(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2008-0106954
(43) 공개일자 2008년12월09일

(51) Int. Cl.
G07C 9/00 (2006.01) *B60R 25/00* (2006.01)
(21) 출원번호 10-2008-7023905
(22) 출원일자 2008년09월30일
심사청구일자 없음
번역문제출일자 2008년09월30일
(86) 국제출원번호 PCT/EP2007/052459
국제출원일자 2007년03월15일
(87) 국제공개번호 WO 2007/113093
국제공개일자 2007년10월11일
(30) 우선권주장
10 2006 015 212.3 2006년03월30일 독일(DE)

(71) 출원인
분데스드룩커라이 게엠베하
독일 데-10958 베를린 오라닌슈트라쎄 91
(72) 발명자
치스카, 안드레아스
독일 베를린 12107, 임 레자흐탈 42
뮈펠만, 군다
독일 쉐나이헤 15566, 호이벡 43
(뒷면에 계속)
(74) 대리인
임훈빈

전체 청구항 수 : 총 28 항

(54) 동산, 특히 차량을 무단 사용으로부터 보호하는 방법

(57) 요 약

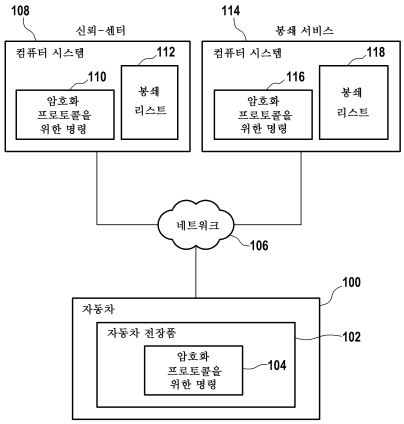
본 발명은 동산, 특히 자동차(100)를 무단 사용으로부터 보호하는 방법에 관한 것으로,

외부 컴퓨터 시스템(108)에서 차량의 암호화 정체성 검증 및/또는 암호화 인증을 실행하는 단계,

상기 자동차에 대하여 봉쇄가 저장되어 있는 지를 검증하는 단계, 및

상기 자동차에 대하여 어떤 봉쇄도 저장되어 있지 않는 경우 자동차의 사용을 허락하도록 컴퓨터 시스템으로부터 차량에 신호를 전송하는 단계를 포함하는 것을 특징으로 한다.

대 표 도 - 도1



(72) 발명자

퀴데어, 조아힘

독일 베를린 10179, 암 크뢰겔 3

볼트펠드트-헤르켄텔, 실레이

독일 베를린 10117, 라이프치거 스트라쎄 66

특허청구의 범위

청구항 1

동산(100)을 무단 사용으로부터 보호하는 방법에 있어서,

외부 컴퓨터 시스템(108)을 이용해서 동산의 암호화 정체성 검증 및/또는 암호화 인증을 실행하는 단계,

상기 동산에 대해 봉쇄가 저장되어 있는 지를 검증하는 단계, 및

상기 동산에 대해 어떤 봉쇄도 저장되어 있지 않는 경우 동산의 사용을 허락하도록 컴퓨터 시스템으로부터 동산에 신호를 전송하는 단계를 포함하는 것을 특징으로 하는 동산을 무단 사용으로부터 보호하는 방법.

청구항 2

제1항에 있어서, 상기 암호화 정체성 검증 및/또는 암호화 인증은 동산에 부여되는 비대칭 쌍의 키를 사용하여 행하여지는 것을 특징으로 하는 동산을 무단 사용으로부터 보호하는 방법.

청구항 3

제1항 또는 제2항에 있어서, 상기 컴퓨터 시스템은 봉쇄를 저장하는 데이터베이스(112)를 포함하며, 또한 상기 컴퓨터 시스템은 데이터베이스에 동산의 봉쇄가 저장되어 있는 지를 검증하도록 동산의 암호화 정체성 검증 및/또는 암호화 인증이 완료된 후 상기 컴퓨터 시스템은 데이터베이스를 액세스하는 것을 특징으로 하는 동산을 무단 사용으로부터 보호하는 방법.

청구항 4

제1항, 제2항 또는 제3항에 있어서,

동산에 의해 서명된 코드를 수신하는 단계, 및

서명된 코드의 유효성을 검증하는 단계를 더 포함하며,

상기 서명된 코드가 유효할 경우에만 상기 신호가 전송되는 것을 특징으로 하는 동산을 무단 사용으로부터 보호하는 방법.

청구항 5

제4항에 있어서, 상기 서명된 코드 및 인증서(130)가 수신되며, 또한 상기 인증서는 코드를 포함하는 것을 특징으로 하는 동산을 무단 사용으로부터 보호하는 방법.

청구항 6

제4항에 있어서, 상기 서명된 코드 및 인증서(130)가 수신되며, 상기 인증서는 동산을 식별하는 식별자를 포함하고, 상기 코드의 유효성이 식별자에 의해 검증되는 것을 특징으로 하는 방법.

청구항 7

제1항 내지 제6항 중 어느 한 항에 있어서, 상기 신호는 컴퓨터 시스템의 비밀키(134)를 사용하여 서명되는 것을 특징으로 하는 동산을 무단 사용으로부터 보호하는 방법.

청구항 8

제1항 내지 제7항 중 어느 한 항에 있어서, 만약 동산에 대하여 봉쇄가 저장되어 있는 경우 동산의 사용을 봉쇄하기 위하여 컴퓨터 시스템으로부터 동산으로 봉쇄 신호가 전송되는 것을 특징으로 하는 동산을 무단 사용으로부터 보호하는 방법.

청구항 9

제8항에 있어서, 상기 봉쇄 신호는 컴퓨터 시스템의 비밀키(134)를 사용하여 서명되는 것을 특징으로 하는 동산을 무단 사용으로부터 보호하는 방법.

청구항 10

제1항 내지 제9항 중 어느 한 항에 있어서,

상기 컴퓨터 시스템에 의해 동산의 분실을 나타내는 메시지를 수신하는 단계, 및

상기 동산에 대한 봉쇄를 저장하는 단계를 더 포함하는 것을 특징으로 하는 동산을 무단 사용으로부터 보호하는 방법.

청구항 11

제1항 내지 제10항 중 어느 한 항에 있어서,

상기 컴퓨터 시스템에 의해 보조 코드를 수신하는 단계,

상기 보조 코드에 대한 보조 인증서를 발생하는 단계, 및

저장된 인증서(130)를 대체하도록 동산(100)에 대한 안전 접속을 통하여 보조 인증서를 전송하는 단계를 더 포함하는 것을 특징으로 하는 동산을 무단 사용으로부터 보호하는 방법.

청구항 12

제11항에 있어서, 상기 인증서는 공인 정비소의 요구에 따라 보조 코드에 의해 대체되는 것을 특징으로 하는 동산을 무단 사용으로부터 보호하는 방법.

청구항 13

제1항 내지 제12항 중 어느 한 항에 있어서, 상기 컴퓨터 시스템은 신뢰-센터에 속해있는 것을 특징으로 하는 방법.

청구항 14

제1항 내지 제13항 중 어느 한 항에 있어서, 상기 동산은 항공기, 차량, 특히 승용차 또는 건설기계, 이동 가능한 설비, 포터블 컴퓨터, 특히 랩톱 컴퓨터, 또는 휴대전화인 것을 특징으로 하는 동산을 무단 사용으로부터 보호하는 방법.

청구항 15

제1항 내지 제14항 중 어느 한 항에 따른 방법을 수행하기 위한 실행 명령으로 구성되는 것을 특징으로 하는 컴퓨터 프로그램 제품.

청구항 16

동산의 암호화 정체성 검증 및/또는 암호화 인증을 실행하기 위한 수단(110),

상기 동산의 사용 상태를 판단하기 위한 수단(112), 및

상기 사용 상태에 따라 동산에 대한 신호를 전송하기 위한 수단(108)을 포함하는 것을 특징으로 하는 컴퓨터 시스템.

청구항 17

제16항에 있어서,

동산으로부터 서명된 코드를 수신하기 위한 수단(108), 및

서명된 코드의 유효성을 검사하기 위한 수단(110,136)을 포함하며,

상기 전송수단은 상기 서명된 코드의 유효성을 검사하는 것에 따라 신호를 전송하도록 채택되는 것을 특징으로 하는 컴퓨터 시스템.

청구항 18

동산(100)을 무단 사용으로부터 보호하는 방법에 있어서,

외부 컴퓨터 시스템(108)에서 동산(100)의 암호화 정체성 검증 및/또는 암호화 인증을 실행하는 단계, 및

컴퓨터 시스템으로부터 사용 신호 또는 봉쇄 신호를 수신하는 단계를 포함하는 것을 특징으로 하는 동산을 무단 사용으로부터 보호하는 방법.

청구항 19

제18항에 있어서,

코드를 서명하는 단계, 및

컴퓨터 시스템에 동산의 서명된 코드를 전송하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 20

제19항에 있어서,

상기 코드는 동산의 전자 부품(120)의 일 또는 몇 개의 식별자로부터 발생되는 것을 특징으로 하는 방법.

청구항 21

제18항, 제19항 또는 제20항에 있어서, 동산이 봉쇄 신호를 수신한 후 동산의 지리학적 위치를 정의하는 위치 신호가 동산에 의해 전송되는 것을 특징으로 하는 방법.

청구항 22

제18항 내지 제21항 중 어느 한 항에 따른 방법을 수행하기 위한 명령으로 구성되는 것을 특징으로 하는 컴퓨터 프로그램 제품.

청구항 23

동산, 특히 자동차 전장품 장치를 위한 전자 장치에 있어서,

컴퓨터 시스템(108)에서 동산(100)의 암호화 정체성 검증 및/또는 암호화 인증을 실행하는 수단(104;126,128,130), 및

컴퓨터 시스템으로부터 사용 신호 또는 봉쇄 신호를 수신하는 수단(138)을 포함하는 것을 특징으로 하는 전자 장치.

청구항 24

제23항에 있어서,

코드를 서명하기 위한 수단(104), 및

동산으로부터 컴퓨터 시스템에 서명된 코드를 전송하는 수단(138)을 포함하는 것을 특징으로 하는 전자 장치.

청구항 25

제23항 또는 제24항에 있어서, 전자 장치 및/또는 전자 장치와 네트워크를 형성할 수 있는 동산의 다른 전자 부품(120)에 부여된 일 또는 몇 개의 식별자(124)로부터 코드를 발생하기 위한 수단(104)을 포함하는 것을 특징으로 하는 전자 장치.

청구항 26

제25항에 있어서, 다른 전자 부품의 암호화 정체성 검증 및/또는 암호화 인증을 실행하기 위한 수단(146,146',146'',146''')을 포함하는 것을 특징으로 하는 전자 장치.

청구항 27

동산을 무단 사용으로부터 보호하는 방법에 있어서,

제1컴퓨터 시스템(114)으로 동산의 분실을 나타내는 정보를 입력하는 단계, 및

데이터베이스(112)에 정보를 저장하기 위한 제2컴퓨터 시스템(108)에 정보를 전송하되, 상기 제2컴퓨터 시스템은 데이터베이스에 저장된 정보에 따라 동산의 사용을 허락하거나 또는 동산의 사용을 봉쇄하는 신호를 발생하도록 적응되는 단계를 포함하는 것을 특징으로 하는 동산을 무단 사용으로부터 보호하는 방법.

