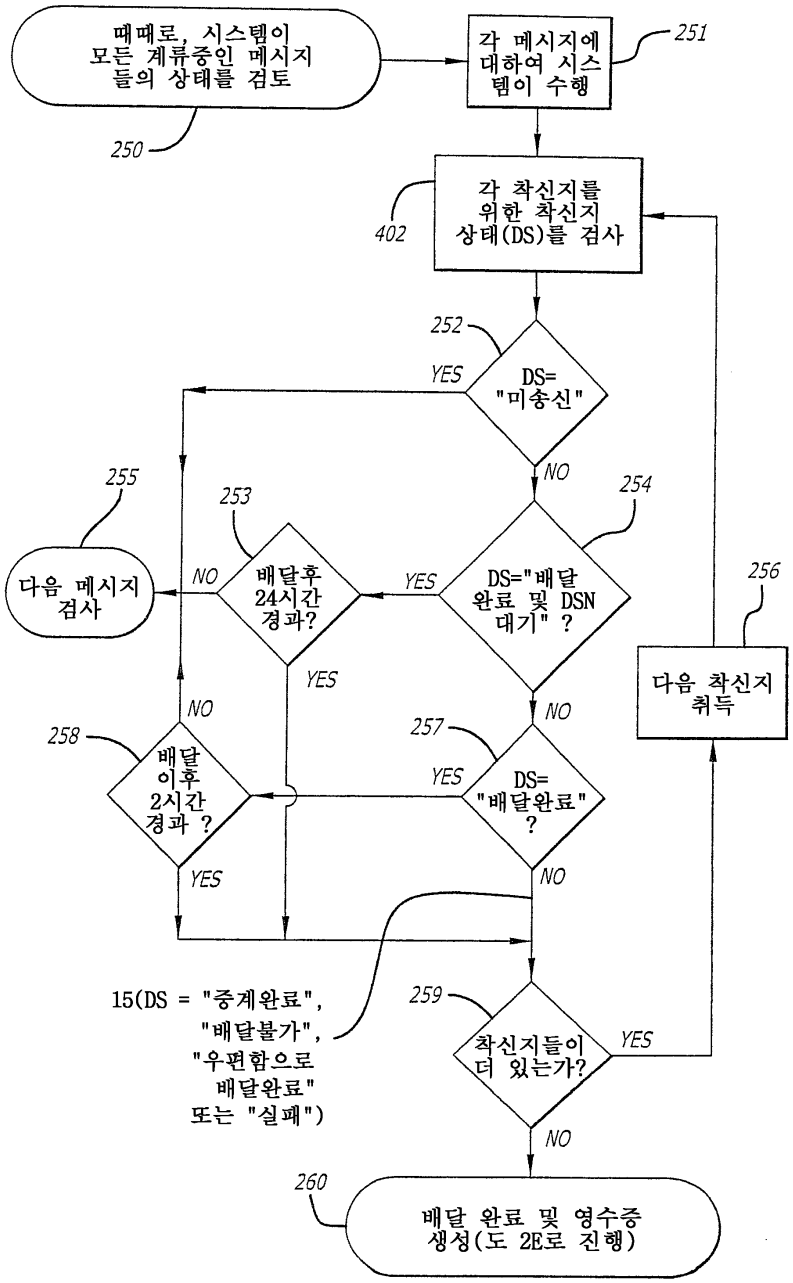
도면2B-2


MTA가 VERIFY를 지원하는가 ?
YES
NO
230
이 착신 주소가 유효한가 ?
NO
YES
231
232
이 착신지의 배달 상태를 "실패"로 기록
MTA가 DSN을 지원하는가 ?
YES
NO
233
성공 또는 실패의 통지에 대한 ESMTP 요청들을 가진 메시지를 송신
234
235
착신지의 배달 상태를 "배달 완료 및 DSN 대기"로 기록
MTA에게 메시지 송신
236
착신지의 배달 상태를 "배달 완료"로 기록
237
(E)SMTP 대화 저장
238
다른 착신지로의 배달 시도
239

