(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 2 338 147 B1**

(12) **EUROPÄISCHE PATENTSCHRIFT**

(45) Veröffentlichungstag und Bekanntmachung des Hinweises auf die Patenterteilung:
02.10.2013 Patentblatt 2013/40

(21) Anmeldenummer: **09781027.9**

(22) Anmeldetag: **24.07.2009**

(51) Int Cl.:
G07C 5/00 *(2006.01)* ***G07C 5/08*** *(2006.01)*

(86) Internationale Anmeldenummer:
PCT/EP2009/059551

(87) Internationale Veröffentlichungsnummer:
WO 2010/031625 (25.03.2010 Gazette 2010/12)

(54) **KRAFTFAHRZEUG-ELEKTRONIKGERÄT, KRAFTFAHRZEUG, VERFAHREN ZUR ANZEIGE VON DATEN AUF EINER KRAFTFAHRZEUG-ANZEIGEVORRICHTUNG UND COMPUTERPROGRAMMPRODUKT**

MOTOR VEHICLE ELECTRONICS DEVICE, MOTOR VEHICLE, METHOD FOR DISPLAYING DATA ON A MOTOR VEHICLE DISPLAY APPARATUS, AND COMPUTER PROGRAM PRODUCT

APPAREIL ÉLECTRONIQUE POUR VÉHICULE À MOTEUR, VÉHICULE À MOTEUR, PROCÉDÉ D'AFFICHAGE DE DONNÉES SUR UN DISPOSITIF D'AFFICHAGE D'UN VÉHICULE À MOTEUR ET PRODUIT PROGRAMME D'ORDINATEUR

(84) Benannte Vertragsstaaten:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR

(30) Priorität: **22.09.2008 DE 102008042259**

(43) Veröffentlichungstag der Anmeldung:
29.06.2011 Patentblatt 2011/26

(73) Patentinhaber: **Bundesdruckerei GmbH**
10958 Berlin (DE)

(72) Erfinder:
- **FISCHER, Jörg**
  13053 Berlin (DE)
- **DIETRICH, Frank**
  12437 Berlin (DE)
- **PAESCHKE, Manfred**
  16348 Wandlitz (DE)

(74) Vertreter: **Richardt Patentanwälte GbR**
Wilhelmstraße 7
65185 Wiesbaden (DE)

(56) Entgegenhaltungen:
WO-A-2005/093668
DE-A1-102006 015 212
DE-A1-102006 025 023
DE-A1-102006 027 253
DE-U1-202004 017 458

- **RANKL, EFFING: "Handbuch der Chipkarten" 1999, HANSER VERLAG , MÜNCHEN , XP002552615 Seite 201 - Seite 203**
- **WOBST: "Abenteuer Kryptologie" 2001, ADDISON-WESLEY , MÜNCHEN , XP002552616 Seite 295; Abbildung 6.5**

Anmerkung: Innerhalb von neun Monaten nach Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents im Europäischen Patentblatt kann jedermann nach Maßgabe der Ausführungsordnung beim Europäischen Patentamt gegen dieses Patent Einspruch einlegen. Der Einspruch gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist. (Art. 99(1) Europäisches Patentübereinkommen).

EP 2 338 147 B1

Beschreibung

[0001] Die Erfindung betrifft ein Kraftfahrzeug-Elektronikgerät, ein Kraftfahrzeug, ein Verfahren zur Anzeige von Daten auf einer Kraftfahrzeug-Anzeigevorrichtung und ein Computerprogrammprodukt.

[0002] Aus US 5,657,008 ist ein elektronisches Kraftfahrzeug-Kennzeichen bekannt, in dem eine Fahrzeug-Identifizierungsnummer gespeichert ist. Die Fahrzeug-Identifizierungsnummer dient zur Prüfung, ob das elektronische Kraftfahrzeug-Kennzeichen auch tatsächlich zu dem Kraftfahrzeug, an welchem es angebracht ist, gehört.

[0003] Aus WO 2007/1137555 A2 ist ein elektronisch konfigurierbares Kraftfahrzeug-Kennzeichen mit einem Display bekannt. Um das Kraftfahrzeug-Kennzeichen zu konfigurieren, werden Daten in einer externen Konfigurationseinheit zusammengestellt und verschlüsselt. Die verschlüsselten Daten werden von einem in die Konfigurationseinheit integrierten Infrarot-Sender als Infrarot-Signale ausgesendet. In der Anzeigeelektronik für das Kraftfahrzeug-Kennzeichen werden die Signale entschlüsselt, wofür eine entsprechende Entschlüsselungs-Software in der Anzeige-elektronik gespeichert ist.

[0004] Aus US 2007/0285361 A1 ist ein System für drahtlose elektronische Kraftfahrzeug-Kennzeichen bekannt Die Eingabe von Daten in das elektronische Kraftfahrzeug-Kennzeichen ist nur hierzu autorisierten Personen möglich, und zwar mit Hilfe eines geheimen Codes.

[0005] Aus DE 102006027253 A1 ist ein Lesegerät für ein Dokument sowie ein Verfahren zum Lesen eines Datenobjekts bekannt. Das Lesegerät umfasst einen Datenspeicher zur Speicherung zumindest eines Datenobjekts, wobei ein externer Lesezugriff auf das Datenobjekt die Durchführung eines kryptographischen Protokolls voraussetzt. Das Lesegerät hat eine Schnittstelle für den externen Lesezugriff auf das Datenobjekt, Mittel zur Durchführung des kryptographischen Protokolls und eine zweite Schnittstelle zur Anforderung der Durchführung eines kryptographischen Algorithmus und zum Empfang eines Ergebnisses der Durchführung des kryptographischen Algorithmus.

[0006] Aus der DE 102006015212 A1 ist ein Verfahren zum Schutz eines beweglichen Gutes, insbesondere eines Fahrzeuges, gegen unberechtigte Nutzung bekannt. Das Verfahren beinhaltet die Schritte der kryptographischen Authentifizierung und/oder kryptographischen Authentisierung des Kraftfahrzeugs gegenüber einem externen Computersystem, den Schritt der Prüfung, ob für das Kraftfahrzeug eine Sperrung gespeichert ist sowie den Schritt des Sendens eines Signals von dem Computersystem an das Kraftfahrzeug, um eine Nutzung des Kraftfahrzeugs zu ermöglichen, wenn für das Kraftfahrzeug keine Sperrung gespeichert ist.

[0007] Aus der DE 202004017458 U Display-Hoheitskennzeichen mit elektrischer Dauerschildfunktion bekannt, die für Fahrzeuge und/oder Spot- und Werbetafel Displays anwendbar ist. Eine veränderbare Beschriftung basierend z.B. auf Flüssigkeitskristallen, digitalen LCD-Modulen und/oder LED-Modulen wird eingesetzt, um z.B. die Herstellung von KFZ-Kennzeichen mit veränderbarem Anzeigeninhalt zu ermöglichen.

[0008] Demgegenüber liegt der Erfindung die Aufgabe zugrunde, ein verbessertes Kraftfahrzeug-Elektronikgerät zu schaffen sowie ein entsprechendes Kraftfahrzeug, ein Verfahren zur Anzeige von Daten auf einer Kraftfahrzeug-Anzeigevorrichtung sowie ein Computerprogrammprodukt.

[0009] Die der Erfindung zugrunde liegenden Aufgaben werden jeweils mit den Merkmalen der unabhängigen Patentansprüche gelöst. Ausführungsformen der Erfindung sind in den abhängigen Patentansprüchen angegeben.

[0010] Nach Ausführungsformen der Erfindung hat das Kraftfahrzeug-Elektronikgerät eine erste Schnittstelle zum Aufbau einer ersten Verbindung zu einem ersten ID-Token, um aus dem ersten ID-Token Daten auszulesen. Bei dem ersten ID-Token kann es sich um ein Dokument, insbesondere ein Wert- oder Sicherheitsdokument, handeln, in welches ein elektronischer Speicher und eine Schnittstelle für den Aufbau der Verbindung zu der ersten Schnittstelle des Kraftfahrzeug-Elektronikgeräts integriert sind. Insbesondere kann in das Dokument ein RFID-Chip integriert sein, in dem die Daten gespeichert sind.

[0011] Unter einem "Dokument" werden erfindungsgemäß papierbasierte und/oder kunststoffbasierte Dokumente verstanden, wie zum Beispiel Ausweisdokumente, insbesondere Reisepässe, Personalausweise, Visa sowie Führerscheine, Fahrzeugscheine, Fahrzeugbriefe, Firmenausweise, Gesundheitskarten oder andere ID-Dokumente wie Dienstausweise sowie auch Chipkarten, Zahlungsmittel, insbesondere Bankkarten und Kreditkarten, Frachtbriefe oder sonstige Berechtigungsnachweise, in die ein Datenspeicher zur Speicherung zumindest eines Attributs integriert ist.

[0012] Bei dem Dokument kann es sich vorzugsweise um einen elektronischen Fahrzeugschein oder Fahrzeugbrief oder ein anderes Kraftfahrzeugdokument handeln.

[0013] Das Kraftfahrzeug-Elektronikgerät hat einen Speicher zur Speicherung eines Zertifikats einer Public-Key-Infrastruktur (PKI). Beispielsweise kann das Zertifikat dem X.509 Standard entsprechen. In demselben oder einem anderen Speicher des Kraftfahrzeug-Elektronikgeräts kann ferner ein sogenanntes Root-Zertifikat dieser PKI gespeichert sein. Das Zertifikat und das Root-Zertifikat haben typischerweise eine begrenzte Gültigkeitsdauer, die in dem Zertifikat bzw. dem Root-Zertifikat angegeben ist.