청구항 28

제27항에 있어서, 제1컴퓨터 시스템의 암호화 정체성 검증 및/또는 암호화 인증은 제2컴퓨터 시스템에서 수행되는 것을 특징으로 하는 동산을 무단 사용으로부터 보호하는 방법.

명 세 서

기 술 분 야

<1> 본 발명은 동산(Movable Object)을 무단 사용으로부터 보호하는 방법, 대응하는 컴퓨터 프로그램 제품, 컴퓨터 시스템 및 자동차 전자 장치(motor vehicle electronics device)에 관한 것이다.

배 경 기 술

<2> 미합중국 특허 제2002/0135466 A1호에는 컴퓨터 서버를 사용해서 자동차와 결합될 수 있는 PDA의 인증이 공지되어 있다. 이 경우, PDA는 차량의 시동키의 기능을 충족시킨다. PDA를 훔치는 경우 도둑 또한 차량을 사용할 수 있다는 단점이 있다. 더욱이, 자동차 전자 장치(motor vehicle electronics)는 차량의 정체성(identity)을 변경하도록 조작될 수 있다.

<3> 독일연방공화국 특허 제4440975 C2호로부터 차량에 대한 제3자 사용 보호장치가 공지되어 있다. 이 장치는 전자기파에 기반을 두고 차량으로부터 전송선로를 통하여 외부 사이트와 상호간에 주기적으로 그리고 순차적으로 사용 신호를 전송하고 2개의 연속된 사용 신호 사이의 시간차 보다 더 긴 규정된 시간 간격 동안 후자에 의해 수신된 사용 신호로부터 일 이상의 차량 집합체는 사용제어장치에 의해 동작 상태에서 차량 동작에 필요로 하는 것이 유지되며, 반면에 규정된 시간 간격 동안 어떤 부가적인 사용 신호가 수신되지 않는 경우 자동차의 추가적인 동작과 그 결과적인 동작은 차단되도록 설계되어 있다. 따라서, 자동차의 사용을 위하여 승인 신호의 수신이 요구된다.

<4> 차량 도난이 발생할 때 승인 받은 자(authorized person)는 그 사실을 사용 신호의 전송 권한 위임된 사이트에 공표하며, 그 결과 사용 신호의 전송을 중지하여, 그 후 사용제어장치가 차량의 후속 동작을 차단하도록 하게 한다. 이것은 사용 신호의 부재 후 즉시 또는 부가적인 시간 간격의 종료 후 즉시 발생할 수 있다. 만약, 예를 들어, 어떤 부가적인 사용 신호도 승인된 총 동작 기간 내에 수신되지 않는 경우, 대응하는 차량 전체는 어떤 안전-임계적인 차량 상태 또는 유용성 문제가 결과적으로 발생하도록 미리 설정된 시간 간격 동안 사용제어장치에 의해 동작 가능한 상태로 유지될 것이다. 시간 간격의 종료 후에 대응하는 차량 집합체는 그 후 차량이 동작 상태로 되돌려질 수 없도록 점화장치를 턴-오프한 다음번 이후에 사용제어장치에 의해 동작 차단 상태로 되게 한다.

<5> 무선 네트워크를 통한 사용 신호의 전송은 시스템을 회피할 목적으로 다른 곳에서 사용 신호를 발생할 수 있도록 하기 위하여 해당 차량을 향하는 사용 신호를 승인 받은 자(authorized person)나 특히 승인 받지 않은 자(unauthorized person)가 다른 차량에 대하여 다수의 방사된 사용 신호로부터 검출하는 것이 가능하지 않다는 사실을 통하여 조작에 대한 큰 저항이 있는 것으로 추정된다. 소망하는 경우 코드 기반의 사용 신호 전송은 일반적으로 있는 일이지만 예를 들어 전자 키 코딩을 사용하는 액세스 승인 시스템에서 사용 코드 전송을 위해 설치될 수 있다.

<6> 그러나, 이러한 코드-기반 사용 신호 전송은 차량이 해당 자동차에 해당하는 코드를 통하여 식별되는 동안, 예를 들어 자동차 전자 장치(motor vehicle electronics)의 조작에 의해 검출되어 회피될 수 있다.

발명의 상세한 설명

<7> 한편, 본 발명은 동산(Movable Object), 특히 차량을 무단 사용으로부터 보호하는 개선된 방법 뿐만 아니라 대응하는 컴퓨터 프로그램 제품과 컴퓨터 시스템, 또한 동산을 무단 사용으로부터 보호하는 개선된 전자 장치를 창작하는 과제에 기초를 두고 있다.

<8> 본 발명의 기초인 과제는 각각 청구범위의 특징을 가지고 해결된다. 본 발명의 바람직한 실시예는 종속항에 기재되어 있다.

<9> 본 발명에 따르면, 동산을 무단 사용으로부터 보호하는 방법은 외부 컴퓨터 시스템을 사용해서 동산의 암호화 정체성 검증 및/또는 암호화 인증을 실행하는 단계, 상기 동산에 대하여 봉쇄가 저장되어 있는 지를 검증하는 단계, 및 상기 동산에 대하여 어떤 봉쇄도 존재하지 않는 경우 동산의 사용을 허락하도록 컴퓨터 시스템으로부터 동산에 신호를 전송하는 단계를 포함하는 것을 특징으로 한다.

<10> 본 발명에 따르면, 동산은 항공기, 차량, 특히 승용차, 건설기계, 이동 가능한 설비, 포터블 컴퓨터, 특히 랩톱 컴퓨터, 휴대전화, 스마트 폰 등, 특히 하나 이상의 전자 부품을 포함하는 고가의 동산과 같이 고가의 동산으로서 이해하여야 한다.

<11> 종래 기술과 다르게, 동산 그 자체, 예를 들어, 자동차의 암호화 정체성 검증 및/또는 암호화 인증이 외부 컴퓨터 시스템를 사용하여 본 발명에 따라 행하여진다. 이는 컴퓨터 시스템에 의해 전송된 사용 신호 또는 봉쇄 신호가 정당한 자동차에 도착하고, 자동차 전장품의 조작에 의해 정체성이 변경되며 또한 도난당하지 않은 자동차에 도착한다.

<12> "인증(authentication)"하에서 자동차의 정체성 증거가 이에 의해 이해된다. 이것은, 예를 들어 차량 또는 자동차 전장품에 부여된 비대칭 쌍의 키 뿐 아니라 대응하는 인증서에 기초를 두고 있는 암호화 방법에 의해 입증된다. 인증서는 자동차 및/또는 자동차 전장품을 식별하는 식별자를 포함한다.

<13> "정체성 검증(identity verification)"하에서 자동차 및/또는 자동차 전장품의 이미 주지된 정체성의 검증이 이에 의해 이해된다. 따라서, 인증은 만약 그 후에 정체성의 검증, 즉 정체성 검증이 암호화 방법 또는 그 반대에 의해 행하여 질 경우 예를 들어, 암호화 방법 없이 또한 이루어질 수 있다. 정체성 검증은 자동차 또는 자동차 전장품에 부여된 비대칭 쌍의 키와 대응하는 인증서에 기반을 두고 있다.

<14> 본 발명의 실시예에 따르면, 암호화 정체성 검증 및/또는 암호화 인증은 자동차에 부여된 비대칭 쌍의 키를 사용함에 의해 행하여진다.

<15> 암호화 정체성 검증 및/또는 암호화 인증을 실행하기 위하여 컴퓨터 시스템은, 예를 들어 난수, 특히 의사 난수를 발생한다. 의사 난수는 동산, 예를 들어 자동차에 암호화 없이 컴퓨터 시스템에 의해 전송된다. 의사 난수는 자동차에 부여된 비밀키에 의해 자동차 전장품에 의해 암호화 된다. 암호화된 의사 난수는 자동차의 인증서와 함께 컴퓨터 시스템에 자동차에 의해 전송된다.

<16> 컴퓨터 시스템은 그 후 수신된 인증서의 공개키에 의해 암호화된 방식으로 수신되었던 의사 난수를 해독한다. 만약 양측 의사 난수가 일치하는 경우, 이는 자동차에 부여되며 비밀키와 공개키로 이루어진 비대칭 쌍의 키와 대응하는 인증서가 유효하다는 것을 의미한다. 따라서, 비대칭 쌍의 키에 부여된 인증서를 통하여 자동차의 정체성이 명확하게 확인된다.

<17> 본 발명의 실시예에 따르면, 외부 컴퓨터 시스템은 봉쇄의 저장을 위한 데이터베이스를 갖고 있다. 만약 예를 들어 자동차가 도난된 것으로 공표된 경우 대응하는 봉쇄가 데이터베이스에 입력된다. 암호화 인증의 실행 후에 컴퓨터 시스템은 암호화 정체성 검증 및/또는 암호화 인증이 행하여진 자동차는 봉쇄로서 데이터베이스에 입력되어 있는 지를 판단하도록 데이터베이스를 액세스한다. 만약 데이터베이스에 봉쇄 신호가 입력되어 있는 경우, 컴퓨터 시스템은 자동차에 대응하는 봉쇄 신호를 전송하며, 그 결과 예를 들어 점화가 오프된 후 자동차가 시동될 수 없다.

<18> 본 발명의 실시예에 따르면, 컴퓨터 시스템은 자동차로부터 서명된 코드를 수신한다. 컴퓨터 시스템은 유효성을 위해 서명 코드를 검증한다. 만약 상기 서명된 코드가 유효한 경우 그리고 부가적으로 자동차의 봉쇄가 데이터베이스에 저장되어 있는 경우 컴퓨터 시스템은 상기 자동차의 사용을 허락하도록 사용 신호를 자동차에 전송한다.

<19> 코드는, 예를 들어 시리얼 넘버, 형식 번호(type number), 제조업자 번호, 및/또는 이러한 번호의 체인 또는 하나 또는 몇 개의 이러한 번호들로부터 다른 알고리즘에 의해 발생된 코드일 수 있다. 예를 들면, 자동차 전장품의 일 또는 몇 개의 부품의 시리얼 넘버가 코드의 발생으로 입력된다. 코드는, 예를 들어 시리얼 넘버를 시퀀싱함에 의해 발생된다. 대체적 및 부가적으로 해쉬값(hash value)은 시리얼 넘버 또는 시퀀스트 시리얼, 형식 및 제조업자 번호로부터 형성되며, 이는 그 후 코드로서 작용한다.

<20> 이렇게 발생된 코드는 자동차 전장품에 의해 서명되어 서명된 코드가 유효한 것으로 검증되는 경우 외부 컴퓨터

시스템에 전송된다. 만약 자동차 전장품의 조작 시도 동안, 예를 들어 코드의 발생을 위해 시리얼 넘버에 의해 공헌하는 자동차 전장품의 한 부품이 변경되면, 이는 변경된 코드로 이끌며, 연속적으로 외부 컴퓨터 시스템에 의해 수신된 서명된 코드를 무효로 이끈다. 만약 외부 컴퓨터 시스템이 코드를 무효화하는 것으로 판단하는 경우, 이것은 봉쇄 신호의 전송으로 이끈다.

<21> 본 발명의 실시예에 따르면, 사용 신호와 봉쇄 신호는 모두 컴퓨터 시스템의 비밀키를 가지고 서명된다. 사용 신호 또는 봉쇄 신호가 효과적으로 되기 전에 이 신호는 자동차 전장품에 의해 두 경우에 검증된다. 이것은 사용 신호 또는 봉쇄 신호가 전송이 공인되지 않은 사이트에 의해 전송될 수 없다.