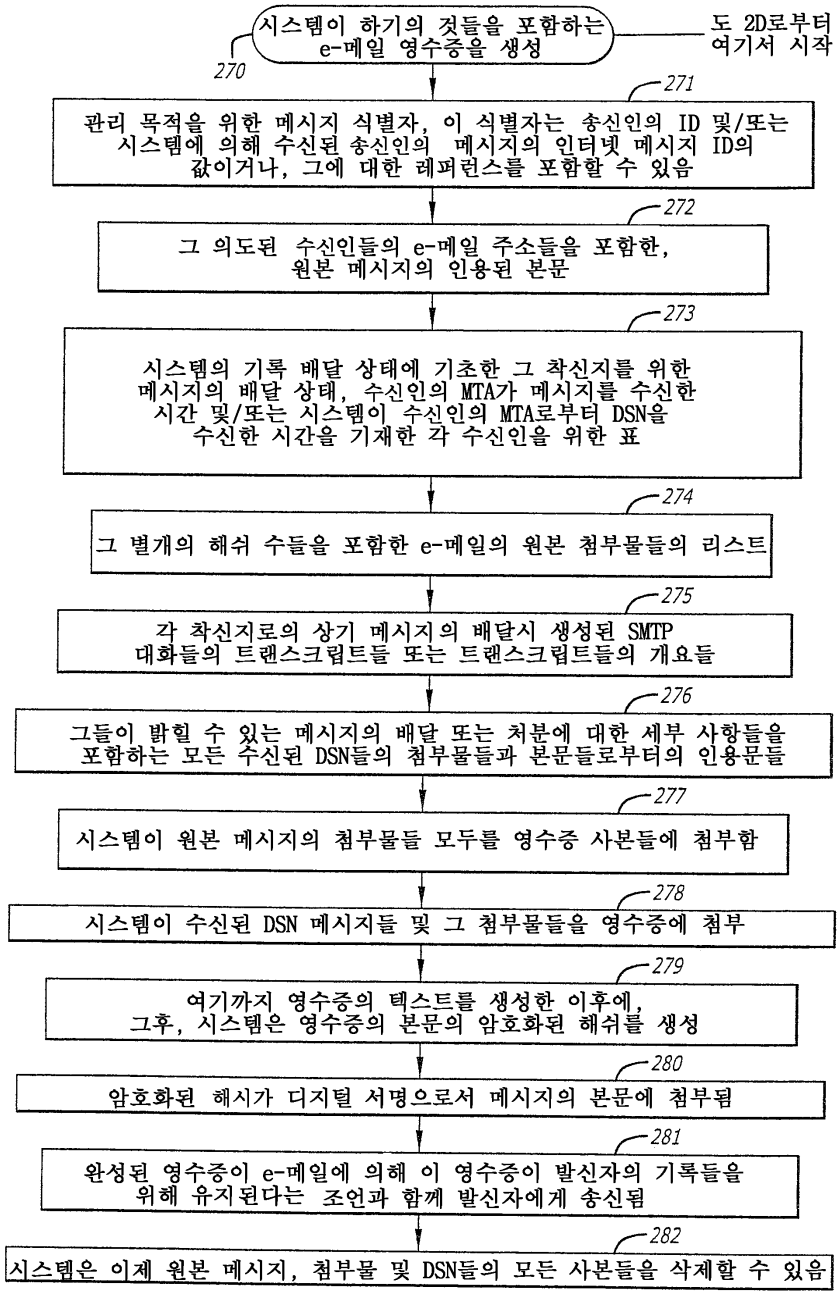
도면2C


시스템이 MTA 통지를 수신
240
시스템이 "rctp"를 포함하는 주소들에 대하여 rpost.com 으로 유입하는 메일을 조사
241
시스템이 "rcptxxxxy@rpost.com으로 보내진 메시지들을 메시지 xxxx의 착신지 y에 대한 배달 통지로서 식별함
242
시스템이 배달 실패, 중계 또는 성공을 나타내는 스트링들에 대한 메시지의 제목 및 본문을 조사
243
244
통지가 성공적 배달을 나타내는가 ?
YES
245
통지가 메시지 xxxx의 착신지 y의 배달 상태를 "우편함으로 배달 완료"로 변경
NO
246
통지가 배달 실패를 나타내는가 ?
YES
247
메시지 xxxx의 착신지 y의 배달 상태를 "실패"로 변경
NO
248
통지가 메시지의 전진 중계를 나타내는가 ?
YES
249
메시지 xxxx의 착신지 y의 배달 상태를 "중계 완료"로 변경
NO
250
MTA 통지 및 첨부물들의 사본들을 저장
처리 완료
251

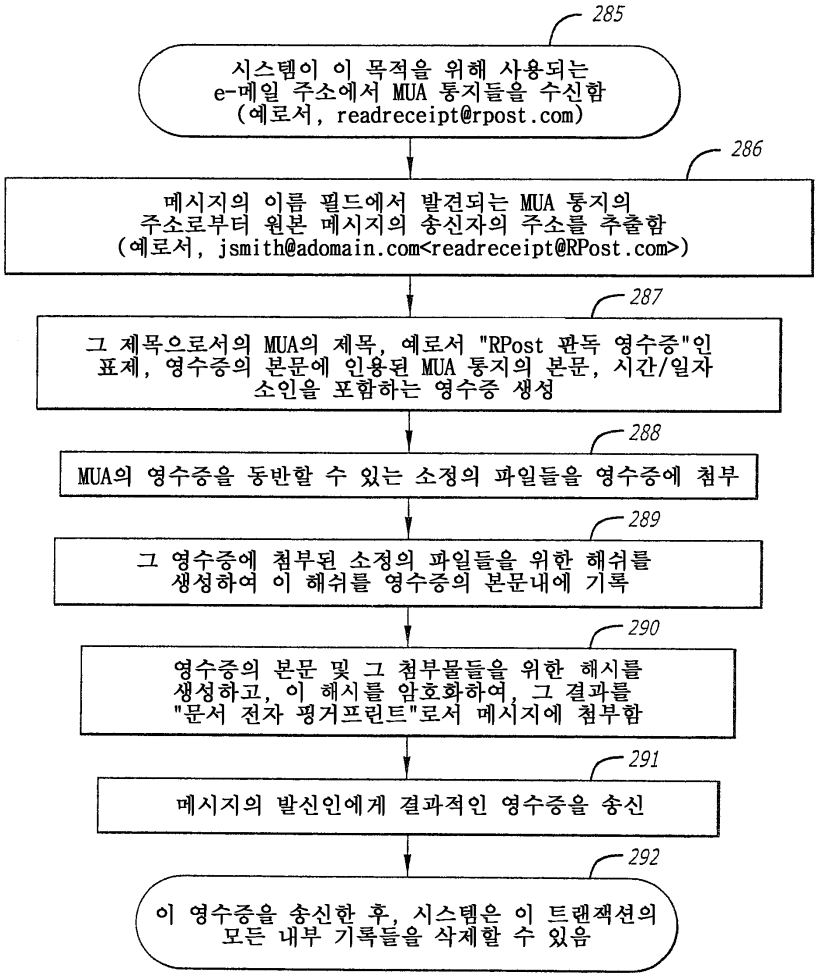
도면2D


때때로, 시스템이 모든 계류중인 메시지들의 상태를 검토
250
각 메시지에 대하여 시스템이 수행
251
각 착신지를 위한 착신지 상태(DS)를 검사
402
252
DS= "미송신"
YES
NO
254
DS="배달 완료 및 DSN 대기" ?
YES
253
배달후 24시간 경과?
NO
255
다음 메시지 검사
YES
NO
256
다음 착신지 취득
257
DS= "배달완료" ?
YES
NO
258
배달 이후 2시간 경과 ?
YES
NO
15(DS = "중계완료", "배달불가", "우편함으로 배달완료" 또는 "실패")
259
착신지들이 더 있는가?
YES
NO
260
배달 완료 및 영수증 생성(도 2E로 진행)

