(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년06월29일
(11) 등록번호 10-1532024
(24) 등록일자 2015년06월22일

(51) 국제특허분류(Int. Cl.)
H04L 12/58 (2006.01)
(52) CPC특허분류
H04L 51/04 (2013.01)
H04L 9/3213 (2013.01)
(21) 출원번호 10-2015-0060215
(22) 출원일자 2015년04월29일
심사청구일자 2015년04월29일
(56) 선행기술조사문헌
KR1020110016387 A
KR1020120052396 A
US20100070755 A1
EP1494429 A2

(73) 특허권자
한밭대학교 산학협력단
대전광역시 유성구 동서대로 125 (덕명동)
(72) 발명자
김은기
대전광역시 유성구 어은로 57 한빛아파트 117동 502호
이재원
대전광역시 서구 가장로 44, 101호
(뒷면에 계속)
(74) 대리인
특허법인충정

전체 청구항 수 : 총 8 항 심사관 : 이형일

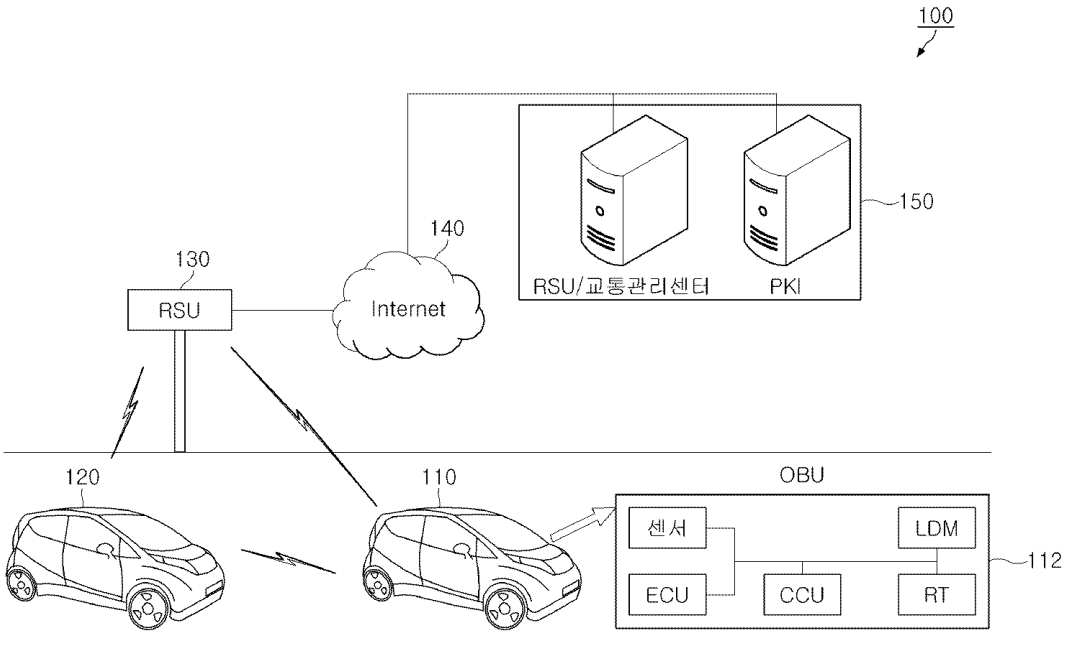
(54) 발명의 명칭 **차량 통신에서의 메시지 전송 방법 및 장치**

(57) 요 약

본 발명은 차량 통신에서의 메시지 전송 방법 및 장치에 관한 것으로서, 보다 구체적으로는, 차량 통신에서의 메시지 전송에 있어서 차량이 소정의 구간에 대하여 유효한 티켓을 발급받고, 상기 티켓을 사용하여 메시지를 구성하고 송신하도록 함으로써, 메시지의 인증에 필요한 데이터 전송량을 최소화하면서, 상기 메시지를 송신한 차량

(뒷면에 계속)

대 표 도



의 익명성도 보장할 수 있는 차량 통신에서의 메시지 전송 방법 및 장치에 관한 것이다.

본 발명은 차량 통신에서 메시지를 전송하는 방법에 있어서, 제 1 차량이 서버로 상기 제1 차량의 공인인증서를 전송하는 단계; 상기 제1 차량이 상기 서버로부터 상기 공인인증서의 유효성에 대한 검증 결과 데이터 및 상기 공인인증서에 대응하는 상기 제1 차량의 공개키를 포함하는 티켓을 발급받는 단계; 상기 제1 차량이 전송하고자 하는 데이터 및 상기 티켓을 포함하는 메시지를 상기 제1 차량의 개인키로 전자서명한 후 송신하는 단계를 포함하는 것을 특징으로 하는 메시지 전송 방법을 개시하는 효과를 갖는다.

(52) CPC특허분류
H04L 9/3263 (2013.01)
H04W 4/12 (2013.01)

(72) 발명자
안재원
세종특별자치시 조치원읍 이화로 5 신흥주공아파트 208동 402호

최범진
대전광역시 대덕구 동춘당로31번길 55-20

이 발명을 지원한 국가연구개발사업
과제고유번호 1345222771
부처명 교육부
연구관리전문기관 한국연구재단
연구사업명 지역혁신창의인력양성사업
연구과제명 IEEE p1609.2 Version 2 규격의 WAVE 보안 시스템 구현
기 여 율 1/1
주관기관 한밭대학교
연구기간 2014.05.01 ~ 2016.04.30

명 세 서

청구범위

청구항 1

차량 통신에서 메시지를 전송하는 방법에 있어서,

제 1 차량이 서버로 상기 제1 차량의 공인인증서를 전송하는 단계;

상기 제1 차량이 상기 서버로부터 상기 공인인증서의 유효성에 대한 검증 결과 데이터 및 상기 공인인증서에 대응하는 상기 제1 차량의 공개키를 포함하는 티켓을 발급받는 단계;

상기 제1 차량이 전송하고자 하는 데이터 및 상기 티켓을 포함하는 메시지를 상기 제1 차량의 개인키로 전자서명한 후 송신하는 단계를 포함하는 것을 특징으로 하는 메시지 전송 방법.

청구항 2

제1항에 있어서,

상기 티켓을 발급받는 단계에서,

상기 서버는 상기 공인인증서의 유효성에 대한 검증 결과 데이터 및 상기 공인인증서에 대응하는 상기 제1 차량의 공개키를 포함하는 티켓을 상기 서버의 개인키로 전자서명한 후 상기 제1 차량으로 발급하는 것을 특징으로 하는 메시지 전송 방법.

청구항 3

제1항에 있어서,

상기 티켓은 상기 제1 차량이 소정의 구간에 진입하는 시점에 발급되고, 상기 제1 차량이 상기 소정의 구간으로부터 이탈하는 시점에 폐기되는 것을 특징으로 하는 메시지 전송 방법.

청구항 4

제1항에 있어서,

상기 송신하는 단계에서는,

상기 제1 차량이 전자서명된 상기 메시지를 하나 이상의 제2 차량 또는 노변 장치(Road Side Unit)로 송신하는 것을 특징으로 하는 메시지 전송 방법.

