(19) österreichisches patentamt

(10) **AT 504 581 A1 2008-06-15**

(12) Österreichische Patentanmeldung

(21) Anmeldenummer: **A 2001/2006**
(22) Anmeldetag: **01.12.2006**
(43) Veröffentlicht am: **15.06.2008**

(51) Int. Cl.[8]: ***G08C 17/02*** (2006.01),
H04L 9/32 (2006.01),
H04Q 7/34 (2006.01),
G08G 1/123 (2006.01)

(73) Patentanmelder:

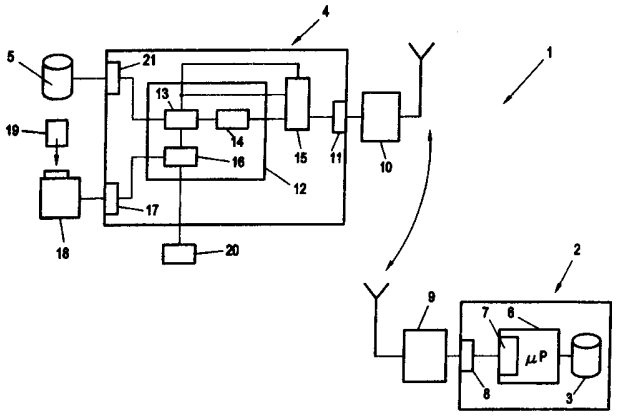
EFKON MOBILITY GMBH
D-13355 BERLIN (DE)

(72) Erfinder:

LYDIKE MATTHIAS
BERLIN (DE)
HOEPPENER BERND
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 eines fernen Geräts (2), z.B. mobilen Geräts, insbesondere Fahrzeuggeräts, 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.



AT 504 581 A1 2008-06-15

Zusammenfassung

Zum Auslesen von Daten aus einem Speicher eines fernen Geräts (2), z.B. mobilen Geräts, insbesondere Fahrzeuggeräts, 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.

(Fig. 1)

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

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

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 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.

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

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

Es ist daher eine Aufgabe der Erfindung, ein Verfahren bzw. ein System zum Auslesen von Daten aus einem Speicher eines fernen, insbesondere mobilen Geräts 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 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 Standard 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.

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.

Mit der erfindungsgemäßen Technik können von einem Server Daten aus einem fernen Gerät, insbesondere einem mobilen (Fahrzeug-) Gerät, angefordert und heruntergeladen werden, wobei hierfür eine herkömmliche Funkverbindung, insbesondere über GPRS oder GSM, genützt wird. Im Einzelnen wird nach Aufbau einer derartigen Funkverbindung eine VPN (Virtuelle Private Netzwerks) -Verbindung zwischen dem Server und dem Gerät realisiert, und es werden die entsprechenden Applikationen am Server und am fernen Gerät 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 Verschlüsselung erfolgt. Auf diese Weise können von unterschiedlichen Unternehmen gewünschte 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 Geräte, beispielsweise mobile Geräte in bestimmten Fahrzeugen, 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 Gerät;

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 fernen Gerät 2 veranschaulicht, bei dem es sich insbesondere um ein mobiles Gerät, nämlich ein Fahrzeuggerät, wie etwa 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. Rechnermitteln 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.

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 (µC) gebildet sein können, wobei ein Teil davon eine eigene Steuereinheit 13 bildet, die eine 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 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.

In Fig. 2 ist schematisch die Verbindung zwischen Server 4 und Gerät 2 mit den vorgesehenen mehreren Sicherheits-Leveln ganz schematisch veranschaulicht. Dabei ist als erste Maßnahme (äußere Hülle) die Herstellung einer Funkverbindung 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, 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 Datenüber-

tragung, 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 eine 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 fernen Geräts (2), z.B. mobilen Geräts, insbesondere Fahrzeuggeräts, 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 oder 2, dadurch gekennzeichnet, dass die Authentifizierung durch Auslesen eines Codes aus einer Berechtigungskarte (19) durchgeführt wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass mit der Authentifizierung eine Zugriffsberechtigung auf die Daten wenigstens eines vorgegebenen Fahrzeugs, nicht jedoch auf jene anderer Fahrzeuge erteilt wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass die Daten verschlüsselt übertragen werden.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass die Daten zum Fernauslesen von Zählern oder Tachographen übertragen werden.

7. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass die Daten zum Fernauslesen von Versorgungseinrichtungen übertragen werden.

8. System (1) zum Auslesen von Daten aus einem Speicher (3) eines fernen Geräts (2), z.B. mobilen Geräts, insbesondere Fahr-

zeuggeräts, durch einen Server (4), dem ebenso wie dem Gerät (2) ein Modem (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.

9. System nach Anspruch 8, dadurch gekennzeichnet, dass die VPN-Einrichtung (15) eingerichtet ist, die VPN-Verbindung nur bei gegebener Authentifizierung aufzubauen.

10. System nach einem der Ansprüche 8 oder 9, dadurch gekennzeichnet, dass die Modems (10; 9) zur drahtlosen Kommunikation Mobiltelefon-Modems sind.

11. System nach einem der Ansprüche 8 bis 10, dadurch gekennzeichnet, dass die Authentifiziereinheit (16) mit einem Kartenleser (18) zum Auslesen von Berechtigungskarten (19) verbunden ist.

12. System nach einem der Ansprüche 8 bis 11, dadurch gekennzeichnet, dass das Gerät (2) und der Server (4) eine Verschlüsselungseinheit bzw. Entschlüsselungseinheit (7; 14) für einen Datentransfer unter Verschlüsselung aufweisen.

