

(12)

Patentschrift

(48) Ausgabetag der Berichtigung: 2009-08-15

(21) Anmeldenummer: A 818/2007

(22) Anmeldetag: 2007-05-23

(43) Veröffentlicht am: 2009-06-15

(51) Int. Cl.⁸: **G08C 17/02**

H04L 9/32

H04Q 7/34

G08G 1/123

(30) Priorität:

01.12.2006 AT A 2001/06 beansprucht.

(56) Entgegenhaltungen:

WO 2006/004231A1

US 2006/0155822A1

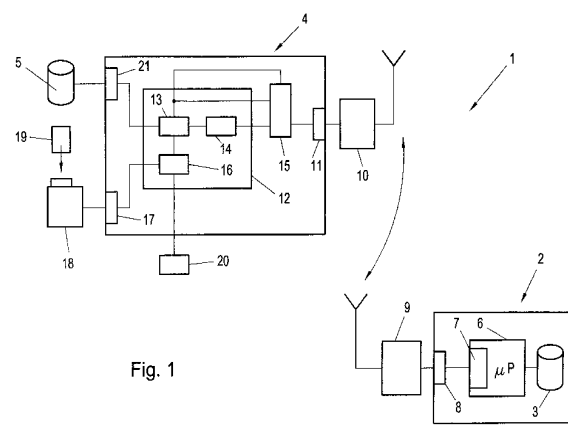
(73) Patentinhaber:

EFKON MOBILITY GMBH

D-13355 BERLIN (DE)

(54) VERFAHREN UND SYSTEM ZUM AUSLESEN VON DATEN AUS EINEM SPEICHER EINES FERNEN GERÄTS DURCH EINEN SERVER

(57) Zum Auslesen von Daten aus einem Speicher (3) eines mobilen fernen Fahrzeuggeräts (2) durch einen Server (4) wird zwischen dem Server (4) und dem Gerät (2) eine drahtlose Kommunikationsverbindung aufgebaut, wonach auf der Server-Seite eine Authentifizierungs-Überprüfung durchgeführt und von der Seite des Servers (4) her eine VPN-(virtuelle private Netzwerks-)Verbindung aufgebaut wird, wonach die Daten aus dem Speicher (3) des Geräts (2) ausgelesen, zum Server (4) über die VPN-Verbindung übertragen und gespeichert werden.



Die Erfindung betrifft ein Verfahren zum Auslesen von Daten aus einem Speicher eines mobilen fernen Fahrzeuggeräts durch einen Server, wobei zwischen dem Server und dem Gerät eine drahtlose Kommunikationsverbindung aufgebaut wird.

- 5 In entsprechender Weise bezieht sich die Erfindung auf ein System zum Auslesen von Daten aus einem Speicher eines mobilen fernen Fahrzeuggeräts durch einen Server, dem ebenso wie dem Gerät ein Modem zur drahtlosen Kommunikation zugeordnet ist.

10 Hinsichtlich der Kommunikation zwischen einem mobilen Gerät und einem Server ist es bei elektronischen Mautsystemen oder dergl. Systemen zum Einheben von Gebühren vielfach bekannt, im Zuge einer Kommunikation zwischen einem Fahrzeuggerät und einem zentralen Server Daten, nämlich zur Identifizierung des Fahrzeugs und zur Abbuchung bzw. Bezahlung von Gebühren, vom Fahrzeuggerät zum Server zu senden. Darüber hinaus ist es auch bekannt geworden, andere Arten von Daten aus einem mobilen Gerät zu einem zentralen Rechner zu
15 übermitteln, vgl. beispielsweise die EP 996 105 A, gemäß der ein ortsfestes Schreib/Lesegerät Daten betreffend Temperatur usw. aus einem mobilen Gerät übermittelt bekommt. Aus der US 7 034 683 B ist weiters ein System zur Überwachung von Fahrzeugen, Produkten und Personen bekannt, wobei RFID-Tags verwendet werden, und wobei entsprechende Daten betreffend Ort, Art der Ladung usw. über GSM zu einem Server übertragen werden.

20 Andererseits ist es beispielsweise aus der EP 1 655 921 A1 bekannt geworden, Benutzer eines Kommunikationssystems für einen Netzwerkzugriff einer Authentifizierung zu unterwerfen, so dass nur autorisierte Teilnehmerendgeräte einen Zugang zum Netz erhalten.

25 In der Praxis ergibt sich vielfach die Situation, Daten von einem mobilen fernen Fahrzeuggerät zu einem Rechner auf dessen Anforderung hin zu übertragen, wobei diese Datenübertragung ohne besonderen Aufwand auf Seiten des mobilen fernen Fahrzeuggeräts durchführbar sein soll, und wobei andererseits Aspekte des Datenschutzes zu berücksichtigen sind.

