(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0095860
(43) 공개일자 2014년08월04일

(51) 국제특허분류(Int. Cl.)
G06Q 50/28 (2012.01)
(21) 출원번호 10-2013-0008766
(22) 출원일자 2013년01월25일
심사청구일자 2013년01월25일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
이동훈
서울 종로구 사직로8길 34, 1404호 (내수동, 경희궁의아침3단지)
최민석
서울 성북구 안암로 145, 정보보호대학원 (안암동5가, 고려대학교)
(뒷면에 계속)
(74) 대리인
특허법인충현

전체 청구항 수 : 총 5 항

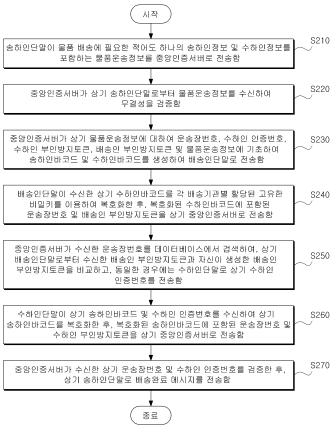
(54) 발명의 명칭 **개인정보 보호를 위한 물류 운송 방법**

(57) 요 약

본 발명은 개인정보 보호를 위한 물류 운송 방법에 관한 것으로, 보다 구체적으로는 송하인단말이 물품 배송에 필요한 적어도 하나의 송하인정보 및 수하인정보를 포함하는 물품운송정보를 중앙인증서버로 전송하는 단계; 상기 중앙인증서버가 상기 송하인단말로부터 물품운송정보를 수신하여 무결성을 검증하는 단계; 상기 중앙인증서버가 상기 물품운송정보에 대하여 운송장번호, 수하인 인증번호, 수하인 부인방지토큰, 배송인 부인방지토큰 및 물품운송정보에 기초하여 송하인바코드 및 수하인바코드를 생성하여 배송인단말로 전송하는 단계; 상기 배송인단말이 수신한 상기 수하인바코드를 각 배송기관별 할당된 고유한 비밀키를 이용하여 복호화한 후, 복호화된 수하인바코드에 포함된 운송장번호 및 배송인 부인방지토큰을 상기 중앙인증서버로 전송하는 단계; 상기 중앙인증서버가 수신한 운송장번호를 데이터베이스에서 검색하여, 상기 배송인단말로부터 수신한 배송인 부인방지토큰과 자신이 생성한 배송인 부인방지토큰을 비교하고, 동일한 경우에는 수하인단말로 상기 수하인 인증번호를 전송하는 단계; 상기 수하인단말이 상기 송하인바코드 및 수하인 인증번호를 수신하여 상기 송하인바코드를 복호화한 후, 복호화된 송하인바코드에 포함된 운송장번호 및 수하인 부인방지토큰을 상기 중앙인증서버로 전송하는 단계; 및 상기 중앙인증서버가 수신한 상기 운송장번호 및 수하인 인증번호를 검증한 후, 상기 송하인단말로 배송완료 메시지를 전송하는 단계;를 포함한다.

이러한 구성에 의해, 본 발명의 개인정보 보호를 위한 물류 운송 방법은 물류 운송 시, 물품을 보내는 송하인 또는 물품을 받는 수하인의 개인정보가 외부로 노출되는 것을 방지하여, 사용자의 개인정보를 용이하게 보호할 수 있는 효과가 있다.

대 표 도 - 도1



(72) 발명자

조관태

서울 노원구 동일로184길 13-6, 2층 (공릉동)

박진형

서울 성북구 안암로 145, 정보보호대학원 (안암동5가, 고려대학교)

이 발명을 지원한 국가연구개발사업

과제고유번호	H2101-12-1001
부처명	지식경제부
연구사업명	지식정보 보안 인력양성
연구과제명	지식정보 보안 인력양성
기 여 율	1/1
주관기관	고려대학교
연구기간	2013.01.01 ~ 2013.12.01

특허청구의 범위

청구항 1

송하인단말이 물품 배송에 필요한 적어도 하나의 송하인정보 및 수하인정보를 포함하는 물품운송정보를 중앙인증서버로 전송하는 단계;

상기 중앙인증서버가 상기 송하인단말로부터 물품운송정보를 수신하여 무결성을 검증하는 단계;

상기 중앙인증서버가 상기 물품운송정보에 대하여 운송장번호, 수하인 인증번호, 수하인 부인방지토큰, 배송인 부인방지토큰 및 물품운송정보에 기초하여 송하인바코드 및 수하인바코드를 생성하여 배송인단말로 전송하는 단계;

상기 배송인단말이 수신한 상기 수하인바코드를 각 배송기관별 할당된 고유한 비밀키를 이용하여 복호화한 후, 복호화된 수하인바코드에 포함된 운송장번호 및 배송인 부인방지토큰을 상기 중앙인증서버로 전송하는 단계;

상기 중앙인증서버가 수신한 운송장번호를 데이터베이스에서 검색하여, 상기 배송인단말로부터 수신한 배송인 부인방지토큰과 자신이 생성한 배송인 부인방지토큰을 비교하고, 동일한 경우에는 수하인단말로 상기 수하인 인증번호를 전송하는 단계;

상기 수하인단말이 상기 송하인바코드 및 수하인 인증번호를 수신하여 상기 송하인바코드를 복호화한 후, 복호화된 송하인바코드에 포함된 운송장번호 및 수하인 부인방지토큰을 상기 중앙인증서버로 전송하는 단계; 및

상기 중앙인증서버가 수신한 상기 운송장번호 및 수하인 인증번호를 검증한 후, 상기 송하인단말로 배송완료 메시지를 전송하는 단계;

를 포함하는 개인정보 보호를 위한 물류 운송 방법.