<22> 본 발명의 실시예에 따르면, 만약 예를 들어 자동차 전장품의 부품이 수리를 위하여 교환되어야 하는 경우 자동차 전장품에 부여된 쌍의 키에 대한 인증서가 보조 인증서로 대체된다. 이 경우, 코드는 부품의 교환에 의해 변할 수 있다. 보조 인증서에 대한 요구는 공인 정비소에 대하여 지정되는 것이 바람직하다

<23> 본 발명의 실시예에 따르면, 외부 컴퓨터 시스템은 소위 공개키 기반구조(PKI : Public Key Infrastructure)의 신뢰-센터에 속한다.

<24> 다른 양상에서, 본 발명은 예를 들어 신뢰-센터의 컴퓨터 시스템에 본 발명에 따른 방법의 실행을 위한 컴퓨터 프로그램 제품에 관한 것이다.

<25> 다른 양상에서, 본 발명은 차량의 암호화 정체성 검증 및/또는 암호화 인증을 실행하기 위한 수단, 상기 차량의 사용 상태를 판단하기 위한 수단, 및 상기 사용 상태의 함수로서 차량에 대한 신호를 전송하기 위한 수단을 포함하는 것을 특징으로 하는 컴퓨터 시스템에 관한 것이다.

<26> 다른 양상에서, 본 발명은 자동차 전장품에 의해 수행되는 자동차의 보호방법에 관한 것이다. 이 방법은 외부 컴퓨터 시스템에서 자동차의 암호화 정체성 검증 및/또는 암호화 인증을 실행하는 단계, 및 컴퓨터 시스템으로부터 사용 신호 또는 봉쇄 신호를 수신하는 단계를 포함한다.

<27> 본 발명의 실시예에 따르면, 차량에 부여된 코드는 자동차 전장품에 의해 서명되고, 서명된 코드는 외부 컴퓨터 시스템으로 전송되며, 또한 서명된 코드는 거기서 유효성에 대하여 검증될 수 있다. 자동차에 부여된 코드는 예를 들어 자동차 전장품의 부품에 저장된 시리얼, 형식 및/또는 제조업자 식별자와 같은 자동차 전장품의 부품의 일 또는 몇 개의 식별자로부터 발생될 수 있다. 자동차에 부여된 코드는 따라서 그것의 부품의 현재 위치에 의해 정의되는 자동차의 특성이며, 따라서 말하자면 자동차의 "지문”으로 간주될 수 있다.

<28> 본 발명의 실시예에 따르면, 봉쇄 신호가 수신된 후 자동차의 현재 지리적인 위치를 정의하는 위치 신호가 발생된다. 이러한 것은 도난으로 공표된 자동차의 발견을 용이하게 한다.

<29> 다른 양상에서, 본 발명은 자동차 전장품에 의해 수행될 본 발명에 따른 방법의 실행을 위한 명령을 구비한 컴퓨터 프로그램 제품에 관한 것이다.

<30> 다른 양상에서, 본 발명은 전자 제어 장치(ECU : Electronic Control Unit)와 같은 자동차 전장품 장치에 관한 것으로, 컴퓨터 시스템에서 자동차의 암호화 정체성 검증 및/또는 암호화 인증을 실행하는 수단, 및 컴퓨터 시스템으로부터 사용 신호 또는 봉쇄 신호를 수신하는 수단을 포함하는 것을 특징으로 한다.

<31> 자동차에 대한 코드 특성의 발생을 위하여 자동차 전장품의 개별적인 부품이 조작을 방지하도록 제어장치 및/또는 상호간에 암호화 정체성 검증 및/또는 암호화 인증을 위해 형성될 수 있다.

실 시 예

<43> 서로 대응하는 다음 실시예의 요소들에는 동일한 참조번호가 지정된다.

<44> 도 1은 예를 들어 승용차 또는 상용차일 수 있는 자동차(100)를 개략적으로 보여준다. 자동차(100)는 특히 도난으로부터 보호되어야 할 고가의 자동차이다.

<45> 자동차(100)는 자동차 전장품(102)을 포함하며, 이 자동차 전장품은 하나 이상의 자동차 전자 장치를 포함할 수 있다. 자동차 전자 장치는 예를 들어 CAN 및/또는 LIN 버스를 통하여 서로 통신이 이루어질 수 있는 예를 들어 소위 ECUs(Electronic Control Units)일 수 있다.

<46> 명령(104)은 암호화 프로토콜을 구현하도록 자동차 전장품(102)에 의해 실현될 수 있다. 대체 방법 또는 부가적으로 자동차 전장품(102)은 예를 들어 명령(104)의 실행을 위한 마이크로매소드(micromethod)를 포함하는 가입

자 식별 모듈(SIM: Subscriber Identity Module) 포맷에서 칩 카드를 위해 칩 카드 리더를 포함할 수 있다.

<47> 자동차(100)는 네트워크(106)를 통하여 컴퓨터 시스템(108)과 접속될 수 있다. 네트워크(106)는 공중 통신 네트워크, 예를 들어 셀룰러 무선통신 및/또는 컴퓨터 네트워크, 특히 인터넷 일 수 있다. 자동차 전장품(102)과 컴퓨터 시스템(108) 사이에 통신은 GSM, UMTS, 또는 CDMA와 같은 셀방식 무선접속을 통하여 구현될 수 있으며 또한, 예를 들어 아날로그 FM 또는 TMC의 일부로서 다른 무선 접속의 도움으로 구현될 수 있다. 또한, 업링크, 즉, 자동차 전장품(102)으로부터 컴퓨터 시스템(108) 및 다운링크, 즉 컴퓨터 시스템(108)으로부터 자동차 전장품(102)으로의 통신 접속에 상이한 메시징 채널이 사용될 수 있다. 이것은 컴퓨터 시스템(108 및 114) 사이의 통신에 대하여도 유사하게 적용된다.

<48> 컴퓨터 시스템(108)은 예를 들어 소위 신뢰-센터(Trust-Center)에 높은 보안 환경에 위치되는 것이 바람직하다. 컴퓨터 시스템(108)은 암호화 프로토콜의 구현을 위해 컴퓨터 프로그램의 명령(110)을 실행하는 역할을 한다.

<49> 암호화 프로토콜에 의하여 자동차(100)의 정체성은 결정 및/또는 검증된다. 자동차(100)는 예를 들어 자동차의 공인 등록증과 같은 다른 식별자(identifier) 또는 자동차 특수 코드에 의해 명확하게 식별된다. 이러한 자동차 식별 코드 또는 이러한 식별자나 차량 ID는 자동차 식별자(자동차 ID)로서 다음에 지정될 것이다.

<50> 키로서 자동차 ID를 갖는 경우 컴퓨터 시스템(108)은 저장장치(112)를 액세스할 수 있으며, 저장장치에는 봉쇄된 자동차의 자동차 ID가 분실 메시지가 이루어진 경우에 저장되어 있다. 봉쇄된 자동차의 대응하는 봉쇄 9blocking) 리스트는 데이터베이스 형태로 저장장치(112)에 기억될 수 있다.

<51> 저장장치(112)로의 봉쇄 입력은 컴퓨터 시스템(108)을 통하여 직접적으로 이루어질 수 있다. 그러나, 이러한 봉쇄는 또한 네트워크(106) 또는 다른 통신 접속을 통하여 컴퓨터 시스템(108)과 데이터를 교환할 수 있는 다른 컴퓨터 시스템(114)으로부터 입력될 수 있는 것도 가능하다.

<52> 본 실시예에서 컴퓨터 시스템(114)은 또한 암호화 프로토콜의 구현을 위해 컴퓨터 프로그램의 명령(116)을 실행하는 역할을 한다. 암호화 프로토콜에 의해 컴퓨터 시스템(114)의 정체성 및 저장장치(112)로 자동차의 봉쇄를 입력하기 위한 인증이 결정 및/또는 검증된다. 더욱이, 컴퓨터 시스템(114)은 자동차의 분실 메시지를 녹음하는 역할을 하는 애플리케이션 프로그램(118)을 구비하고 있다.

<53> 만약 자동차(100)의 사용이 승인 받은 사용자에 의해 수행되는 경우 자동차(100)에 대한 저장장치(112)에 어떤 봉쇄도 저장되지 않는다. 자동차(100)의 시동시에 명령(104)의 실행이 예를 들어 자동차 전장품(102) 또는 칩 카드에 의해 시작된다. 자동차 전장품(102)은 명령의 실행이 여기서 개시되도록 네트워크(106)를 통하여 컴퓨터 시스템(108)과 접속을 수립한다. 자동차 전장품(102)에 의한 명령(104)의 실행 및 컴퓨터 시스템(108)에 의한 명령(110)의 실행에 의해 암호화 프로토콜은 예를 들어 자동차의 자동차 ID의 진정성(authenticity)이 검증되는 데 기반을 두고 실현된다. 네트워크(106)를 통하여 자동차 전장품(102)과 컴퓨터 시스템(108) 사이의 통신은 예를 들어 소위 요구-응답 프로토콜(Request-Response Protocol), 즉 http 또는 https에 따라 이루어진다.

<54> 자동차(100)의 정체성이 암호화 프로토콜의 방법에 의해 검증 및/또는 인증된 후, 컴퓨터 시스템(108)은 자동차(100)의 봉쇄가 저장장치(112)에 저장되어 있는지 여부를 검증한다. 여기서는 그렇지 않기 때문에 컴퓨터 시스템(108)은 그 후 자동차(100)에 네트워크(106)를 통하여 전송되는 사용 신호를 전송한다. 자동차(100)의 사용은 단지 사용 신호의 수신에 기초하여 구현될 수 있다. 자동차(100)의 엔진은 단지 예를 들어 사용 신호의 수신 후에 비활성화된 이모빌라이저(immobilizer) 시스템에 의해 시동되거나 또는 사용 신호의 수신 후에 자동차(100)의 수동 브레이크 및/또는 브레이크가 단지 해제될 수 있다.

<55> 사용 신호는 유효 기간의 종료 전에 자동차(100)의 동작 동안 매번 이런 방법이 반복되도록 일정한 유효 기간을 가질 수 있다.

<56> 만약 자동차(100)가 도난된 경우, 자동차(100)의 소유자는 컴퓨터 시스템(114)을 동작시키는 봉쇄 서비스와 접촉할 수 있다. 이러한 봉쇄 서비스는 예를 들어, 서비스 회사, 공인 기관 또는 경찰에 의해 유효하게 될 수 있다.

<57> 만약 소유자가 자동차(100)의 분실을 공고하는 경우 이는 애플리케이션 프로그램(118)에 의해 등록된다. 컴퓨터 시스템(114)은 컴퓨터 시스템(108)과 접속을 수립하며 컴퓨터 시스템(114)의 암호화 정체성 검증 및/또는 암호화 인증이 컴퓨터 시스템(108)과 끝나면 봉쇄 요구가 단지 이러한 목적으로 승인받은 컴퓨터 시스템에 의해서만 등록이 이루어지는 것을 보장한다. 컴퓨터 시스템(114)과 컴퓨터 시스템(108) 사이에 성공적인 암호화 정체성 검증 및/또는 암호화 인증이 이루어진 후 봉쇄 신호는 예를 들어 자동차 ID를 가지고 컴퓨터 시스템(114)으로부

터 네트워크(106)를 통하여 저장장치(112)에 저장되도록 컴퓨터 시스템(108)에 전송된다.