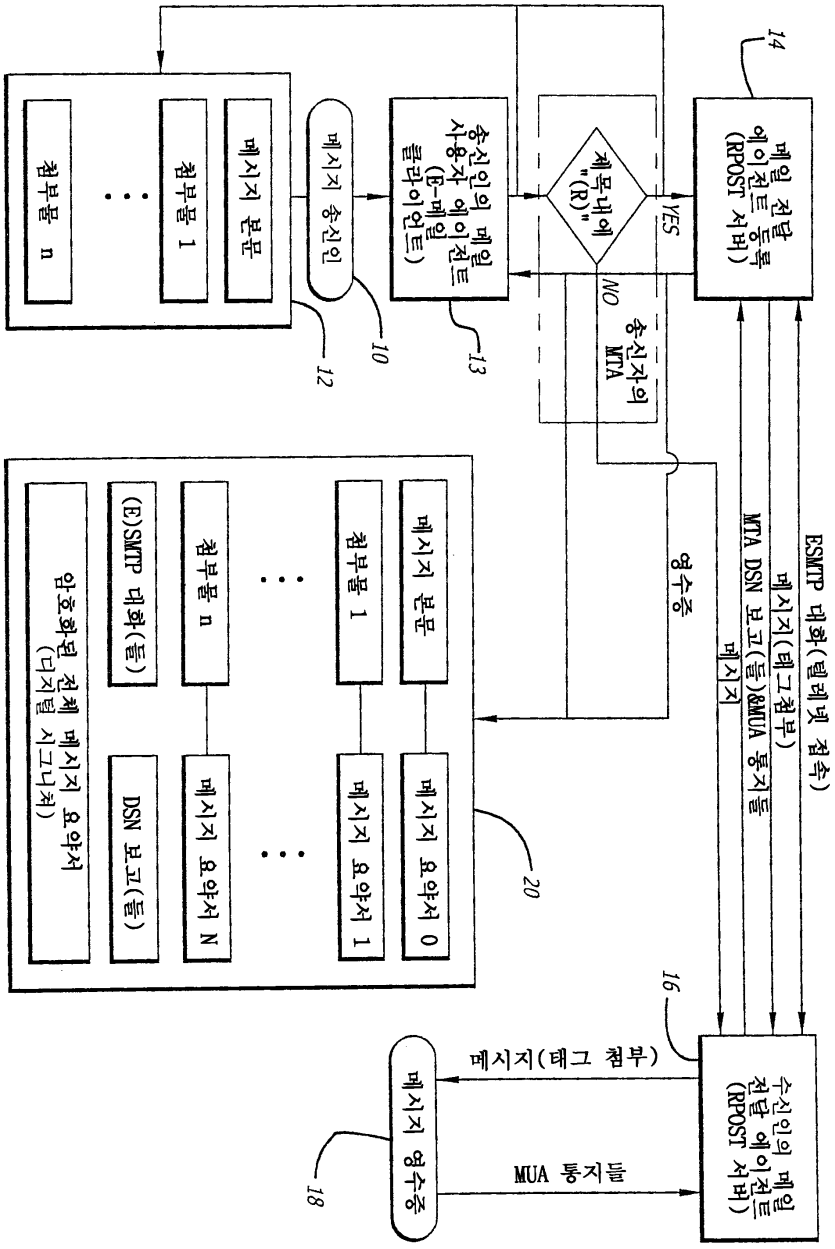
도면2E


시스템이 하기의 것들을 포함하는 e-메일 영수증을 생성
도 2D로부터 여기서 시작
270
271
관리 목적을 위한 메시지 식별자, 이 식별자는 송신인의 ID 및/또는 시스템에 의해 수신된 송신인의 메시지의 인터넷 메시지 ID의 값이거나, 그에 대한 레퍼런스를 포함할 수 있음
272
그 의도된 수신인들의 e-메일 주소들을 포함한, 원본 메시지의 인용된 본문
273
시스템의 기록 배달 상태에 기초한 그 착신지를 위한 메시지의 배달 상태, 수신인의 MTA가 메시지를 수신한 시간 및/또는 시스템이 수신인의 MTA로부터 DSN을 수신한 시간을 기재한 각 수신인을 위한 표
274
그 별개의 해쉬 수들을 포함한 e-메일의 원본 첨부물들의 리스트
275
각 착신지로의 상기 메시지의 배달시 생성된 SMTP 대화들의 트랜스크립트들 또는 트랜스크립트들의 개요들
276
그들이 밝힐 수 있는 메시지의 배달 또는 처분에 대한 세부 사항들을 포함하는 모든 수신된 DSN들의 첨부물들과 본문들로부터의 인용문들
277
시스템이 원본 메시지의 첨부물들 모두를 영수증 사본들에 첨부함
278
시스템이 수신된 DSN 메시지들 및 그 첨부물들을 영수증에 첨부
279
여기까지 영수증의 텍스트를 생성한 이후에, 그후, 시스템은 영수증의 본문의 암호화된 해쉬를 생성
280
암호화된 해시가 디지털 서명으로서 메시지의 본문에 첨부됨
281
완성된 영수증이 e-메일에 의해 이 영수증이 발신자의 기록들을 위해 유지된다는 조언과 함께 발신자에게 송신됨
282
시스템은 이제 원본 메시지, 첨부물 및 DSN들의 모든 사본들을 삭제할 수 있음

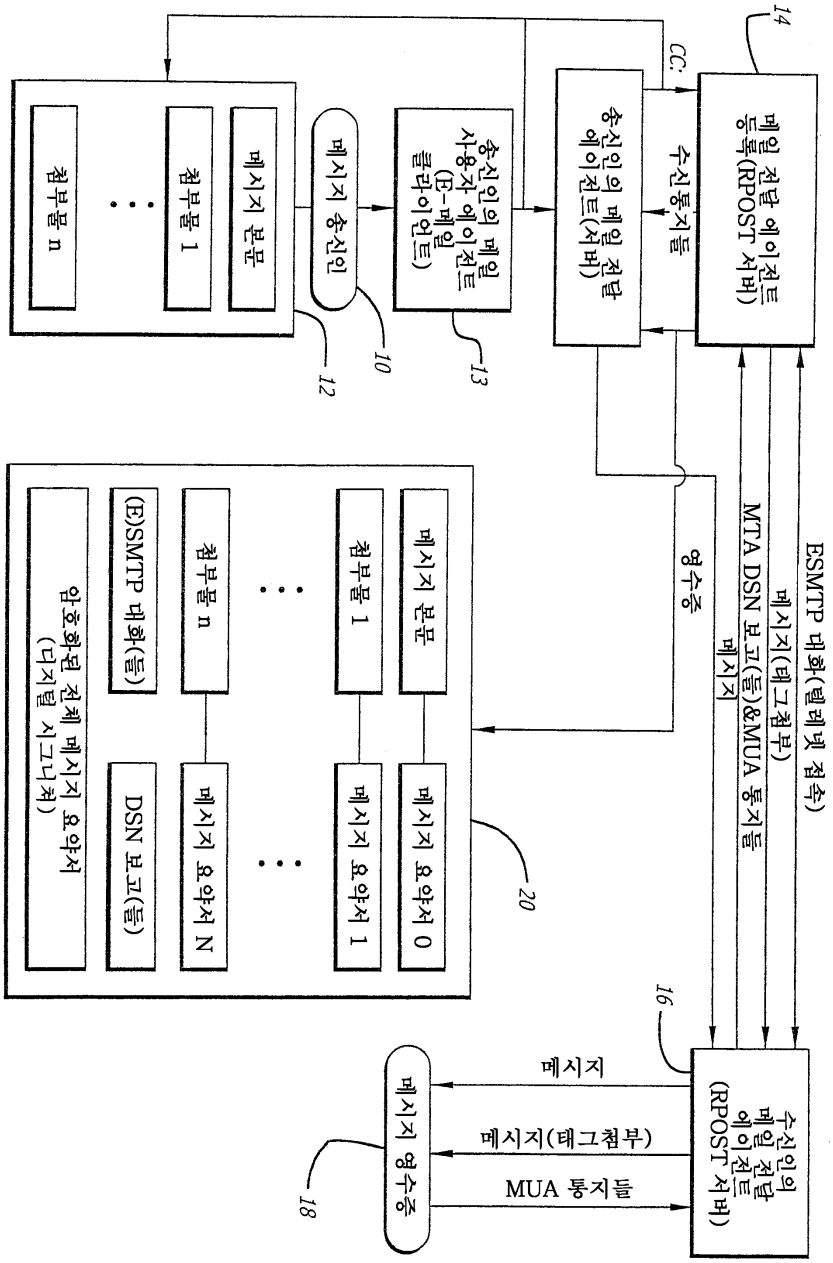
도면2F


285
시스템이 이 목적을 위해 사용되는 e-메일 주소에서 MUA 통지들을 수신함 (예로서, readreceipt@rpost.com)
286
메시지의 이름 필드에서 발견되는 MUA 통지의 주소로부터 원본 메시지의 송신자의 주소를 추출함 (예로서, jsmith@adomain.com<readreceipt@RPost.com>)
287
그 제목으로서의 MUA의 제목, 예로서 "RPost 판독 영수증"인 표제, 영수증의 본문에 인용된 MUA 통지의 본문, 시간/일자 소인을 포함하는 영수증 생성
288
MUA의 영수증을 동반할 수 있는 소정의 파일들을 영수증에 첨부
289
그 영수증에 첨부된 소정의 파일들을 위한 해쉬를 생성하여 이 해쉬를 영수증의 본문내에 기록
290
영수증의 본문 및 그 첨부물들을 위한 해시를 생성하고, 이 해시를 암호화하여, 그 결과를 "문서 전자 핑거프린트"로서 메시지에 첨부함
291
메시지의 발신인에게 결과적인 영수증을 송신
292
이 영수증을 송신한 후, 시스템은 이 트랜잭션의 모든 내부 기록들을 삭제할 수 있음