30 Es ist daher eine Aufgabe der Erfindung, ein Verfahren bzw. ein System zum Auslesen von Daten aus einem Speicher eines mobilen fernen Fahrzeuggeräts durch einen Server wie eingangs angegeben vorzusehen, um auf einfache und sichere Weise auch unter Verwendung eines öffentlichen Netzes sowie unter Einhaltung datenschutzrechtlicher Bestimmungen Daten zu einem Server, auf dessen Anforderung hin, zu übertragen. Insbesondere soll damit ein
35 Herunterladen von authentischen Daten dann, wenn das die Daten enthaltende Objekt oder Gerät zu weit entfernt ist, als dass man es direkt erreichen könnte, oder aber aufgrund der mobilen Ausbildung seinen Standort laufend ändert, ermöglicht werden. Dabei soll es weiters auch möglich sein, bestimmte Daten aus unterschiedlichen Geräten, insbesondere auch im Auftrag von berechtigten Unternehmen, anzufordern und herunterzuladen.

40 Zur Lösung dieser Aufgabe sieht die Erfindung ein Verfahren bzw. ein System zum Auslesen von Daten wie in den unabhängigen Ansprüchen angeführt vor. Vorteilhafte Ausführungsformen und Weiterbildungen sind in den abhängigen Ansprüchen angegeben.

45 Mit der erfindungsgemäßen Technik können von einem Server, der beispielsweise außer stationär auch mobil sein kann, Daten aus einem mobilen fernen Fahrzeuggerät angefordert und heruntergeladen werden, wobei hierfür beispielsweise eine herkömmliche Funkverbindung, insbesondere über GPRS oder GSM, aber auch eine Infrarot (IR)-Verbindung genutzt werden kann. Im Einzelnen wird nach Aufbau einer derartigen Kommunikationsverbindung eine VPN
50 (Virtuelle Private Netzwerks)-Verbindung zwischen dem Server und dem Gerät realisiert, und es werden die entsprechenden Applikationen am Server und am mobilen fernen Fahrzeuggerät in die Verbindung eingebunden. Mit Hilfe des Authentifizierungs-Prozesses wird sichergestellt, dass nur mit entsprechender Berechtigung die gewünschten Daten heruntergeladen werden können, wobei diese Datenübertragung aus Sicherheitsgründen bevorzugt überdies unter
55 Verschlüsselung erfolgt. Auf diese Weise können von unterschiedlichen Unternehmen ge-

wünschte Daten aus den verschiedensten Geräten angefordert und zum Server heruntergeladen werden, und der Server (oder einer von mehreren im Netz arbeitenden Servern) kann für derartige Download-Dienstleistungen auch für diverse Kunden zur Verfügung gestellt werden. So ist es beispielsweise denkbar, aus Fahrzeugen fahrzeugspezifische Daten, wie etwa Tachograph-Daten, aber auch von Zählern, von Versorgungseinrichtungen usw. herunterzuladen, d.h. derartige Objekte „fern auszulesen“. Bei den zu übertragenden Daten kann es sich somit um persönliche, beispielsweise fahrerbezogene Daten oder andere spezifische Daten handeln, die aus datenschutzrechtlicher Sicht zu schützen sind, und die jeweils nur einem berechtigten Unternehmen zugänglich gemacht werden dürfen; darüber hinaus ist für die Daten beim Transport über ein öffentliches Netz eine Sicherung gegen Manipulationen von Vorteil. Dies wird durch die erfindungsgemäßen Maßnahmen mit dem VPN-Kommunikationspfad im Rahmen eines öffentlichen Netzes und durch die Authentifizierung sowie gegebenenfalls durch die Verschlüsselung, mit Schlüsseltausch, für eine gesicherte Verbindung, erreicht. Bevorzugt wird die Authentifizierung mit Hilfe einer Authentifizierungskarte vorgenommen, die in einem Kartenleser - nach Übergabe beispielsweise von einem Kunden des Servers - ausgelesen wird, um so eine Zugriffsberechtigung auf bestimmte mobile ferne Fahrzeuggeräte, im Feld, zu erhalten. Darüber hinaus sind keine zusätzlichen Maßnahmen erforderlich. Die Rufnummern der Geräte im Fall von Mobiltelefonverbindungen können durchaus öffentlich sein, und die Zugriffsberechtigung zu den Daten erfolgt erfindungsgemäß wie erwähnt über die Authentifizierung, insbesondere über eine Authentifizierungskarte.

Die Erfindung wird nachfolgend anhand von bevorzugten Ausführungsbeispielen, auf die sie jedoch nicht beschränkt sein soll, und unter Bezugnahme auf die Zeichnung noch weiter erläutert. In der Zeichnung zeigen dabei im Einzelnen:

Fig. 1 schematisch in einem Blockschaltbild ein System zum Fernauslesen von Daten mit einem Server und einem mobilen fernen Fahrzeuggerät;
 Fig. 1A schematisch in einem vergleichbaren Blockschaltbild ein gegenüber Fig. 1 modifiziertes System zum Fernauslesen von Daten;
 Fig. 2 schematisch den Verbindungsaufbau zwischen Server und Gerät unter Aufbau einer VPN-Verbindung und unter Vorsehen einer Authentifizierungs- und Verschlüsselungsprozedur;
 Fig. 3 ein Ablaufdiagramm zur Veranschaulichung der grundsätzlichen Vorgangsweise beim erfindungsgemäßen Verfahren zum Fernauslesen von Daten; und
 die Fig. 4 und 5 Detail-Ablaufdiagramme zu Abschnitten im Ablaufdiagramm gemäß Fig. 3, zur Veranschaulichung der Authentifizierungsprozedur und der Datenübertragung.