<58> 만약 자동차(100)의 도난 후에 저장장치(112)에 봉쇄가 저장된 후 자동차(100)의 점화장치가 활성화되면 그 후 명령(104)의 실행이 자동차 전장품(102)에 의해 다시 개시된다. 컴퓨터 시스템(108)에 의한 자동차(100)의 정체성 검증 및/또는 인증이 이루어진 후, 컴퓨터 시스템(108)은 자동차(100)에 대한 봉쇄가 저장장치(112)의 파일에 보존되어 있는 것을 사실상 결정하게 된다. 따라서, 컴퓨터 시스템(108)은 자동차(100)가 사용될 수 없도록 자동차(100)에 사용 신호를 전송하지 않는다. 한편, 컴퓨터 시스템(108)은 이 경우 자동차(100)에 봉쇄 신호를 전송하여 자동차를 움직이지 못하게 한다.

<59> 만약 자동차 전장품(102)의 하나 이상의 부품을 변경함에 의해 이러한 보안 메커니즘을 회피하도록 자동차 전장품(102)에 대한 조작 시도가 취해질 경우 이는 암호화 정체성 검증 및/또는 암호화 인증이 확실하게 실패하도록 자동차 ID의 변경으로 이끈다.

<60> 명령(104 및 110 또는 116 및 110)에 의해 구현되는 암호화 프로토콜은 예를 들어 다음과 같이 진행될 수 있다:

<61> 자동차 전장품(102)은 컴퓨터 시스템(108)에 요구(request)를 전송한다. 컴퓨터 시스템(108)은 그 후 난수(random number), 특히 의사 난수(pseudo random number)를 생성한다. 난수는 컴퓨터 시스템(108)에 의해 네트워크(106)를 통하여 자동차(100)에 전송된다. 자동차 전장품(102)은 자동차 전장품이 암호화된 수를 수신하도록 예를 들어 칩 카드에 저장된 비밀키(secret key)에 의해 수신된 난수를 부호화한다.

<62> 이 암호화된 수 뿐 아니라 자동차 전장품(102)의 인증서(certificate)가 자동차 전장품(102)에 의해 컴퓨터 시스템(108)에 응답(response)으로서 전송된다. 컴퓨터 시스템은 인증서의 공개키(public key)에 의해 암호화된 수를 해독한다. 만약 컴퓨터 시스템(108)에 의해 생성된 난수가 자동차 전장품(102)으로부터 응답으로서 수신된 난수와 일치하는 경우, 그 후 자동차(100)의 정체성 검증 및/또는 인증이 성공적으로 완료된다.

<63> 예로서, 자동차 전장품(102)은 암호화 프로토콜의 시작을 위한 최초 요구를 한쌍의 키에 속하는 인증서와 함께 컴퓨터 시스템(108)에 전송한다. 인증서는 이 차량에 대하여 봉쇄가 저장되어 있는 지를 검증하도록 저장장치(112)에 대한 액세스용 액세스키(access key)를 자동차 ID 형태로 컴퓨터 시스템(108)이 수신하도록 자동차(100)의 자동차 ID를 포함할 수 있다.

<64> 동일한 원리에 따르면 또한 컴퓨터 시스템(108)과 컴퓨터 시스템(114)의 암호화 정체성 검증 및/또는 암호화 인증이 진행될 수 있다. 컴퓨터 시스템(114)은 또한 컴퓨터 시스템(108)으로부터 컴퓨터 시스템(114)의 공개키를 사용하여 부호화된 난수를 수신하며, 컴퓨터 시스템(114)은 비밀키를 사용하여 해독한 후, 컴퓨터 시스템(108)에 난수를 다시 전송한다. 만약 컴퓨터 시스템(108)에 의해 부호화된 난수가 컴퓨터 시스템(114)으로부터의 응답으로서 수신된 난수와 일치하는 경우, 그 후 다시 암호화 정체성 검증 및/또는 암호화 인증이 성공적으로 완료된다.

<65> 각각이 네트워크(106)를 통하여 컴퓨터 시스템(108)과 통신을 할 수 있는 상이한 컴퓨터 시스템들(114)이 분실 메시지의 등록을 위해 분권적으로 분산되어 존재할 수 있다. 예를 들면, 이러한 컴퓨터 시스템들(114)은 자동차의 분실이 전화 또는 이메일과 같은 다른 수단에 의해 알려질 수 있는 경찰서, 공인 카 딜러 또는 정비소, 및/또는 카센터에 위치될 수 있다.

<66> 이는 무단 사용에 대한 자동차의 보호가 효과적으로 이루어지며, 차량 절도를 흥미 없게 만든다. 본 발명에 따르면 생체측정 안전장치 또는 알람과 같은 운전자에 의해 직접적으로 영향을 받는 어떤 안전 장비도 존재하지 않기 때문에 자동차의 승인 받은 사용자에 대한 잠재적인 위협은 부가적으로 감소된다.

<67> 도 2는 대응하는 흐름도를 나타낸다. 단계(200)에서 예를 들어 자동차의 문을 열기 위하여 중앙 로킹(central locking)의 활성화, 엔진을 시동시키기 위하여 자동차의 시동장치의 활성화 또는 브레이크를 해제하기 위하여 수동 또는 풋 브레이크의 활성화와 같은 자동차의 동작 소자의 활성화가 이루어진다.

<68> 단계(200)에서 이러한 활동을 통하여 사용 또는 봉쇄 신호의 수신에 대한 암호화 정체성 검증 및/또는 암호화 인증을 위한 후속된 방법이 개시된다. 만약 예를 들어 자동차의 문을 열기 위한 원격 제어의 활성화에 의해 이미 순서가 개시된 경우, 이러한 것은 운전자가 자동차에 접근하여 자동차에 타는 동안 이미 방법이 작동되고 있으며, 운전자가 자동차에 도착할 때 이미 결론이 날 수 있으며, 그 결과 운전자가 차에 들어간 후 운전자는 단지 약간의 시간 지연이 있거나 또는 지연 없이 자동차의 동작을 개시할 수 있는 장점을 갖게 된다.

<69> 이러한 방법의 시작은 또한 예를 들어 소위 키레스-고 록킹 시스템(Keyless-go locking system)이 활성화된 후에 자동적으로 행하여질 수 있다. 따라서, 만약 록킹 시스템이 자동차의 근접 위치에서 RFID 키 카드를 감지하

는 경우, 방법은 시작된다.

<70> 단계(202)에서 대응하는 신뢰-센터의 컴퓨터에서 자동차의 정체성 검증 및/또는 인증이 암호화 프로토콜을 통한 방법의 실행에 의해 행하여진다(또한 도 1의 명령(104 및 110) 참조).

<71> 자동차에 대한 성공적인 암호화 정체성 검증 및/또는 암호화 인증이 이루어진 후, 신뢰-센터는 만약 자동차가 봉쇄 리스트에 등록되어 있는 지를 검증한다. 만약 자동차가 봉쇄 리스트에 등록되어 있지 않는 경우, 자동차-특유의 사용 신호가 자동차에 대하여 발생되어 단계(206)에서 자동차로 전송된다.

<72> 사용 신호는 바람직하게는 신뢰-센터에 의해 서명된다. 사용 신호의 서명은 신뢰-센터의 공개키의 도움으로 자동차 전장품에 의해 검증된다. 만약 사용 신호의 서명이 유효할 경우에만 자동차의 사용이 가능하도록 자동차 전장품에 의해 받아들여질 것이다. 사용 신호는 또한 바람직하게는 대응하는 자동차의 자동차 ID를 포함한다.

<73> 반대의 경우, 즉 만약 자동차가 봉쇄 리스트에 등록되어 있는 경우, 봉쇄 신호가 발생되어 자동차로 전송된다(단계 208). 이는 즉시 또는 예를 들어 자동차의 다음 시동시에 자동차를 움직이지 못하게 유도한다.

<74> 자동차 전장품은 자동차의 현재 지리적인 위치 데이터를 포함하는 메시지를 가진 봉쇄 신호에 응답할 수 있다. 이것은 자동차의 발견을 단순하게 한다.

<75> 도 3은 신뢰-센터의 컴퓨터 시스템(108)과 자동차 전장품(102)의 부가적인 실시예를 나타낸다. 컴퓨터 시스템(108)에서 암호화 프로토콜의 실행 뿐 아니라 사용 및 봉쇄 신호의 서명을 위한 신뢰-센터(108)의 공개키(132)와 비밀키(134)가 저장되어 있다.

<76> 여기에 언급된 실시예에서 자동차 전장품(102)은 예를 들어 차량 네트워크(122)를 통하여 서로 연결되어 있는 부품(A,B,C...)과 같이 상이한 부품(120)을 갖고 있다. 차량 네트워크(122)는 예를 들어, CAN 및/또는 LIN Bus 일 수 있다.

<77> 각각의 부품(120)에는 식별자가 부여되어 있으며 이는 대응하는 부품의 비휘발성 또는 쉽게 조작되지 않는 저장장치에 기억되어 있다. 이러한 코드는 예를 들어 대응하는 부품(120)의 저장장치(124)에 기억되어 있는 대응하는 시리얼 넘버일 수 있다.

<78> 적어도 부품들(120) 중의 하나는 자동차(100)에 할당된 공개키(126)와 비밀코드(128)로 구성되는 한쌍의 키에 대하여 접근할 수 있다. 인증서(130)는 한쌍의 키(126,128)에 속한다.

<79> 인증서(130)에서 코드는 예를 들어 자동차(100)의 식별에 소용이 되도록 저장되어 있다. 이 코드는 명령(104)의 실행에 의해 발생되며, 이 명령은 미리 설정된 알고리즘의 도움으로 이들 시리얼 넘버(A,B,C)에 기초한 코드를 발생하도록 상이한 부품(120)의 시리얼 넘버(A,B,C)가 문의되는 방식으로 미리 설정된 알고리즘을 구현한다.

<80> 암호화 프로토콜의 실행을 위하여 명령(104)은 부품(120)으로부터 시리얼 넘버(A,B,C)를 문의함에 의해 코드를 결정한다. 따라서, 발생된 코드는 비밀키(128)를 가지고 서명된 후 인증서(130)와 함께 컴퓨터 시스템(108)에 전송된다. 컴퓨터 시스템(108)은 공개키(126)를 사용하여 서명된 코드의 유효성을 검증한다. 만약 서명된 코드가 정확한 경우, 즉 인증서(130)에 저장된 코드에 대응하는 경우에만 암호화 정체성 검증 및/또는 인증이 성공적으로 이루어진다.

<81> 암호화 정체성 검증의 목적으로 시리얼 넘버로부터 이러한 코드를 발생하는 것은 자동차 전장품(102)의 부품(120) 중 하나의 변경에 따라 결과적인 코드가 필연적으로 변하게 되는 장점을 갖게 된다. 이러한 경우, 인증서(130)에 저장된 코드와 시리얼 넘버의 쿼리 동작(querying)을 통하여 얻어진 코드는 더 이상 일치하지 않아 그 결과 암호화 정체성 검증은 반드시 실패하게 된다. 따라서, 이러한 과정을 통하여 하나 또는 몇 개 부품(120)의 교환에 의해 자동차 전장품(102)의 조작이 방지된다.

<82> 한쌍의 키(126,128)와 인증서(130)가 또한 적어도 명령(104)의 일부를 실행하는 칩 카드에 저장될 수 있다. 이 경우, 부품(A)은 대응하는 암호화 기능성을 액세스할 수 있도록 칩 카드가 삽입되어 있는 칩 카드 리더를 갖고 있다.