청구항 5

차량 통신에서 메시지를 전송하는 방법에 있어서,

서버가 제 1 차량으로부터 상기 제1 차량의 공인인증서를 전송받는 단계;

상기 서버가 상기 공인인증서의 유효성에 대한 검증을 수행하는 단계;

상기 서버가 상기 공인인증서의 유효성에 대한 검증 결과 데이터 및 상기 공인인증서에 대응하는 상기 제1 차량의 공개키를 포함하는 티켓을 발급하고 상기 제1 차량으로 전송하여,

상기 제1 차량이 전송하고자 하는 데이터 및 상기 티켓을 포함하는 메시지를 상기 제1 차량의 개인키로 전자서명한 후 송신하도록 하는 단계를 포함하는 것을 특징으로 하는 메시지 전송 방법.

청구항 6

제5항에 있어서,

상기 서버는,

상기 공인인증서의 유효성에 대한 검증 결과 데이터 및 상기 공인인증서에 대응하는 상기 제1 차량의 공개키를

포함하는 티켓을 상기 서버의 개인키로 전자서명한 후 상기 제1 차량으로 발급하는 것을 특징으로 하는 메시지 전송 방법.

청구항 7

차량 통신에서 메시지를 전송하는 장치에 있어서,

제 1 차량의 공인인증서를 서버로 전송하는 공인인증서 전송부;

상기 서버로부터 상기 공인인증서의 유효성에 대한 검증 결과 데이터 및 상기 공인인증서에 대응하는 상기 제1 차량의 공개키를 포함하는 티켓을 전송받는 티켓 수신부;

상기 제1 차량이 전송하고자 하는 데이터 및 상기 티켓을 포함하는 메시지를 상기 제1 차량의 개인키로 전자서명한 후 송신하는 메시지 전송부를 포함하는 것을 특징으로 하는 메시지 전송 장치.

청구항 8

제7항에 있어서,

상기 티켓 수신부에서는,

상기 서버로부터 상기 공인인증서의 유효성에 대한 검증 결과 데이터 및 상기 공인인증서에 대응하는 상기 제1 차량의 공개키를 포함하는 티켓을 상기 서버의 개인키로 전자서명한 후 전송받는 것을 특징으로 하는 메시지 전송 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 차량 통신에서의 메시지 전송 방법 및 장치에 관한 것으로서, 보다 구체적으로는, 차량 통신에서의 메시지 전송에 있어서 차량이 소정의 구간에 대하여 유효한 티켓을 발급받고, 상기 티켓을 사용하여 메시지를 구성하고 송신하도록 함으로써, 메시지의 인증에 필요한 데이터 전송량을 최소화하면서, 상기 메시지를 송신한 차량의 익명성도 보장할 수 있는 차량 통신에서의 메시지 전송 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 근래에 들어 자동차는 종래의 단순한 이동 수단으로서의 한계를 넘어서 정보통신 기술과의 결합을 통하여 다양한 부가 기능을 구비한 복합 시스템으로 발전하고 있다.

[0003] 예를 들어, 최근에는 지능형 자동차 기술과 모바일 컴퓨팅 기술의 결합을 통해 차량 대 차량 (Vehicle-to-Vehicle, 이하 V2V), 차량 대 교통인프라 (Vehicle-to-Infrastructure, 이하 V2I), 차량 대 모바일 기기 (Vehicle-to-Nomadic devices, 이하 V2N) 간의 네트워크를 형성하여 도로상에서 차량의 안전하고 편안한 주행을 위한 교통정보서비스나 인포테인먼트(infotainment) 서비스 등을 제공할 수 있는 차량 통신 시스템에 대한 연구와 표준화가 활발하게 진행되고 있다.

[0004] 상기 차량 통신 시스템은 자동차에 전자, 제어 및 통신 기술 등을 접목하여, 교통체계의 운영과 관리를 자동화하고 교통의 효율성과 안전성을 향상시키는 형태로 발전하고 있으며, 특히 차량 통신은 기존의 인터넷 등 일반적인 통신 서비스와 달리 통신에서의 보안이 확보되지 못하는 경우 운전자의 안전에 심각한 위험을 초래할 수 있어 높은 보안성이 요구된다는 특성을 가진다.

[0005] 이에 따라, 종래 차량 통신에서는 메시지의 인증을 위하여 도 1에서 볼 수 있는 바와 같이 송신 차량(110)에서 자신의 공인인증서(Certificate)를 포함하여 메시지를 발신하고, 상기 메시지를 수신한 수신 차량(120)에서는 상기 공인인증서를 공인인증서 검증 서버(152)로 전송하여 그 유효성을 검증하는 등의 방법으로 메시지에 대한 인증 절차를 수행하였다.

[0006] 그러나, 이러한 경우에는 수신 차량(120)이 메시지를 수신할 때마다 각 메시지에 대한 공인인증서를 상기 공인인증서 검증 서버(152)로 전송하여 그 유효성을 검증하여야 하므로, 그에 따라 데이터 전송량(data traffic)이 매우 커지는 문제가 나타나게 된다. 또한, 송신 차량(110)으로서도 메시지의 전송을 위해서는 상기 공인인증서를 외부로 전송하여야 하는데, 상기 공인인증서에는 발급자의 성명 등 개인 식별정보가 포함되므로 익명성을 보

장하기 어려워 송신 차량(110)의 시간별 위치나 이동 경로 등 프라이버시 정보가 노출될 위험이 따르게 된다.

[0007] 이에 따라, 차량 통신에 있어서 메시지의 인증을 위한 과도한 데이터 전송량의 발생을 억제할 수 있고, 메시지 송신 차량에 대한 익명성을 보장할 수 있는 메시지 전송 방법 등에 대한 요구가 지속되고 있으나, 아직 이에 대한 적절한 해법이 제시되지 못하고 있다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) 대한민국 특허공개공보 제10- 2011-0016387호(2011년 02월 17일 공개)

발명의 내용

해결하려는 과제

[0009] 본 발명은 상기와 같은 종래 기술의 문제점을 해결하기 위해 창안된 것으로, 차량 통신에 있어서 공인인증서의 유효성 검증 과정에서 발생할 수 있는 과도한 데이터 전송량을 억제할 수 있는 메시지 전송 방법 및 장치를 제공하는 것을 목적으로 한다.

[0010] 또한, 본 발명은 차량 통신에 있어서 메시지 송신 차량에 대한 익명성을 보장할 수 있는 메시지 전송 방법 및 장치를 제공하는 것을 목적으로 한다.

과제의 해결 수단

[0011] 상기한 과제를 해결하기 위한 본 발명의 한 측면에 따른 메시지 전송 방법은,

[0012] 차량 통신에서 메시지를 전송하는 방법으로서, 제 1 차량이 서버로 상기 제1 차량의 공인인증서를 전송하는 단계; 상기 제1 차량이 상기 서버로부터 상기 공인인증서의 유효성에 대한 검증 결과 데이터 및 상기 공인인증서에 대응하는 상기 제1 차량의 공개키를 포함하는 티켓을 발급받는 단계; 상기 제1 차량이 전송하고자 하는 데이터 및 상기 티켓을 포함하는 메시지를 상기 제1 차량의 개인키로 전자서명한 후 송신하는 단계를 포함하는 것을 특징으로 한다.