In Fig. 1 ist schematisch ein System 1 zum Auslesen von Daten aus einem mobilen fernen Fahrzeuggerät 2 veranschaulicht, bei dem es sich etwa um eine so genannte OBU (On board Unit), aber auch um ein anderes Gerät, wie etwa ein mit einem Tachographen verbundenes Gerät im Fall von Lastkraftwagen, handeln kann. Aus diesem Gerät 2, d.h. genauer aus einem Speicher 3 dieses Geräts 2, fordert ein Server 4 die jeweiligen Daten an, um sie unter Einhaltung von Sicherheitsvorkehrungen, wie nachstehend noch näher zu erläutern ist, übertragen zu bekommen. Dabei sollte selbstverständlich sein, dass der dargestellte eine Server 4 nur als Beispiel zu verstehen ist, und dass auch mehrere Server im Netz, gegebenenfalls in Verbindung mit einer gemeinsamen Datenbank 5, als Speicher, wo die heruntergeladenen Daten gespeichert werden, vorliegen können, und dass insbesondere auch eine Vielzahl von Geräten 2, beispielsweise mehrere tausend Geräte 2, vorliegen können.

Der Speicher 3 im jeweiligen Gerät 2 kann in den verschiedensten bekannten Ausführungen vorliegen, und die Daten werden mit Hilfe eines Prozessors 6 oder dergl. Rechermitteln in diesen Speicher 3 eingeschrieben bzw. aus dem Speicher 3 ausgelesen. Dem Prozessor 6 (nachfolgend der Einfachheit halber μP 6 genannt) ist eine Verschlüsselungs-/Entschlüsselungseinheit 7 zugeordnet, die als eine eigene Komponente ausgebildet und mit dem μP 6 verbunden sein kann, die aber auch als Software-Modul in einem Programmspeicher des μP 6 gebildet sein kann. Der μP 6 enthält weiters auch ein entsprechendes Kommunikationsmodul

(nicht näher veranschaulicht), um über eine Schnittstelle 8 sowie ein damit verbundenes Modem 9 zur drahtlosen Kommunikation, wie insbesondere ein GPRS-Modem 9, mit dem Server 4 zu kommunizieren.

5 Der jeweilige Verbindungsaufbau über diese drahtlosen Kommunikationswege erfolgt vom Server 4 aus, der ein entsprechendes Kommunikationsmodem 10, insbesondere GPRS-Modem 10, zugeordnet hat, mit dem er über eine Schnittstelle 11 verbunden ist. Der Server 4 enthält Rechnermittel 12, die durch einen oder mehrere Prozessoren oder Mikrocomputer (μ C) gebildet sein können, wobei ein Teil davon eine eigene Steuereinheit 13 bildet, die eine
10 Verschlüsselungs-/Entschlüsselungseinheit 14 zugeordnet hat und über eine VPN-Einrichtung 15 und die Schnittstelle 11 mit dem Modem 10 verbunden ist.

Weiters ist in den Rechnermitteln 12 eine Authentifizierungseinheit 16 vorgesehen, welche über eine Schnittstelle 17 mit einem Kartenleser 18 zum Auslesen von Berechtigungskarten 19, die
15 einen Code enthalten und die in den Kartenleser 18 eingeschoben werden, verbunden ist. Zusätzlich ist eine Eingabeeinheit 20 vorgesehen, wobei hier ebenfalls eine entsprechende Authentifizierungs-Prozedur denkbar ist, um eine Zugriffsberechtigung für die Anforderung von Daten aus dem jeweiligen Gerät 2 nachzuweisen. Die Steuereinheit 13 der Rechnermittel 12 ist weiters über eine Schnittstelle 21 mit dem Speicher 5 verbunden.

20 In Fig. 1A ist ein gegenüber dem System gemäß Fig. 1 abgewandeltes System 1 zum Auslesen von Daten aus einem fernen, mobilen Fahrzeuggerät 2, beispielsweise wiederum einem OBU-Fahrzeuggerät, veranschaulicht. Das System 1 weist auch hier einen Server 4 zum Abfragen von Daten aus dem Gerät 2, konkret aus dessen Speicher 3, auf. Der Server 4 ist dabei bevorzugt als mobiler Server ausgeführt, und er ist im Prinzip ähnlich dem Server 4 gemäß Fig. 1
25 ausgebildet, so dass sich, soweit Übereinstimmung gegeben ist, eine neuerliche detaillierte Beschreibung erübrigen kann, ähnlich wie im Fall des Geräts 2. Es wurden jedenfalls einander entsprechende Komponenten des Servers 4 ebenso wie des Geräts 2 mit gleichen Bezugszahlen versehen.

30 Insbesondere weist der Server 4 gemäß Fig. 1A wiederum Rechnermittel 12 mit einer Steuereinheit 13, einer Verschlüsselungs-/Entschlüsselungseinheit 14 sowie einer Authentifizierungseinheit 16 auf. Anders als im Fall von Fig. 1 ist beim System 1 gemäß Fig. 1A der Kartenleser 18 in den Server 4 integriert, um Berechtigungskarten 19 direkt in den Server 4 einschieben
35 und von diesem auslesen zu können.