<83> 도 4는 인증서가 시리얼 넘버로부터 얻은 코드를 포함하지 않고 다른 명확한 자동차 ID를 포함하는 다른 실시예를 나타낸다. 이러한 자동차 ID는 예를 들어 자동차 자체의 시리얼 넘버, 차대번호, 공인등록번호 또는 임의의 다른 명확한 코드일 수 있다.

<84> 암호화 프로토콜의 실행을 위하여 자동차 전장품은 따라서 상이한 시리얼 넘버의 부품(120)으로부터 자동차-특

정 코드를 결정한다. 이 코드는 비밀키(128)를 사용하여 서명된 후 인증서(130)와 함께 네트워크(106)를 통하여 컴퓨터 시스템(108)으로 전송된다. 컴퓨터 시스템(108)은 이로부터 자동차 ID에 부여된 자동자-특정 코드를 판독하도록 키(key)로서 자동차 ID를 사용하여 속성 테이블(attribution table)(136)을 액세스한다. 이 코드는 컴퓨터 시스템(108)이 인증서(130)와 함께 자동차 전장품(102)으로부터 수신한 서명된 코드와 일치하여야만 하며, 그 결과 암호화 정체성 검증 및/또는 인증이 실행될 수 있다.

<85> 도 5는 대응하는 흐름도를 나타낸다. 자동차의 암호화 정체성 검증 및/또는 인증이 도 2의 실시예의 단계(202)에서와 유사하게 도 5의 실시예의 단계(202')의 방법에 따라 이루어질 수 있다. 교대로 또는 부가적으로 코드, 즉 시리얼 넘버의 쿼리(query)가 이 방법을 위해 형성된 제어장치에 의해 자동차 전장품의 하나 이상의 부품에 의해 단계(300)에서 수행된다. 예를 들어, 시리얼 넘버로부터 이 제어장치는 단계(302)에서 차량-특정 코드를 발생하며, 또한 이 차량-특정 코드는 단계(304)에서 자동차의 비밀키의 도움으로 서명된 후 단계(306)에서 대응하는 인증서와 함께 신뢰-센터의 컴퓨터 시스템에 전송된다. 만약 이 코드가 유효하지 않은 지를 여기서 검증된다(단계 308). 만약 코드가 무효인 경우 단계(208)가 실행되고, 반대인 경우 단계(204)가 이어서 행하여진다.

<86> 제어장치(120)와 서버(140) 사이의 통신이 안전 메시징 절차(Secure Messaging procedure)를 통하여 행하여지는 것이 바람직하다.

<87> 도 6은 셀룰러 네트워크(106)를 통하여 컴퓨터 시스템(108)과 통신을 하는 모바일 무선 안테나(138)를 구비한 자동차(100)의 실시예를 나타낸다. 컴퓨터 시스템(108)은 명령(110)을 실행하도록 작용하는 서버(140)를 구비하고 있다.

<88> 컴퓨터 시스템(140)의 한쌍의 키는 공개키(132)와 비밀키(134)로 이루어져 있으며, 이 실시예에서 칩 카드 판독장치를 통하여 서버(140)를 액세스할 수 있는 칩 카드(142)에 기억되어 있다. 봉쇄 리스트 또는 봉쇄 정보를 저장하기 위한 저장장치(112)는 이 실시예에서 서버(140)와 연결되어 있는 분리된 데이터베이스로서 형성되어 있다.

<89> 자동차 전장품의 부품(A)(도 3 및 도 4 참조)은 이 경우 제어장치로서 형성되며, 자동차(100)에 부여된 비대칭 쌍의 키(126,128)는 대응하는 칩 카드 판독장치를 통하여 제어장치(120)에 의해 액세스될 수 있는 칩 카드(144)에 기억되어 있다.

<90> 자동차 전장품의 부가적인 부품(120)은 이 경우 엔진 전자 부품, 2개의 전자 부품 뿐 아니라 차대 전자 부품이며, 이들 각각은 분리된 ECU로서 형성될 수 있다. ECU 각각에서 분리된 비대칭 쌍의 키(146, 146', 146", 146''')는 저장된다.

<91> 부품(120)의 코드, 예를 들어, 시리얼 넘버의 쿼리 전에 이들의 정체성이 우선 대응하는 쌍 키의 도움으로 제어장치(120)에 의해 암호방식으로 검증 및/또는 인증이 이루어져야 한다.

<92> 이를 위해 제어장치(120)는 의사 난수를 발생하여, 대응하는 쌍의 키, 예를 들어 한쌍의 키(146)의 공개키를 가지고 부호화한 후, 네트워크(122)를 통하여 대응하는 부품(120), 고려된 예에서는 엔진 전자 부품(120)에 전송하는 방식으로 진행하는 것이 가능하게 될 것이다.

<93> 엔진 전자 부품(120)은 그 후 쌍의 키(146)의 비밀키의 도움으로 제어장치에 의해 수신된 암호화된 수를 해독하여 제어장치에 해독된 수를 다시 전송한다. 만약 엔진 제어 전장품에 의해 수신되어 해독된 암호화된 수가 원래 전송된 난수와 일치하는 경우에만 엔진 전자 부품(120)의 정체성이 제어장치(120)에 의해 검증 및/또는 인증되며, 이 때 시리얼 넘버가 쿼리될 수 있다.

<94> 만약 제어장치에서 부품(120) 중 하나의 암호화 정체성 검증 및/또는 인증이 실패하는 경우, 그 후 후자는 코드를 발생할 수 없으며 따라서 컴퓨터 시스템(108)에 대응하는 에러 메시지를 전송하며, 이는 그 후 자동차(100)의 봉쇄를 개시할 수 있다.

<95> 도 7은 본 발명에 따른 방법의 다른 실시예를 나타낸다. 단계(400)에서 차량이 예를 들어, 시동버튼을 누름에 의해 활성화된다(도 2 및 도 5의 단계(200)를 참조). 이 이후에 단계(402)에서 차량과 신뢰-센터 사이에 통신 접속이 설정된다. 데이터 접속에 의해 단계(404)에서 제1 암호화 인증 단계가 예를 들어 상기한 의사 난수의 교환에 의해 수행된다.

<96> 단계(404)에서 암호화 인증의 제1단계의 성공적인 완료 후에 신뢰-센터는 단계(406)에서 자동차로부터 서명된 자동차 ID를 요구한다. 자동차는 그 후 단계(408)에서 자동차 ID에 대한 서명을 발생하여 단계(410)에서 신뢰-센터에 서명을 전송한다. 여기서 서명은 단계(412)에서 검증된다. 만약 서명이 유효한 경우, 그 후 암호화 인증

의 제2단계가 또한 성공적으로 완료된다.

<97> 이어서, 단계(414)에서 자동차에 대한 봉쇄 리스트로 봉쇄가 입력되어 있는 지 여부가 검증된다. 만약 봉쇄 리스트에 등록되어 있지 않는 경우 해제 코드 형태의 사용 신호는 단계(416)에서 자동차에 전송되어, 단계(418)에서 자동차에 수신되어 자동차의 사용이 허락된다.

<98> 그러나, 만약 단계(414)에서 자동차의 봉쇄 리스트에 봉쇄가 등록되어 있는 것이 밝혀지면 그 후 연속하여 봉쇄 코드의 형태로 봉쇄 신호가 단계(419)에서 자동차에 전송되어 단계(420)에서 자동차에 수신된다. 이어서, 자동차는 단계(422)에서 예를 들어 GPS 수신기의 요구에 의해 현재 지리적인 위치를 결정하여 단계(422)에서 현재 위치를 신뢰-센터에 전송한다. 신뢰-센터는 그 후 단계(424)에서 예를 들어, 경찰에 이 위치 정보를 전송한다.

<99> 도 8은 봉쇄 리스트의 업데이트를 위한 본 발명에 따른 방법의 실시예를 나타낸다. 단계(500)에서 예를 들어, 자동차의 사용자 또는 소유자가 이 자동차의 도난을 공표하는 분실 메시지가 봉쇄 서비스에 도달한다. 이어서, 단계(502)에서 봉쇄 서비스와 신뢰-센터 사이에 데이터 접속이 확립된다.

<100> 단계(504)에서 봉쇄 서비스는 신뢰-센터에서 인증된다. 성공적인 인증 후에 신뢰-센터는 단계(506)에서 봉쇄 마스크를 발생하며, 봉쇄 마스크에 의해 도난으로 공표된 자동차에 부여된 인증서의 봉쇄가 봉쇄 서비스에 의해 입력될 수 있다(단계 508). 인증서의 봉쇄 요구가 단계(510)에서 봉쇄 서비스의 비밀키를 사용하여 서명되며 이는 신뢰-센터에 전송된다. 신뢰-센터는 단계(412)에서 봉쇄 서비스의 서명을 검증하며 서명이 유효할 경우 단계(514)에서 봉쇄 리스트를 업데이트한다.

<101> 고가의 자동차일지라도 자동차 전장품(102)의 부품(120) 중의 하나가 때때로 고장날 수 있으며 새로운 것으로 대체되어야 한다(도 3 및 도 4 참조). 부품(120) 중 하나를 교환함에 의해 그들의 식별자가 연속하여 예를 들어, 시리얼 넘버를 변경하며 따라서 또한 결과적으로 코드가 변하게 된다. 이러한 경우 인증서(130)는 요구에 따라 새로운 인증서에 의해 교환되어야 하며, 새로운 인증서는 업데이트된 코드를 포함한다. 조작을 피할 수 있도록 도 9에 도시된 바와 같은 이러한 목적으로 공인된 정비소에서 인증서의 교환이 이루어져야 한다.

<102> 공인 정비소는 정비소 컴퓨터(148), 예를 들어 자동차 전장품(102)에 대한 상이한 진단 기능을 가진 특수 개인용 컴퓨터를 구비한다. 정비소 컴퓨터(148)는 예를 들어 자동차 전장품(102)과 하나 이상의 케이블(150)을 통하여 직접 연결될 수 있다.

<103> 정비소 컴퓨터는 공개키(152)와 비밀키(154)로 이루어진 비대칭 쌍의 키 뿐 아니라 대응하는 공인 정비소에 부여된 대응하는 인증서(156)를 포함하고 있다. 공인 정비소는 인증서(156)에 등재되어 있다.

<104> 정비소 컴퓨터(156)는 예를 들어, 네트워크(106)를 통하여 신뢰-센터의 컴퓨터 시스템(108)과 통신할 수 있다. 컴퓨터 시스템(108)은 인증서의 발생을 위하여 인증서 발생기(158)를 구비한다.

<105> 자동차 전장품(102)의 하나 이상의 부품(120)이 대응하는 교체품으로 교체된 후, 정비소 컴퓨터(148)는 자동차 전장품(102)으로부터 결과적인 코드를 판독한다. 정비소 컴퓨터(148)는 그 후 컴퓨터 시스템(108)과 접속을 확립하고 그 컴퓨터 자체를 인증한다. 성공적인 인증이 이루어진 후 정비소 컴퓨터(148)는 컴퓨터 시스템(108)에 새로운 코드를 갖는 새로운 인증서에 대한 요구를 전송한다. 이어서, 인증서 발생기(158)가 개시되어 정비소 컴퓨터(148)를 통하여 입력되거나 또는 자동차 전장품(102)으로 직접 입력되는 대응하는 업데이트된 인증서(130)를 발생하여 종전 인증서(130)에 겹쳐 쓴다.