청구항 2

제1항에 있어서,

상기 수하인 부인방지토큰은 수하인정보, 운송장번호, 서비스 요청 시간정보를 중앙인증서버용 비밀키를 이용하여 암호화된 메시지 인증 코드(MAC: Message Authentication)이고,

상기 배송인 부인방지토큰은 송하인정보, 운송장번호, 서비스 요청 시간정보를 중앙인증서버용 비밀키를 이용하여 암호화된 메시지 인증 코드인 것을 특징으로 하는 개인정보 보호를 위한 물류 운송 방법.

청구항 3

제1항에 있어서,

상기 송하인바코드는

상기 운송장번호, 수하인 부인방지토큰 및 상기 물품운송정보를 상기 수하인 인증번호를 이용하여 암호화된 것을 특징으로 하는 개인정보 보호를 위한 물류 운송 방법.

청구항 4

제1항에 있어서,

상기 수하인바코드는

상기 운송장번호, 배송인 부인방지토크 및 물품운송정보를 각 배송기관별로 할당된 고유한 비밀키로 암호화된 것을 특징으로 하는 개인정보 보호를 위한 물류 운송 방법.

청구항 5

제1항 내지 제4항 중 어느 한 항에 따른 방법을 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독가능 기록매체.

명 세 서

기 술 분 야

[0001] 본 발명은 개인정보 보호를 위한 물류 운송 방법에 관한 것으로, 특히 물류 운송 시, 물품을 보내는 송하인 또는 물품을 받는 수하인의 개인정보가 외부로 노출되는 것을 방지할 수 있는 개인정보 보호를 위한 물류 운송 방법에 관한 것이다.

배 경 기 술

[0002] 인터넷이 널리 보급됨에 따라, 온라인 시장이 활발하게 되어, 남녀노소를 불문하고, 많은 사람들이 온라인 쇼핑을 널리 이용하고 있다. 이에 따라, 사용자가 온라인 쇼핑을 통해 구매한 물품이 택배 등을 통해 운송이 이루어지고 있다.

[0003] 이러한 물류운송형태는 물품을 보내는 사람 즉, 송하인 또는 해당 물품을 받는 사람 즉, 수하인 등의 개인정보가 보내고자 하는 물품의 외관에 부착되는 운송장을 통해 노출되고 있는 실정이다. 상기 운송장에는 송하인 및 수하인의 휴대전화번호, 자택주소, 사무실주소, 이메일주소 뿐만 아니라, 구매한 물품의 이름, 가격, 구매일자 등이 기재되어 있다. 그러므로, 물품의 배송 시, 운송장이 외부로 노출되거나, 수하인에게 정상적으로 물품의 배송이 완료되었다고 해도 운송장 폐기와 관련한 문제점이 발생했다.

[0004] 뿐만 아니라, 물품의 출고부터 배송 시, 물품의 분실 또는 배송오류가 발생하는 경우, 사고원인과 책임을 정확하게 파악하기 어려운 문제점이 발생했다.

[0005] 상술한 바와 같이, 개인정보 보호를 위한 물류 운송 방법을 살펴보면 다음과 같다.

[0006] 선행기술 1은 한국등록특허공보 제0757159호(2007.09.03)로서, 피오에스 택배용 운송장에 관한 것이다. 이러한 선행기술 1은 소정의 이미지 또는 문구가 표시되는 광고 인쇄부와; 발송일, 운송장 번호, 분류코드, 바코드, 도착지터미널 코드 등이 기재되는 택배업체용 배달정보부와; 수하인 및 송하인 정보가 기재되는 수하인용 정보부와; 택배 운송장을 상부 및 하부의 반으로 나누어 접을 수 있으며, 배송완료시 절취 가능하도록 형성된 절취부와; 물품 정보, 운송장 번호, 수하인 및 송하인 정보, 운송료 정보 등이 기재되는 회수용 송수하인 정보부와; 택배 물품을 전달받은 인수자가 기명 날인하는 인수자 서명부를 포함하고, 영수증 프린터를 사용하여 한 장의 인쇄면에 택배 운송장 정보를 인쇄하며, 소화물 박스에 부착되는 박스부착용 투명봉투 내에 삽입된다. 따라서, 본 발명은 택배 운송장의 원가를 크게 줄일 수 있고, 소화물 박스에 부착되는 박스부착용 투명봉투에 편리하게 넣어 사용할 수 있음은 물론, 회수용 운송장을 편리하게 회수할 수 있으며, 택배 운송장에 삽입된 광고를 통해 광고효율을 극대화할 수 있는 효과를 제공한다.

[0007] 또한, 선행기술 2는 한국공개특허공보 제2008-0001389호(2008.01.03)로서, 알에프 아이디를 이용한 택배 보관 및 수령 시스템과 방법에 관한 것이다. 이러한 선행기술 2는 RFID Reader, 데이터 변환부, 제어부, 잠금장치, 배송자의 휴대단말에 상품의 정보를 송신할 수 있는 송신기를 포함하는 택배보관함과; 상기 택배보관함에 보관되어 있는 상품의 정보를 수신하고, 상기 수신된 정보를 내장되어 있는 RFID Writable Tag에 쓸 수 있는 RFID Writer를 포함하고 있는 휴대단말을 포함하고; 상기 택배보관함은 상기 RFID Reader를 통하여 상기 휴대단말의 RFID Writable Tag의 정보를 수신한 뒤 상기 수신된 정보와 보관되어 있는 상품의 정보를 비교 판단함으로써 택배보관함의 상기 잠금장치의 개폐여부를 결정함으로써, 구매자가 부재중이더라도 상품을 안전하게 보관할 수 있고, 이를 통하여 구매자에게 안전하게 택배 상품을 전달할 수 있는 이점이 있다.