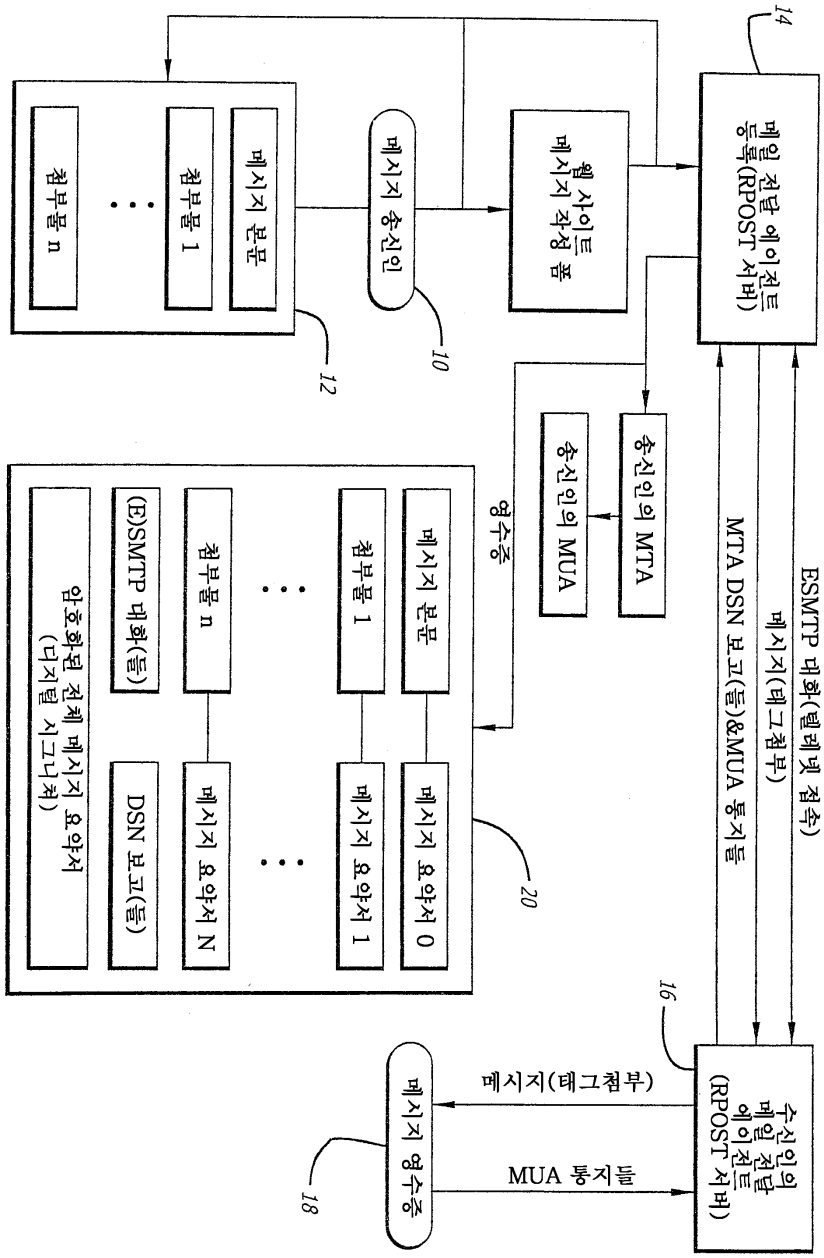
도면3


14
메일 전달 에이전트 등록 (RPOST 서버)
계속내에 "(R)"
YES
NO
송신자의 MTA
송신인의 메일 사용자 에이전트 (E-메일 클라이언트)
13
메시지 송신인
10
12
메시지 본문
첨부물 1
첨부물 n
ESMTP 대화(텔레넷 접속)
메시지(태그첨부)
MTA DSN 보고(들)&MUA 통지들
메시지
영수증
20
메시지 본문
첨부물 1
첨부물 n
메시지 요약서 0
메시지 요약서 1
메시지 요약서 N
(E)SMTP 대화(들)
DSN 보고(들)
암호화된 전체 메시지 요약서 (디지털 시그니쳐)
16
수신인의 메일 전달 에이전트 (RPOST 서버)
메시지(태그 첨부)
MUA 통지들
메시지 영수증
18

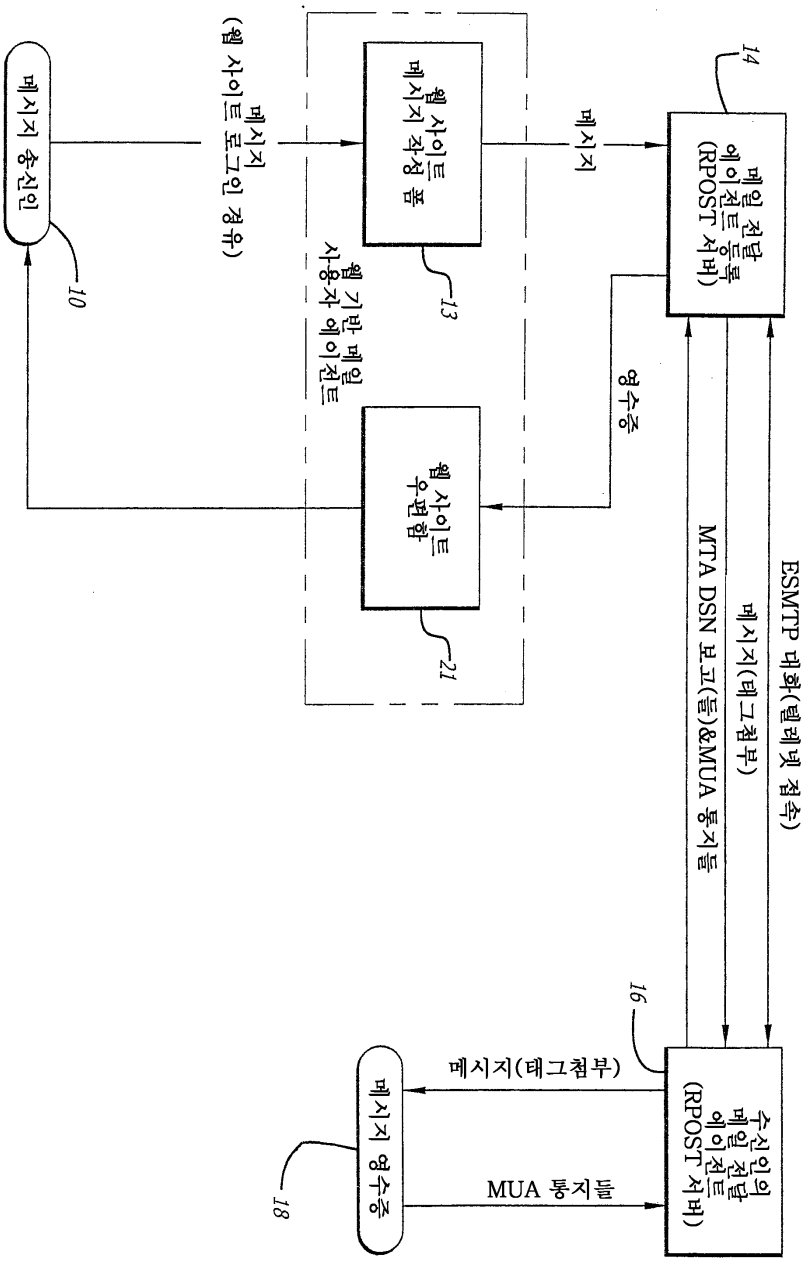
도면4


14
메일 전달 에이전트 등록(RPOST 서버)
CC:
수신통지들
송신인의 메일 전달 에이전트(서버)
송신인의 메일 사용자 에이전트 (E-메일 클라이언트)
13
메시지 송신인
10
메시지 본문
첨부물 1
첨부물 n
12
ESMTP 대화(텔레넷 접속)
메시지(태그첨부)
MTA DSN 보고(들)&MUA 통지들
메시지
영수증
20
메시지 요약서 0
메시지 요약서 1
메시지 요약서 N
DSN 보고(들)
암호화된 전체 메시지 요약서 (디지털 시그니쳐)
16
수신인의 메일 전달 에이전트 (RPOST 서버)
메시지
메시지(태그첨부)
MUA 통지들
메시지 영수증
18