<106> 도 10은 대응하는 흐름도이다. 자동차 전장품이 수리된 후 자동차 전장품과 정비소 컴퓨터 사이에 데이터 접속이 확립되며(단계 600), 단계(602)에서 정비소 컴퓨터와 신뢰-센터 사이에 데이터 접속이 확립된다. 이어서, 정비소 컴퓨터의 정체성이 단계(604)에서 신뢰-센터에서 암호방식으로 식별 및/또는 인증된다.

<107> 신뢰-센터에서 정비소 컴퓨터의 성공적인 암호화 인증이 이루어진 후, 정비소 컴퓨터는 단계(606)에서 자동차 전장품으로부터 전장품의 하나 이상의 부품의 교환에 따른 결과로 부여된 새로운 코드를 판독하여 이에 기초하여 단계(608)에서 신뢰-센터에 대응하는 새로운 인증서에 대한 요구(request)를 전송한다.

<108> 이 요구는 또한 새로운 코드를 포함한다. 이어서, 신뢰-센터는 단계(610)에서 새로운 인증서를 확립하여 그것을 단계(612)에서 정비소 컴퓨터에 전송한다. 정비소 컴퓨터는 그 후 단계(614)에서 예를 들어, 새로운 인증서로 종래의 인증서를 겹쳐 쓰는 방식으로 자동차 전장품에 새로운 인증서를 설치한다. 예로서 새로운 인증서는 안전 메시징에 의해 자동차 전장품의 제어장치의 칩 카드로 직접 기록된다(도 6의 제어장치(120)와 칩 카드(144) 참조).

<109> 부재번호 리스트

<110> -

<111> 100 : 자동차

<112> 102 : 자동차 전장품

<113> 104 : 명령

<114> 106 : 네트워크

<115> 108 : 컴퓨터 시스템

<116> 110 : 명령

<117> 112 : 저장장치

<118> 114 : 컴퓨터 시스템

<119> 116 : 명령

<120> 118 : 애플리케이션 프로그램

<121> 120 : 부품

<122> 122 : 네트워크

<123> 124 : 저장장치

<124> 126 : 공개키

<125> 128 : 비밀키

<126> 130 : 인증서

<127> 132 : 공개키

<128> 134 : 비밀키

<129> 136 : 속성 테이블

<130> 138 : 모바일 무선 안테나

<131> 140 : 서버

<132> 142 : 칩 카드

<133> 144 : 칩 카드

<134> 146 : 한쌍의 키

<135> 148 : 정비소 컴퓨터

<136> 150 : 케이블

<137> 152 : 공개키

<138> 154 : 비밀키

<139> 156 : 인증서

<140> 158 : 인증서 발생기

도면의 간단한 설명

<32> 이하에 본 발명의 실시예에 대한 예가 도면을 참조하여 더욱 상세하게 설명된다.

<33> 도 1은 본 발명에 따른 컴퓨터 시스템과 자동차 전자 장치의 실시예의 블록도,

<34> 도 2는 본 발명에 따른 방법의 실시예의 흐름도,

<35> 도 3은 본 발명에 따른 컴퓨터 시스템과 자동차 전자 장치의 다른 실시예의 블록도,

<36> 도 4는 본 발명에 따른 컴퓨터 시스템과 자동차 전자 장치의 다른 실시예의 블록도,

<37> 도 5는 본 발명에 따른 방법의 실시예의 흐름도,

<38> 도 6은 본 발명에 따른 신뢰-센터(Trust-Center)와 차단 서비스(blocking service)의 컴퓨터 시스템과 자동차 전자 장치의 다른 실시예의 블록도,

<39> 도 7은 본 발명에 따른 방법의 다른 실시예의 흐름도,

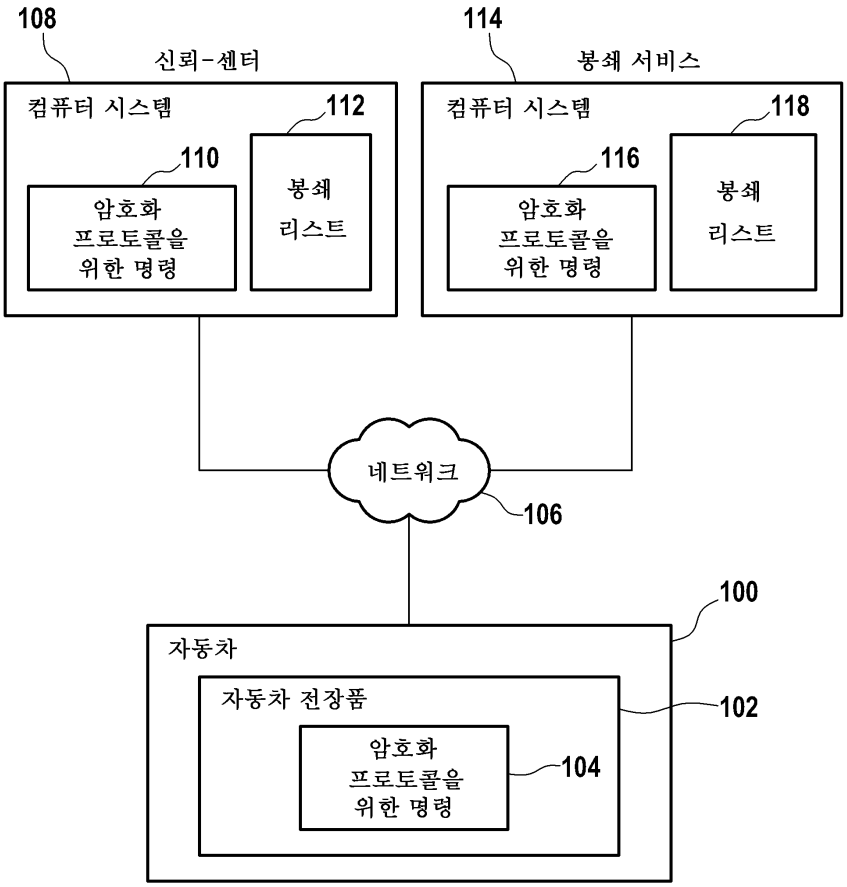
<40> 도 8은 본 발명에 따른 방법의 다른 실시예의 흐름도,

<41> 도 9는 본 발명에 따른 신뢰-센터(Trust-Center)의 컴퓨터 시스템과, 정비공장의 컴퓨터 시스템 및 자동차 전자 장치의 다른 실시예의 블록도, 및

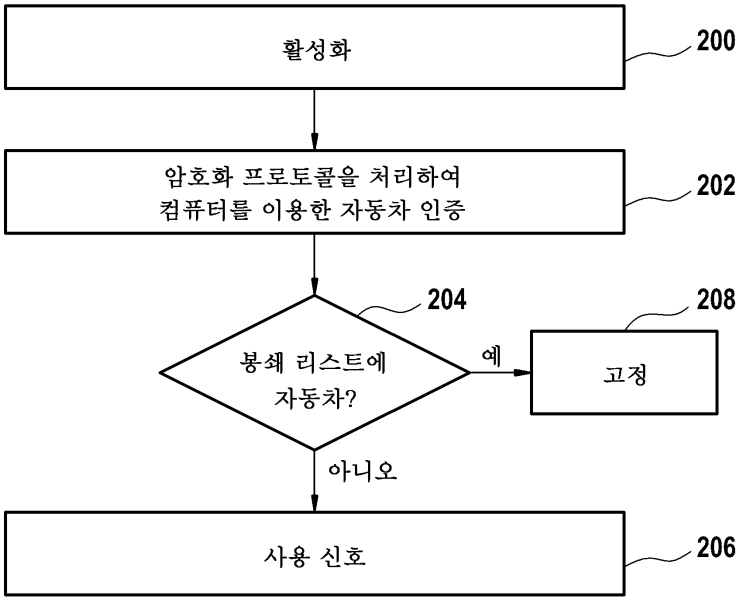
<42> 도 10은 본 발명에 따른 방법의 다른 실시예의 흐름도.