[0014] Das Kraftfahrzeug-Elektronikgerät hat ferner Mittel zur Authentifizierung gegenüber dem ersten ID-Token mit Hilfe des Zertifikats. Beispielsweise erfolgt die Authentifizierung mit Hilfe eines Challenge-Response-Verfahrens. Hierzu überträgt das Kraftfahrzeug-Elektro-

nikgerät sein Zertifikat über die erste Verbindung an den ersten ID-Token. Dieser generiert eine Challenge, beispielsweise in der Form einer Zufallszahl, welche der erste ID-Token mit dem öffentlichen Schlüssel des Zertifikats verschlüsselt und das Chiffrat über die erste Verbindung an das Kraftfahrzeug-Elektronikgerät überträgt. Das Kraftfahrzeug-Elektronikgerät muss dann über den privaten Schlüssel verfügen, der dem Zertifikat zugeordnet ist, um dieses Chiffrat korrekt entschlüsseln zu können.

[0015] Optional kann vorgesehen sein, dass sich auch der erste ID-Token gegenüber dem Kraftfahrzeug-Elektronikgerät authentifizieren muss, bevor die Daten aus dem ersten ID-Token ausgelesen werden. Dies kann in analoger Weise zu der Authentifizierung des Kraftfahrzeug-Elektronikgeräts gegenüber dem ID-Token geschehen. Beispielsweise wird also so vorgegangen, dass der ID-Token sein Zertifikat an das Kraftfahrzeug-Elektronikgerät über die erste Verbindung überträgt und danach das Challenge-Response Verfahren durchgeführt wird. Für die Prüfung der Validität des Zertifikats des ersten ID-Tokens kann das Kraftfahrzeug-Elektronikgerät das Root-Zertifikat verwenden.

[0016] Das Kraftfahrzeug-Elektronikgerät verfügt über Mittel zur Ansteuerung zumindest einer Anzeigevorrichtung zur Wiedergabe der Daten. Beispielsweise sind zwei Anzeigevorrichtungen vorhanden, die anstelle der üblichen Nummernschilder vorne und hinten an einem Kraftfahrzeug angeordnet sind. Die Anzeigevorrichtungen können als Displays ausgebildet sein, wobei verschiedene Displaytechnologien zum Einsatz kommen können.

[0017] Beispielsweise sind die Anzeigevorrichtungen so ausgebildet, dass die Wiedergabe der Daten auch ohne ständige Energieversorgung erfolgen kann. Solche Anzeigevorrichtungen benötigen nur dann elektrische Energie, wenn sich die wiederzugebenden Daten ändern.

[0018] Hierbei handelt es sich beispielsweise um bistabile Anzeigen, wie zum Beispiel elektrophoretische Anzeigen, elektrochrome Anzeigen, Drehelementanzeigen, ferroelektrische Anzeigen, Anzeigen auf der Basis des Elektrowetting-Effekts sowie bistabile LCD-Anzeigen, zum Beispiel twisted nematic, super twisted nematic, cholesterische oder nematische LCD-Anzeigen. Dabei kann es sich ferner auch um Hybridanzeigen handeln, die verschiedene dieser Anzeigetechnologien miteinander kombinieren.

[0019] Ferner sind aus dem Stand der Technik flexible, bistabile Anzeigen bekannt, die von der Firma Citala kommerziell erhältlich sind. Solche Anzeigen sind auch aus US 2006/0250534 A1 bekannt. Weitere bistabile elektrophoretische Anzeigen sind beispielsweise aus WO 99/53371 und EP 1 715 374 A1 bekannt.

[0020] Bistabile Anzeigen werden auch als "Electronic Paper Display" (EPD) bezeichnet.

[0021] Solchen bistabilen Anzeigen haben im Allgemeinen den Vorteil, dass sie sich bei heller Beleuchtung sehr gut lesen lassen, und dass keine Energieversorgung erforderlich ist, um über lange Zeit gleich bleibende Bilddaten wiederzugeben.

[0022] Es können auch emissive Anzeigevorrichtungen zum Einsatz kommen, die zur Wiedergabe der Daten eine Energieversorgung benötigen. Hierbei kann es sich zum Beispiel um LED-Anzeigen, insbesondere anorganische, organische oder Hybrid-LED-Anzeigen handeln. Die Anzeigevorrichtung kann auch auf der Basis eines elektrolumineszierenden Mediums realisiert sein, wie es zum Beispiel an sich aus der US 2002/0079494 A1 und US 6,091,194 bekannt ist.

[0023] Die Anzeigevorrichtung kann auch drucktechnisch aufgebracht sein und so eine innige und nicht lösbare Verbindung mit dem Kraftfahrzeug bzw. mit Teilen des Kraftfahrzeuges bilden. Die Herstellung beispielsweise von TFTs zur Herstellung solcher Anzeigevorrichtungen durch direktes Aufbringen mit Hilfe von Drucktechnik ist an sich bekannt aus WO 03/098696 A1.

[0024] Das Kraftfahrzeug-Elektronikgerät hat ferner eine zweite Schnittstelle zur Speicherung des Zertifikats in dem Speicher. Über die zweite Schnittstelle kann also auf den Speicher des Kraftfahrzeug-Elektronikgeräts zugegriffen werden, um das Zertifikat dorthin zu übertragen und zu speichern, beispielsweise um bei einem neuen Kraft-fahrzeug das Zertifikat erstmals in den Speicher einzubringen oder um das Zertifikat zu aktualisieren.

[0025] Nach einer Ausführungsform der Erfindung beinhalten die Daten, die über die erste Schnittstelle von dem ersten ID- Token ausgelesen werden, das amtliche Kraftfahr- zeug- Kennzeichen für das Kraftfahrzeug. Beispielsweise hat sich das Kraftfahrzeug- Kennzeichen aufgrund einer Ummeldung bei einer Kraftfahrzeug- Meldestelle geändert. Das geänderte Kraftfahrzeug- Kennzeichen wird von der Meldestelle in dem ersten ID- Token gespeichert. Dies kann online erfolgen, indem eine sichere Verbindung zwischen dem ersten ID- Token und einem Servercomputer aufgebaut wird, über die die Daten mit dem neuen Kraftfahrzeug- Kennzeichen in den ersten ID- Token geschrieben werden. Eine solche sichere Verbindung kann zum Beispiel mittels Ende- zu-Ende- Verschlüsselung über einen Client- Computer, an den ein Lesegerät für den ersten ID- Token angeschlossen ist, realisiert werden. Die Daten mit dem neuen amtlichen Kraftfahrzeug- Kennzeichen können von der Kraftfahrzeug- Meldestelle signiert sein.

[0026] Ausführungsformen der vorliegenden Erfindung sind besonders vorteilhaft, da eine vollständig elektronische Abwicklung der Aktualisierung des amtlichen Kraftfahrzeug-Kennzeichens ermöglicht wird. Insbesondere ist die Herstellung und Anbringung von neuen Nummernschildern nicht mehr notwendig. Hierdurch können in erheblichen Maßen Ressourcen eingespart werden und Abfall vermieden werden. Ferner erübrigen sich auch die bislang mit der Ausstellung von neuen Kraftfahrzeug-Nummemschildern verbundenen Behördengänge.

[0027] Ausführungsformen der vorliegenden Erfin-

dung sind besonders vorteilhaft, da die Aktualisierung des amtlichen Kraftfahrzeug-Kennzeichens durch Übertragung der Daten vom dem ersten ID-Token an das Kraftfahrzeug-Elektronikgerät auf besonders sichere Art und Weise bei maximaler Bequemlichkeit für den Nutzer erfolgt Dies wird durch den Einsatz kryptographischer Verfahren basierend auf einer PKI erreicht, beispielsweise zur einseitigen oder gegenseitigen Authentifizierung des Kraftfahrzeug-Elektronikgeräts und des ersten ID-Tokens und/oder durch Prüfung der Signatur der von dem ersten ID-Token empfangenen Daten durch das Kraftfahrzeug-Elektronikgerät und/oder durch einen kryptographischen Schutz der ersten Verbindung, über die die Daten von dem ersten ID-Token durch das Kraftfahrzeug-Elektronikgerät empfangen werden.

[0028] Nach einer Ausführungsform der Erfindung ist die erste Schnittstelle des Kraftfahr-zeug-Elektronikgeräts kontaktlos ausgebildet, beispielsweise als Funk-Schnittstelle, insbesondere als kontaktlose Schnittstelle, die nach einem RFID-Verfahren arbeitet. Insbesondere kann die erste Schnittstelle so ausgebildet sein, dass über sie auch ein elektronischer Schlüssel des Kraftfahrzeugs angesprochen wird. Bei dem elektronischen Schlüssel kann es sich zum Beispiel um eine Chipkarte handeln, wie zum Beispiel eine RFID-Chipkarte. Es kann aber auch eine weitere Schnittstelle zur Kommunikation mit dem elektronischen Schlüssel vorhanden sein, insbesondere eine RFID Schnittstelle.

[0029] Nach einer Ausführungsform der Erfindung ist die zweite Schnittstelle des Kraftfahr-zeug-Elektronikgeräts kontaktbehaftet ausgebildet. Beispielsweise ist die zweite Schnittstelle zum Anschluss eines Kabels vorgesehen. Insbesondere kann das Kraftfahrzeug-Elektronikgerät als sogenannte Electronic Control Unit (ECU) des Kraftfahrzeugs ausgebildet sein. Für Diagnose- und/ oder Wartungszwecke wird die ECU mit einem externen Gerät, beispielsweise einem Terminal, einer Kraftfahrzeug-Werkstatt oder einer technischen Prüfstelle verbunden. Über dieses Kabel kann dann zwischen dem externen Gerät und der ECU eine Verbindung aufgebaut werden, über die das Zertifikat in dem Speicher gespeichert werden kann, um es beispielsweise zu aktualisieren. Dies kann beispielsweise anlässlich einer Wartung des Kraftfahrzeugs oder anlässlich einer sogenannten Hauptuntersuchung des Kraftfahrzeugs vorgenommen werden.