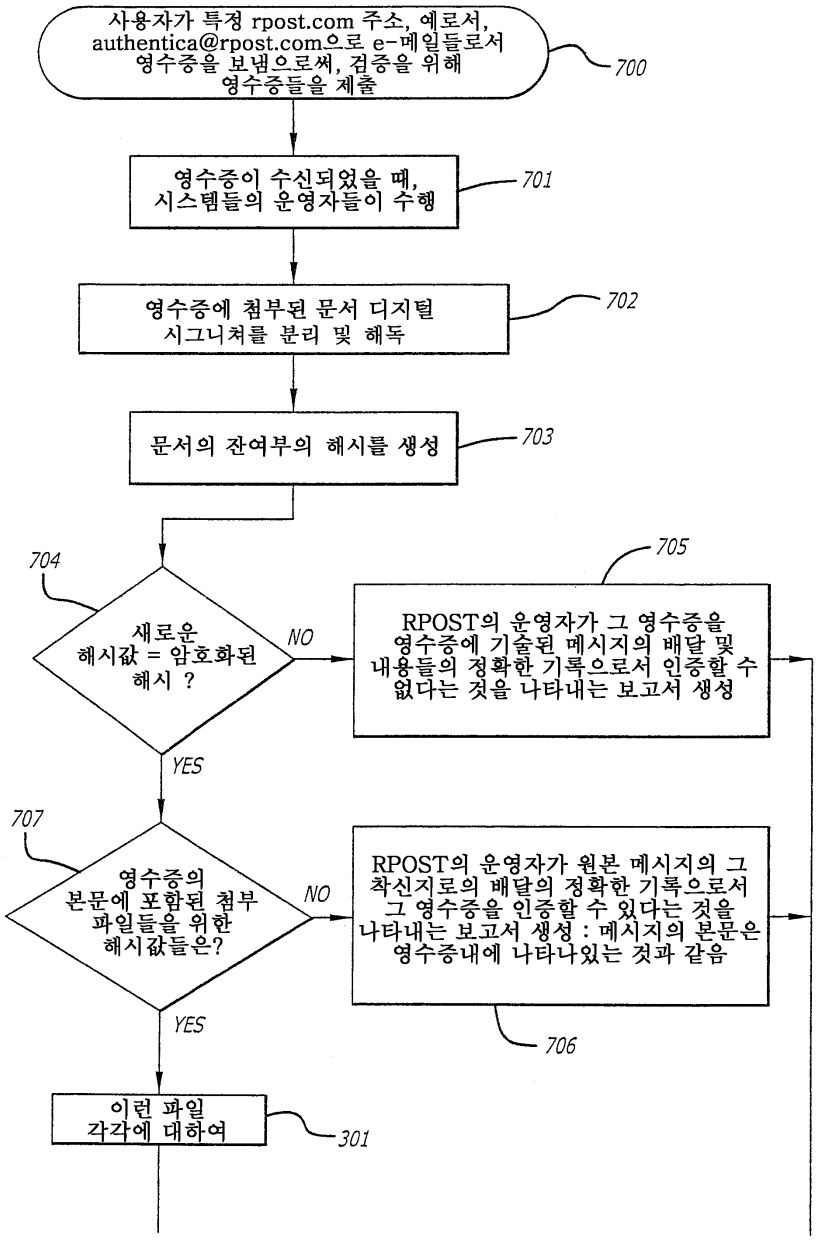
도면5


14
메일 전달 에이전트 등록(RPOST 서버)
웹 사이트 메시지 작성 폼
메시지 송신인
10
메시지 본문
첨부물 1
첨부물 n
12
송신인의 MTA
송신인의 MUA
영수증
20
메시지 본문
첨부물 1
첨부물 n
메시지 요약서 0
메시지 요약서 1
메시지 요약서 N
(E)SMTP 대화(들)
DSN 보고(들)
암호화된 전체 메시지 요약서 (디지털 시그니쳐)
ESMTP 대화(텔레넷 접속)
메시지(태그첨부)
MTA DSN 보고(들)&MUA 통지들
16
수신인의 메일 전달 에이전트 (RPOST 서버)
메시지(태그첨부)
MUA 통지들
메시지 영수증
18