Ähnlich wie in Fig. 1 ist auch beim System 1 gemäß Fig. 1A eine VPN-Einrichtung 15 mit den Rechnermitteln 13 verbunden, wobei ein Mobiltelefon-Modem 10, z.B. ein GSM-Modem, über eine Schnittstelle 11 an die VPN-Einrichtung 15 angeschlossen ist.

40 Zusätzlich ist nun gemäß Fig. 1A auch ein an sich bekanntes Modem 10' für eine Infrarot-Kommunikation mit der VPN-Einrichtung 15 verbunden. Dieses IR-Modem 10' enthält beispielsweise IR-Sendemittel 22, z.B. in Form von entsprechenden LEDs, sowie auch IR-Empfängermittel 23, beispielsweise in Form von einer oder mehreren IR-empfindlichen Dioden.

45 Korrespondierend dazu hat auch das ferne Gerät 2 ein IR-Modem 9' mit IR-Sendemitteln 22' und IR-Empfangsmitteln 23', wobei dieses IR-Modem 9' über die Verschlüsselungs-/Entschlüsselungseinheit 7 mit dem Prozessor 6 des Geräts 2 verbunden ist. Dieses IR-Modem 9' kann anstatt des Funk-Modems bzw. Mobiltelefon-Modems 9 gemäß Fig. 1 oder aber bevorzugt, wie
50 in Fig. 1A gezeigt, zusätzlich zu letzterem Modem 9 vorgesehen sein, um so das Auslesen von Daten auf Anfrage seitens des Servers 4 hin je nach Wahl bzw. nach günstigeren Kommunikationsbedingungen entweder über die Mobiltelefonverbindung (Modems 9, 10) oder über die Infrarot-Kommunikationsverbindung (Modems 9', 10') vorzusehen.

55 Im Fall eines mobilen Servers 4 ist es auch zweckmäßig, die Verbindung dieses Servers 4 mit

der Datenbank 5 über ein drahtloses Netz (Funknetz) herzustellen, sofern nicht die Datenbank 5 in den Server 4 integriert ist. Demgemäß ist in Fig. 1A auch mit strichlierten Linien beispielhaft eine Anordnung von Sende- und Empfangs-Funkmodems 24 bzw. 25 für die Kommunikation zwischen dem mobilen Server 4 und der Datenbank 5 veranschaulicht.

In Fig. 2 ist schematisch die Verbindung zwischen Server 4 und Gerät 2 mit den vorgesehenen mehreren Sicherheits-Levels ganz schematisch veranschaulicht. Dabei ist als erste Maßnahme (äußere Hülle) die Herstellung einer Kommunikationsverbindung 30 und als nächstinnere „Schale“ die Herstellung einer VPN-Verbindung 31 veranschaulicht. Als zusätzliche Sicherheitsmaßnahmen auf der nächst höheren Ebene sind die beschriebene Authentifizierung 32 sowie die Verschlüsselung 33 bei der Übertragung der Daten zwischen den jeweiligen Applikationen 34, 35 des Servers 4 bzw. des Geräts 2 veranschaulicht. Dabei sind im Einzelnen bei 36 zusätzlich die Datenanforderung sowie der Authentifizierungs-Prozess und die Übergabe der Schlüssel und bei 37 die Übertragung der Daten angedeutet.

Nachfolgend soll nun anhand der Figuren 3 bis 5, in denen Ablaufdiagramme zur Veranschaulichung der Vorgangsweise bei der Fernauslesung der Daten, wie vorstehend bereits beschrieben veranschaulicht sind, ein konkreter Vorgang bei der Datenübertragung näher erläutert werden. Dabei ist in Fig. 3 allgemein gezeigt, dass gemäß einem Feld 40 anfangs, wenn ein Wunsch nach Datenübertragung besteht, eine drahtlose Verbindung zum Gerät 2 vom Server 4 aus aufgebaut wird. Gemäß einem Abfragefeld 41 wird sodann geprüft, ob diese drahtlose Verbindung, beispielsweise über GSM oder GPRS, oder aber über IR, hergestellt ist, und wenn nicht, wird zum Anfangsfeld 40 zurückgekehrt. Sobald jedoch die drahtlose Verbindung besteht, wird gemäß einem weiteren Abfragefeld 42 abgefragt, ob eine berechtigte Abfrage vorliegt, d.h. ob eine Authentifizierung vorliegt bzw. erfolgt ist. Trifft dies nicht zu, wird sofort zum Ende 43 des Vorgangs weitergegangen. Wenn jedoch bei der Überprüfung gemäß Abfragefeld 42 das Ergebnis eine Berechtigung der Abfrage ist, wird sodann gemäß einem Feld 44 die VPN-Verbindung vom Server aus aufgebaut. Im Anschluss daran werden gemäß einem Feld 45 die Daten vom Gerät 2 zum Server 4 übertragen, wobei laufend gemäß einem Abfragefeld 46 abgefragt wird, ob die Daten bereits vollständig übertragen wurden. Trifft dies nicht zu, wird weiterhin gemäß Feld 45 die Datenübertragung vorgenommen. Wenn die Daten jedoch vollständig übertragen wurden, ist das Ende 43 des Vorgangs erreicht.