[0030] Nach einer Ausführungsform der Erfindung ist die zweite Schnittstelle zur Ausbildung einer Netzwerkverbindung vorgesehen, was kontaktbehaftet oder kontaktlos erfolgen kann. Beispielsweise ist die zweite Schnittstelle als Mobilfunk-Schnittstelle nach einem Mobilfunkstandard ausgebildet, sodass das Zertifikat über Mobilfunk empfangen werden kann.

[0031] Nach einer Ausführungsform der Erfindung wird über die zweite Schnittstelle zunächst ein eindeutiger Kraftfahrzeug-Identifikator, der in dem Kraftfahrzeug-Elektronikgerät gespeichert ist, abgefragt. Bei dem Kraftfahrzeug-Identifikator kann es sich zum Beispiel um die Fahrgestellnummer des Kraftfahrzeugs handeln. Mit Hilfe dieses Kraftfahrzeug-Identifikators wird dann ein Zertifikat generiert oder abgerufen, welches zu dem betreffenden Kraftfahrzeug gehört.

[0032] Nach einer Ausführungsform der Erfindung ist die erste Schnittstelle zur Kommunikation mit einem zweiten ID- Token ausgebildet. Der zweite ID- Token dient zur Zugangskontrolle für das Kraftfahrzeug. Der Besitz des zweiten ID- Tokens ist Voraussetzung dafür, dass sich das Kraftfahrzeug von dem Benutzer öffnen und/ oder starten lässt. Beispielsweise handelt es sich bei dem zweiten ID- Token um eine RFID- Chipkarte, welche als elektronischer Schlüssel ("E- Schlüssel") dient.

[0033] In dem zweiten ID-Token ist ein Schlüssel-Identifikator gespeichert. Dieser Schlüssel-Identifikator wird von dem Kraftfahrzeug-Elektronikgetät über dessen erste Schnittstelle von dem zweiten ID-Token abgefragt. Wenn der aus dem zweiten ID-Token über die erste Schnittstelle empfangene Schlüssel-Identifikator zu einem in dem Kraftfahrzeug-Elektronikgerät gespeicherten Referenzwert des Schlüssel-Identifikators passt, generiert das Kraftfahrzeug-Elektronikgerät ein Signal, um zum Beispiel die Zentralverriegelung des Kraftfahrzeugs zu entriegeln und/oder das Starten des Motors des Kraftfahrzeugs freizugeben.

[0034] Statt der ersten Schnittstelle kann auch eine weitere Schnittstelle für die Kommunikation zwischen dem Kraftfahrzeug-Elektronik-Gerät und zweiten ID-Token vorhanden sein, z.B. eine weitere RFID-Schnittstelle, die eine größere Reichweite als die erste Schnittstelle hat. Die Reichweite der weiteren Schnittstelle ist so gewählt, dass der zweite ID-Token von dem Kraftfahrzeug-Elektronikgerät erfasst wird, wenn sich der zweite ID-Token noch außerhalb des Kraftfahrzeugs befindet, wohingegen die Reichweite der ersten Schnittstelle so gewählt ist, dass sich der erste ID-Token innerhalb der Kraftfahrzeuginnenraums befinden muss, damit die erste Verbindung aufgebaut werden kann. Voraussetzung für die Aktualisierung der Kraftfahrzeug-kennzeichens ist dann also, dass zunächst der Nutzer das Kraftfahrzeug entriegeln und einsteigen muss.

[0035] Vorzugsweise wird als Schlüssel-Identifikator nicht der Kraftfahrzeug-Identifikator gewählt. Dies hat den Vorteil, dass bei einem Verlust des zweiten ID-Tokens dieser zweite ID-Token durch einen anderen ersetzt werden kann, indem ein anderer Schlüssel-Identifikator gespeichert ist. Die zweite Schnittstelle des Kraftfahrzeug-Elektronikgeräts ist vorzugsweise so ausgebildet, dass hierüber auf den Speicher-bereich des Kraftfahrzeug-Elektronikgeräts zugegriffen werden kann, in dem der Schlüssel-Identifikator gespeichert ist, um den dort gespeicherten Schlüssel-Identifikator des verlorengegangenen zweiten ID-Tokens durch den neuen Schlüssel-Identifikator des neuen zweiten ID-Tokens zu ersetzen. Beispielsweise ist der neue Schlüssel-Identifikator signiert, wobei das Kraftfahrzeug-Elektronikgerät die Validität der Signatur prüft, bevor der alte Schlüssel-Identi-

fikator durch den neuen Schlüssel-Identifikator ersetzt wird.

[0036] Nach einer Ausführungsform der Erfindung hat das Kraftfahrzeug-Elektronikgerät Mittel zum Aufbau eines gesicherten Datenübertragungskanals zur Ansteuerung der zumindest einen Anzeigevorrichtung. Beispielsweise erfolgt die Datenübertragung über diesen Datenübertragungskanal verschlüsselt, um eine Manipulation der Ansteuerung der zumindest einen Anzeigevorrichtung zu unterbinden.

[0037] In einem weiteren Aspekt betrifft die Erfindung ein Kraftfahrzeug mit einer Ausführungsform des erfindungsgemäßen Kraftfahrzeug-Elektronikgeräts und zumindest einer von außen sichtbaren Anzeigevorrichtung, die mit dem Kraftfahrzeug-Elektronikgerät verbunden ist.

[0038] In einem weiteren Aspekt betrifft die Erfindung ein Verfahren zum Anzeigen von Daten, beispielsweise eines amtlichen Kennzeichens, auf einer Kraftfahrzeug-Anzeigevorrichtung mit folgenden Schritten: Aufbau einer ersten Verbindung zwischen einem Kraftfahrzeug-Elektronikgerät und einem ersten ID-Token, Zugriff auf einen Speicher des Kraftfahrzeug-Elektronikgeräts zum Lesen eines Zertifikats, kryptografische Authentifizierung des Kraftfahrzeug-Elektronikgeräts gegenüber dem ID-Token mit Hilfe des Zertifikats, Auslesen von Daten aus dem ersten ID-Token über die erste Verbindung, nachdem die Authentifizierung des Kraftfahrzeug-Elektronikgeräts gegenüber dem ersten ID-Token erfolgreich durchgeführt worden ist, Ansteuerung der Kraftfahrzeug-Anzeigevorrichtung zur Wiedergabe der Daten

[0039] In einem weiteren Aspekt betrifft die Erfindung ein Computerprogrammprodukt mit von einem Kraftfahrzeug-Elektronikgerät ausführbaren Programminstruktionen zur Anzeige von Daten auf einer Kraftfahrzeug-Anzeigevorrichtung.

[0040] Im Weiteren werden Ausführungsformen der Erfindung mit Bezugnahme auf die Zeichnungen näher erläutert. Es zeigen:

Figur 1 ein Blockdiagramm einer ersten Ausführungsform eines erfindungsgemäßen Kraftfahrzeug-Elektronikgeräts und eines erfindungsgemäßen Kraftfahrzeugs,

Figur 2 ein Flussdiagramm einer Ausführungsform eines erfindungsgemäßen Verfahrens,

Figur 3 ein Blockdiagramm einer weiteren Ausführungsform eines erfindungsgemäßen Kraftfahrzeug-Elektronikgeräts und eines erfindungsgemäßen Kraftfahrzeugs.

[0041] Einander entsprechende Elemente der nachfolgenden Ausführungsformen werden jeweils mit denselben Bezugszeichen gekennzeichnet.

[0042] Die Figur 1 zeigt schematisch ein Kraftfahrzeug 100, wie zum Beispiel einen Personenkraftwagen. Das Kraftfahrzeug 100 hat zumindest ein Kraftfahrzeug-Elektronikgerät 102, welches beispielsweise als sogenannte Electronic Control Unit (ECU) ausgebildet sein kann.

[0043] Das Kraftfahrzeug-Elektronikgerät 102 hat einen elektronischen Speicher 104 mit zumindest den Speicherbereichen 106, 108, 110, 112 und 114. Der Speicherbereich 106 dient zur Speicherung eines Kraftfahrzeug-Identifikators, d.h. eines sogenannten Unique Identifiers, wie zum Beispiel der Fahrgestellnummer des Kraftfahrzeugs 100. Vorzugsweise ist der Speicherbereich 106 so ausgebildet, dass der dort gespeicherte Kraftfahrzeug-Identifikator nicht geändert werden kann, sodass also das Kraftfahrzeug-Elektronikgerät 102 dem Kraftfahrzeug 100 fest zugeordnet ist.

[0044] Der Speicherbereich 108 dient zur Speicherung von Daten, die das amtliche Kraftfahrzeug-Kennzeichen des Kraftfahrzeugs 100 beinhalten. Diese Daten können über eine Schnittstelle 116 des Kraftfahrzeug-Elektronikgeräts 102 aktualisiert werden. Die Schnittstelle 116 ist bei der hier betrachteten Ausführungsform kontaktlos als Funk-Schnittstelle ausgebildet, die nach einem RFID-Verfahren arbeitet.

[0045] Der Speicherbereich 110 dient zur Speicherung eines Zertifikats des Kraftfahrzeugs 100, wobei es sich bei dem Zertifikat beispielsweise um ein standardisiertes Zertifikat einer PKI handeln kann. Der Speicherbereich 112 dient zur Speicherung eines sogenannten Root Zertifikats der PKI.

[0046] In dem Speicherbereich 114 des Speichers 104 ist der zu dem Zertifkat 110 gehörende private Schlüssel des Kraftfahrzeugs 100 gespeichert. Auf diesen Speicherbereich 114 ist ein externer Zugriff über die Schnittstelle 116 oder über eine weitere Schnittstelle 118 des Kraftfahrzeug-Elektronikgeräts 102 prinzipiell nicht möglich.

[0047] Die Schnittstelle 118 ist zum Beispiel kontaktbehaftet zum Anschluss eines Kabels ausgebildet. Über die Schnittstelle 118 kann ein externer Zugriff auf die Speicherbereiche 110 und 112 erfolgen, um das Zertifikat bzw. das Root-Zertifikat zu aktualisieren.