발명의 내용

해결하려는 과제

[0008] 상기와 같은 종래 기술의 문제점을 해결하기 위해, 본 발명은 물류 운송 서비스를 이용하고자 하는 송하인 또는 수하인의 정보가 외부로 노출되는 것을 막아 사용자의 사생활 침해방지를 수행할 수 있는 개인정보 보호를 위한 물류 운송 방법을 제공하고자 한다.

[0009] 또한, 상기와 같은 종래 기술의 문제점을 해결하기 위해, 본 발명은 물류 운송 중 분실 또는 물품의 미수신 등의 사고가 발생하는 경우, 사고원인 및 책임을 명확히 할 수 있는 개인정보 보호를 위한 물류 운송 방법을 제공하고자 한다.

과제의 해결 수단

[0010] 위와 같은 과제를 해결하기 위한 본 발명의 한 실시 예에 따른 개인정보 보호를 위한 물류 운송 방법은 송하인 단말이 물품 배송에 필요한 적어도 하나의 송하인정보 및 수하인정보를 포함하는 물품운송정보를 중앙인증서버로 전송하는 단계; 상기 중앙인증서버가 상기 송하인단말로부터 물품운송정보를 수신하여 무결성을 검증하는 단계; 상기 중앙인증서버가 상기 물품운송정보에 대하여 운송장번호, 수하인 인증번호, 수하인 부인방지토큰, 배송인 부인방지토큰 및 물품운송정보에 기초하여 송하인바코드 및 수하인바코드를 생성하여 배송인단말로 전송하는 단계; 상기 배송인단말이 수신한 상기 수하인바코드를 각 배송기관별 할당된 고유한 비밀키를 이용하여 복호화한 후, 복호화된 수하인바코드에 포함된 운송장번호 및 배송인 부인방지토큰을 상기 중앙인증서버로 전송하는 단계; 상기 중앙인증서버가 수신한 운송장번호를 데이터베이스에서 검색하여, 상기 배송인단말로부터 수신한 배송인 부인방지토큰과 자신이 생성한 배송인 부인방지토큰을 비교하고, 동일한 경우에는 수하인단말로 상기 수하인 인증번호를 전송하는 단계; 상기 수하인단말이 상기 송하인바코드 및 수하인 인증번호를 수신하여 상기 송하인바코드를 복호화한 후, 복호화된 송하인바코드에 포함된 운송장번호 및 수하인 부인방지토큰을 상기 중앙인증서버로 전송하는 단계; 및 상기 중앙인증서버가 수신한 상기 운송장번호 및 수하인 인증번호를 검증한 후, 상기 송하인단말로 배송완료 메시지를 전송하는 단계; 를 포함한다.

[0011] 보다 바람직하게는 수하인정보, 운송장번호, 서비스 요청 시간정보를 중앙인증서버용 비밀키를 이용하여 암호화된 메시지 인증 코드(MAC: Message Authentication)인 수하인 부인방지토큰을 포함할 수 있고, 송하인정보, 운송장번호, 서비스 요청 시간정보를 중앙인증서버용 비밀키를 이용하여 암호화된 메시지 인증 코드인 배송인 부인방지토큰을 포함할 수 있다.

[0012] 특히, 상기 운송장번호, 수하인 부인방지토큰 및 상기 물품운송정보를 상기 수하인 인증번호를 이용하여 암호화되는 송하인바코드를 포함할 수 있다.

[0013] 특히, 상기 운송장번호, 배송인 부인방지토크 및 물품운송정보를 각 배송기관별로 할당된 고유한 비밀키로 암호화되는 수하인바코드를 포함할 수 있다.

발명의 효과

[0014] 본 발명의 개인정보 보호를 위한 물류 운송 방법은 물류 운송 시, 물품을 보내는 송하인 또는 물품을 받는 수하인의 개인정보가 외부로 노출되는 것을 방지하여, 사용자의 개인정보를 보호할 수 있는 효과가 있다.

[0015] 또한 본 발명의 개인정보 보호를 위한 물류 운송 방법은 배송인 부인방지토큰 및 수하인 부인방지토큰을 각각 비교함으로써, 물류 운송 중 물품의 미수신, 분실 등의 사고가 발생하는 경우, 사고원인 및 책임을 명확히 할 수 있는 효과가 있다.

도면의 간단한 설명

[0016] 도 1은 본 발명의 일 실시 예에 따른 개인정보 보호를 위한 물류 운송 방법의 순서도이다.

도 2는 물품배송을 요청하는 단계를 나타낸 순서도이다.

도 3은 물품의 배송과정을 나타낸 순서도이다.

도 4는 물품의 배송완료를 나타낸 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0017] 이하, 본 발명을 바람직한 실시 예와 첨부한 도면을 참고로 하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 여기에서 설명하는 실시 예에 한정되는 것은 아니다.

[0018] 먼저, 도 1을 참조하여, 본 발명의 개인정보 보호를 위한 물류 운송 방법에 대하여 자세히 살펴보도록 한다.

[0019] 도 1은 본 발명의 일 실시 예에 따른 개인정보 보호를 위한 물류 운송 방법의 순서도이다.