In Fig. 4 ist mehr im Detail der Vorgang bei der Authentifizierung veranschaulicht, wobei davon ausgegangen wird, dass die Sicherheitsmodule (Crypto-Control) des Servers 4 und des Endgeräts 2 jeweils über spezielle Schlüssel verfügen; der Unternehmensschlüssel muss zusammen mit dem Endgerät (Frontend)-Schlüssel ein gültiges Paar ergeben.

Gemäß Fig. 4 wird entsprechend einem Feld 50 vom Server 4 zwecks Authentifizierung die Unternehmenskennung gesendet, d.h. eine Identifikation jenes Unternehmens, für das die Datenübertragung zu veranlassen ist, und das zur Übertragung der Daten aus dem jeweiligen Endgerät 2 berechtigt ist. Gemäß einem Abfragefeld 51 wird sodann diese Unternehmenskennung im Gerät 2 geprüft, und wenn das Gerät 2 eine Ablehnung ausspricht, d.h. die Unternehmenskennung dem Gerät 2 nicht bekannt ist, erfolgt der Übergang zum Ende 43 wie beschrieben. Im anderen Fall sendet das Gerät 2 eine Bestätigungsmeldung zum Server 4 zurück, s. Feld 52 in Fig. 4. Danach liefert der Server 4 einen VPN-Schlüssel für den Aufbau einer VPN-Verbindung, s. Feld 53, wonach der Aufbau der VPN-Verbindung gemäß Feld 54 erfolgt.

Im Anschluss daran folgt wie bereits ausgeführt die Datenübertragung, was mehr im Detail in Fig. 5 gezeigt ist. Einleitend fragt gemäß Feld 55 der Server 4 nach einer Liste von zugänglichen Daten; hierbei ist zu berücksichtigen, dass mehrere berechtigte Teilnehmer denkbar sind, denen jeweils Daten zugeordnet sind, die aber auch gegeneinander geschützt werden müssen. Gemäß Feld 56 sendet das Gerät 2 dann die Liste der zugänglichen Daten zum Server 4, danach erfolgt vom Server 4 aus einer Abfrage der Daten nach der übermittelten Liste, s. Feld 57 in Fig. 5, und gemäß Feld 58 sendet das Gerät 2 die Daten sowie die zugehörige Signatur,

sofern, wie dies bevorzugt wird, die Daten bereits signiert im Speicher 3 des Geräts 2 abgelegt sind. Im Server 4 wird weiters laufend gemäß Abfragefeld 59 abgefragt, ob das Listen-Ende erreicht ist, d.h. ob alle Daten gemäß Liste übertragen wurden; wenn nein, wird zum Feld 57 zurückgekehrt, um weitere Daten anzufordern. Ist jedoch eine komplette Übertragung der Daten gemäß Liste gegeben, so wird gemäß Feld 60 der Datentransfer beendet, gemäß Feld 61 die VPN-Verbindung geschlossen und schließlich gemäß Feld 62 die drahtlose Kommunikationsverbindung (GSM, GPRS) beendet, wobei der Ende-Schritt 43 dann erreicht ist.

Patentansprüche:

1. Verfahren zum Auslesen von Daten aus einem Speicher (3) eines mobilen fernen Fahrzeuggeräts (2) durch einen Server (4), wobei zwischen dem Server (4) und dem Gerät (2) eine drahtlose Kommunikationsverbindung aufgebaut wird, *dadurch gekennzeichnet*, dass nach dem Aufbau der drahtlosen Kommunikationsverbindung (30) auf der Server-Seite eine Authentifizierungs-Überprüfung (31) durchgeführt und von der Seite des Servers her eine VPN-(virtuelle private Netzwerks-)Verbindung (32) aufgebaut wird, wonach die Daten aus dem Speicher (3) des Geräts (2) ausgelesen, zum Server (4) über die VPN-Verbindung übertragen und gespeichert werden.
2. Verfahren nach Anspruch 1, *dadurch gekennzeichnet*, dass die drahtlose Kommunikationsverbindung über ein Mobiltelefonnetz, z.B. GPRS, aufgebaut wird.
3. Verfahren nach Anspruch 1, *dadurch gekennzeichnet*, dass die drahtlose Kommunikationsverbindung über Infrarot aufgebaut wird.
4. Verfahren nach einem der Ansprüche 1 bis 3, *dadurch gekennzeichnet*, dass die Authentifizierung durch Auslesen eines Codes aus einer Berechtigungskarte (19) durchgeführt wird.
5. Verfahren nach einem der Ansprüche 1 bis 4, *dadurch gekennzeichnet*, dass mit der Authentifizierung eine Zugriffsberechtigung auf die Daten wenigstens eines vorgegebenen Fahrzeugs, nicht jedoch auf jene anderer Fahrzeuge erteilt wird.
6. Verfahren nach einem der Ansprüche 1 bis 5, *dadurch gekennzeichnet*, dass die Daten verschlüsselt übertragen werden.
7. Verfahren nach einem der Ansprüche 1 bis 6, *dadurch gekennzeichnet*, dass die Daten zum Fernauslesen von Zählern oder Tachographen übertragen werden.
8. Verfahren nach einem der Ansprüche 1 bis 6, *dadurch gekennzeichnet*, dass die Daten zum Fernauslesen von Versorgungseinrichtungen übertragen werden.
9. System (1) zum Auslesen von Daten aus einem Speicher (3) eines mobilen fernen Fahrzeuggeräts (2) durch einen Server (4), dem ebenso wie dem Gerät (2) ein Modem (10, 9; 10', 9') zur drahtlosen Kommunikation zugeordnet ist, *dadurch gekennzeichnet*, dass der Server (4) eine VPN-Einrichtung (15) zum Aufbau einer VPN-Verbindung zum Gerät (2) nach Errichtung einer drahtlosen Kommunikationsverbindung aufweist, und dass dem Server (4) eine Authentifiziereinheit (16) zugeordnet ist.
10. System nach Anspruch 9, *dadurch gekennzeichnet*, dass die VPN-Einrichtung (15) eingerichtet ist, die VPN-Verbindung nur bei gegebener Authentifizierung aufzubauen.
11. System nach einem der Ansprüche 9 oder 10, *dadurch gekennzeichnet*, dass die Modems (10; 9) zur drahtlosen Kommunikation Mobiltelefon-Modems sind.