[0048] Das Kraftfahrzeug-Elektronikgerät 102 hat ferner zumindest einen Prozessor 120 zur Ausführung von Programmmodulen 122, 124, 126, 128, 130 und 132.

[0049] Das Programmmodul 122 dient zur Ausführung der das Kraftfahrzeug-Elektronikgerät 102 betreffenden Schritte eines kryptografischen Protokolls zur Authentifizierung des Kraftfahrzeug-Elektronikgeräts 102 gegenüber einem ID-Token 134. Vorzugsweise ist das Programmmodul 122 so ausgebildet, dass auch eine Authentifizierung des ID-Tokens 134 gegenüber dem Kraftfahrzeug-Elektronikgerät 102 erfolgt.

[0050] Das Programmmodul 124 dient zur Verschlüsselung von Daten, die zwischen dem Kraftfahrzeug-Elektronikgerät 102 und dem ID-Token 134 ausgetauscht werden. Hierbei kann eine Verschlüsselung mit einem symmetrischen oder einem asymmetrischen Schlüssel erfolgen.

[0051] Das Programmmodul 126 dient zur Durchführung einer Signaturprüfung einer von dem ID-Token 134

empfangenen elektronischen Signatur. Hierzu greift das Programmmodul 126 auf den Speicherbereich 112 zu, um dort das Root-Zertifikat abzurufen.

[0052] Das Programmmodul 128 wird zur Aktualisierung der in dem Speicherbereich 108 gespeicherten Daten, welche das amtliche Kraftfahrzeug-Kennzeichen beinhalten, gestartet. Das Programmmodul 130 dient zur Ansteuerung der Displays 136 und 138 des Kraftfahrzeugs 100. Die Displays 136 und 138 können dort an dem Kraftfahrzeug 100 angeordnet sein, wo üblicherweise die Nummernschilder angeordnet sind. Die Displays 136 und 138 sind mit dem Kraftfahrzeug-Elektronikgerät 102 über gesicherte Datenübertragungskanäle 140 bzw. 142 verbunden. Beispielsweise können die Datenübertragungskanäle 140 und/oder 142 über ein Bussystem des Kraftfahrzeugs 100 realisiert werden.

[0053] Das Programmmodul 132 wird gestartet, um das in dem Speicherbereich 110 gespeicherte Zertifikat und/oder das in dem Speicherbereich 112 gespeicherte Root-Zertifikat über die Schnittstelle 118 zu aktualisieren.

[0054] Das Kraftfahrzeug-Elektronikgerät 102 kann als System bestehend aus mehreren räumlich voneinander getrennten elektronischen Komponenten realisiert sein, welche zum Beispiel über ein Bussystem des Kraftfahrzeugs 100 miteinander verbunden sind. Dementsprechend kann auch der Speicher 104 über verschiedene solcher Komponenten, die insgesamt das Kraftfahrzeug-Elektronikgerät 102 bilden, verteilt realisiert sein. Entsprechendes gilt für den Prozessor 120.

[0055] Der ID-Token 134 hat einen elektronischen Speicher 144 mit geschützten Speicherbereichen 146, 148, 150 und 152. Der Speicherbereich 146 dient zur Speicherung des Kraftfahrzeug-Identifikators, der auch in dem Speicherbereich 106 des Speichers 104 des Kraftfahrzeug-Elektronikgeräts 102 gespeichert ist. Hierdurch ist der ID-Token 134 dem Kraftfahrzeug 100 eindeutig zugeordnet. In dem Speicherbereich 146 kann zusätzlich eine Signatur des Kraftfahrzeug-Identifikators gespeichert sein.

[0056] In dem Speicherbereich 148 sind Daten gespeichert, die das aktuelle amtliche Kraftfahrzeug-Kennzeichen des Kraftfahrzeugs 100 beinhalten. Zusätzlich kann in dem Speicherbereich 148 eine digitale Signatur dieser Daten gespeichert sein. Diese Daten können von einem Servercomputer der Kraftfahrzeug-Meldestelle in den Speicherbereich 148 geschrieben worden sein.

[0057] Der Speicherbereich 150 dient zur Speicherung eines Zertifikats des ID-Tokens 134. Der Speicherbereich 152 dient zur Speicherung eines privaten Schlüssels, dem das in dem Speicherbereich 150 gespeicherte Zertifikat zugeordnet ist.

[0058] Der ID- Token 134 hat ferner einen Prozessor 154 zur Ausführung von Programmmodulen 156 und 158, die den Programmmodulen 122 und 124 entsprechen. Das Programmmodul 156 dient zur Ausführung derjenigen Schritte des kryptografischen Protokolls, welche den ID- Token 134 betreffen. Das Programmmodul 158 dient zum Aufbau der verschlüsselten Verbindung mit dem Kraftfahrzeug- Elektronikgerät 102, insbesondere einer Verbindung mit Ende- zu- Ende- Verschlüsselung mit Hilfe eines symmetrischen oder asymmetrischen Schlüssels.

[0059] Der ID-Token 134 hat ferner eine Schnittstelle 160, die der Schnittstelle 116 des Kraftfahrzeug-Elektronikgeräts 102 entspricht, und beispielsweise als Funkschnittstelle ausgebildet ist, die nach einem RFID-Verfahren arbeitet.

[0060] Bei dem ID-Token 134 kann es sich um ein Dokument handeln, wie zum Beispiel einen elektronischen Kraftfahrzeugbrief oder einen elektronischen Kraftfahrzeugschein, wie in der Figur 1 gezeigt. Das Dokument kann zum Beispiel kartenförmig ausgebildet sein.

[0061] Das Kraftfahrzeug-Elektronikgerät 102 ist über seine Schnittstelle 118 mit einem Terminal 162 verbindbar. Das Terminal 162 hat eine Schnittstelle 164, die der Schnittstelle 118 des Kraftfahrzeug-Elektronikgeräts 102 entspricht. Die Schnittstellen 164 und 118 können zum Beispiel mit einem Kabel verbunden werden, wozu typischerweise die Motorhaube des Kraftfahrzeugs 100 geöffnet werden muss.

[0062] Der Terminal 162 hat zumindest einen Prozessor 166 zur Ausführung eines Pro-gramms 168 sowie eine Netzwerk-Schnittstelle 170 zur Kommunikation mit einem Servercomputer 172 über ein Netzwerk 174.

[0063] Durch den Servercomputer 172 wird ein Zertifikat-Provider zur Verfügung gestellt, beispielsweise in Form einer Datenbank 176, in der aktuelle Zertifikate für verschiedene Kraftfahrzeuge gespeichert sind. Als Zugriffsschlüssel für die in der Datenbank 176 gespeicherten Zertifikate dient dabei der jeweilige Kraftfahrzeug-Identifikator. Zusätzlich kann der Servercomputer 172 auch ein aktualisiertes Root-Zertifikat 178 liefern.

[0064] Bei Betrieb des Kraftfahrzeugs 100 wird durch Ausführung des Programmmoduls 130 auf den Speicherbereich 108 zugegriffen, um von dort die Daten zu lesen, mit denen die Displays 136 und 138 über die Datenübertragungskanäle 140 bzw. 142 zur Wiedergabe des Kraftfahrzeug-Kennzeichens angesteuert werden.

[0065] Für eine Aktualisierung des Kraftfahrzeug-Kennzeichens wird so vorgegangen:

1. Zunächst ruft der Benutzer, d.h. zum Beispiel der Halter des Kraftfahrzeugs 100 einen Online-Dienst eines Servercomputers, zum Beispiel einer KraftfahrzeugMeldebehörde, auf. Dies kann über einen Personalcomputer des Halters über das Internet erfolgen. Der Personalcomputer hat ein Lesegerät zur Kommunikation mit dem ID-Token 134. Über den Personalcomputer und dessen Lesegerät wird eine gesicherte Verbindung mit dem Server der Kraftfahrzeug-Meldestelle aufgebaut, über die die Daten mit dem aktualisierten Kraftfahrzeug-Kennzeichen und gegebenenfalls deren Signatur in den Speicherbereich 146 des ID-Tokens 134 geschrieben werden.

2. Wenn sich der Benutzer mit dem ID- Token 134 im Empfangsbereich der Schnittstelle 116 befindet, wird das Programmmodul 128 gestartet, um das Kraftfahrzeug- Kennzeichen zu aktualisieren. Dies kann manuell erfolgen, indem der Benutzer ein Bedienelement des Kraftfahrzeugs 100 bestätigt, das zum Beispiel an der Instrumententafel des Kraftfahrzeugs 100 angeordnet sein kann. Das Programmmodul 128 kann aber auch ständig ausgeführt werden. Durch Ausführung des Programmmoduls 128 werden dann zyklisch innerhalb gewisser zeitlicher Abstände Signale von der Schnittstelle 116 ausgesendet, um zu prüfen, ob sich im Empfangsbereich der Schnittstelle 116 das ID- Token 134 befindet.
Die Aktualisierung des Kraftfahrzeug- Kennzeichens erfolgt dann so, dass eine Verbindung zwischen den Schnittstellen 116 und 160 hergestellt wird. Beispielsweise greift das Programmmodul 128 auf das in dem Speicherbereich 110 gespeicherte Zertifikat zu, um es von der Schnittstelle 116 an den ID- Token 134 zu senden. Durch das Programmmodul 156 des ID- Tokens 134 wird dann eine sogenannte Challenge generiert, d.h. beispielsweise eine Zufallszahl. Diese Zufallszahl wird mit dem in dem Zertifikat beinhalteten öffentlichen Schlüssel des Kraftfahrzeugs 100 verschlüsselt.
Das resultierende Chiffrat wird von dem ID- Token 134 über die Verbindung an die Schnittstelle 116 des Kraftfahrzeug- Elektronikgeräts 102 gesendet. Das Programmmodul 122 entschlüsselt das Chiffrat mit Hilfe des in dem Speicherbereich 114 gespeicherten privaten Schlüssels des Kraftfahrzeugs 100 und erhält so die Zufallszahl. Diese Zufallszahl sendet das Programmmodul 122 über die Schnittstelle 116 an den ID- Token 134 zurück.
Durch Ausführung des Programmmoduls 156 wird dort geprüft, ob die von dem Kraftfahrzeug- Elektronikgerät 102 empfangene Zufallszahl mit der ursprünglich generierten Zufallszahl, d.h. der Challenge, übereinstimmt. Ist dies der Fall, so gilt das Kraftfahrzeug- Elektronikgerät 102 als gegenüber dem ID- Token 134 authentifiziert. Die Zufallszahl kann als symmetrischer Schlüssel für die Ende- zu- Ende-Verschlüsselung verwendet werden, die von den Programmmodulen 124 bzw. 158 durchgeführt wird. Optional kann in analoger Art und Weise eine Authentifizierung des ID- Tokens 134 gegenüber dem Kraftfahrzeug- Elektronikgerät 102 erfolgen.
In die einseitige oder gegenseitige Authentisierung kann auch der Kraftfahrzeug- Identifikator, der in den Speicherbereichen 106 bzw. 146 gespeichert ist, mit eingehen. Beispielsweise sendet der ID- Token 134 den von dem ID- Token 134 signierten Kraftfahrzeug- Identifikator an das Kraftfahrzeugelektronik-Gerät 102. Das Kraftfahrzeugelektronik- Gerät 102 prüft dann die Signatur und vergleicht den von dem ID- Token 134 empfangenen Kraftfahrzeug- Identifikator mit dem in dem Speicherbereich 106 gespeicherten Kraftfahrzeug- Identifikator. Wenn die Signatur valide ist und die Kraftfahrzeug- Identifikatoren übereinstimmen, gilt der ID- Token 134 als authentisch.