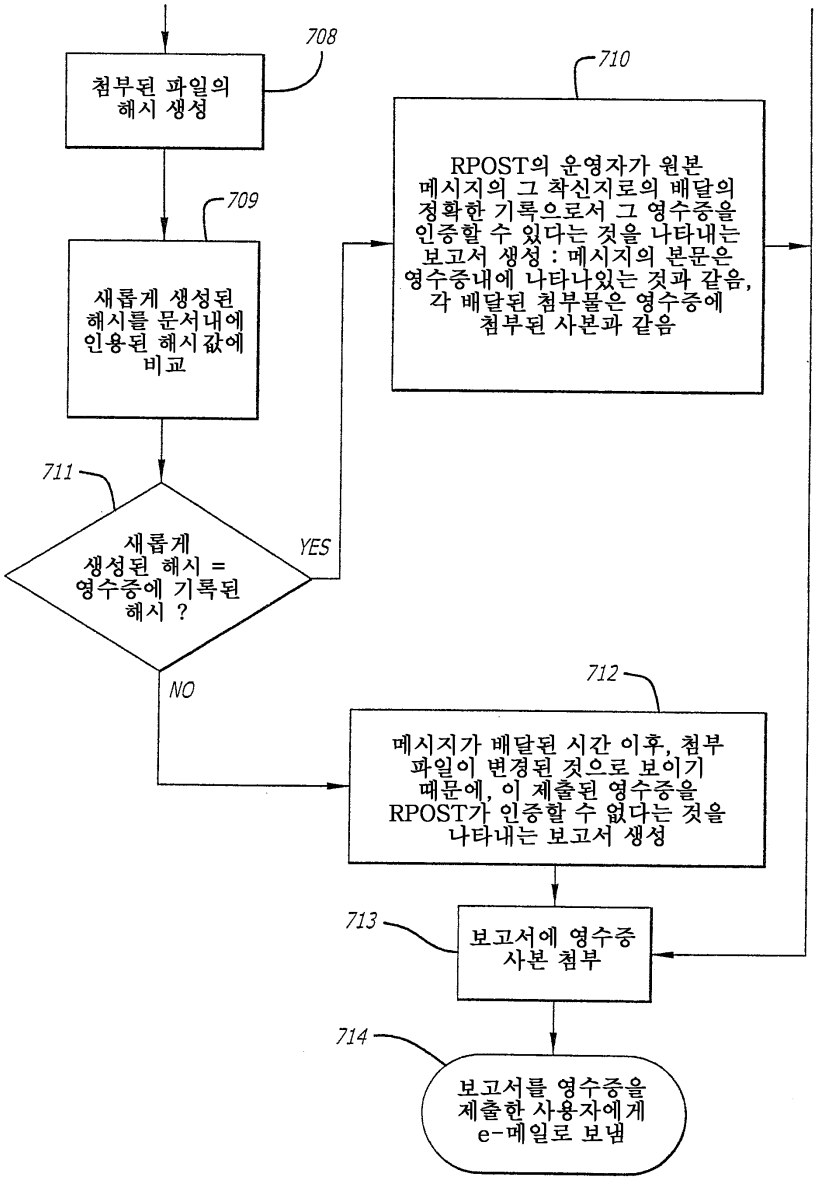
도면6


14
메일 전달 에이전트등록 (RPOST 서버)
메시지
웹 사이트 메시지 작성 폼
13
메시지 (웹 사이트 로그인 경유)
메시지 송신인
10
웹 기반 메일 사용자 에이전트
영수증
웹 사이트 우편함
21
ESMTP 대화(텔레넷 접속)
메시지(태그첨부)
MTA DSN 보고(들)&MUA 통지들
16
수신인의 메일 전달 에이전트 (RPOST 서버)
메시지(태그첨부)
MUA 통지들
메시지 영수증
18

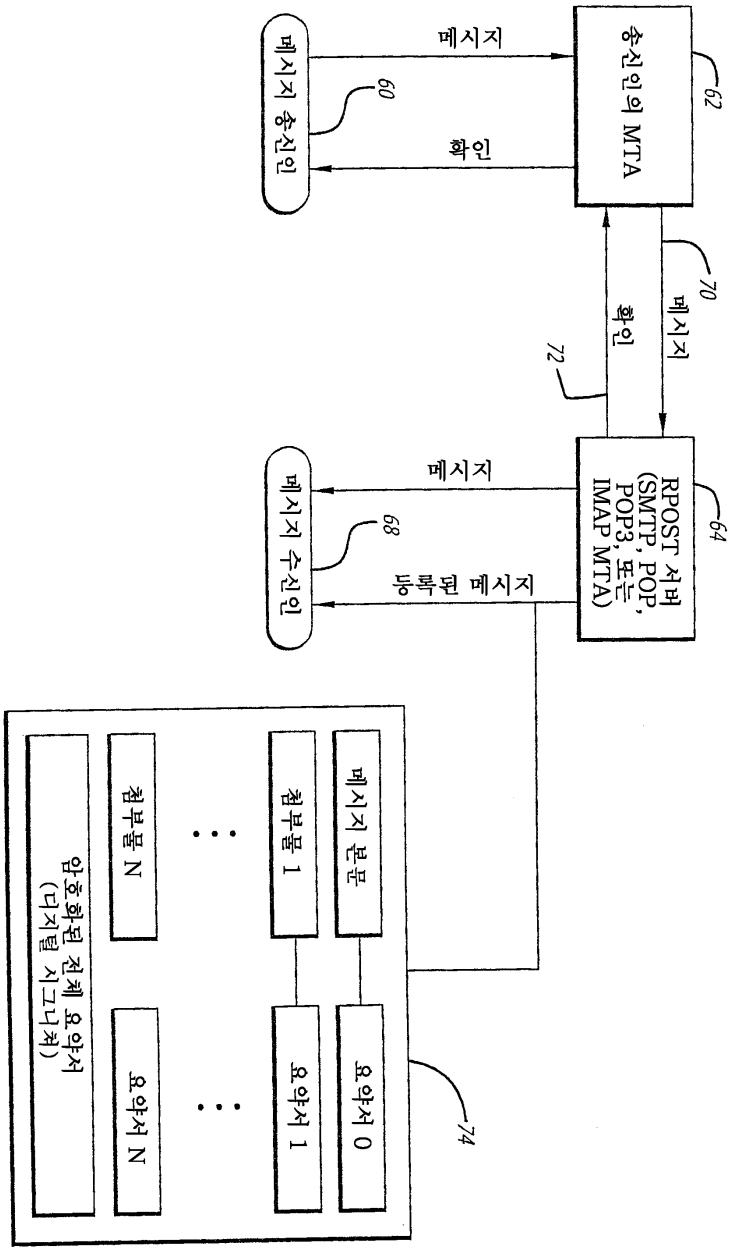
도면7A


사용자가 특정 rpost.com 주소, 예로서, authentica@rpost.com으로 e-메일들로서 영수증을 보냄으로써, 검증을 위해 영수증들을 제출
700
영수증이 수신되었을 때, 시스템들의 운영자들이 수행
701
영수증에 첨부된 문서 디지털 시그니쳐를 분리 및 해독
702
문서의 잔여부의 해시를 생성
703
704
새로운 해시값 = 암호화된 해시 ?
NO
705
RPOST의 운영자가 그 영수증을 영수증에 기술된 메시지의 배달 및 내용들의 정확한 기록으로서 인증할 수 없다는 것을 나타내는 보고서 생성
YES
707
영수증의 본문에 포함된 첨부 파일들을 위한 해시값들은?
NO
RPOST의 운영자가 원본 메시지의 그 착신지로의 배달의 정확한 기록으로서 그 영수증을 인증할 수 있다는 것을 나타내는 보고서 생성 : 메시지의 본문은 영수증내에 나타나있는 것과 같음
706
YES
이런 파일 각각에 대하여
301

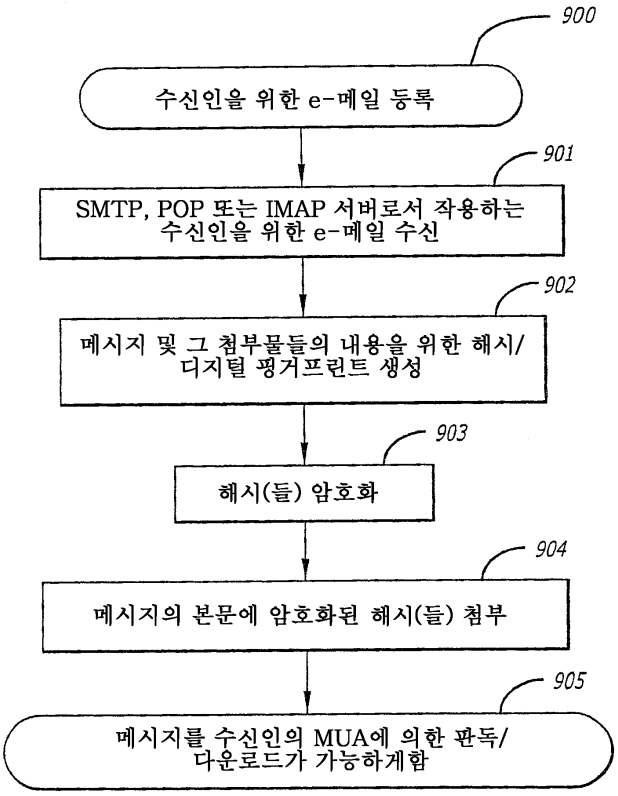
도면7B


708
첨부된 파일의 해시 생성
709
새롭게 생성된 해시를 문서내에 인용된 해시값에 비교
711
새롭게 생성된 해시 = 영수증에 기록된 해시 ?
YES
NO
710
RPOST의 운영자가 원본 메시지의 그 착신지로의 배달의 정확한 기록으로서 그 영수증을 인증할 수 있다는 것을 나타내는 보고서 생성 : 메시지의 본문은 영수증내에 나타나있는 것과 같음, 각 배달된 첨부물은 영수증에 첨부된 사본과 같음
712
메시지가 배달된 시간 이후, 첨부 파일이 변경된 것으로 보이기 때문에, 이 제출된 영수증을 RPOST가 인증할 수 없다는 것을 나타내는 보고서 생성
713
보고서에 영수증 사본 첨부
714
보고서를 영수증을 제출한 사용자에게 e-메일로 보냄