[0020] 도 1에 도시된 바와 같이, 먼저 물품을 보내고자 하는 송하인이 자신의 전용단말인 송하인단말(120)로 송하인정보, 수하인정보 및 물품정보를 입력하면, 송하인단말(120)이 물품 배송에 필요한 적어도 하나의 송하인정보, 수하인정보 및 물품정보를 포함하는 물품운송정보를 중앙인증서버(140)로 전송한다(S210). 이때, 상기 송하인정보란, 물품을 보내고자하는 송하인의 이름, 집주소, 이메일주소, 휴대전화번호, 자택전화번호, 사무실 전화번호 중 적어도 하나를 포함하며, 상기 수하인 정보는 물품을 받고자 하는 수하인의 이름, 집주소, 이메일주소, 휴대전화번호, 자택전화번호, 사무실 전화번호 중 적어도 하나를 포함하고, 상기 물품정보는 보내고자 하는 물품의 제품이름, 가격정보, 구매일자 중 적어도 하나를 포함한다.

[0021] 상기 중앙인증서버(140)가 상기 송하인단말(120)로부터 물품운송정보를 수신하여 무결성을 검증한다(S220).

[0022] 상기 중앙인증서버(140)가 무결성 검증을 수행한 상기 물품운송정보에 대한운송장번호, 일회용 수하인 인증번호, 수하인 부인방지토큰, 배송인 부인방지토큰 및 물품운송정보에 기초하여 송하인바코드 및 수하인바코드를 생성한 후, 생성한 송하인바코드 및 수하인바코드를 배송인단말로 전송한다(S230). 이때, 상기 수하인 부인방지토큰은 수하인정보, 운송장번호, 서비스 요청 시간정보를 중앙인증서버용 비밀키를 이용하여 암호화된 메시지 인증 코드(MAC: Message Authentication)이고, 상기 상기 배송인 부인방지토큰은 송하인정보, 운송장번호, 서비스 요청 시간정보를 중앙인증서버용 비밀키를 이용하여 암호화된 메시지 인증 코드를 나타낸다. 또한, 상기 송하인바코드는 상기 운송장번호, 수하인 부인방지토큰 및 상기 물품운송정보를 상기 수하인 인증번호를 이용하여 암호화되며, 상기 수하인바코드는 상기 운송장번호, 배송인 부인방지토크 및 물품운송정보를 각 배송기관별로 할당된 고유한 비밀키로 암호화된다.

[0023] 뿐만 아니라, 상기 송하인바코드 및 수하인 바코드는 서로 다른 굵기를 갖는 검은 막대와 하얀 막대를 조합시켜 문자 또는 숫자를 코드화한 1차원바코드 또는 문자, 숫자, 사진 등의 대량의 정보를 작은 사각형 안에 2차원 심벌로 고밀도 코드화한 2차원바코드로 이루어진다.

[0024] 이처럼, 송하인이 배송을 원하는 물품에 대하여 배송기관으로 접수가 완료되면, 상기 중앙인증서버(140)는 송하인단말(120)로 물품접수완료 메시지를 전송한다.

[0025] 상기 배송인단말(160)이 수신한 상기 수하인바코드를 각 배송기관별 할당된 고유한 비밀키를 이용하여 복호화한 후, 복호화된 수하인바코드에 포함된 운송장번호 및 배송인 부인방지토큰을 상기 중앙인증서버(140)로 전송한다(S240).

[0026] 상기 중앙인증서버(140)가 수신한 운송장번호를 데이터베이스에서 검색하여, 상기 배송인단말(160)로부터 수신한 배송인 부인방지토큰과 자신이 생성한 배송인 부인방지토큰을 비교하고, 동일한 경우에는 수하인단말(180)로 상기 수하인 인증번호를 전송한다(S250).

[0027] 이후, 상기 배송인단말(160)이 수하인단말(180)로부터 수하인 인증번호를 수신한 후, 배송인이 수하인에게 해당 물품을 전달한다.

[0028] 따라서, 상기 수하인단말(180)이 상기 송하인바코드 및 수하인 인증번호를 수신하여 상기 송하인바코드를 복호화한 후, 복호화된 송하인바코드에 포함된 운송장번호 및 수하인 부인방지토큰을 상기 중앙인증서버(140)로 전송한다(S260).

[0029] 이후, 해당 물품의 사고가 발생하는 경우, 수하인에게 사고의 책임이 있다고 판단할 수 있다.

[0030] 상기 중앙인증서버(140)가 수신한 상기 운송장번호 및 수하인 인증번호를 검증한 후, 상기 송하인단말(120)로 배송완료 메시지를 전송한다(S270).

[0031] 이하, 도 2 내지 도 4를 참조하여 본 발명의 물류운송의 주요 단계에 대하여 보다 자세히 살펴보도록 한다.

[0032] 도 2는 물품배송을 요청하는 단계를 나타낸 순서도이다.

[0033] 도 2에 도시된 바와 같이, 먼저, 물품의 배송을 요청하기 위하여, 송하인단말(120, A)이 중앙인증서버(140, CAS)로 송하인정보 S_info, 수하인정보 R_info, 배송기관코드 D_code, 물품정보 P_info를 포함하는 배송메시지 M 를 전송한다. 또한, 상기 송하인단말(120)은 상기 배송메시지 M 를 해시하고, 해시한 값 hash(M)을 자신의 고유한 개인키 s_key로 전자서명한 값 SD을 상기 중앙인증서버(140)로 전송한다.

[0034] 이후, 상기 중앙인증서버(140)가 자신이 데이터베이스 내 기저장하고 있는 송하인정보 S_info, 수하인정보 R_info, 배송기관코드 D_code, 물품정보 P_info 를 이용하여 배송메시지 M' 를 생성하고, 이를 해시한 값 hash(M') 과, 상기 송하인단말(120)로부터 수신한 전자서명한 값 SD 를 상호 비교하여 동일한지 여부를 판단하고, 동일한 경우에는 상기 송하인단말(120)에 대한 검증을 완료한다.