[0013] 이때, 상기 티켓을 발급받는 단계에서, 상기 서버는 상기 공인인증서의 유효성에 대한 검증 결과 데이터 및 상기 공인인증서에 대응하는 상기 제1 차량의 공개키를 포함하는 티켓을 상기 서버의 개인키로 전자서명한 후 상기 제1 차량으로 발급할 수 있다.

[0014] 또한, 상기 티켓은 상기 제1 차량이 소정의 구간에 진입하는 시점에 발급되고, 상기 제1 차량이 상기 소정의 구간으로부터 이탈하는 시점에 폐기될 수 있다.

[0015] 또한, 상기 송신하는 단계에서는, 상기 제1 차량이 전자서명된 상기 메시지를 하나 이상의 제2 차량 또는 노변장치(Road Side Unit)로 송신할 수 있다.

[0016] 상기한 과제를 해결하기 위한 본 발명의 다른 측면에 따른 메시지 전송 방법은,

[0017] 차량 통신에서 메시지를 전송하는 방법으로서, 서버가 제 1 차량으로부터 상기 제1 차량의 공인인증서를 전송받는 단계; 상기 서버가 상기 공인인증서의 유효성에 대한 검증을 수행하는 단계; 상기 서버가 상기 공인인증서의 유효성에 대한 검증 결과 데이터 및 상기 공인인증서에 대응하는 상기 제1 차량의 공개키를 포함하는 티켓을 발급하고 상기 제1 차량으로 전송하여, 상기 제1 차량이 전송하고자 하는 데이터 및 상기 티켓을 포함하는 메시지를 상기 제1 차량의 개인키로 전자서명한 후 송신하도록 하는 단계를 포함하는 것을 특징으로 한다.

[0018] 여기서, 상기 서버는, 상기 공인인증서의 유효성에 대한 검증 결과 데이터 및 상기 공인인증서에 대응하는 상기 제1 차량의 공개키를 포함하는 티켓을 상기 서버의 개인키로 전자서명한 후 상기 제1 차량으로 발급할 수 있다.

[0019] 상기한 과제를 해결하기 위한 본 발명의 또 다른 측면에 따른 메시지 전송 장치는,

[0020] 차량 통신에서 메시지를 전송하는 장치로서, 제 1 차량의 공인인증서를 서버로 전송하는 공인인증서 전송부; 상기 서버로부터 상기 공인인증서의 유효성에 대한 검증 결과 데이터 및 상기 공인인증서에 대응하는 상기 제1 차량의 공개키를 포함하는 티켓을 전송받는 티켓 수신부; 상기 제1 차량이 전송하고자 하는 데이터 및 상기 티켓

을 포함하는 메시지를 상기 제1 차량의 개인키로 전자서명한 후 송신하는 메시지 전송부를 포함하는 것을 특징으로 한다.

[0021] 여기서, 상기 티켓 수신부에서는, 상기 서버로부터 상기 공인인증서의 유효성에 대한 검증 결과 데이터 및 상기 공인인증서에 대응하는 상기 제1 차량의 공개키를 포함하는 티켓을 상기 서버의 개인키로 전자서명한 후 전송받을 수 있다.

발명의 효과

[0022] 본 발명의 실시예에 따르면, 차량 통신에서의 메시지 전송에 있어서 차량이 소정의 구간에 대하여 유효한 티켓을 발급받고, 상기 티켓을 사용하여 메시지를 구성하고 송신하도록 함으로써, 메시지의 인증에 필요한 데이터 전송량을 최소화하면서, 상기 메시지를 송신한 차량의 익명성도 보장할 수 있는 차량 통신에서의 메시지 전송 방법 및 장치를 제공할 수 있게 된다.

도면의 간단한 설명

[0023] 본 발명에 관한 이해를 돕기 위해 상세한 설명의 일부로 포함되는, 첨부도면은 본 발명에 대한 실시예를 제공하고, 상세한 설명과 함께 본 발명의 기술적 사상을 설명한다.

도 1은 종래 기술에 따른 차량간 메시지 전송 시 공인인증서의 유효성을 확인하는 과정을 도시하는 설명도이다.

도 2는 본 발명의 일 실시예에 따른 차량 통신 시스템의 구성도이다.

도 3은 본 발명의 일 실시예에 따른 차량 통신에서의 메시지 전송 방법의 순서도이다.

도 4는 본 발명의 일 실시예에 따른 고속도로 진입시 티켓의 발급 과정을 도시하는 설명도이다.

도 5는 본 발명의 일 실시예에 따라 발급 받은 티켓의 데이터 구조의 예시도이다.

도 6은 본 발명의 일 실시예에 따른 차량 통신에서의 메시지 전송을 설명하기 위한 도면이다.

도 7은 본 발명의 일 실시예에 따른 메시지의 데이터 구조에 대한 비교도이다.

도 8은 본 발명의 다른 실시예에 따른 차량 통신에서의 메시지 전송 방법의 순서도이다.

도 9는 본 발명의 일 실시예에 따른 차량 통신에서의 메시지 전송 장치의 구성도이다.

발명을 실시하기 위한 구체적인 내용

[0024] 본 발명은 다양한 변환을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 이하에서는 특정 실시예들을 첨부된 도면을 기초로 상세히 설명하고자 한다.

[0025] 이하의 실시예는 본 명세서에서 기술된 방법, 장치 및/또는 시스템에 대한 포괄적인 이해를 돕기 위해 제공된다. 그러나 이는 예시에 불과하며 본 발명은 이에 제한되지 않는다.

[0026] 본 발명의 실시예들을 설명함에 있어서, 본 발명과 관련된 공지기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다. 그리고, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다. 상세한 설명에서 사용되는 용어는 단지 본 발명의 실시 예들을 기술하기 위한 것이며, 결코 제한적이어서는 안 된다. 명확하게 달리 사용되지 않는 한, 단수 형태의 표현은 복수 형태의 의미를 포함한다. 본 설명에서, "포함" 또는 "구비"와 같은 표현은 어떤 특성들, 숫자들, 단계들, 동작들, 요소들, 이들의 일부 또는 조합을 가리키기 위한 것이며, 기술된 것 이외에 하나 또는 그 이상의 다른 특성, 숫자, 단계, 동작, 요소, 이들의 일부 또는 조합의 존재 또는 가능성을 배제하도록 해석되어서는 안 된다.

[0027] 또한, 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되는 것은 아니며, 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다.

[0028] 이하에서는, 본 발명에 따른 차량 통신에서의 메시지 전송 방법 및 장치의 예시적인 실시 형태들을 첨부된 도면을 참조하여 상세히 설명한다.

[0029] 먼저, 도 2에서는 본 발명의 일 실시예에 따른 차량 통신에서의 메시지 전송 시스템(100)의 구성도를 예시하고 있다.