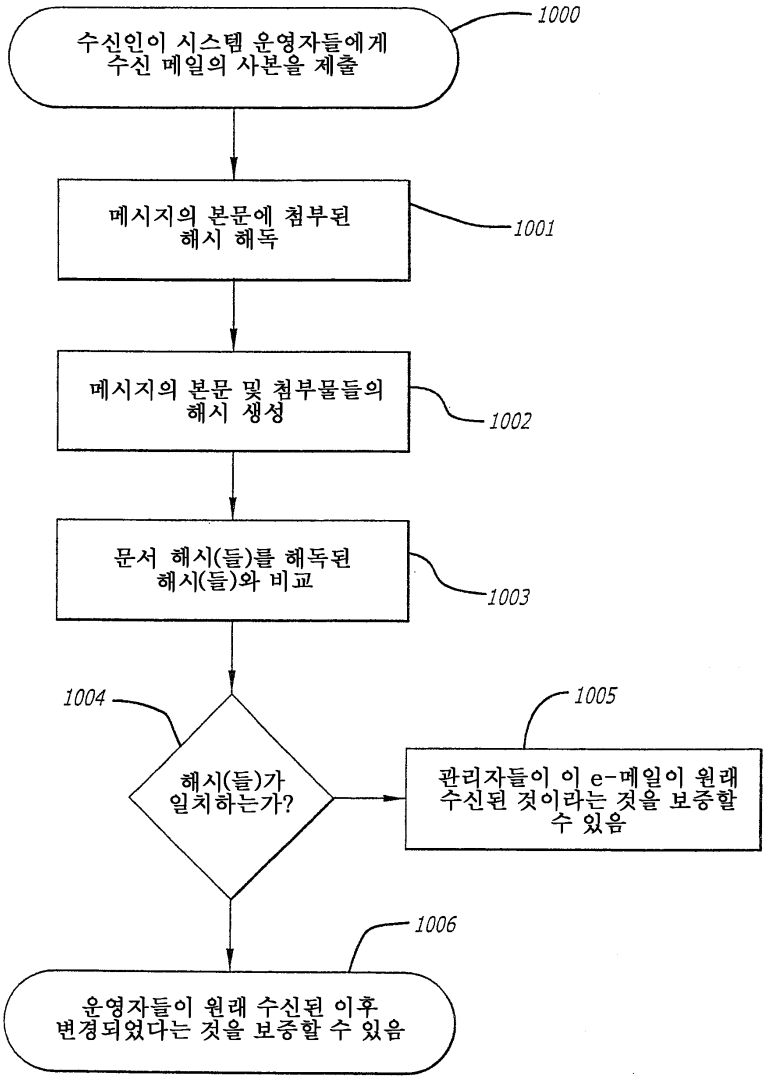
도면8


메시지
메시지 송신인
60
확인
송신인의 MTA
62
70
메시지
확인
72
메시지
메시지 수신인
68
등록된 메시지
RPOST 서버
(SMTP, POP,
POP3, 또는
IMAP MTA)
64
메시지 본문
첨부물 1
첨부물 N
요약서 0
요약서 1
요약서 N
암호화된 전체 요약서
(디지털 시그니쳐)
74

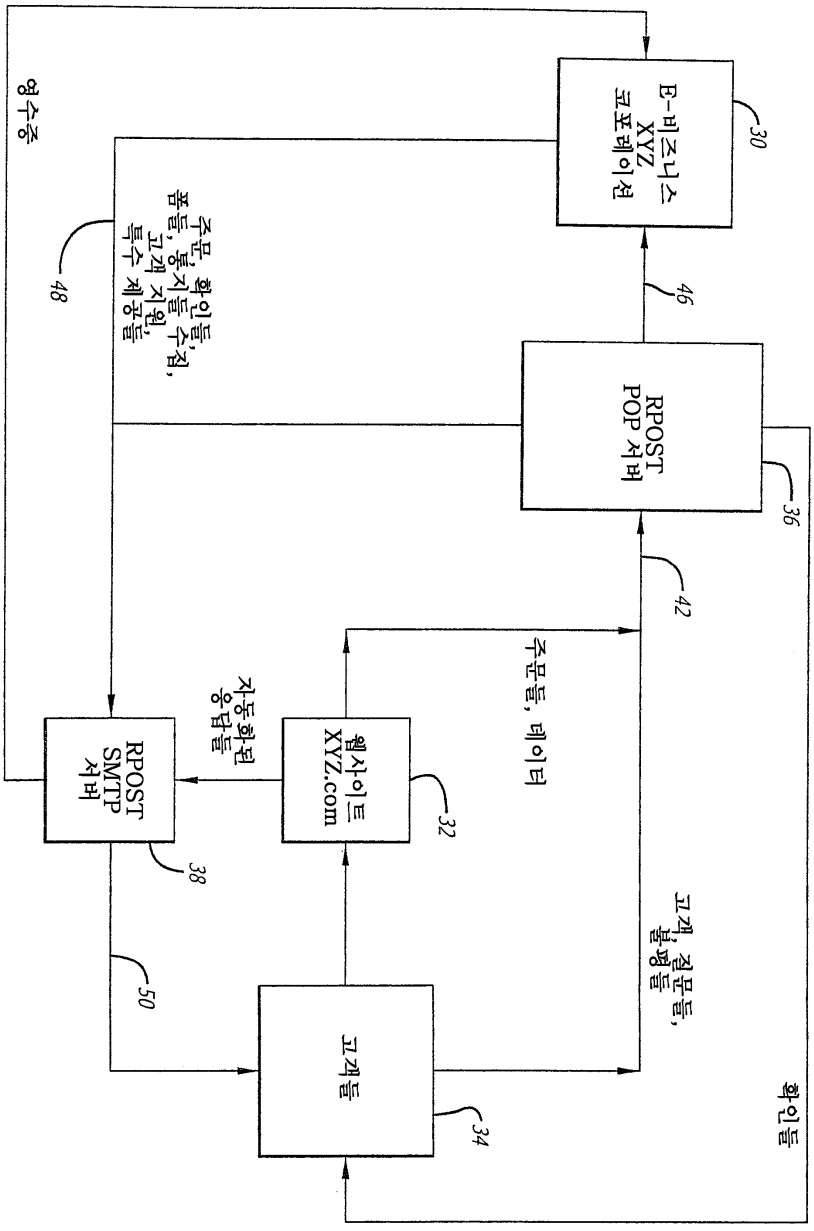
도면9


900
수신인을 위한 e-메일 등록
901
SMTP, POP 또는 IMAP 서버로서 작용하는 수신인을 위한 e-메일 수신
902
메시지 및 그 첨부물들의 내용을 위한 해시/디지털 핑거프린트 생성
903
해시(들) 암호화
904
메시지의 본문에 암호화된 해시(들) 첨부
905
메시지를 수신인의 MUA에 의한 판독/다운로드가 가능하게함