12. System nach einem der Ansprüche 9 oder 10, *dadurch gekennzeichnet*, dass die Modems (10', 9') zur drahtlosen Kommunikation Infrarot-Modems sind.
- 5 13. System nach einem der Ansprüche 9 bis 12, *dadurch gekennzeichnet*, dass die Authentifiziereinheit (16) mit einem Kartenleser (18) zum Auslesen von Berechtigungskarten (19) verbunden ist.
- 10 14. System nach einem der Ansprüche 9 bis 13, *dadurch gekennzeichnet*, dass das Gerät (2) und der Server (4) eine Verschlüsselungseinheit bzw. Entschlüsselungseinheit (7; 14) für einen Datentransfer unter Verschlüsselung aufweisen.
- 15 15. System nach einem der Ansprüche 9 bis 14, *dadurch gekennzeichnet*, dass der Server (4) ein mobiler Server ist.
16. System nach einem der Ansprüche 9 bis 15, *dadurch gekennzeichnet*, dass der Server (4) sowohl ein Mobiltelefon-Modem (10) als auch ein IR-Modem (10') zur drahtlosen Kommunikation aufweist.
- 20 17. System nach einem der Ansprüche 9 bis 16, *dadurch gekennzeichnet*, dass das Gerät (2) sowohl ein Mobiltelefon-Modem (9) als auch ein IR-Modem (9') zur drahtlosen Kommunikation aufweist.