[0030] 도 2에서 볼 수 있는 바와 같이 본 발명의 일 실시예에 따른 차량 통신에서의 메시지 전송 시스템(100)은 메시지 전송 장치(112)를 구비하여 메시지를 전송하는 제1 차량(110), 상기 제1 차량(110)으로부터 메시지를 전송받는 제2 차량(120), 상기 제1 차량(110) 및 제2 차량(120)에 대하여 티켓을 발급하거나 소정의 서비스 제공에 사용되는 서버(150) 및 상기 서버(150)와 상기 제1 차량(110) 및 제2 차량(120) 간의 데이터 송수신에 사용되는 노변 장치(130) 및 통신 네트워크(140)를 포함하여 구성될 수 있다.

[0031] 이때, 상기 제1 차량(110)은 상기 노변 장치(130)과 통신 네트워크(140)를 거쳐 서버(150)로 자신의 공인인증서를 전송한다.

[0032] 이어서, 상기 서버(150)는 상기 제1 차량(110)의 공인인증서의 유효성을 검증한 후, 그 검증 결과 데이터와 상기 제1 차량(110)의 공인인증서에 포함되는 공개키를 포함하여 티켓을 구성하고, 이를 자신의 개인키로 전자서명한 후 상기 제1 차량(110)으로 전송한다.

[0033] 상기 제1 차량(110)은 자신이 전송하고자 하는 데이터(예를 들어, 차량에 발생한 사고 시간, 장소 등)와 함께 상기 전송받은 티켓을 포함하는 메시지를 구성하고, 이를 자신의 개인키로 전자서명한 후 이를 상기 제2 차량(120) 등으로 송신하게 된다.

[0034] 상기 제2 차량(120)은 제1 차량(110)의 공개키를 사용하여 상기 제1 차량(110)으로부터 수신한 상기 전자서명된 메시지의 무결성을 검증한 후, 상기 메시지에 포함된 데이터를 처리하여, 사고 관련 정보 등 교통 정보를 얻거나 다양한 데이터 서비스를 제공받을 수 있게 된다.

[0035] 이에 따라, 종래 기술에서 공인인증서를 사용하여 차량간 메시지를 주고 받는 경우, 각 메시지에 대하여 공인인증서의 유효성을 검증하기 위하여 과도한 데이터 전송량(data traffic)이 발생할 수 있고, 또한 개인 정보를 포함하는 공인인증서를 포함하는 메시지를 전송함으로써 개인 정보가 유출될 수 있다는 문제점에 대하여, 상기 제1 차량(110)이 서버(150)로부터 유효한 티켓을 발급받아 메시지를 구성하여 송신하도록 함으로써, 메시지의 인증에 필요한 데이터 전송량을 최소화하면서, 상기 메시지를 송신한 차량의 익명성도 보장할 수 있게 된다.

[0036] 여기서, 상기 서버(150)에는 상기 제1 차량(110)으로부터 전송받는 공인인증서의 유효성을 검증할 수 있는 공인인증서 검증 서버(152)가 포함될 수도 있다. 나아가, 상기 서버(150)에는 상기 공인인증서의 유효성 검증 결과 데이터 및 상기 공인인증서에 대응하는 상기 제1 차량(110)의 공개키를 포함하는 티켓을 발급하거나, 나아가 상기 발급된 티켓에 자신의 개인키로 전자서명을 한 후 이를 상기 제1 차량(110)으로 전송하는 기능이 포함될 수도 있다. 상기 서버(150)는 하나의 물리적 서버로 구현될 수도 있으나, 필요에 따라서는 복수개의 물리적 서버로 구현하는 것도 당연히 가능하다.

[0037] 또한, 상기 통신 네트워크(140)는 유선 네트워크와 무선 네트워크를 포함할 수 있으며, 구체적으로, 근거리 네트워크(LAN: Local Area Network), 도시권 네트워크(MAN: Metropolitan Area Network), 광역 네트워크(WAN: Wide Area Network) 등의 다양한 네트워크를 포함할 수 있다. 나아가, 상기 통신 네트워크(140)는 상기 열거된 네트워크에 국한되지 않고, 공지의 무선 데이터 네트워크나 공지의 유무선 네트워크를 적어도 일부로 포함할 수도 있다.

[0038] 또한, 도 3에서는 본 발명의 일 실시예에 따른 차량 통신에서의 메시지 전송 방법의 순서도를 도시하고 있다.

[0039] 도 3에서 볼 수 있는 바와 같이, 본 발명의 일 실시예에 따른 차량 통신에서의 메시지 전송 방법은, 제 1 차량(110)이 서버(150)로 상기 제1 차량(110)의 공인인증서를 전송하는 단계 (S310), 상기 제1 차량(110)이 상기 서버(150)로부터 상기 공인인증서의 유효성에 대한 검증 결과 데이터 및 상기 공인인증서에 대응하는 상기 제1 차량(110)의 공개키를 포함하는 티켓을 발급받는 단계(S320) 및 상기 제1 차량(110)이 전송하고자 하는 데이터 및 상기 티켓을 포함하는 메시지를 상기 제1 차량(110)의 개인키로 전자서명한 후 송신하는 단계(S330)를 포함할 수 있으며, 나아가 제2 차량(120)이 상기 제1 차량(110)의 공개키를 사용하여 상기 제1 차량(110)으로부터 수신한 메시지의 무결성을 검증하는 단계(S340)를 더 포함할 수도 있다.

[0040] 아래에서는 도 2 및 도 3을 참조하여, 본 발명의 일 실시예에 따른 차량 통신에서의 메시지 전송 시스템(100) 및 방법을 보다 자세하게 살핀다.

[0041] 먼저, S310 단계에서는 제 1 차량(110)이 서버(150)로 상기 제1 차량(110)의 공인인증서를 전송하게 된다. 예를 들어, 상기 제1 차량(110)은 도 4에서 볼 수 있는 바와 같이 상기 서버(150)로 티켓의 발급을 요청하면서 자신

의 공인인증서를 상기 서버(150)로 전송할 수 있다. 이때, 상기 제1 차량(110)의 티켓의 발급 요청 및 공인인증서는 노변 장치(130)와 통신 네트워크(140) 등을 거쳐 상기 서버(150)로 전달될 수 있다.

[0042] 이어서, S320 단계에서는 도 4에서 볼 수 있는 바와 같이 상기 서버(150)가 상기 제1 차량(110)에 대한 티켓을 발급하여 상기 제1 차량(110)으로 전송하게 된다. 이때, 상기 서버(150)은 상기 제1 차량(110)으로부터 전달받은 상기 제1 차량(110)의 공인인증서에 대한 유효성을 검증하고, 그 결과 데이터를 상기 티켓에 포함시킬 수 있다. 또한, 상기 서버(150)는 상기 제1 차량(110)의 공인인증서로부터 상기 제1 차량(110)의 공인인증서에 대응하는 공개키를 추출하여 상기 티켓에 포함시킬 수 있다.