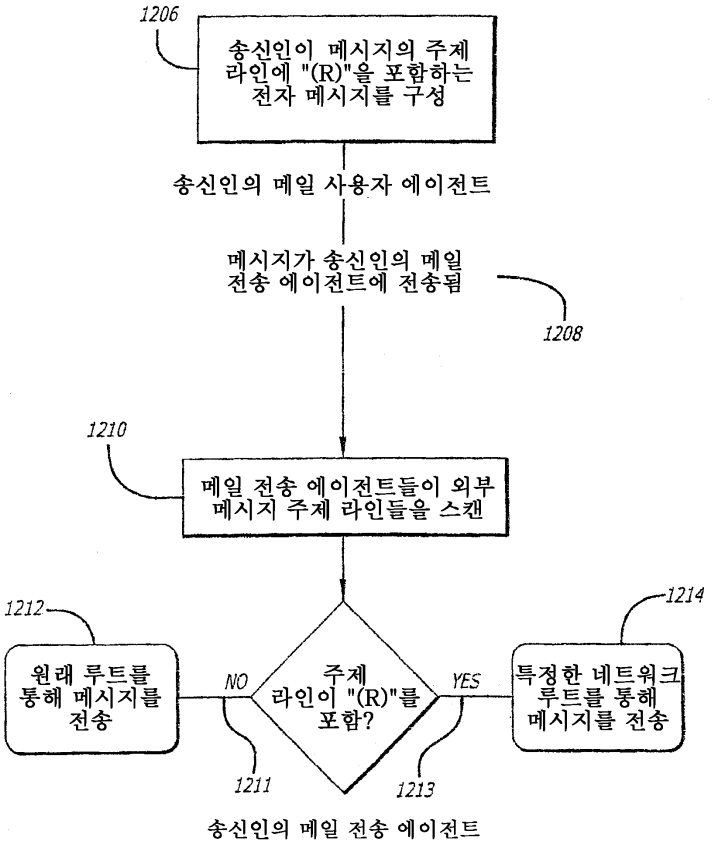
도면10


수신인이 시스템 운영자들에게 수신 메일의 사본을 제출
1000
메시지의 본문에 첨부된 해시 해독
1001
메시지의 본문 및 첨부물들의 해시 생성
1002
문서 해시(들)를 해독된 해시(들)와 비교
1003
1004
해시(들)가 일치하는가?
1005
관리자들이 이 e-메일이 원래 수신된 것이라는 것을 보증할 수 있음
1006
운영자들이 원래 수신된 이후 변경되었다는 것을 보증할 수 있음

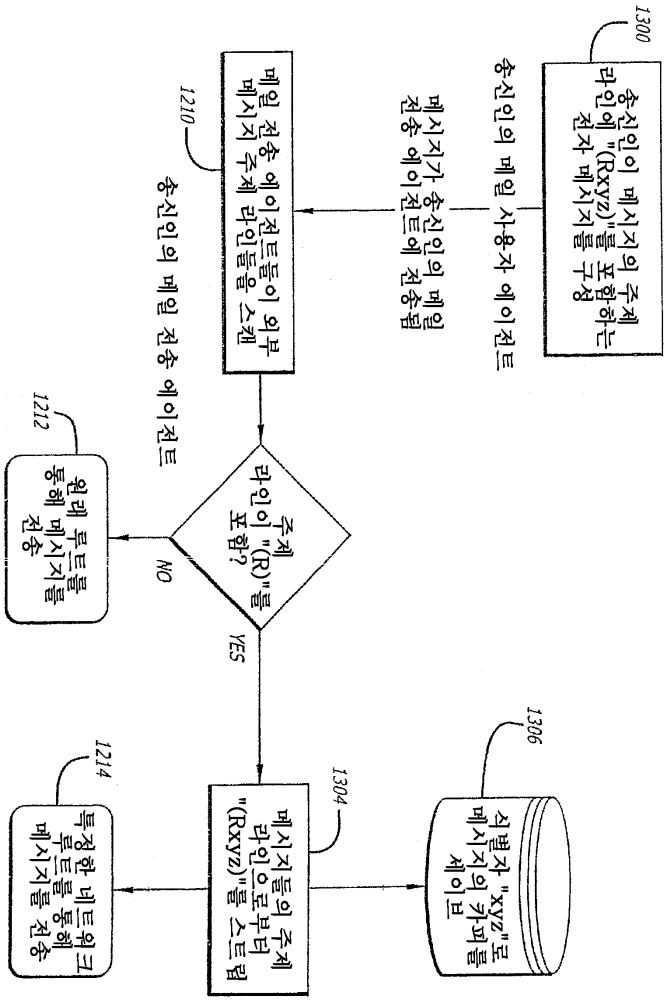
도면11


E-비즈니스 XYZ 코포레이션
30
영수증
주문, 확인들, 품들, 꽃지들 수집, 고객 지원, 특수 제공들
48
46
RPOST POP 서버
36
42
주문들, 데이터
자동화된 응답들
웹사이트 XYZ.com
32
RPOST SMTP 서버
38
50
고객들
34
고객 질문들, 불평들
확인들

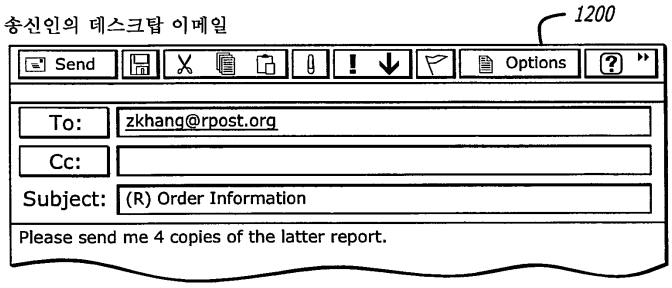
도면12


1206
송신인이 메시지의 주제 라인에 "(R)"을 포함하는 전자 메시지를 구성
송신인의 메일 사용자 에이전트
메시지가 송신인의 메일 전송 에이전트에 전송됨
1208
1210
메일 전송 에이전트들이 외부 메시지 주제 라인들을 스캔
1212
원래 루트를 통해 메시지를 전송
NO
주제 라인이 "(R)"를 포함?
YES
1214
특정한 네트워크 루트를 통해 메시지를 전송
1211
1213
송신인의 메일 전송 에이전트

도면13


1300
송신인이 메시지의 주제 라인에 "(Rxyz)"를 포함하는 전자 메시지를 구성
송신인의 메일 사용자 에이전트
메시지가 송신인의 메일 전송 에이전트에 전송됨
1210
메일 전송 에이전트들이 외부 메시지 주제 라인들을 스캔
송신인의 메일 전송 에이전트
주제 라인이 "(R)"를 포함?
YES
NO
1212
원래 루트를 통해 메시지를 전송
1304
메시지들의 주제 라인으로부터 "(Rxyz)"를 스트립
1306
식별자 "xyz"로 메시지의 카피를 세이브
1214
특정한 네트워크 루트를 통해 메시지를 전송

도면14


송신인의 데스크탑 이메일
1200
Send
Options
To:
zkhang@rpost.org
Cc:
Subject:
(R) Order Information
Please send me 4 copies of the latter report.