도면

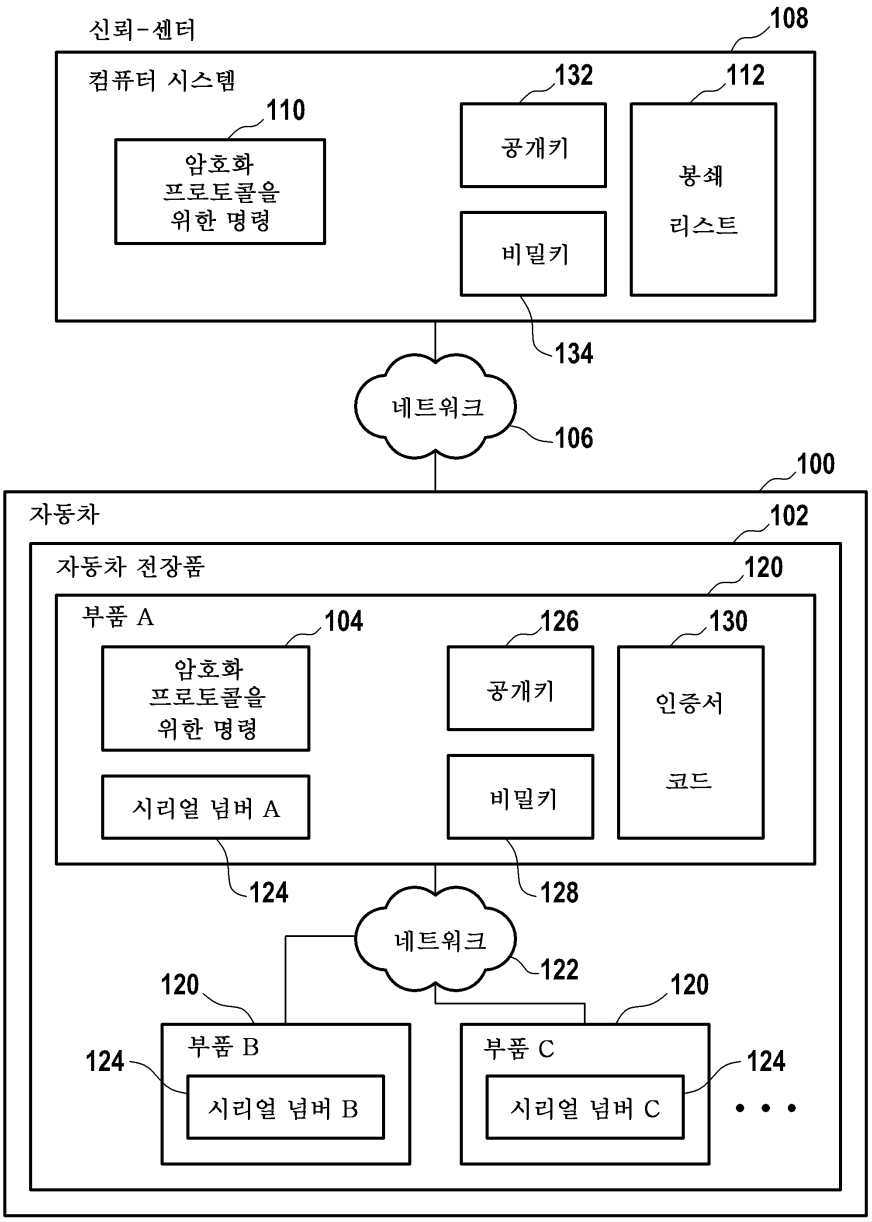
도면1



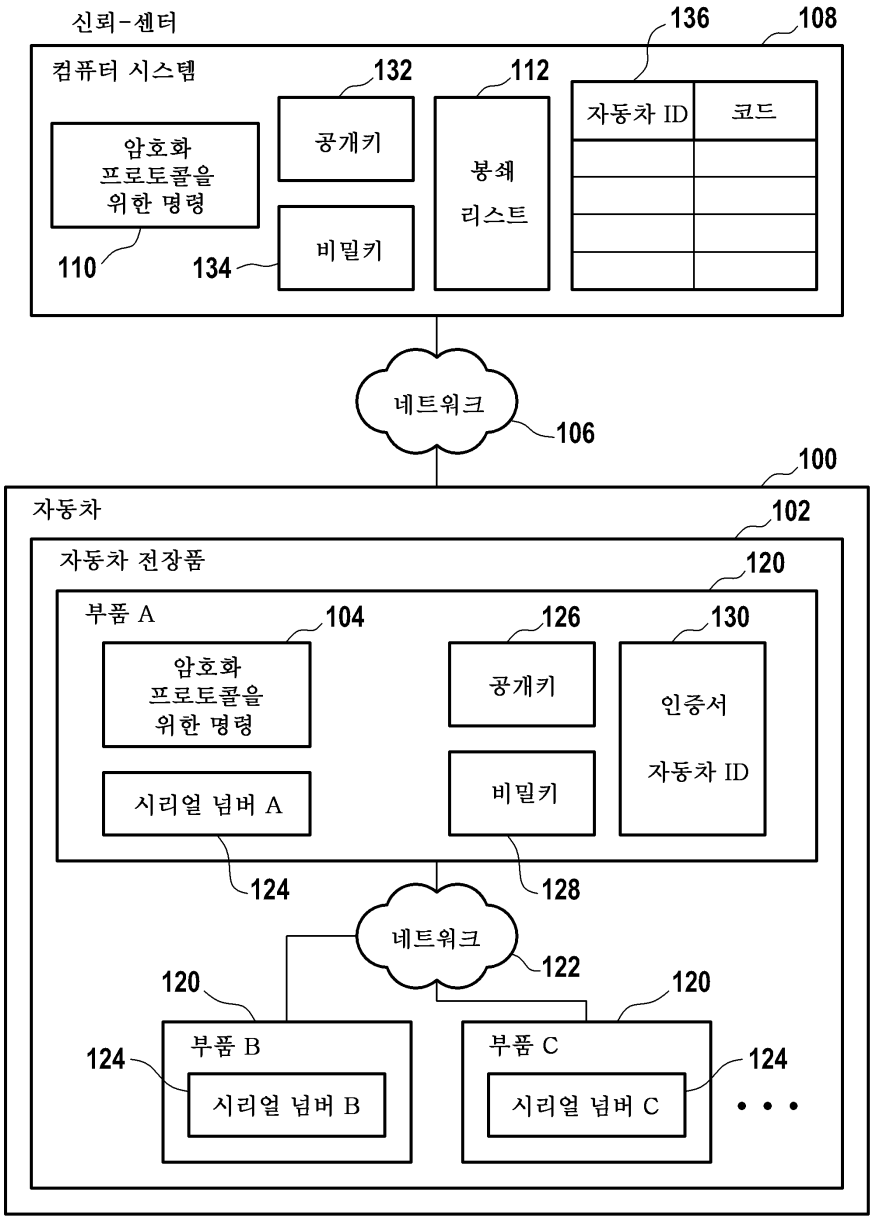
도면2


활성화
200
암호화 프로토콜을 처리하여
컴퓨터를 이용한 자동차 인증
202
204
208
봉쇄 리스트에
자동차?
예
고정
아니오
사용 신호
206

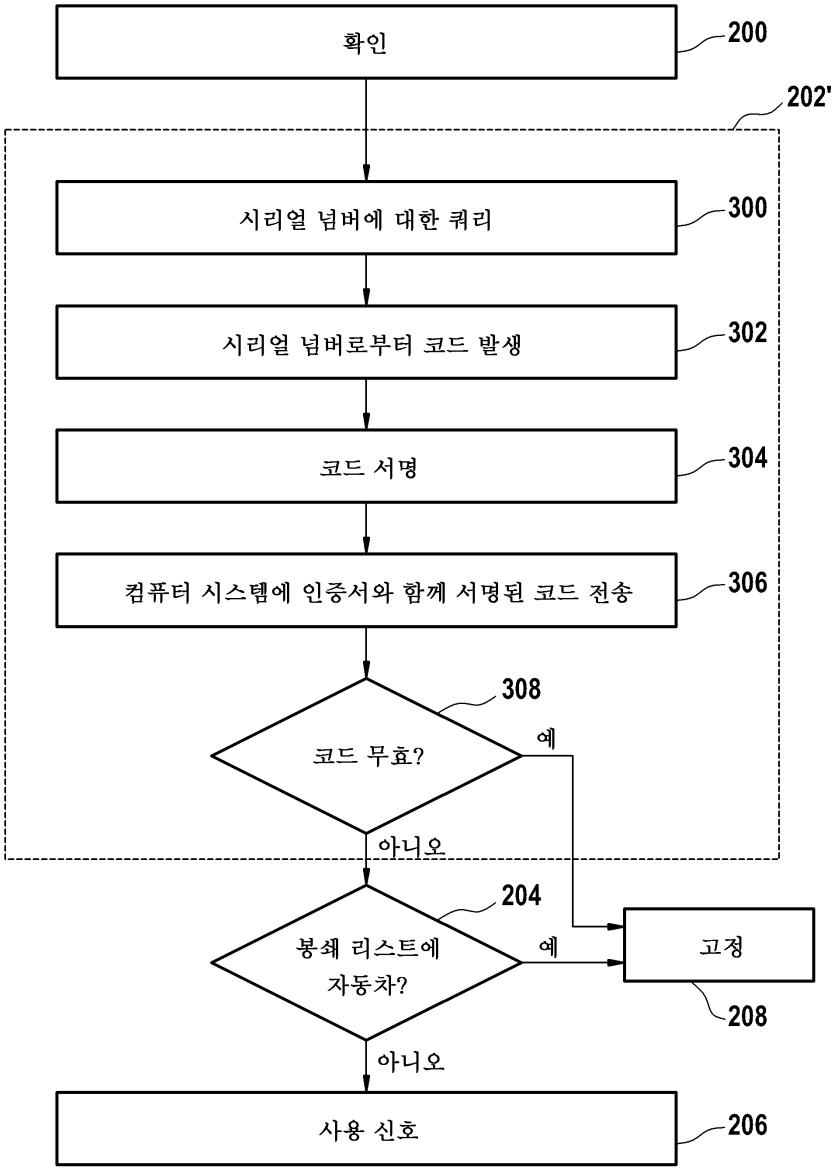
도면3


신뢰-센터
108
컴퓨터 시스템
110
암호화
프로토콜을
위한 명령
132
공개키
112
봉쇄
리스트
비밀키
134
네트워크
106
100
자동차
102
자동차 전장품
120
부품 A
104
암호화
프로토콜을
위한 명령
126
공개키
130
인증서
코드
시리얼 넘버 A
비밀키
124
128
네트워크
122
120
120
부품 B
124
시리얼 넘버 B
부품 C
시리얼 넘버 C
124
• • •

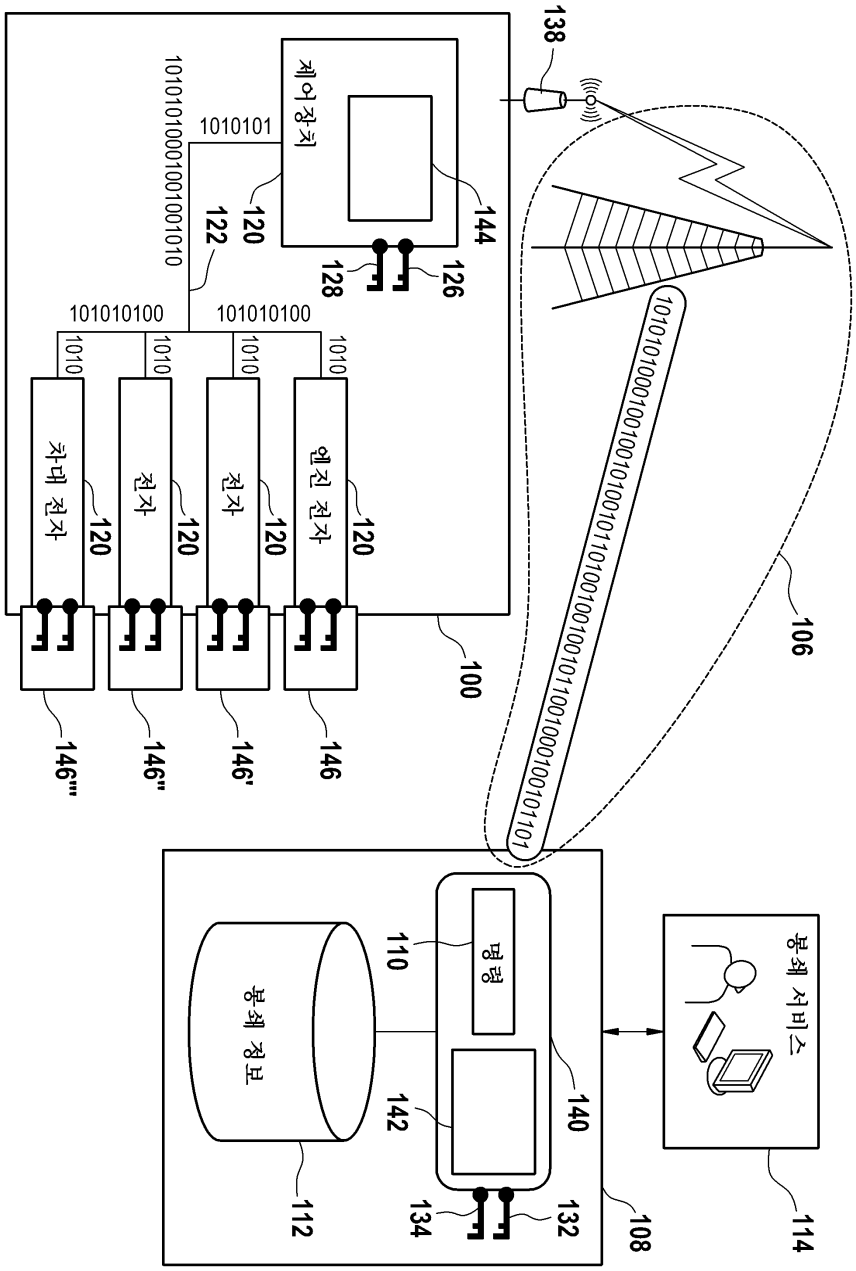
도면4


신뢰-센터
136
108
컴퓨터 시스템
132
112
자동차 ID
코드
암호화 프로토콜을 위한 명령
공개키
봉쇄 리스트
비밀키
110
134
네트워크
106
100
자동차
102
자동차 전장품
120
부품 A
104
126
130
암호화 프로토콜을 위한 명령
공개키
인증서
자동차 ID
시리얼 넘버 A
비밀키
124
128
네트워크
122
120
120
부품 B
부품 C
124
124
시리얼 넘버 B
시리얼 넘버 C
• • •