3. Nachdem die einseitige oder gegenseitige Authentifizierung des Kraftfahrzeug- Elektronikgeräts 102 und des ID- Tokens 134 erfolgt ist, erhält das Kraftfahrzeug- Elektronikgerät 102 eine Leseberechtigung zum Zugriff auf den Speicherbereich 148 des ID- Tokens 134. Das Programmmodul 128 sendet dann ein entsprechendes Lesekommando von der Schnittstelle 116 an den ID- Token 134. Der ID-Token 134 liest daraufhin die Daten, ggf. einschließlich der Signatur, aus dem Speicherbereich 148 und sendet diese über die Verbindung mit Ende- zu- Ende- Verschlüsselung an die Schnittstelle 116. Das Programmmodul 128 startet dann das Programmmodul 126, um die Signatur der Daten mit Hilfe des Root- Zertifikats 112 zu prüfen. Wenn die Signatur valide ist, werden die Daten in den Speicherbereich 108 gespeichert, wobei die dort zuvor gespeicherten Daten überschrieben werden können. Das Programmmodul 130 steuert die Displays 136 und 138 dann mit diesen aktualisierten Daten an, sodass das aktualisierte amtliche Kennzeichen auf den Displays 136 und 138 wiedergegeben wird.

[0066] Zur Aktualisierung der in den Speicherbereichen 110 und 112 gespeicherten Zertifikate wird wie folgt vorgegangen:

[0067] Zwischen den Schnittstellen 118 und 164 wird zum Beispiel über ein Kabel eine Verbindung hergestellt. Durch Ausführung des Programms 168 wird der Kraftfahrzeug-Identifikator aus dem Speicherbereich 106 des Kraftfahrzeug-Elektronikgeräts 102 ausgelesen. Das Programm 168 generiert dann eine Anforderung für den Servercomputer 172, welche diesen Kraftfahrzeug-Identifikator beinhaltet.

[0068] Diese Anforderung sendet das Terminal 162 von seiner Netzwerk-Schnittstelle 170 über das Netzwerk 174 an den Servercomputer 172. Aufgrund dieser Anforderung greift der Servercomputer auf die Datenbank 176 zu, um mit Hilfe des Kraftfahrzeug-Identifikators das dem Kraftfahrzeug-Identifikator zugeordnete aktuelle Zertifikat auszulesen. Das Zertifikat und das aktuelle Root-Zertifikat 178 werden von dem Servercomputer 172 über das Netzwerk 174 an das Terminal 162 gesendet, und von dort durch Ausführung des Programms 168 über die Verbindung zwischen der Schnittstelle 164 und der Schnittstelle 118 zu dem Kraftfahrzeug-Elektronikgerät 102 übertragen, wo das aktuelle Zertifikat in den Speicherbereich 110 und das aktuelle Root-Zertifikat in dem Speicherbereich 112 gespeichert werden, indem die dort jeweils zuvor gespeicherten Zertifikate überschrieben werden.

[0069] Das Terminal kann beispielsweise zu einer Werkstatt gehören, die auf diese Art und Weise die Zer-

tifikate anlässlich einer turnusmäßigen Wartung des Kraftfahrzeugs 100 aktualisiert. Der Terminal kann auch zu einer Prüfstelle, wie zum Beispiel dem Technischen Überprüfungsverein (TÜV) gehören, welcher die Aktualisierung der Zertifikate anlässlich einer sogenannten Hauptuntersuchung vornimmt.

[0070] In einer alternativen Ausführungsform ist die Schnittstelle 118 so ausgebildet, dass sie unmittelbar mit dem Servercomputer 172 kommunizieren kann, wie zum Beispiel über eine Mobilfunkverbindung.

[0071] Die Figur 2 zeigt ein Flussdiagramm einer Ausführungsform eines entsprechenden erfindungsgemäßen Verfahrens.

[0072] In dem Schritt 200 wird eine Verbindung zwischen dem ID-Token, d.h. beispielsweise dem elektronischen Kraftfahrzeugschein, und dem Kraftfahrzeug-Elektronikgerät, beispielsweise einer ECU des Kraftfahrzeugs aufgebaut. Dies kann automatisch erfolgen, sobald sich der elektronische Kraftfahrzeugschein innerhalb der Reichweite der RFID-Schnittstelle des Kraftfahrzeug-Elektronikgeräts befindet (vgl. Schnittstelle 116 in der Ausführungsform der Figur 1).

[0073] In dem Schritt 202 erfolgt zumindest eine einseitige kryptografische Authentifizierung der ECU gegenüber dem elektronischen Kraftfahrzeugschein, wobei hierzu das Zertifikat der ECU verwendet wird. Zusätzlich zu der kryptografischen Authentifizierung können auch die in dem elektronischen Kraftfahrzeugschein und der ECU jeweils gespeicherten Kraftfahrzeug-Identifikatoren auf Übereinstimmung geprüft werden.

[0074] Nach der kryptografischen Authentifizierung wird in dem Schritt 204 das aktuelle amtliche Kraftfahrzeug-Kennzeichen von der ECU aus dem elektronischen Kraftfahrzeugschein ausgelesen und in dem Schritt 206 werden die Displays von der ECU zur Anzeige des neuen Kraftfahrzeug-Kennzeichens angesteuert.

[0075] Die Figur 3 zeigt eine weitere Ausführungsform der Erfindung. Zusätzlich zu der Ausführungsform der Figur 1 ist die Schnittstelle 116 des Kraftfahrzeug-Elektronikgeräts 102 dazu ausgebildet, mit einer entsprechenden Schnittstelle 160 eines weiteren ID-Tokens 180 zu kommunizieren. Der ID-Token 180 kann zum Beispiel als elektronischer Schlüssel ausgebildet sein. Der ID-Token 180 hat einen Speicher 182 zur Speicherung eines Schlüssel-Identifikators 184 des ID-Tokens 180. Bei dem Schlüssel-Identifikator handelt es sich um einen Identifikator, durch den der ID-Token 180 eindeutig oder nahezu eindeutig identifiziert wird.

[0076] Ein Referenzwert für diesen Schlüssel-Identifikator 184 ist in einem Speicherbereich 186 des Kraftfahrzeug-Elektronikgeräts 102 gespeichert.

[0077] Der Prozessor 120 des Kraftfahrzeug-Elektronikgeräts 102 dient hier zusätzlich zur Ausführung eines Steuerungsprogramms 188.

[0078] Durch Ausführung des Steuerungsprogramms 188 werden zyklisch Signale von der Schnittstelle 116 abgegeben. Wenn sich der ID-Token 180 in der Reichweite der Schnittstelle 116 befindet, so antwortet der ID-Token 180 auf ein solches Signal mit der Übertragung des Schlüssel-Identifikators 184 an die Schnittstelle 116. Das Steuerungsprogramm 188 prüft dann den über die Schnittstelle 116 empfangenen Schlüssel-Identifikator 184 mit dem in dem Speicherbereich 186 gespeicherten Referenzwert. Bei Übereinstimmung steuert das Steuerungsprogramm 188 eine Zentralverriegelung des Kraftfahrzeugs 100 an, um die Öffnung der Türen freizugeben. Alternativ oder zusätzlich kann das Steuerungsprogramm 188 die Betätigung des Anlassers des Kraftfahrzeugs 100 freigeben.

[0079] Wenn sich neben dem ID-Token 180 auch der ID-Token 134 innerhalb der Reichweite der Schnittstelle 116 befindet, so startet das Steuerungsprogramm 188 das Programmmodul 128 für die Aktualisierung des Kennzeichens.