[0035] 이후, 상기 중앙인증서버(140)는 운송장번호 SN, 일회용 수하인 인증번호 r_key를 생성한다.

[0036] 이어서, 상기 중앙인증서버(140)가 수하인 부인방지토큰 R_token과, 배송인 부인방지토큰 D_token을 각각 생성한다. 먼저, 수하인 부인방지토큰 R_token은 상기 송하인단말(120)로부터 수신한 송하인정보 S_info, 앞서 생성한 운송장번호 SN 및 서비스 요청시간 정보 TD를 중앙인증서버용 비밀키 cas_key를 이용하여 인증한 메시지 인증 코드(MAC: Message Authentication)로서 생성될 수 있다. 상기 배송인 부인방지토큰 D_token은 상기 송하인단말(120)로부터 수신한 수하인정보 R_info, 앞서 생성한 운송장번호 SN 및 서비스 요청시간 정보 TD를 중앙인증서버용 비밀키 cas_key 를 이용하여 인증한 메시지 인증 코드(MAC: Message Authentication)로서 생성될 수 있다.

[0037] 이어서, 상기 중앙인증서버(140)는 송하인바코드 S_code 및 수하인바코드 R_code를 생성한다. 이때, 상기 송하인바코드 S_code는 상기 송하인단말(120)로부터 수신한 물품정보 P_info 와 운송장번호 SN 및 앞서 생성한 수하인 부인방지토큰 R_token을 수하인 인증번호 r_key를 이용하여 암호화함으로써, 생성될 수 있다. 또한, 수하인바코드 R_code는 수하인정보 R_info와 운송장번호 SN 및 앞서 생성한 배송인 부인방지토큰 D_token을 배송기관의 고유한 비밀키 d_key를 이용하여 암호화함으로써 생성될 수 있다.

[0038] 이에 따라, 상기 중앙인증서버(140)는 상기 송하인단말(120)로부터 수신한 배송메시지 M, 송하인바코드 S_code, 수하인바코드 R_code 및 운송장번호 SN 를 배송인단말(160, DA)로 전송한다.

[0039] 이어서, 상기 중앙인증서버(140)는 상기 송하인단말(120)로 전송한 배송메시지 M, 운송장번호 SN 및 배송접수완료 메시지 PON를 전송한다.

[0040] 도 3은 물품의 배송과정을 나타낸 순서도이다.

[0041] 도 3에 도시된 바와 같이, 배송인단말(160)이 송하인바코드 S_code, 수하인바코드 R_code, 운송장번호 SN 를 출력하고, 물품을 접수한다.

[0042] 이후, 배송인단말(160)은 상기 중앙인증서버(140)로부터 수신한 수하인바코드 R_code 내 포함된 배송기관용 비밀키 d_key 를 획득한다. 이후, 배송인단말(160)은 획득한 배송기관용 비밀키 d_key를 이용하여 상기 수신한 수하인바코드 R_code 를 복호화하고, 이에 따라 수하인정보 R_info, 운송장번호 SN, 배송인 부인방지토큰 D_token을 획득한다.

[0043] 따라서, 상기 배송인단말(160)은 배송인 부인방지토큰 D_token, 위치정보 GPS_info, 운송장번호 SN, 배송인정보 D_info를 중앙인증서버(140)로 전송한다.

[0044] 이어서, 상기 중앙인증서버(140)는 상기 배송인단말(160)로부터 수신한 운송장번호 SN, 배송인정보 D_info를 송하인단말(120)로 전송한다.

[0045] 이후, 상기 중앙인증서버(140)는 수하인단말(180)로 송하인정보 S_info, 일회용 수하인 인증번호 r_key, 운송장번호 SN, 물품정보 P_info 를 전송한다.

[0046] 도 4는 물품의 배송완료를 나타낸 순서도이다.

[0047] 도 4에 도시된 바와 같이, 배송인단말(160)이 상기 수하인단말(180)로 송하인바코드 S_code를 전송하고, 일회용 수하인 인증번호 r_key에 대한 전송을 요청한다.

[0048] 이에 응답하여, 상기 수하인단말(180)이 상기 배송인단말(160)로 일회용 수하인 인증번호 r_key 를 전송한다.

[0049] 이후, 상기 배송인단말(160)은 상기 수하인단말(180)로부터 수신한 수하인 인증번호 r_key 를 이용하여 송하인 바코드 S_code를 복호화하고, 이에 따라 물품정보 P_info, 운송장번호 SN, 수하인 부인방지토큰 R'_token을 획득한다.

[0050] 상기 배송인단말(160)은 획득한 상기 수하인 부인방지토큰 R'_token, 위치정보 GPS_info, 운송장번호 SN 를 상기 중앙인증서버(140)로 전송한다.

[0051] 따라서, 상기 중앙인증서버(140)는 운송장번호 SN, 수하인단말에 대한 검증을 완료한 검증 처리결과 메시지 PON 를 상기 배송인단말(160)로 전송한다.

[0052] 이후, 배송인이 수하인에게 물품을 인계하여 배송을 완료한다.

[0053] 결국, 중앙인증서버(140)는 송하인정보 S_info, 수하인정보 R_info, 배송기관코드 D_code, 물품정보 P_info 를 포함하는 배송메시지 M, 운송장번호 SN, 수하인단말에 대한 검증을 완료한 검증처리결과 메시지 PON 를 송하인단말(120)로 전송하여 배송완료를 전달한다.