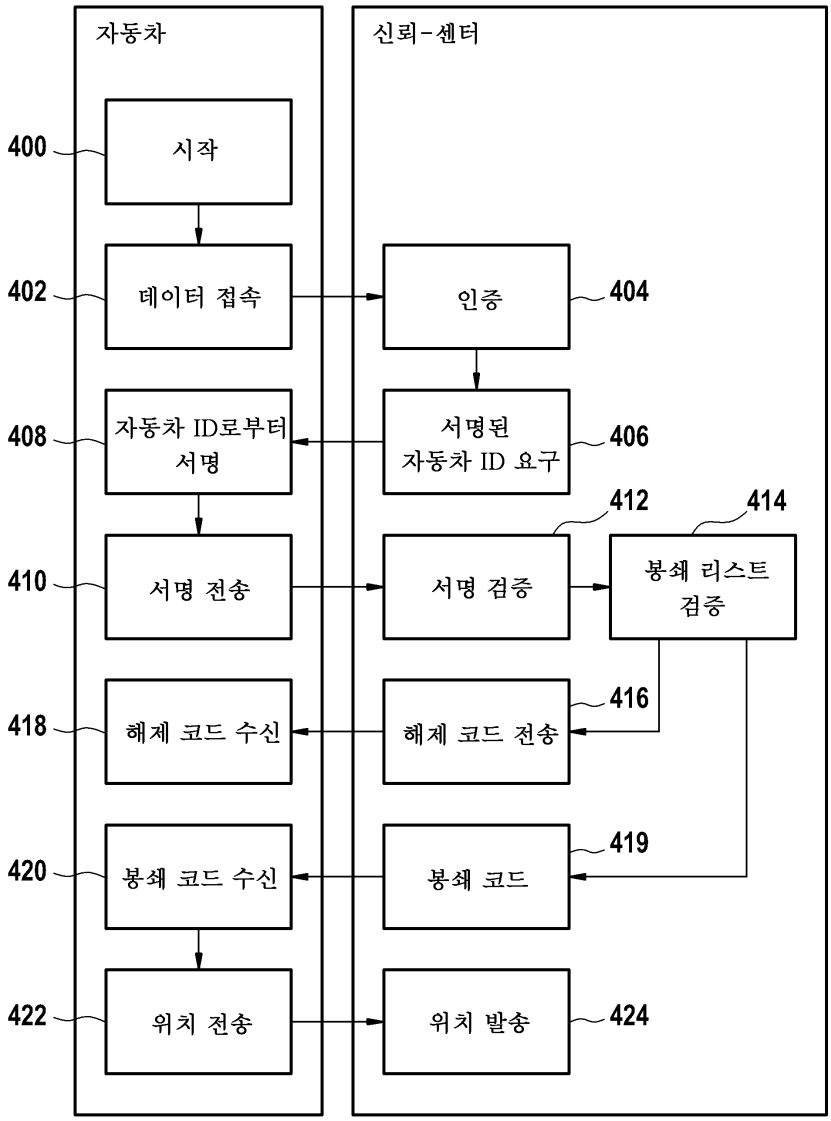
도면5


확인
200
202'
시리얼 넘버에 대한 쿼리
300
시리얼 넘버로부터 코드 발생
302
코드 서명
304
컴퓨터 시스템에 인증서와 함께 서명된 코드 전송
306
308
코드 무효?
예
아니오
204
봉쇄 리스트에
자동차?
예
고정
208
아니오
사용 신호
206

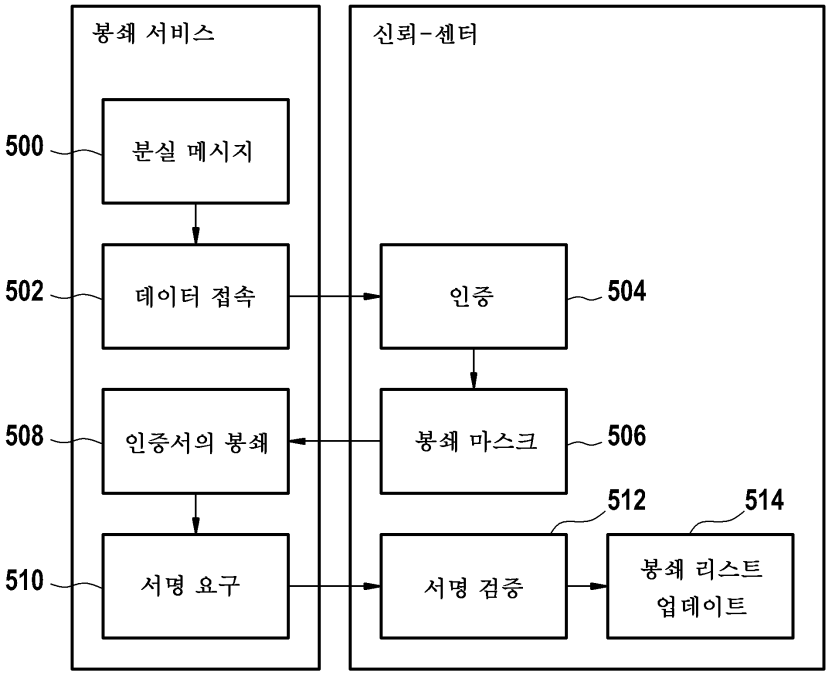
도면6


138
제어장치
1010101
1010101000100100101010
120
122
144
128
126
101010100
101010100
1010
1010
1010
1010
차대 전자
전자
전자
엔진 전자
120
120
120
120
146'''
146''
146'
146
100
106
101010100010010010110100100101100100010010101
봉쇄 서비스
114
명령
110
봉쇄 정보
142
140
112
134
132
108

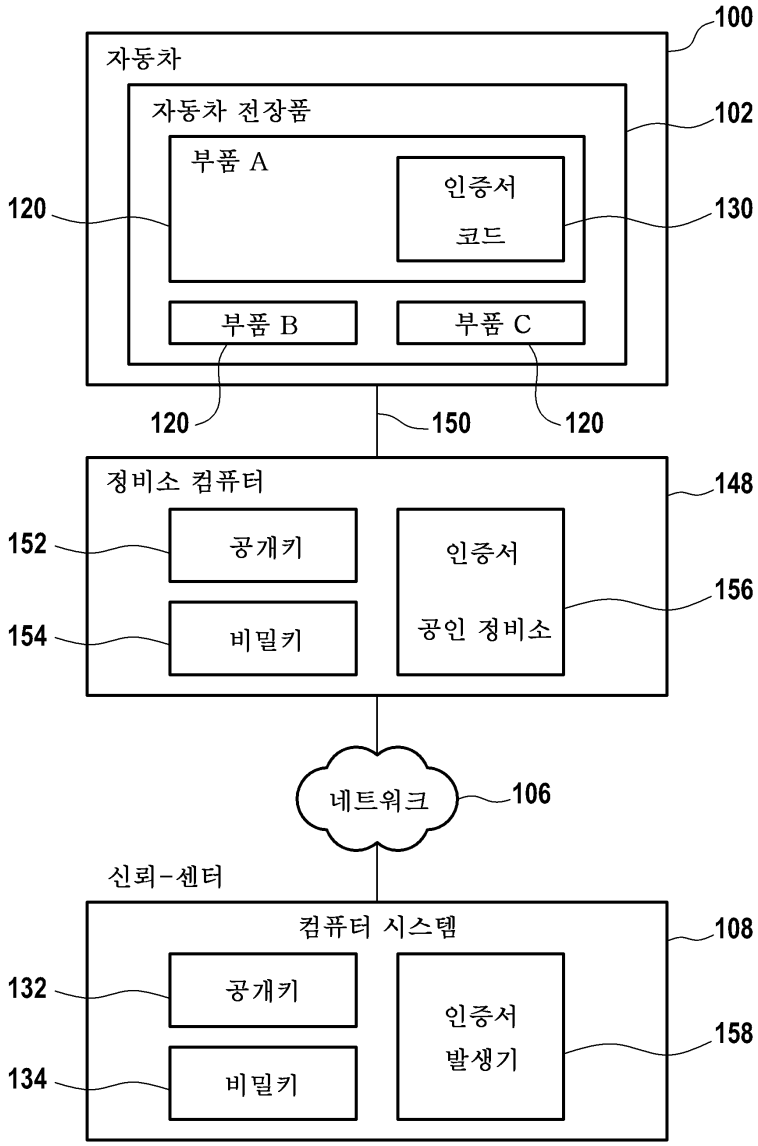
도면7


자동차
신뢰-센터
400
시작
402
데이터 접속
404
인증
406
서명된
자동차 ID 요구
408
자동차 ID로부터
서명
410
서명 전송
412
서명 검증
414
봉쇄 리스트
검증
416
해제 코드 전송
418
해제 코드 수신
419
봉쇄 코드
420
봉쇄 코드 수신
422
위치 전송
424
위치 발송

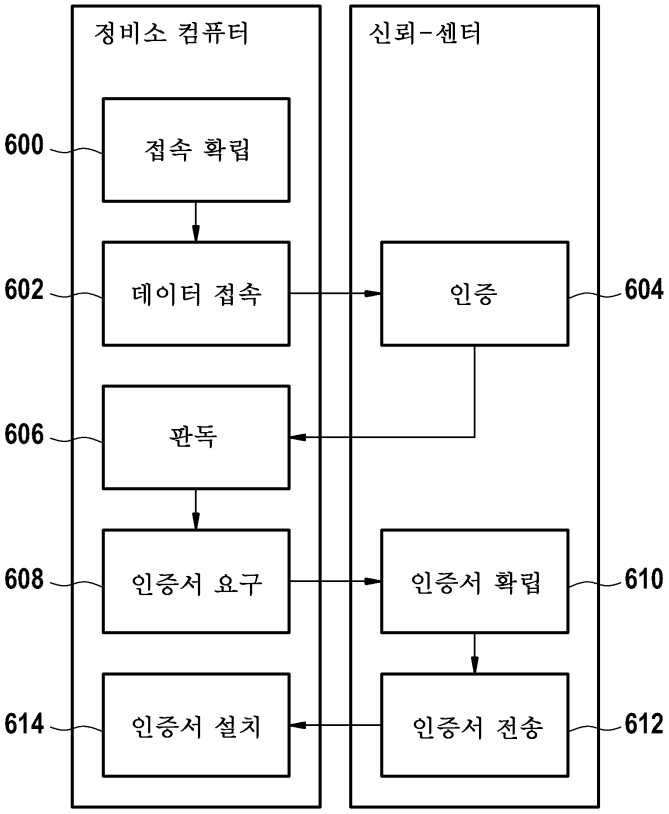
도면8


봉쇄 서비스
신뢰-센터
500
분실 메시지
502
데이터 접속
504
인증
508
인증서의 봉쇄
506
봉쇄 마스크
512
514
510
서명 요구
서명 검증
봉쇄 리스트
업데이트

도면9


100
자동차
자동차 전장품
102
부품 A
인증서
코드
120
130
부품 B
부품 C
120
150
120
정비소 컴퓨터
148
152
공개키
인증서
156
154
비밀키
공인 정비소
네트워크
106
신뢰-센터
컴퓨터 시스템
108
132
공개키
인증서
발생기
158
134
비밀키

도면10


정비소 컴퓨터
신뢰-센터
600
접속 확립
602
데이터 접속
인증
604
606
판독
608
인증서 요구
인증서 확립
610
614
인증서 설치
인증서 전송
612