Bezugszeichenliste

[0080]

100	Kraftfahrzeug
102	Kraftfahrzeug- Elektronikgerät
104	Speicher
106	Speicherbereich
108	Speicherbereich
110	Speicherbereich
112	Speicherbereich
114	Speicherbereich
116	Schnittstelle
118	Schnittstelle
120	Prozessor
122	Programmmodul
124	Programmmodul
126	Programmmodul
128	Programmmodul
130	Programmmodul
132	Programmmodul
134	ID- Token
136	Display
138	Display
140	Datenübertragungskanal
142	Datenübertragungskanal
144	Speicher
146	Speicherbereich
148	Speicherbereich
150	Speicherbereich
152	Speicherbereich
154	Prozessor
156	Programmmodul
158	Programmmodul
160	Schnittstelle
162	Terminal
164	Schnittstelle
166	Prozessor
168	Programm
170	Netzwerk- Schnittstelle
172	Servercomputer

174 Netzwerk
176 Datenbank
178 Root- Zertifikat
180 ID- Token
182 Speicher
184 Schlüssel- Identifikator
186 Speicherbereich
188 Steuerungsprogramm

Patentansprüche

1. Kraftfahrzeug-Elektronikgerät mit

- einer ersten Schnittstelle (116) zum Aufbau einer ersten Verbindung zu einem ersten ID-Token (134), um aus dem ersten ID-Token Daten auszulesen, wobei es sich bei dem ersten ID-Token um ein Dokument, insbesondere um ein Wert- oder Sicherheitsdokument, handelt, in welches ein elektronischer Speicher und eine Schnittstelle für den Aufbau der Verbindung zu der ersten Schnittstelle des Kraftfahrzeug-Elektronikgeräts integriert sind,
- einem Speicher (104) zur Speicherung eines Zertifikats,
- Mittel (122) zur kryptografischen Authentifizierung gegenüber dem ersten ID-Token mit Hilfe des Zertifikats,

gekennzeichnet durch

- Mittel (130) zur Ansteuerung von zwei Anzeigevorrichtungen (136, 138) zur Wiedergabe der Daten, wobei die Anzeigevorrichtungen vorne und hinten an einem Kraftfahrzeug angeordnet sind,
- eine zweite Schnittstelle (118), über die auf den Speicher zugegriffen werden kann, um das Zertifikat dorthin zu übertragen und zu speichern,

wobei das Kraftfahrzeug-Elektronikgerät zum Aufbau einer zweiten Verbindung zu einem zweiten ID-Token (180) ausgebildet ist, wobei die Ansteuerung der Anzeigevorrichtungen zur Wiedergabe der Daten nur dann erfolgt, wenn die zweite Verbindung aufgebaut werden kann, wobei es sich bei dem zweiten ID-Token um eine RFID-Chipkarte handelt oder wobei das zweite ID-Token als elektronischer Schlüssel ausgebildet ist.

2. Kraftfahrzeug-Elektronikgerät nach Anspruch 1, wobei die Daten ein Kraftfahrzeug-Kennzeichen beinhalten.

3. Kraftfahrzeug-Elektronikgerät nach Anspruch 1 oder 2, wobei die erste Schnittstelle kontaktlos ausgebildet ist, wobei die erste Schnittstelle insbesondere als Funkschnittstelle ausgebildet ist.

4. Kraftfahrzeug-Elektronikgerät nach einem der vorhergehenden Ansprüche, wobei die zweite Schnittstelle kontaktbehaftet ausgebildet ist, wobei die zweite Schnittstelle insbesondere zum Anschluss eines Kabels ausgebildet ist.

5. Kraftfahrzeug-Elektronikgerät nach einem der vorhergehenden Ansprüche, wobei die zweite Schnittstelle als Netzwerk-Schnittstelle, insbesondere als Mobilfunk-Schnittstelle ausgebildet ist.

6. Kraftfahrzeug-Elektronikgerät nach einem der vorhergehenden Ansprüche, wobei ein Identifikator in dem Kraftfahrzeug-Elektronikgerät gespeichert ist, und wobei die zweite Schnittstelle zum Auslesen des Identifikators ausgebildet ist.

7. Kraftfahrzeug-Elektronikgerät nach einem der vorhergehenden Ansprüche, wobei die zweite Verbindung zum Auslesen eines Schlüssel-Identifikators aus dem zweiten ID-Token dient, und wobei in dem Kraftfahrzeug-Elektronikgerät ein Referenzwert für den Schlüssel-Identifikator gespeichert ist.

8. Kraftfahrzeug-Elektronikgerät nach einem der vorhergehenden Ansprüche, mit Mitteln zum Aufbau eines gesicherten Datenübertragungskanals (140, 142) zur Ansteuerung der Anzeigevorrichtungen.

9. Kraftfahrzeug mit einem Kraftfahrzeug-Elektronikgerät nach einem der vorhergehenden Ansprüche und mit zwei Anzeigevorrichtungen, die zur Ansteuerung durch das Kraftfahrzeug-Elektronikgerät ausgebildet ist, wobei das Kraftfahrzeug insbesondere ferner Mittel zum Aufbau eines gesicherten Datenübertragungskanals (140, 142) zwischen dem Kraftfahrzeug-Elektronikgerät und der Anzeigevorrichtungen beinhaltet.

10. Verfahren zur Anzeige von Daten auf zwei Kraftfahrzeug-Anzeigevorrichtungen (136, 138) mit folgenden Schritten:

- Aufbau einer ersten Verbindung zwischen einem Kraftfahrzeug-Elektronikgerät (102) und einem ersten ID-Token (134), wobei es sich bei dem ersten ID-Token um ein Dokument, insbesondere um ein Wert- oder Sicherheitsdokument, handelt, in welches ein elektronischer Speicher und eine Schnittstelle für den Aufbau der Verbindung zu der ersten Schnittstelle des Kraftfahrzeug-Elektronikgeräts integriert sind
- Zugriff auf einen Speicher (104) des Kraftfahrzeug-Elektronikgeräts zum Lesen eines Zertifikats,
- kryptografische Authentifizierung des Kraftfahrzeug-Elektronikgeräts gegenüber dem ID-Token mit Hilfe des Zertifikats,

- Auslesen von Daten aus dem ersten ID-Token über die erste Verbindung, nachdem die Authentifizierung des Kraftfahrzeug-Elektronikgeräts gegenüber dem ersten ID-Token erfolgreich durchgeführt worden ist,
- Ansteuerung der Kraftfahrzeug-Anzeigevorrichtungen zur Wiedergabe der Daten, wobei die Anzeigevorrichtungen vorne und hinten an einem Kraftfahrzeug angeordnet sind,
wobei das Kraftfahrzeug-Elektronikgerät zum Aufbau einer zweiten Verbindung zu einem zweiten ID-Token (180) ausgebildet ist, wobei die Ansteuerung der Anzeigevorrichtungen zur Wiedergabe der Daten nur dann erfolgt, wenn die zweite Verbindung aufgebaut werden kann wobei es sich bei dem zweiten ID-Token um eine RFID-Chipkarte handelt oder wobei das zweite ID-Token als elektronischer Schlüssel ausgebildet ist.

11. Verfahren nach Anspruch 10, wobei über eine zweite Schnittstelle (118) des Kraftfahrzeug-Elektronikgeräts eine dritte Verbindung aufgebaut wird, über die eine Aktualisierung des Zertifikats und/oder eines Root-Zertifikats erfolgt.

12. Verfahren nach Anspruch 10, oder 11, wobei die zweite Verbindung zum Auslesen eines Schlüssel-Identifikators aus dem zweiten ID-Token dient, und wobei in dem Kraftfahrzeug-Elektronikgerät ein Referenzwert für den Schlüssel-Identifikator gespeichert ist.

13. Computerprogrammprodukt mit von einem Kraftfahrzeug-Elektronikgerät ausführbaren Programminstruktionen zur Durchführung eines Verfahrens nach einem der vorhergehenden Ansprüche 10 bis 12.

Claims

1. A motor vehicle electronics device, comprising:

- a first interface (116) for establishing a first connection to a first ID token (134) in order to read out data from the first ID token, the first ID token being a document, in particular a value or security document, into which an electronic memory and an interface for establishing the connection to the first interface of the motor vehicle electronics device are integrated;
- a memory (104) for storing a certificate;
- means (122) for the cryptographic authentication with respect to the first ID token using the certificate,

characterized by

- means (130) for controlling two display units (136, 138) for the reproduction of the data, the display units being disposed in the front and in the back of a motor vehicle,
- a second interface (118), via which the memory can be accessed so as to transmit the certificate to and store it in the memory,
wherein the motor vehicle electronics device is designed to establish a second connection to a second ID token (180), the control of the display units for reproduction of the data takes place only if the second connection can be established, the second ID token is an RFID chip card or the second ID token is designed as an electronic key.

2. The motor vehicle electronics device according to claim 1, wherein the data include a motor vehicle license plate number.

3. The motor vehicle electronics device according to claim 1 or 2, wherein the first interface has a contactless design, the first interface being designed in particular as a radio interface.

4. A motor vehicle electronics device according to any one of the preceding claims, wherein the second interface has a conventional design with contacts, the second interface being designed in particular for the connection of a cable.

5. A motor vehicle electronics device according to any one of the preceding claims, wherein the second interface is designed as a network interface, and more particularly as a mobile communication interface.

6. A motor vehicle electronics device according to any one of the preceding claims, wherein an identifier is stored in the motor vehicle electronics device, and the second interface is designed for reading out the identifier.

7. A motor vehicle electronics device according to any one of the preceding claims, wherein the second connection is used to read out a key identifier from the second ID token, and a reference value for the key identifier is stored in the motor vehicle electronics device.

8. A motor vehicle electronics device according to any one of the preceding claims, comprising means for establishing a secure data transmission channel (140, 142) for controlling the display units.

9. A motor vehicle comprising a motor vehicle electronics device according to any one of the preceding claims and comprising two display units, which are designed to be controlled by the motor vehicle electronics device, wherein the motor vehicle in particular

further comprises means for establishing a secure data transmission channel (140, 142) between the motor vehicle electronics device and the display units.