25 **Hiezu 5 Blatt Zeichnungen**

30

35

40

45

50

55

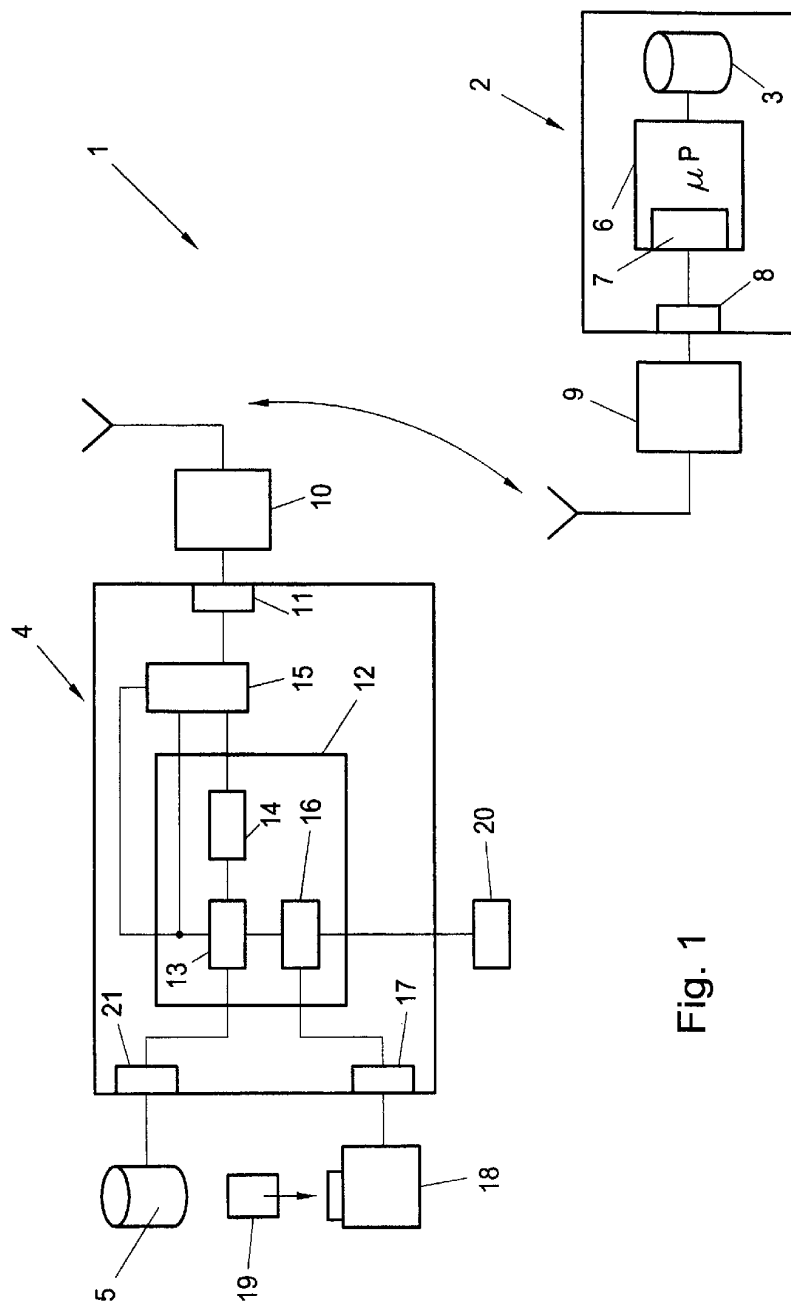


Fig. 1

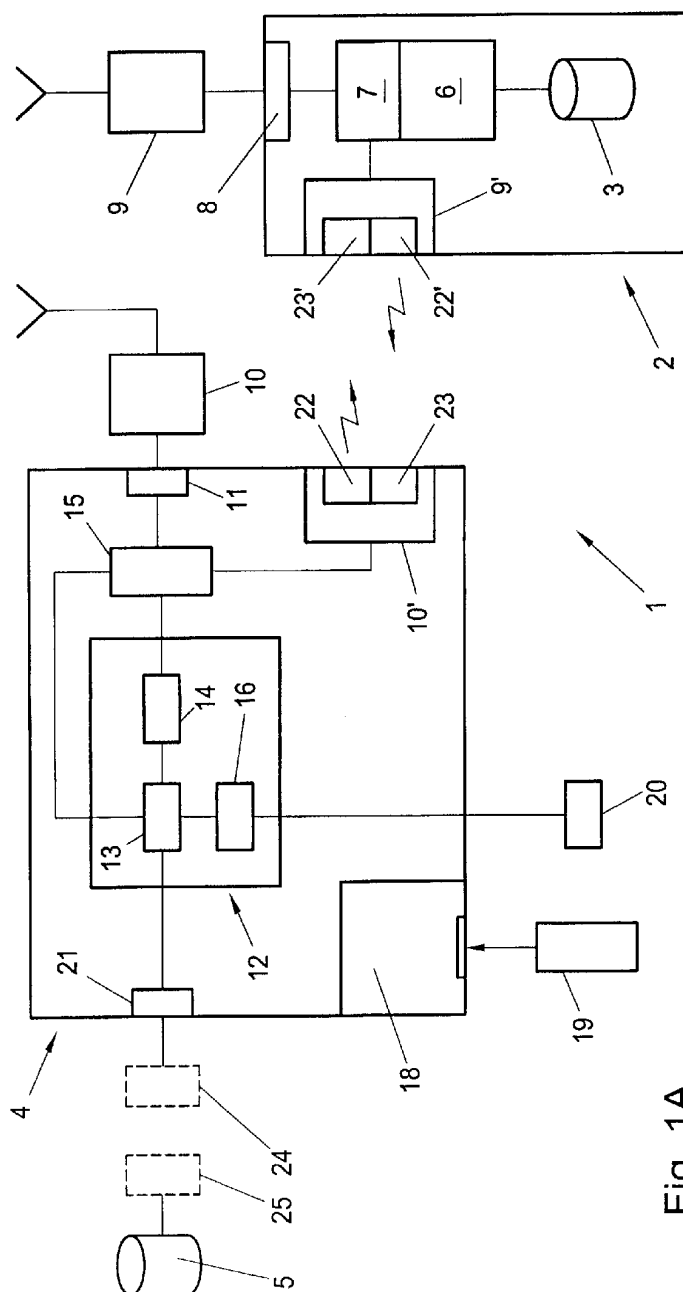


Fig. 1A