[0054] 또한, 이러한 개인정보 보호를 위한 물류 운송 방법은 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독 가능 기록매체에 저장될 수 있다. 이때, 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 장치의 예로는 ROM, RAM, CD-ROM, DVD±ROM, DVD-RAM, 자기 테이프, 플로피 디스크, 하드 디스크(hard disk), 광데이터 저장장치 등이 있다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 장치에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

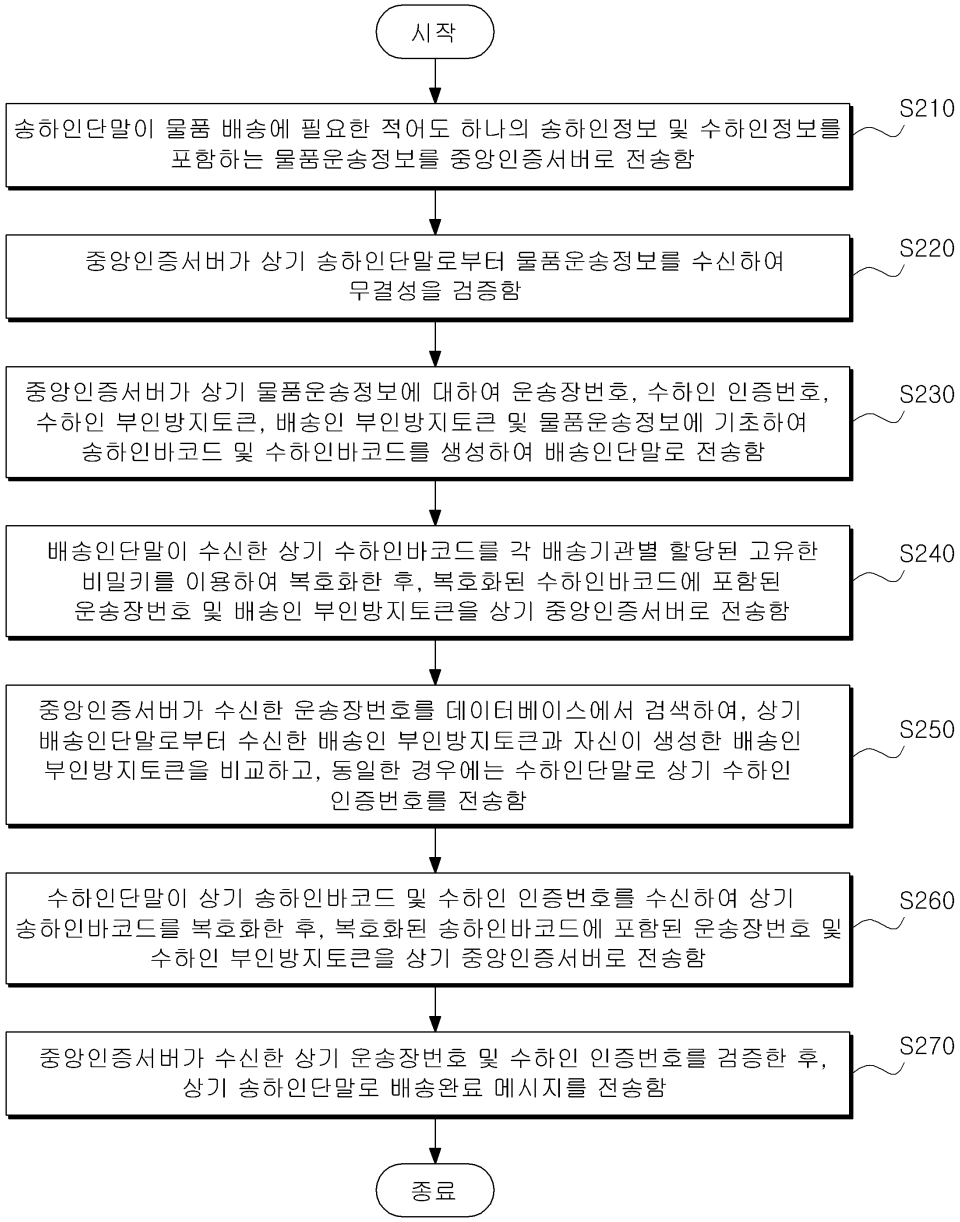
[0055] 본 발명의 개인정보 보호를 위한 물류 운송 방법은 물류 운송 시, 물품을 보내는 송하인 또는 물품을 받는 수하인의 개인정보가 외부로 노출되는 것을 방지하여, 사용자의 개인정보를 용이하게 보호할 수 있는 효과가 있다.

[0056] 또한 본 발명의 개인정보 보호를 위한 물류 운송 방법은 배송인 부인방지토큰 및 수하인 부인방지토큰을 각각 비교함으로써, 물류 운송 중 물품의 미수신, 분실 등의 사고가 발생하는 경우, 사고원인 및 책임을 명확히 할 수 있는 효과가 있다.