10. A method for displaying data on two motor vehicle display units (136, 138), comprising the following steps:

- establishing a first connection between a motor vehicle electronics device (102) and a first ID token (102), wherein the first ID token is a document, in particular a value or security document, into which an electronic memory and an interface for establishing the connection to the first interface of the motor vehicle electronics device are integrated;
- accessing a memory (104) of the motor vehicle electronics device for reading a certificate;
- cryptographically authenticating the motor vehicle electronics device with respect to the ID token using the certificate;
- reading out data from the first ID token via the first connection after the authentication of the motor vehicle electronics device with respect to the first ID token has been successfully carried out; and
- controlling the motor vehicle display units for the reproduction of the data, wherein the display units are disposed in the front and in the back of a motor vehicle,

wherein the motor vehicle electronics device is designed to establish a second connection to a second ID token (180), the control of the display units for reproduction of the data takes place only if the second connection can be established, the second ID token is an RFID chip card or the second ID token is designed as an electronic key.

11. The method according to claim 10, wherein a third connection is established via a second interface (118) of the motor vehicle electronics device, the certificate and/or a root certificate being updated via this third connection.

12. The method according to claim 10 or 11, wherein the second connection is used to read out a key identifier from the second ID token, and a reference value for the key identifier is stored in the motor vehicle electronics device.

13. A computer program product, comprising program instructions that can be executed by a motor vehicle electronics device for carrying out the method according to any one of the preceding claims 10 to 12.

Revendications

1. Appareil électronique pour véhicule à moteur, avec

- une première interface (116) pour l'établissement d'une première liaison avec premier jeton d'identification (134), permettant de lire des données à partir du premier jeton d'identification, dans lequel le premier jeton d'identification est un document, en particulier un document de valeur ou de sécurité, dans lequel sont intégrées une mémoire électronique et une interface pour l'établissement d'une liaison avec la première interface de l'appareil électronique de véhicule à moteur,
- une mémoire (104) pour le stockage d'un certificat,
- des moyens (122) pour l'authentification cryptographique par rapport au premier jeton d'identification à l'aide du certificat,

caractérisé par

- des moyens (130) pour l'actionnement de deux dispositifs d'affichage (136, 138) pour la reproduction de données, les dispositifs d'affichage étant agencés à l'avant et à l'arrière d'un véhicule à moteur,
- une deuxième interface (118) permettant d'accéder à la mémoire pour y transférer et y stocker le certificat,

dans lequel l'appareil électronique de véhicule à moteur est conçu pour l'établissement d'une deuxième liaison avec un deuxième jeton d'identification (180), dans lequel l'actionnement des dispositifs d'affichage pour la reproduction de données n'a lieu que si la deuxième liaison peut être établie, dans lequel le deuxième jeton d'identification est une carte à puce RFIP ou dans lequel le deuxième jeton d'identification est conçu comme une clé électronique.

2. Appareil électronique de véhicule à moteur selon la revendication 1, dans lequel les données contiennent une immatriculation de véhicule à moteur.

3. Appareil électronique de véhicule à moteur selon la revendication 1 ou 2, dans lequel la première interface est conçue sans contact, dans lequel la première interface est en particulier conçue comme une interface radio.

4. Appareil électronique de véhicule à moteur selon l'une des revendications précédentes, dans lequel la deuxième interface est conçue avec contact, dans lequel la deuxième interface est en particulier conçue pour le raccordement d'un câble.

5. Appareil électronique de véhicule à moteur selon l'une des revendications précédentes, dans lequel

la deuxième interface est conçue comme une interface de réseau, en particulier comme une interface radio mobile.

6. Appareil électronique de véhicule à moteur selon l'une des revendications précédentes, dans lequel un identifiant est enregistré dans l'appareil électronique de véhicule à moteur, et dans lequel la deuxième interface est conçue pour lire l'identifiant.

7. Appareil électronique de véhicule à moteur selon l'une des revendications précédentes, dans lequel la deuxième liaison permet de lire un identifiant de clé à partir du deuxième jeton d'identification, et dans lequel une valeur de référence pour l'identifiant de clé est enregistré dans l'appareil électronique de véhicule à moteur.

8. Appareil électronique de véhicule à moteur selon l'une des revendications précédentes, avec des moyens pour l'établissement d'un canal de transmission de données sécurisé (140, 142) pour l'actionnement des dispositifs d'affichage.

9. Véhicule à moteur avec un appareil électronique de véhicule à moteur selon l'une des revendications précédentes, et avec deux dispositifs d'affichage conçus pour être actionnés par l'appareil électronique de véhicule à moteur, le véhicule à moteur comprenant en particulier également des moyens pour l'établissement d'un canal de transmission de données sécurisé (140, 142) entre l'appareil électronique de véhicule à moteur et les dispositifs d'affichage.

10. Procédé pour l'affichage de données sur deux dispositifs d'affichage de véhicule à moteur (136, 138), avec les étapes suivantes :

- établissement d'une première liaison entre un appareil électronique de véhicule à moteur (102) et un premier jeton d'identification (134), dans lequel le premier jeton d'identification est un document, en particulier un document de valeur ou de sécurité, dans lequel sont intégrées une mémoire électronique et une interface pour l'établissement de la liaison avec la première interface de l'appareil électronique de véhicule à moteur,
- accès à une mémoire (104) de l'appareil électronique de véhicule à moteur, pour la lecture d'un certificat,
- authentification cryptographique de l'appareil électronique de véhicule à moteur par rapport au premier jeton d'identification, à l'aide du certificat,
- lecture de données à partir du premier jeton d'identification, par la première liaison, après la réussite de l'authentification de l'appareil électronique de véhicule à moteur par rapport au premier jeton d'identification,
- actionnement des dispositifs d'affichage de véhicule à moteur pour la reproduction des données, les dispositifs d'affichage étant agencés à l'avant et à l'arrière d'un véhicule à moteur,

dans lequel l'appareil électronique de véhicule à moteur est conçu pour l'établissement d'une deuxième liaison avec un deuxième jeton d'identification (180), dans lequel l'actionnement des dispositifs d'affichage pour la reproduction de données n'a lieu que si la deuxième liaison peut être établie, dans lequel le deuxième jeton d'identification est une carte à puce RFIP ou dans lequel le deuxième jeton d'identification est conçu comme une clé électronique.

11. Procédé selon la revendication 10, dans lequel une troisième liaison est établie par une deuxième interface (118) de l'appareil électronique de véhicule à moteur, permettant d'actualiser le certificat et/ou un certificat racine.

12. Procédé selon la revendication 10 ou 11, dans lequel la deuxième liaison permet de lire un identifiant de clé à partir du deuxième jeton d'identification, et dans lequel une valeur de référence pour l'identifiant de clé est enregistrée dans l'appareil électronique de véhicule à moteur.

13. Produit de programme informatique avec des instructions de programme exécutables par un appareil électronique de véhicule à moteur, pour l'exécution d'un procédé selon l'une des revendications précédentes 10 à 12.