[0043] 이로써, 상기 티켓에는 상기 제1 차량(110)의 공인인증서에 대한 검증 결과가 포함될 수 있어, 메시지의 송신자에 대한 인증이 가능하면서도, 종래 기술과 달리 메시지에 상기 제1 차량(110)에 대한 공인인증서가 포함되지 않아, 상기 공인인증서에 포함되는 발급자의 성명 등 개인 식별정보의 유출을 방지할 수 있게 된다.

[0044] 나아가, 상기 서버(150)는 상기 티켓을 상기 서버(150)의 개인키로 전자서명한 후, 상기 티켓을 상기 제1 차량 110)으로 발급할 수 있다. 이러한 경우, 상기 제1 차량(110)이 임의로 상기 티켓의 내용을 수정하고, 수정된 티켓을 이용하여 만들어진 메시지를 발송하는 것을 방지할 수 있게 된다.

[0045] 도 5에서는 본 발명의 일 실시예에 따라 발급된 티켓의 데이터 구조를 예시하고 있다. 도 5에서 볼 수 있는 바와 같이, 본 발명의 일 실시예에 따른 티켓에는, 상기 제1 차량(110)의 공인인증서의 상태(유효(Good), 폐기(Revoked), 알 수 없음(Unknown))에 대한 검증 결과 데이터 및 상기 제1 차량(110)의 공인인증서에 대응하는 공개키가 포함될 수 있으며, 나아가 상기 공인인증서의 상태에 대한 검증 결과 데이터 및 상기 공인인증서에 대응하는 상기 제1 차량의 공개키를 포함하는 티켓은 상기 서버(150)의 개인키로 전자서명되어 상기 제1 차량(110)으로 발급될 수 있다.

[0046] 다음으로, S330 단계에서는 상기 제1 차량(110)이 전송하고자 하는 데이터(예를 들어, 차량에 발생한 사고 시간, 장소 등)와 함께 상기 전송받은 티켓을 포함하는 메시지를 구성하고, 이를 상기 제1 차량(110)의 개인키로 전자서명한 후 이를 송신할 수 있다.

[0047] 이에 대하여, 도 6에서는 본 발명의 일 실시예에 따라 제1 차량(110)이 상기 메시지를 제2 차량(120) 또는 노변 장치(130)로 전송하는 예를 도시하고 있다. 상기 제1 차량(110)에서 송신된 메시지는 상기 제2 차량(120)으로 전송되어, 제1 차량(110) 또는 다른 차량에서의 사고 정보 등 교통 정보를 제2 차량(120)으로 전달함으로써, 상기 제2 차량(120)이 상기 사고 정보 등 교통 정보를 이용하여 보다 안전하게 차량을 운행할 수 있게 된다.

[0048] 또한, 상기 제1 차량(110)은 상기 제2 차량(120) 외에 노변 장치(130) 등으로 상기 메시지를 전송할 수도 있다. 상기 메시지는 상기 노변 장치(130)를 거쳐 서버(150)로 전송될 수도 있고, 필요에 따라서는 상기 노변 장치(130)를 경유하여 다른 차량으로 전달될 수도 있으며, 나아가 외부 서버 등으로 전송되어 다양하게 활용될 수도 있다.

[0049] 나아가, 상기 제1 차량(110)은 상기 사고 정보 등 교통 정보 외에도 인포테인먼트(infotainment) 서비스 등 다양한 서비스를 위한 정보도 제2 차량(120)이나 노변 장치(130) 등으로 전송할 수 있다.

[0050] 나아가, 상기 티켓은 상기 제1 차량(110)이 소정의 구간에 진입하는 시점에 발급된 후, 상기 제1 차량(110)이 상기 소정의 구간으로부터 이탈하는 시점에 폐기되도록 할 수도 있다.

[0051] 상기 티켓에는 상기 제1 차량(110)의 공인인증서에 대한 검증 결과 데이터가 포함되는데, 상기 공인인증서에 대한 검증 결과 데이터는 티켓의 발급 시점에는 그 유효성을 보장할 수 있으나, 일정 시간이 경과된 시점에서는 그 유효성을 보장하기 어렵다는 문제가 있다. 따라서, 상기 제1 차량(110)이 소정의 구간에 진입하는 시점에 티켓을 발급한 후, 상기 차량(110)이 상기 소정의 구간으로부터 이탈하는 경수 상기 티켓을 폐기하도록 함으로써, 상기 티켓의 유효성을 적절하게 보장할 수 있게 된다.

[0052] 예를 들어, 상기 제1 차량(110)이 고속도로에 진입하는 시점에 상기 제1 차량의 공인인증서에 대한 검증을 거쳐 상기 제1 차량에 대한 티켓을 발급한 후, 상기 제1 차량이 상기 고속도로에서 빠져나오는 시점에 상기 티켓을 폐기하도록 함으로써, 상기 고속도로 구간 내에서 상기 티켓의 유효성을 보장함과 동시에 상기 고속도로 외에서 상기 티켓이 부적절하게 사용되는 것을 방지할 수 있게 된다. 나아가, 상기 티켓에 상기 티켓의 유효 조건(특정 고속도로, 또는 일정 시간 범위)에 대한 데이터를 더 포함시킬 수도 있다.

[0053] 나아가, 상기 소정의 구간이 반드시 불연속적인 특정 구간일 필요는 없으며, 하나의 구간을 연속적인 복수의 구간으로 나누어 구성할 수도 있다. 예를 들어, 제1 도로의 20㎞ 구간을 5㎞ 단위로 4개의 구간으로 나눈 후 각

구간의 진입 및 이탈 시점 마다 티켓을 갱신하도록 하는 것도 가능하다.

[0054] 도 7에서는 본 발명의 일 실시예에 따른 메시지의 데이터 구조를 예시하고 이를 종래 기술에 따른 메시지의 데이터 구조와 비교하고 있다. 먼저, 도 7(a)에서는 종래 기술에 따른 메시지의 데이터 구조를 예시하고 있다. 도 7(a)에서 볼 수 있는 바와 같이, 종래 기술에 따른 메시지에서는 메시지의 송신자, 즉 제1 차량(110)에 대한 인증을 위하여, 상기 제1 차량(110)의 공인인증서를 포함하는 메시지를 구성하였다.

[0055] 이에 따라, 상기 공인인증서를 포함하는 메시지를 수신받는 제2 차량(120) 등은 상기 메시지에 포함된 공인인증서의 유효성을 검증하기 위하여, 상기 메시지에 포함된 공인인증서를 공인인증서 검증 서버(152)로 전달하고, 그에 대한 검증 결과를 확인하는 절차를 거쳐야 했다. 이에 따라, 상기 제2 차량(120)은 메시지를 수신할 때마다, 상기 메시지에 포함된 공인인증서를 상기 공인인증서 검증 서버(152)로 전달하고, 그에 대한 검증 결과를 확인하여야 했으므로, 이를 위한 데이터 전송량(data traffic)이 매우 커지게 되는 문제가 있었다.

[0056] 또한, 상기 메시지에 포함되는 공인인증서에는 상기 공인인증서의 발급자의 성명 등, 제1 차량(110)에 대한 식별 정보가 포함되므로, 이로 인하여 상기 제1 차량(110)의 시간별 위치 정보, 이동 경로 등 개인 정보가 유출될 우려가 있었다.