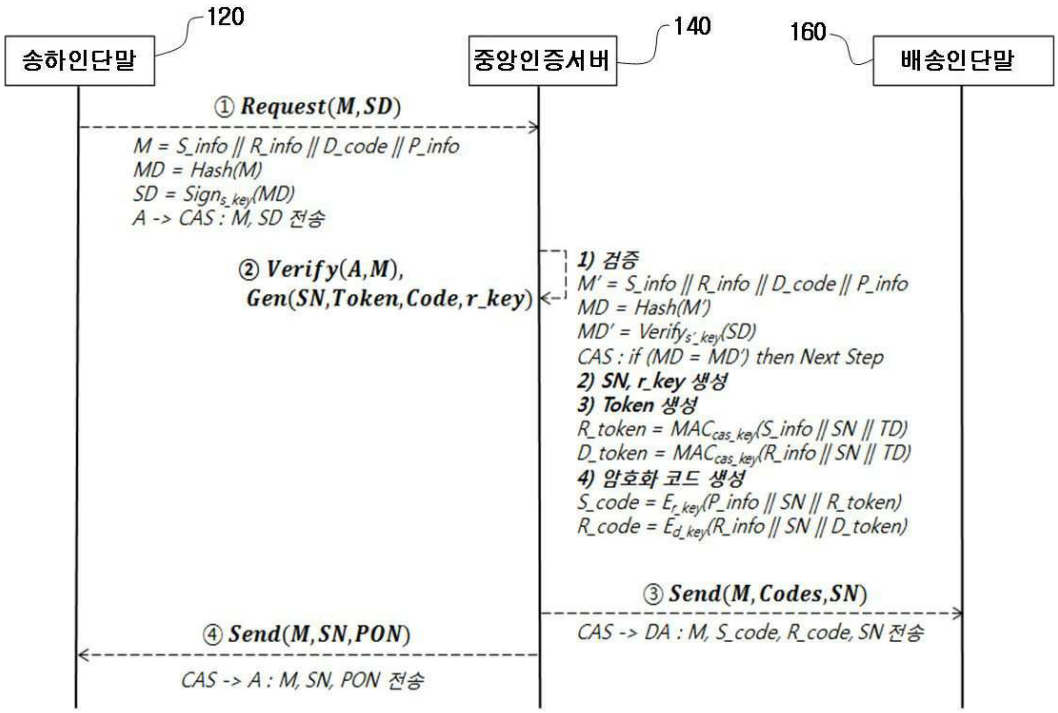
[0057] 상기에서는 본 발명의 바람직한 실시 예에 대하여 설명하였지만, 본 발명은 이에 한정되는 것이 아니고 본 발명의 기술 사상 범위 내에서 여러 가지로 변형하여 실시하는 것이 가능하고 이 또한 첨부된 특허청구범위에 속하는 것은 당연하다.

도면

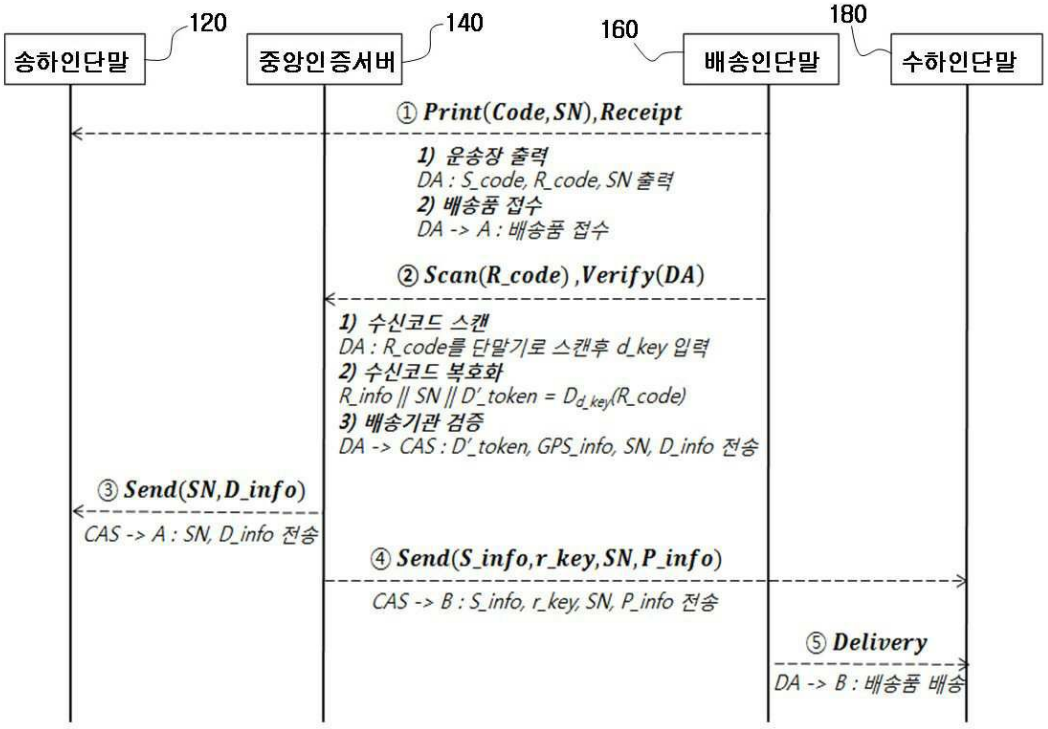
도면1


시작
송하인단말이 물품 배송에 필요한 적어도 하나의 송하인정보 및 수하인정보를 포함하는 물품운송정보를 중앙인증서버로 전송함
S210
중앙인증서버가 상기 송하인단말로부터 물품운송정보를 수신하여 무결성을 검증함
S220
중앙인증서버가 상기 물품운송정보에 대하여 운송장번호, 수하인 인증번호, 수하인 부인방지토큰, 배송인 부인방지토큰 및 물품운송정보에 기초하여 송하인바코드 및 수하인바코드를 생성하여 배송인단말로 전송함
S230
배송인단말이 수신한 상기 수하인바코드를 각 배송기관별 할당된 고유한 비밀키를 이용하여 복호화한 후, 복호화된 수하인바코드에 포함된 운송장번호 및 배송인 부인방지토큰을 상기 중앙인증서버로 전송함
S240
중앙인증서버가 수신한 운송장번호를 데이터베이스에서 검색하여, 상기 배송인단말로부터 수신한 배송인 부인방지토큰과 자신이 생성한 배송인 부인방지토큰을 비교하고, 동일한 경우에는 수하인단말로 상기 수하인 인증번호를 전송함
S250
수하인단말이 상기 송하인바코드 및 수하인 인증번호를 수신하여 상기 송하인바코드를 복호화한 후, 복호화된 송하인바코드에 포함된 운송장번호 및 수하인 부인방지토큰을 상기 중앙인증서버로 전송함
S260
중앙인증서버가 수신한 상기 운송장번호 및 수하인 인증번호를 검증한 후, 상기 송하인단말로 배송완료 메시지를 전송함
S270
종료