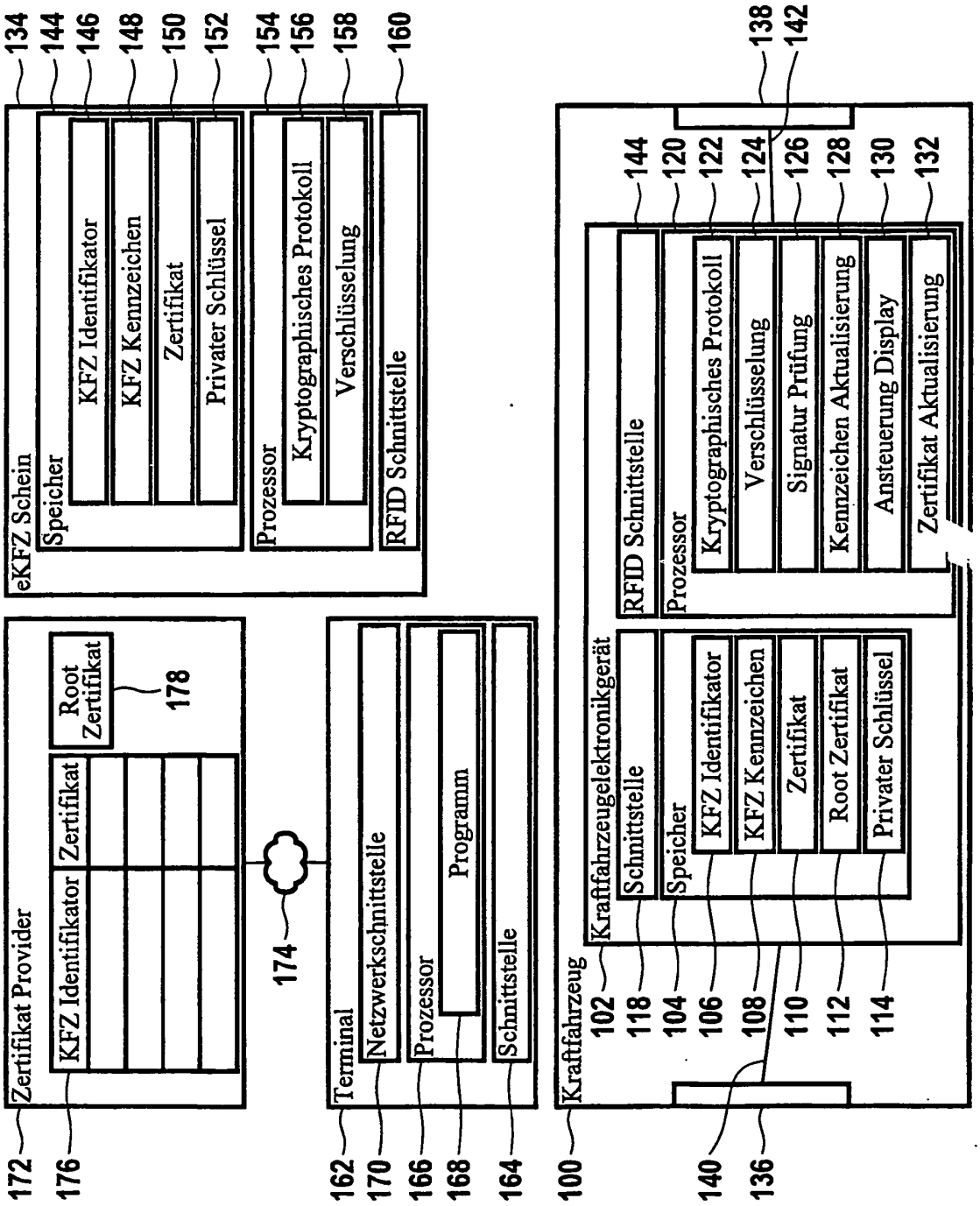

eKFZ Schein
Speicher
KFZ Identifikator
KFZ Kennzeichen
Zertifikat
Privater Schlüssel
Prozessor
Kryptographisches Protokoll
Verschlüsselung
RFID Schnittstelle
134
144
146
148
150
152
154
156
158
160
Zertifikat Provider
KFZ Identifikator
Zertifikat
Root Zertifikat
178
172
176
174
Terminal
Netzwerkschnittstelle
Prozessor
Programm
Schnittstelle
162
170
166
168
164
Kraftfahrzeug
Kraftfahrzeugelektronikgerät
Schnittstelle
Speicher
KFZ Identifikator
KFZ Kennzeichen
Zertifikat
Root Zertifikat
Privater Schlüssel
RFID Schnittstelle
Prozessor
Kryptographisches Protokoll
Verschlüsselung
Signatur Prüfung
Kennzeichen Aktualisierung
Ansteuerung Display
Zertifikat Aktualisierung
100
102
118
104
106
108
110
112
114
140
136
144
120
122
124
126
128
130
132
138
142

Fig. 1

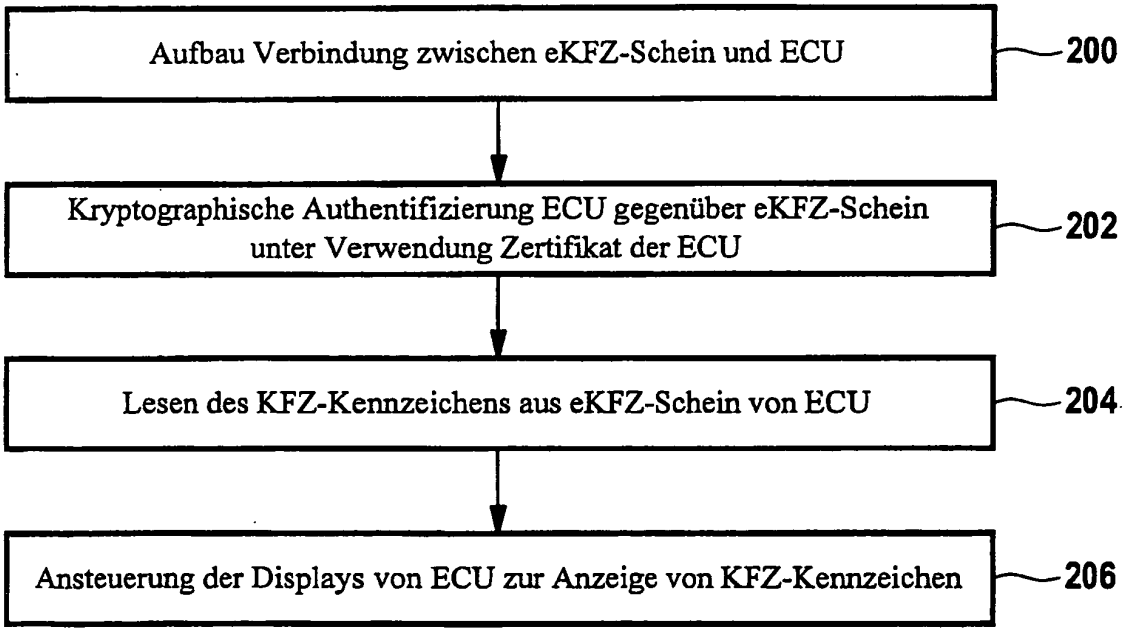

Aufbau Verbindung zwischen eKFZ-Schein und ECU
200
Kryptographische Authentifizierung ECU gegenüber eKFZ-Schein unter Verwendung Zertifikat der ECU
202
Lesen des KFZ-Kennzeichens aus eKFZ-Schein von ECU
204
Ansteuerung der Displays von ECU zur Anzeige von KFZ-Kennzeichen
206

Fig. 2

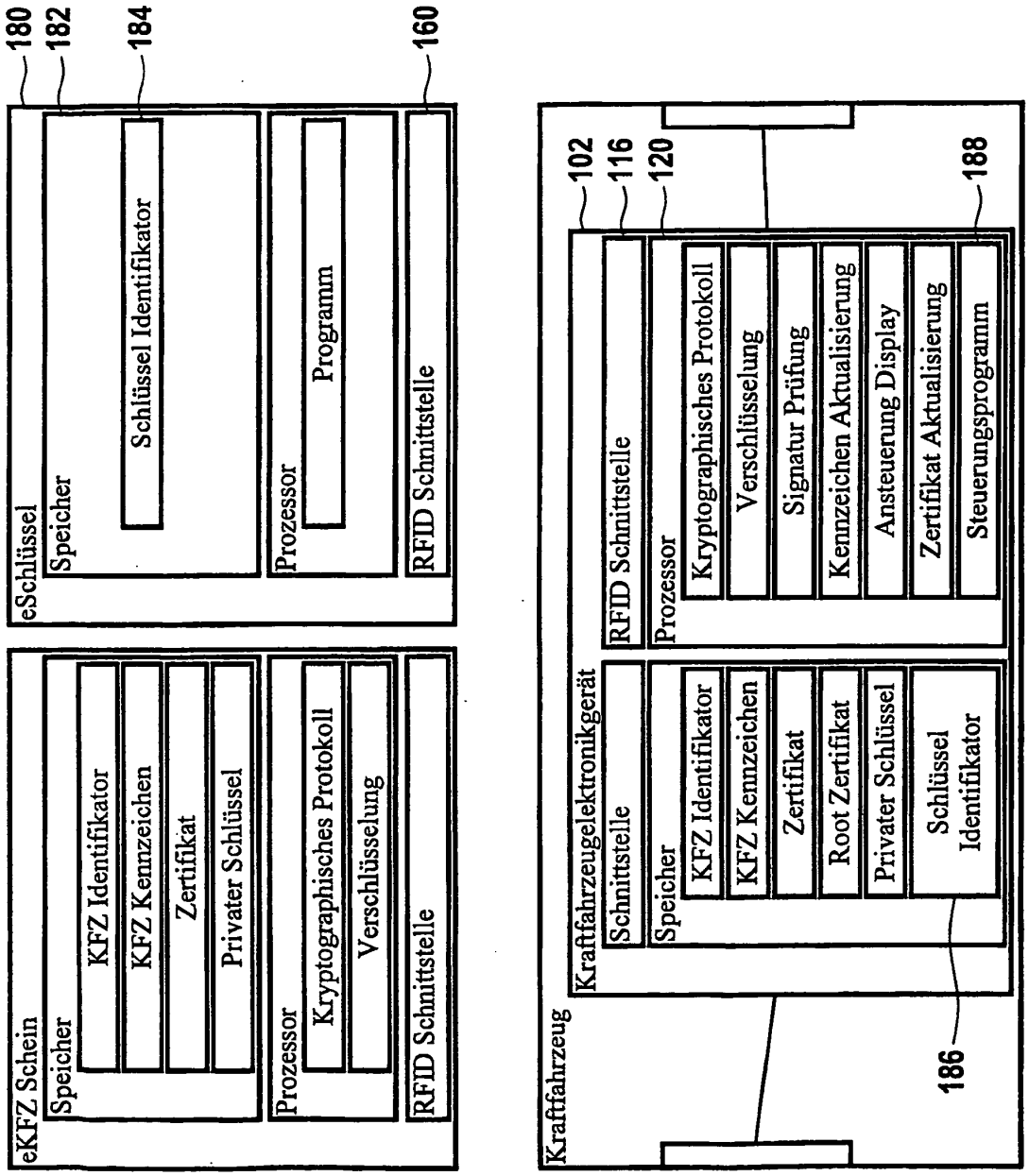

180
182
184
160
eSchlüssel
Speicher
Schlüssel Identifikator
Prozessor
Programm
RFID Schnittstelle
eKFZ Schein
Speicher
KFZ Identifikator
KFZ Kennzeichen
Zertifikat
Privater Schlüssel
Prozessor
Kryptographisches Protokoll
Verschlüsselung
RFID Schnittstelle
102
116
120
188
186
Kraftfahrzeug
Kraftfahrzeugelektronikgerät
Schnittstelle
Speicher
KFZ Identifikator
KFZ Kennzeichen
Zertifikat
Root Zertifikat
Privater Schlüssel
Schlüssel Identifikator
RFID Schnittstelle
Prozessor
Kryptographisches Protokoll
Verschlüsselung
Signatur Prüfung
Kennzeichen Aktualisierung
Ansteuerung Display
Zertifikat Aktualisierung
Steuerungsprogramm

Fig. 3

IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

Diese Liste der vom Anmelder aufgeführten Dokumente wurde ausschließlich zur Information des Lesers aufgenommen und ist nicht Bestandteil des europäischen Patentdokumentes. Sie wurde mit größter Sorgfalt zusammengestellt; das EPA übernimmt jedoch keinerlei Haftung für etwaige Fehler oder Auslassungen.

In der Beschreibung aufgeführte Patentdokumente

- US 5657008 A **[0002]**
- WO 20071137555 A2 **[0003]**
- US 20070285361 A1 **[0004]**
- DE 102006027253 A1 **[0005]**
- DE 102006015212 A1 **[0006]**
- DE 202004017458 U **[0007]**
- US 20060250534 A1 **[0019]**
- WO 9953371 A **[0019]**
- EP 1715374 A1 **[0019]**
- US 20020079494 A1 **[0022]**
- US 6091194 A **[0022]**
- WO 03098696 A1 **[0023]**