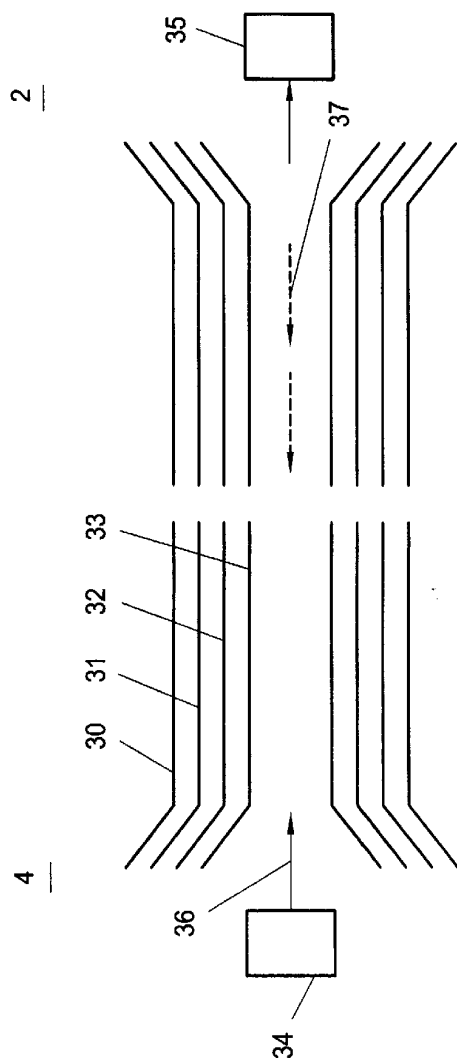


Fig. 2

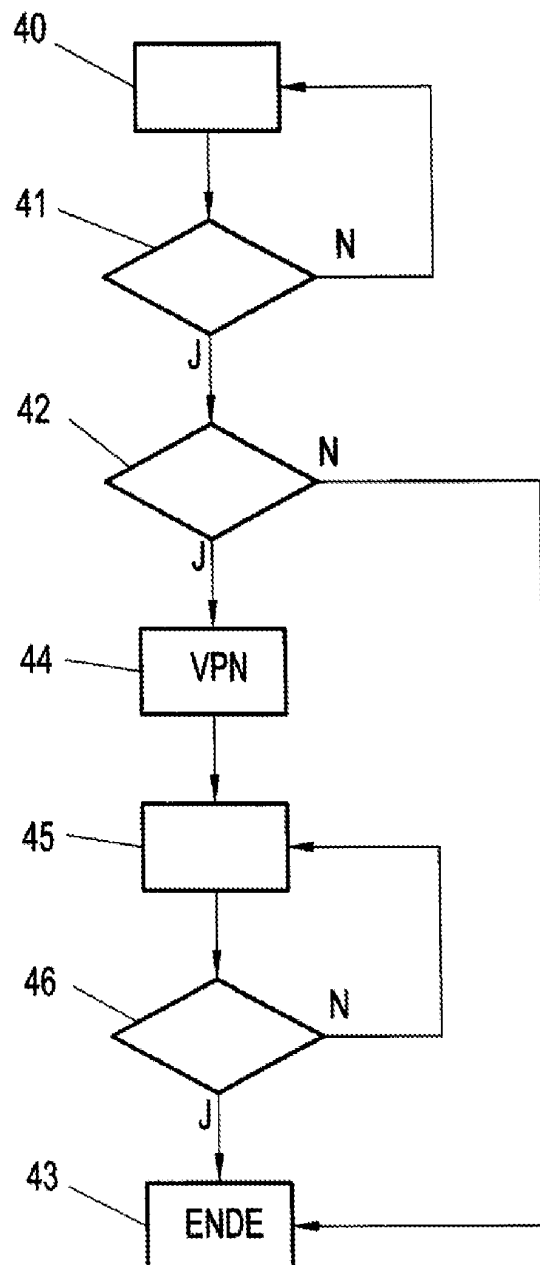


Fig. 3

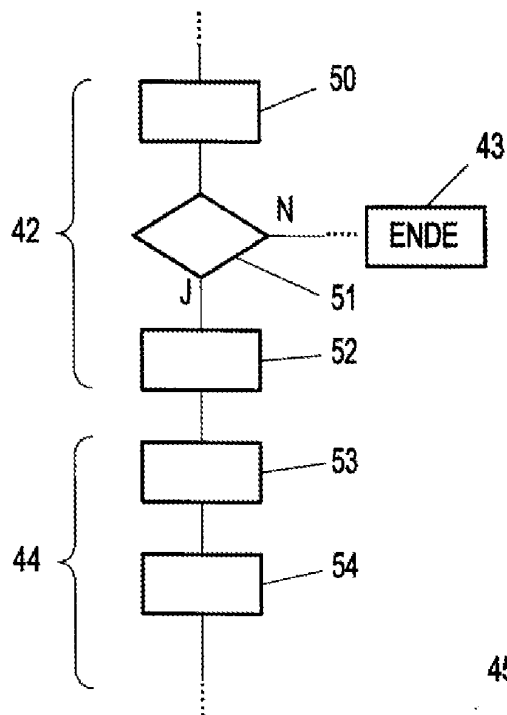


Fig. 4

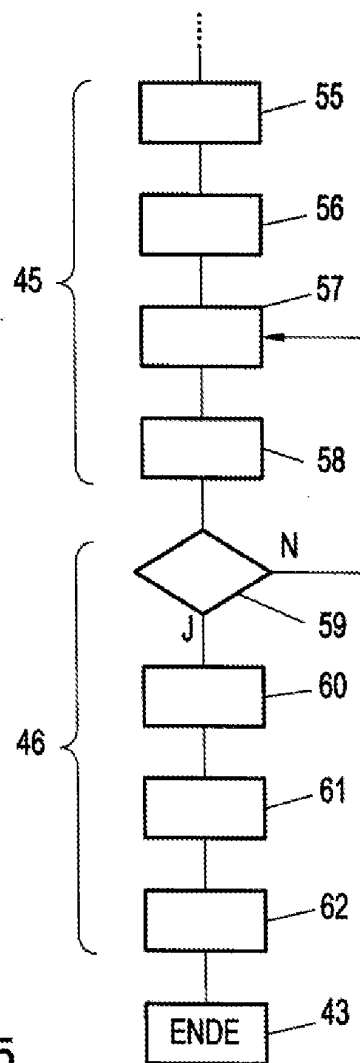


Fig. 5