[0057] 이에 대하여, 도 7(b)에서는 본 발명의 일 실시예에 따른 메시지의 데이터 구조를 예시하고 있다. 도 7(b)에서 볼 수 있는 바와 같이, 본 발명의 일 실시예에 따른 메시지에는, 제1 차량(110)에서 전송하고자 하는 데이터와 함께, 상기 제1 차량(110)의 공인인증서에 대한 검증 결과 데이터 및 상기 제1 차량에 대한 공개키를 포함하여 메시지를 구성할 수 있다. 나아가, 상기 티켓에 대한 무결성을 검증할 수 있도록 상기 메시지를 상기 제1 차량(110)의 개인키로 전자서명한 후 송신할 수 있다.

[0058] 이에 따라, 상기 메시지의 수신자, 즉 제2 차량(120) 등은 메시지를 수신하더라도 별도로 공인인증서에 대한 검증 절차를 거칠 필요없이 이미 서버(150)가 검증한 결과 데이터를 티켓에서 확인할 수 있어, 공인인증서의 검증을 위한 데이터 전송량을 크게 줄일 수 있고, 나아가 본 발명의 일 실시예에 따른 메시지에는 공인인증서를 대신하여 티켓이 포함되게 되므로, 공인인증서에 포함된 발급자의 성명 등으로부터 개인 정보가 유출되는 것을 방지할 수 있게 된다.

[0059] 마지막으로, S340 단계에서는 상기 제2 차량(120) 등이 상기 메시지를 수신한 후, 상기 메시지에 포함된 제1 차량의 개인키를 사용하여 상기 메시지의 무결성을 검증할 수 있다. 이에 따라, 상기 제2 차량(120)은 상기 제1 차량(110)에서 송신한 메시지가 중간에 공격자 등에 의하여 변경되지 않았음을 확인할 수 있고, 이어서 수신한 메시지에 포함된 교통 정보 등 데이터를 처리할 수 있게 된다.

[0060] 도 8에서는 본 발명의 다른 실시예에 따른 서버(150) 관점에서의 차량 통신에서의 메시지 전송 방법의 순서도를 예시하고 있다. 도 8에서 볼 수 있는 바와 같이, 본 발명의 다른 실시예에 따른 차량 통신에서의 메시지 전송 방법은, 서버(150)가 제1 차량(110)으로부터 상기 제1 차량(110)의 공인인증서를 전송받는 단계 (S810), 서버(150)가 상기 공인인증서의 유효성에 대한 검증을 수행하는 단계(S820) 및 서버(150)가 상기 제1 차량(110)으로 상기 공인인증서의 유효성에 대한 검증 결과 데이터 및 상기 공인인증서에 대응하는 상기 제1 차량(110)의 공개키를 포함하는 티켓을 발급하고 상기 제1 차량(110)으로 전송하여, 제1 차량(110)이 전송하고자 하는 데이터 및 상기 티켓을 포함하는 메시지를 상기 제1 차량(110)의 개인키로 전자서명한 후 송신하도록 하는 단계(S830)를 포함할 수 있으며, 나아가 제2 차량(120)이 상기 제1 차량(110)의 공개키를 사용하여 상기 제1 차량(110)으로부터 수신한 메시지의 무결성을 검증하는 단계(S840)를 더 포함할 수도 있다.

[0061] 먼저, S810 단계에서는 서버(150)가 제 1 차량(110)으로부터 상기 제1 차량(110)의 공인인증서를 전송받게 된다. 도 4에서 볼 수 있는 바와 같이, 상기 제1 차량(110)은 상기 서버(150)로 티켓의 발급을 요청하면서 자신의 공인인증서를 상기 서버(150)로 전송할 수 있다.

[0062] 다음으로, S820 단계에서는 상기 서버(150)가 상기 제1 차량(110)으로부터 전송받은 공인인증서의 유효성에 대한 검증 절차를 진행한다.

[0063] 이어서, S830 단계에서는 먼저 상기 서버(150)가 상기 S820 단계에 따른 공인인증서의 유효성에 대한 검증 결과 데이터와 상기 공인인증서에 대응하는 제1 차량(110)의 공개키를 포함하는 티켓을 구성하게 된다(도 5 참조). 또한, 상기 서버(150)는 상기 티켓을 제1 차량(110)으로 전송함으로써, 상기 제1 차량(110)이 자신이 전송하고자 하는 교통 정보 등 데이터와 상기 전송받은 티켓을 포함하는 메시지를 구성하여 제2 차량(120) 등으로 송신하도록 하게 된다. 이때, 상기 메시지는 상기 제1 차량(110)의 개인키로 전자서명되어 송신될 수 있다.

[0064] 마지막으로, S840 단계에서는 상기 제2 차량(120) 등이 상기 메시지를 수신한 후, 상기 메시지에 포함된 제1 차량(110)의 개인키를 사용하여 상기 메시지의 무결성을 검증할 수 있다. 이에 따라, 상기 제2 차량(120)은 상기 제1 차량(110)에서 송신한 메시지가 중간에 공격자 등에 의하여 변경되지 않았음을 확인할 수 있고, 이어서 수신한 메시지에 포함된 교통 정보 등 데이터를 처리할 수 있게 된다.

[0065] 또한, 도 9에서는 본 발명의 일 실시예에 따른 차량 통신에서의 메시지 전송 장치(112)의 구성도를 예시하고 있다. 도 9에서 볼 수 있는 바와 같이, 본 발명의 일 실시예에 따른 차량 통신에서의 메시지 전송 장치(112)는 공인인증서 전송부(1122), 티켓 수신부(1124), 메시지 전송부(1126)를 포함하여 구성될 수 있으며, 나아가 메시지 수신부(1128)를 더 포함하여 구성될 수도 있다.

[0066] 먼저, 상기 메시지 전송 장치(112)는 제1 차량(110)에 탑재되거나, 상기 제1 차량(110)의 일부로서 구현될 수도 있다. 또한, 상기 메시지 전송 장치(112)는 제1 차량(110)에서 메시지를 구성하여 송신하는 기능을 수행하게 되나, 상기 메시지 전송 장치(112)가 제2 차량(120)에 포함되는 경우에는 상기 제1 차량(110)에서 송신된 메시지를 수신하여 처리하게 되므로, 이를 위한 메시지 수신부(1128)를 더 포함하여 구성될 수도 있다.

[0067] 우선, 공인인증서 전송부(1122)에서는 제 1 차량(110)의 공인인증서를 서버(150)로 전송하게 된다.

[0068] 상기 서버(150)에서는 상기 제1 차량(110)의 공인인증서를 전달받아 그에 대한 유효성을 검증하고, 상기 제1 차량(110)의 공인인증서에 대응하는 공개키를 추출한 후, 상기 공인인증서의 유효성에 대한 검증 결과 데이터 및 상기 공인인증서에 대응하는 상기 제1 차량의 공개키를 포함하는 티켓을 생성하여, 상기 제1 차량(110)으로 전송하게 된다.

[0069] 티켓 수신부(1124)에서는 서버(150)로부터 상기 티켓을 수신한다.