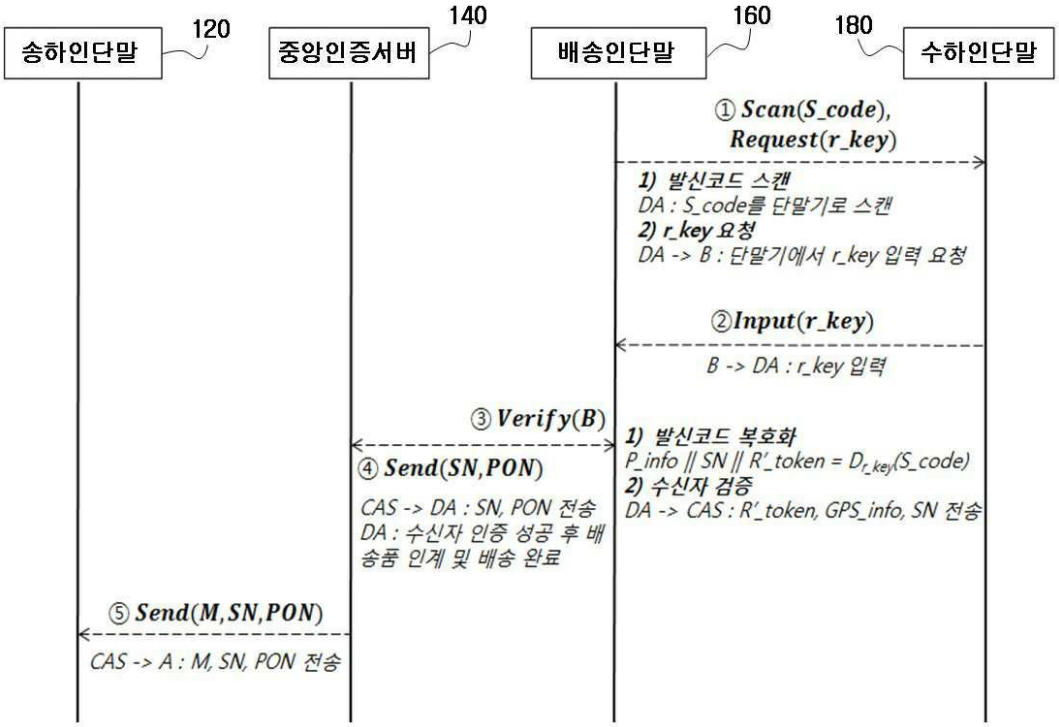
도면2


120
송하인단말
140
중앙인증서버
160
배송인단말
① Request(M,SD)
M = S_info || R_info || D_code || P_info
MD = Hash(M)
SD = Sign_s_key(MD)
A -> CAS : M, SD 전송
② Verify(A,M),
Gen(SN,Token,Code,r_key)
1) 검증
M' = S_info || R_info || D_code || P_info
MD = Hash(M')
MD' = Verify_s_key(SD)
CAS : if (MD = MD') then Next Step
2) SN, r_key 생성
3) Token 생성
R_token = MAC_cas_key(S_info || SN || TD)
D_token = MAC_cas_key(R_info || SN || TD)
4) 암호화 코드 생성
S_code = E_r_key(P_info || SN || R_token)
R_code = E_d_key(R_info || SN || D_token)
③ Send(M,Codes,SN)
CAS -> DA : M, S_code, R_code, SN 전송
④ Send(M,SN,PON)
CAS -> A : M, SN, PON 전송

도면3


120
송하인단말
140
중앙인증서버
160
배송인단말
180
수하인단말
① Print(Code,SN),Receipt
1) 운송장 출력
DA : S_code, R_code, SN 출력
2) 배송품 접수
DA -> A : 배송품 접수
② Scan(R_code) ,Verify(DA)
1) 수신코드 스캔
DA : R_code를 단말기로 스캔후 d_key 입력
2) 수신코드 복호화
R_info || SN || D'_token = D_d_key(R_code)
3) 배송기관 검증
DA -> CAS : D'_token, GPS_info, SN, D_info 전송
③ Send(SN,D_info)
CAS -> A : SN, D_info 전송
④ Send(S_info,r_key,SN,P_info)
CAS -> B : S_info, r_key, SN, P_info 전송
⑤ Delivery
DA -> B : 배송품 배송

도면4


송하인단말
120
중앙인증서버
140
배송인단말
160
수하인단말
180
① Scan(S_code), Request(r_key)
1) 발신코드 스캔
DA : S_code를 단말기로 스캔
2) r_key 요청
DA -> B : 단말기에서 r_key 입력 요청
②Input(r_key)
B -> DA : r_key 입력
③ Verify(B)
④ Send(SN,PON)
CAS -> DA : SN, PON 전송
DA : 수신자 인증 성공 후 배송품 인계 및 배송 완료
1) 발신코드 복호화
P_info || SN || R'_token = D_r_key(S_code)
2) 수신자 검증
DA -> CAS : R'_token, GPS_info, SN 전송
⑤ Send(M,SN,PON)
CAS -> A : M, SN, PON 전송