[0070] 이어서, 메시지 전송부(1126)에서는 상기 서버(150)로부터 수신한 티켓과 함께 전송하고자 하는 데이터를 포함하여 메시지를 구성한 후, 상기 제1 차량의 개인키로 전자서명하여 제2 차량(120) 등으로 송신하게 된다.

[0071] 마지막으로, 메시지 수신부(1128)에서는 다른 차량에서 송신한 메시지를 수신하고, 상기 수신한 메시지에 포함된 다른 차량의 개인키를 사용하여 상기 수신한 메시지의 무결성을 검증한 후, 이어서 상기 수신한 메시지에 포함된 교통 정보 등 데이터를 처리하게 된다.

[0072] 이상에서 본 발명의 대표적인 실시예들을 상세하게 설명하였으나, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 상술한 실시예에 대하여 본 발명의 범주에서 벗어나지 않는 한도 내에서 다양한 변형이 가능함을 이해할 것이다. 그러므로 본 발명의 권리범위는 설명된 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허청구범위뿐만 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

[0073] 100 : 차량 통신에서의 메시지 전송 시스템

110 : 제1 차량

112 : 메시지 전송 장치

120 : 제2 차량

130 : 노변 장치

140 : 통신 네트워크

150 : 서버

152 : 공인인증서 검증 서버

1122 : 공인인증서 전송부

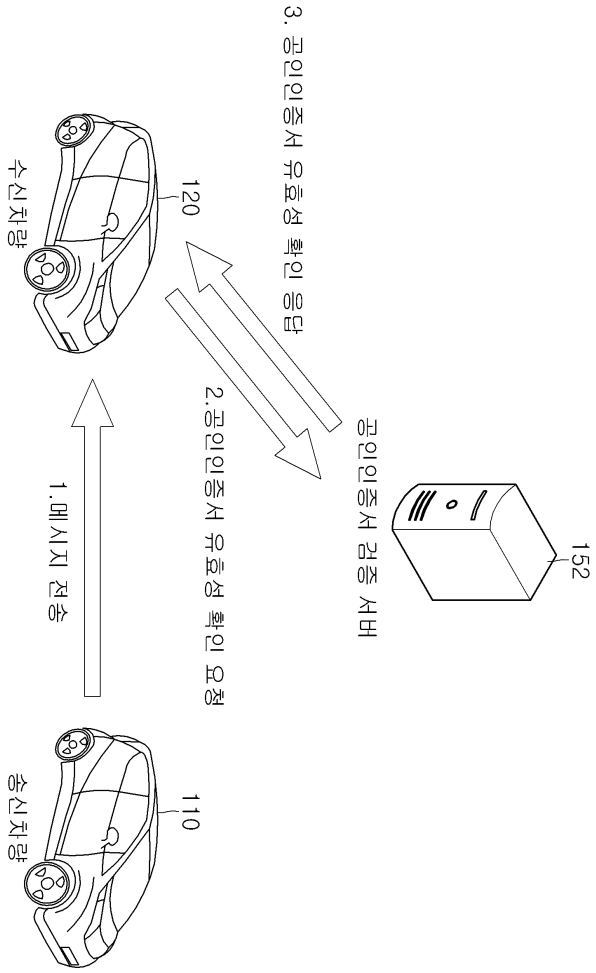
1124 : 티켓 수신부

1126 : 메시지 전송부

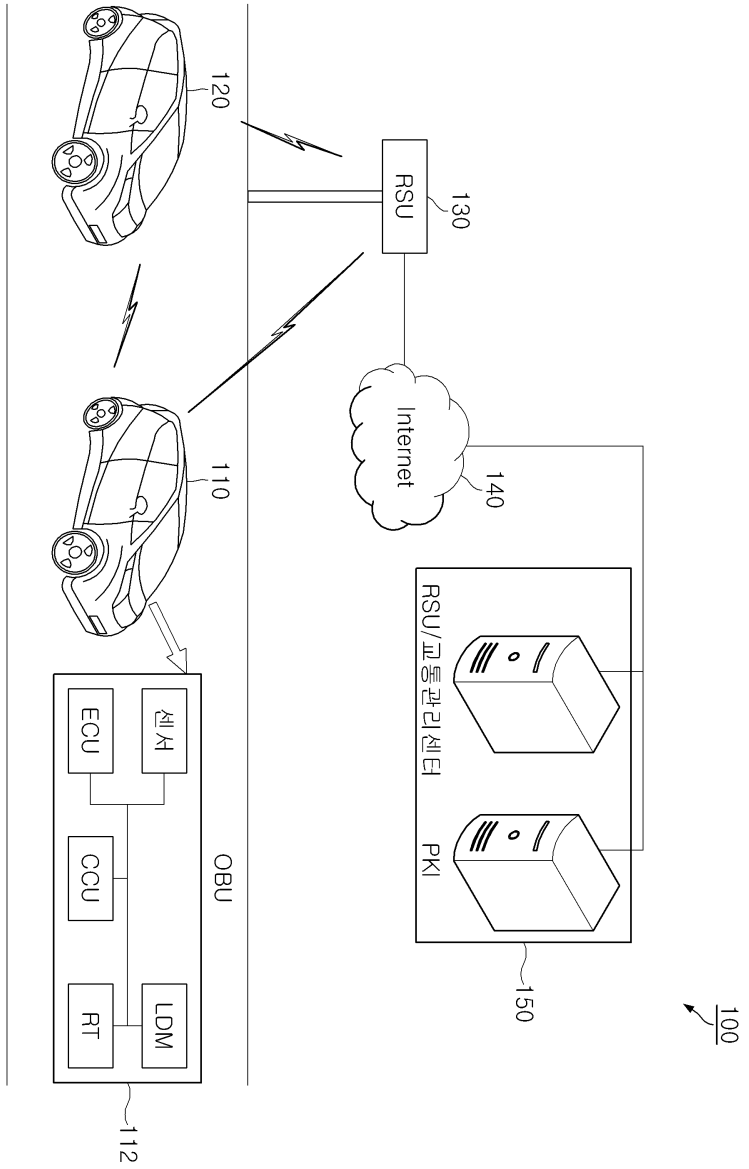
1128 : 메시지 수신부

도면

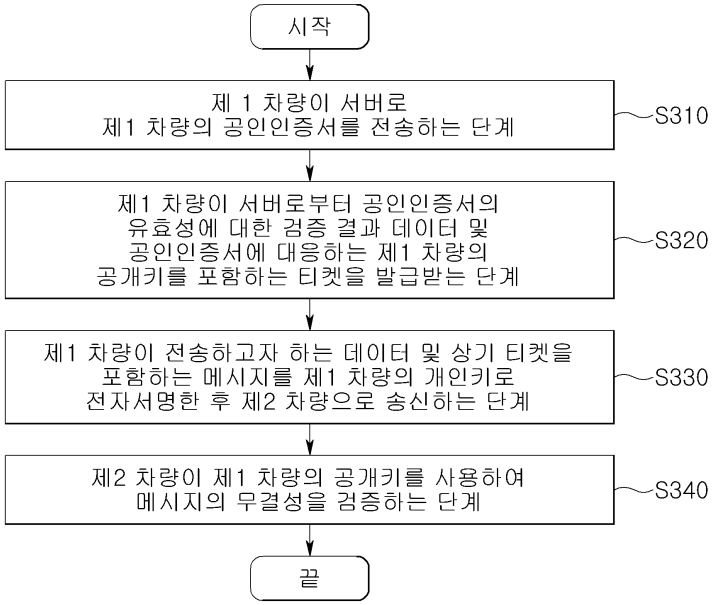
도면1


3. 공인인증서 유효성 확인 응답
2. 공인인증서 유효성 확인 요청
1. 메시지 전송
공인인증서 검증 서버
152
수신차량
120
송신차량
110

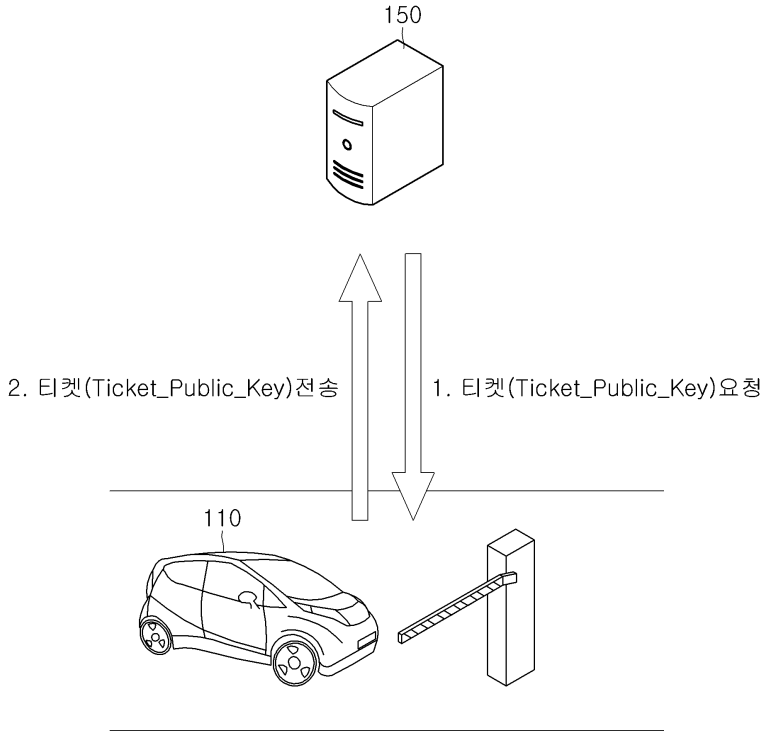
도면2


120
RSU
130
Internet
140
110
RSU/교통관리센터
PKI
150
100
ECU
센서
CCU
RT
LDM
OBU
112

도면3



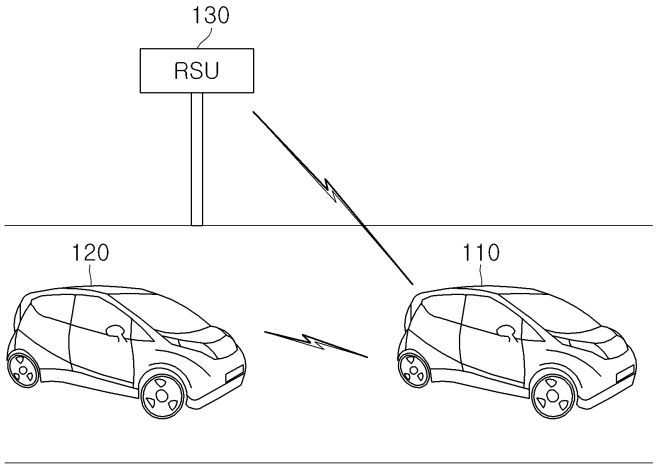
도면4



도면5

공인인증서 상태 (Good, Revoked, Unknown)	차량의 공개키 (Public Key)	전자서명 (Signature)

도면6



도면7

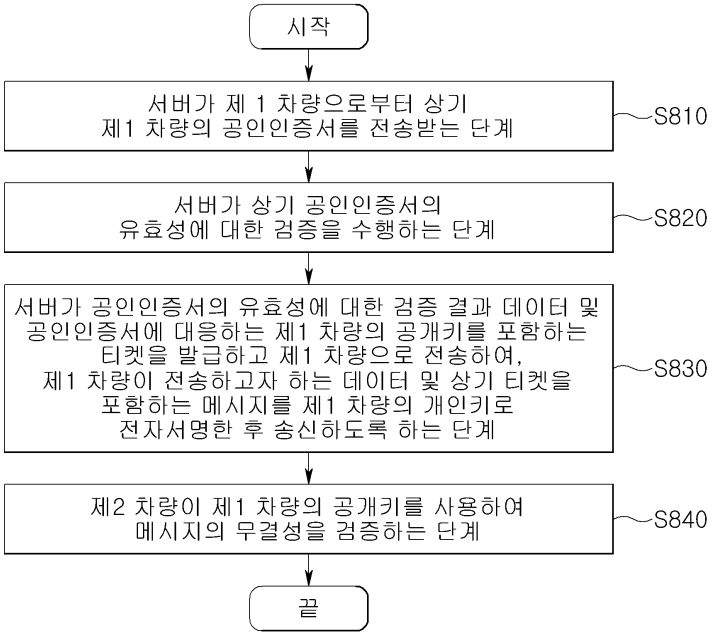
데이터 (사고 시간,장소 등)	공인인증서 (Certificate)	전자서명 (Signature)

(a)

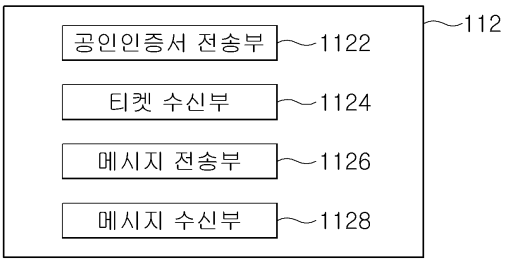
데이터 (사고 시간,장소 등)	공개키를 포함하는 티켓 (Ticket_Public_Key)	전자서명 (Signature)

(b)

도면8


시작
서버가 제 1 차량으로부터 상기 제1 차량의 공인인증서를 전송받는 단계
S810
서버가 상기 공인인증서의 유효성에 대한 검증을 수행하는 단계
S820
서버가 공인인증서의 유효성에 대한 검증 결과 데이터 및 공인인증서에 대응하는 제1 차량의 공개키를 포함하는 티켓을 발급하고 제1 차량으로 전송하여, 제1 차량이 전송하고자 하는 데이터 및 상기 티켓을 포함하는 메시지를 제1 차량의 개인키로 전자서명한 후 송신하도록 하는 단계
S830
제2 차량이 제1 차량의 공개키를 사용하여 메시지의 무결성을 검증하는 단계
S840
끝

도면9


112
공인인증서 전송부
1122
티켓 수신부
1124
메시지 전송부
1126
메시지 수신부
1128