AW/dw/mg

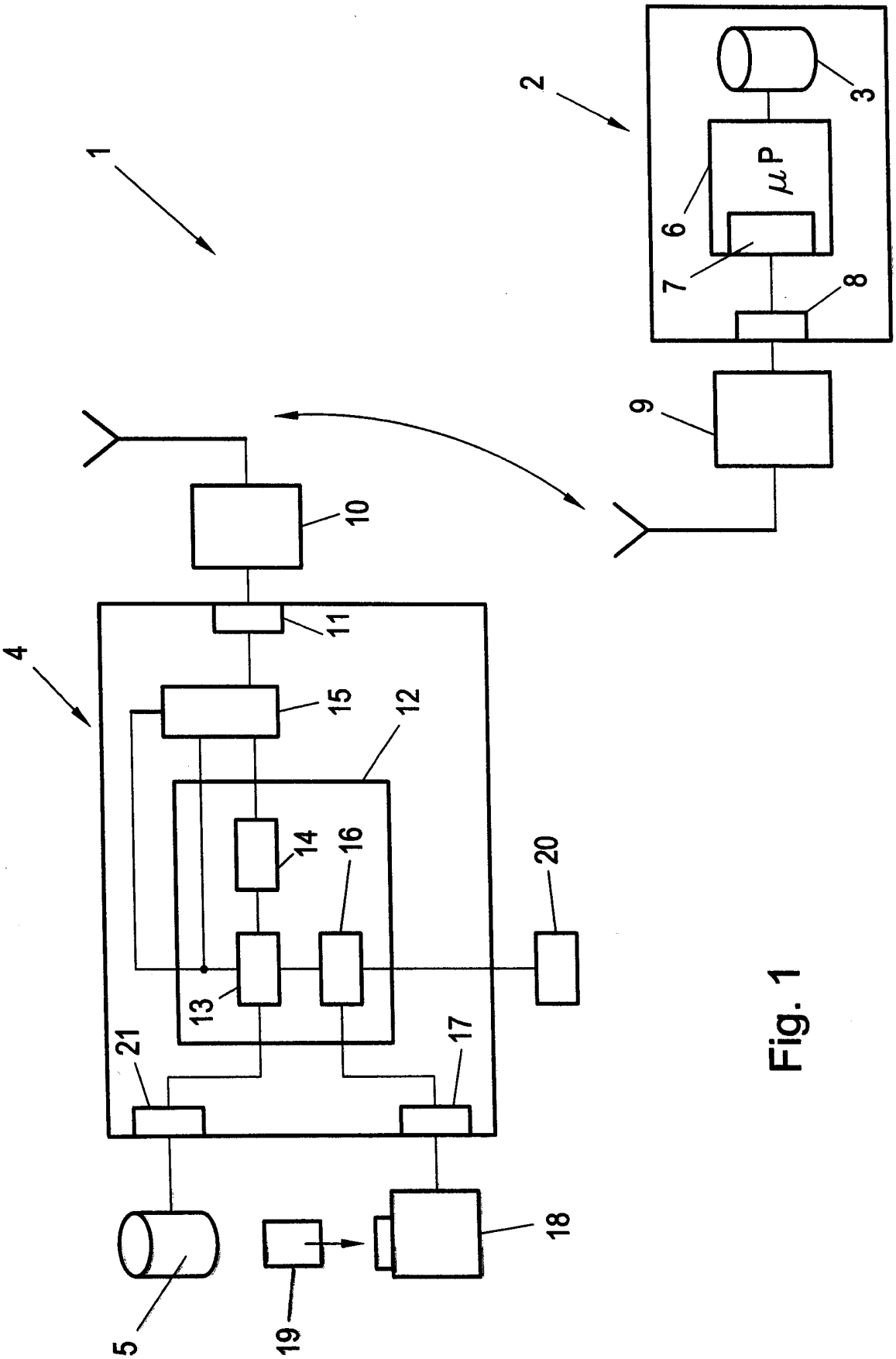


Fig. 1

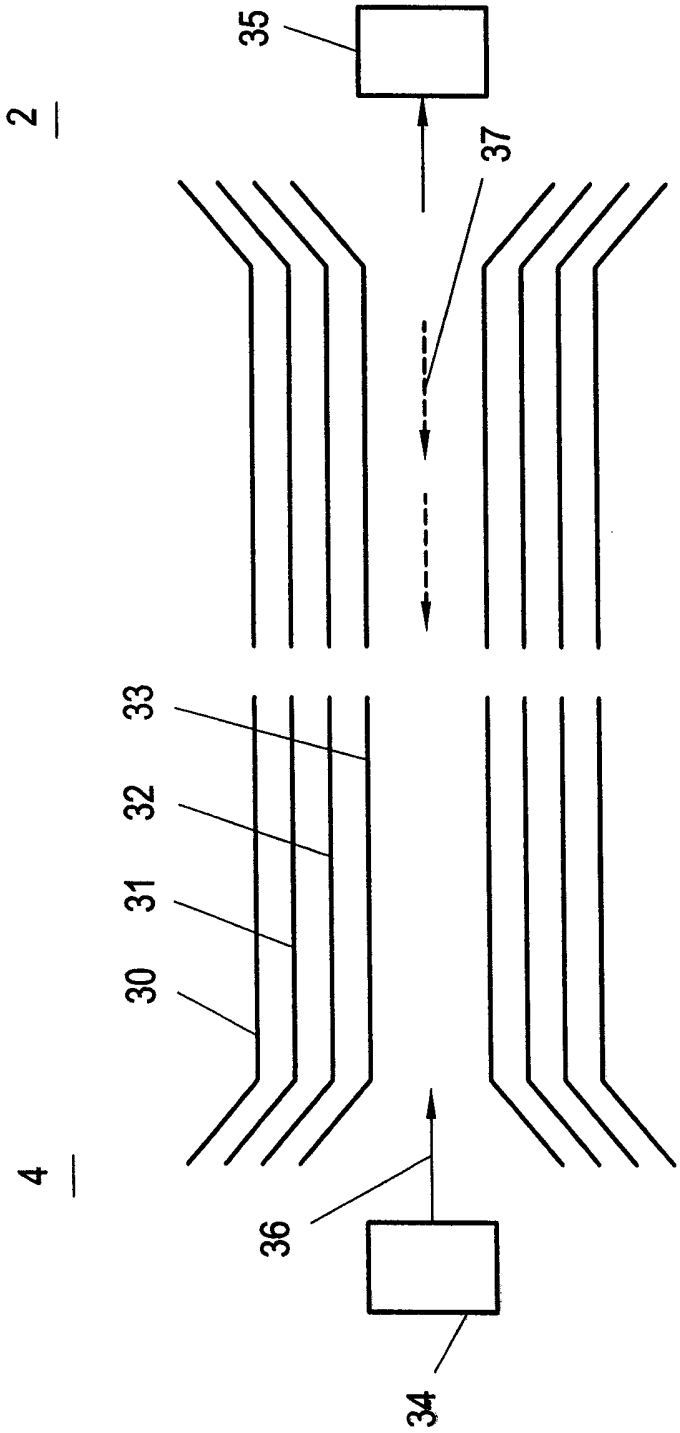


Fig. 2

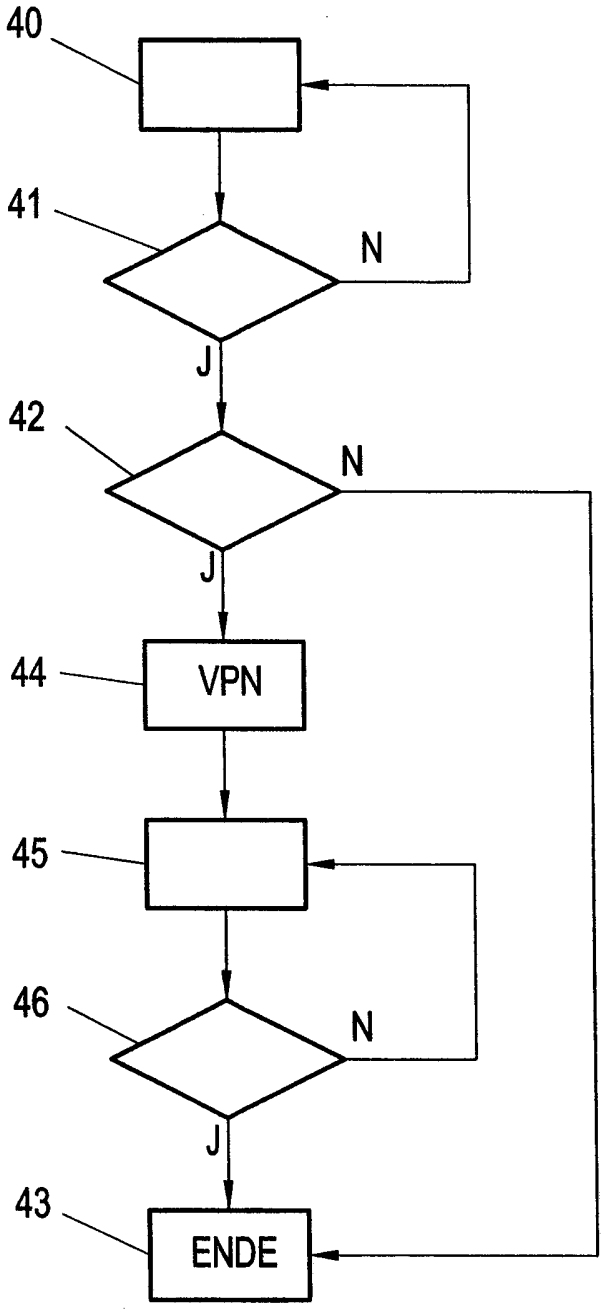


Fig. 3

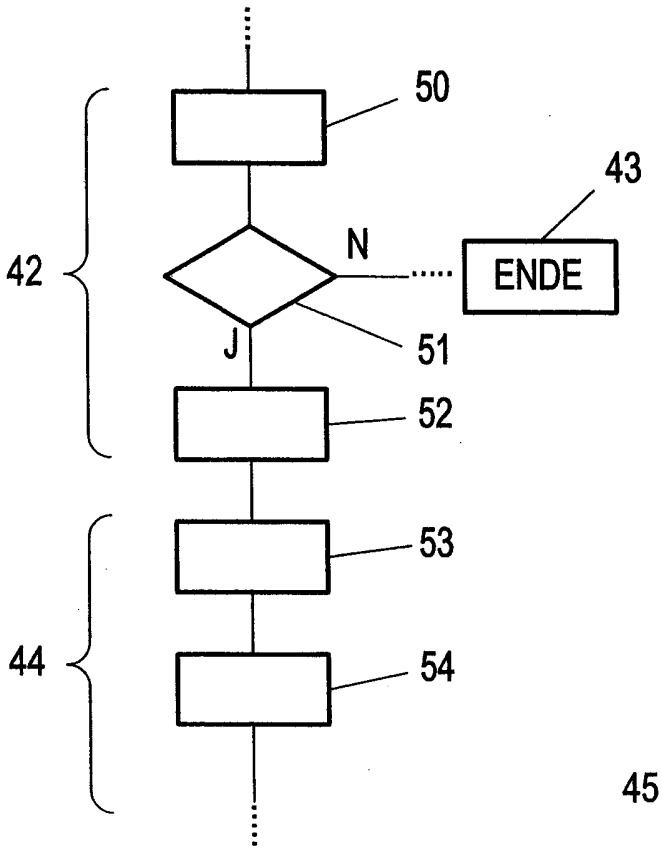

50
43
42
N
ENDE
J
51
52
53
44
54

Fig. 4

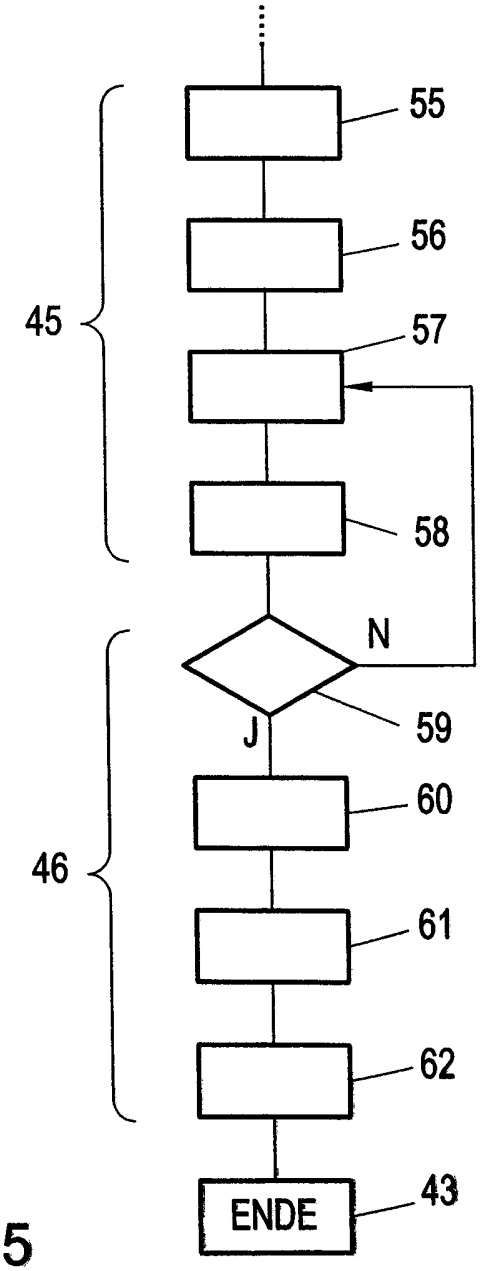

55
56
45
57
58
N
59
J
60
46
61
62
ENDE
43

Fig. 5

Neue Patentansprüche

1. Verfahren zum Auslesen von Daten aus einem Speicher (3) eines mobilen fernen Geräts (2), insbesondere Fahrzeuggeräts, 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) vom Server (4) aus 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 oder 2, dadurch gekennzeichnet, dass die Authentifizierung durch Auslesen eines Codes aus einer Berechtigungskarte (19) durchgeführt wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass mit der Authentifizierung eine Zugriffsberechtigung auf die Daten wenigstens eines vorgegebenen Fahrzeugs, nicht jedoch auf jene anderer Fahrzeuge erteilt wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass die Daten verschlüsselt übertragen werden.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass die Daten zum Fernauslesen von Zählern oder Tachographen übertragen werden.

7. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass die Daten zum Fernauslesen von Versorgungseinrichtungen übertragen werden.

8. System (1) zum Auslesen von Daten aus einem Speicher (3) eines mobilen fernen Geräts (2), insbesondere Fahrzeuggeräts,

NACHGEREICHT

durch einen Server (4), dem ebenso wie dem Gerät (2) ein Modem (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 durch den Server (4) aufweist, und dass dem Server (4) eine Authentifiziereinheit (16) zugeordnet ist.

9. System nach Anspruch 8, dadurch gekennzeichnet, dass die VPN-Einrichtung (15) eingerichtet ist, die VPN-Verbindung nur bei gegebener Authentifizierung aufzubauen.

10. System nach einem der Ansprüche 8 oder 9, dadurch gekennzeichnet, dass die Modems (10; 9) zur drahtlosen Kommunikation Mobiltelefon-Modems sind.

11. System nach einem der Ansprüche 8 bis 10, dadurch gekennzeichnet, dass die Authentifiziereinheit (16) mit einem Kartenleser (18) zum Auslesen von Berechtigungskarten (19) verbunden ist.

12. System nach einem der Ansprüche 8 bis 11, dadurch gekennzeichnet, dass das Gerät (2) und der Server (4) eine Verschlüsselungseinheit bzw. Entschlüsselungseinheit (7; 14) für einen Datentransfer unter Verschlüsselung aufweisen.

AW/dw/mg

NACHGEREICHT

Recherchenbericht zu **A 2001/2006**
Technische Abteilung 3B

österreichisches patentamt

Klassifikation des Anmeldungsgegenstands gemäß IPC[8]: ***G08C 17/02*** (2006.01); ***H04L 9/32*** (2006.01); ***H04Q 7/34*** (2006.01); *G08G 1/123* (2006.01)
Klassifikation des Anmeldungsgegenstands gemäß ECLA: G08C 17/02, H04L 9/32M, H04Q 7/34A
Recherchierter Prüfstoff (Klassifikation): G08C, G08G, H04L, H04Q
Konsultierte Online-Datenbank: WPI, EPODOC
Dieser Recherchenbericht wurde zu den am **1. Dezember 2006** eingereichten Ansprüchen **1-12** erstellt.

Kategorie*)	Bezeichnung der Veröffentlichung: Ländercode, Veröffentlichungsnummer, Dokumentart (Anmelder), Veröffentlichungsdatum, Textstelle oder Figur soweit erforderlich	Betreffend Anspruch
A	WO 2006/004231 A1 (NURI TELECOM CO. LTD) 21. Jänner 2006 (21.01.2006) *Ansprüche 1,2*	1-3,7,8,10
	--	
A	US 2006/0155822 A1 (YANG et al.) 13. Juli 2006 (13.07.2006) *Fig. 2,4; Ansprüche 1,9,11,12*	1-3, 8-10

Datum der Beendigung der Recherche:	☐ Fortsetzung siehe Folgeblatt	Prüfer(in):
30. Mai 2007		Dr. FUSSY

*) **Kategorien** der angeführten Dokumente:

- **X** Veröffentlichung **von besonderer Bedeutung**: der Anmeldungsgegenstand kann allein aufgrund dieser Druckschrift nicht als neu bzw. auf erfinderischer Tätigkeit beruhend betrachtet werden.
- **Y** Veröffentlichung **von Bedeutung**: der Anmeldungsgegenstand kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren weiteren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese **Verbindung für einen Fachmann nahellegend** ist.
- **A** Veröffentlichung, die den **allgemeinen Stand der Technik** definiert.
- **P** Dokument, das **von Bedeutung** ist (Kategorien **X** oder **Y**), jedoch **nach dem Prioritätstag** der Anmeldung **veröffentlicht** wurde.
- **E** Dokument, das **von besonderer Bedeutung** ist (Kategorie **X**), aus dem ein **älteres Recht** hervorgehen könnte (früheres Anmeldedatum, jedoch nachveröffentlicht, Schutz ist in Österreich möglich, würde Neuheit in Frage stellen).
- **&** Veröffentlichung, die Mitglied der selben **Patentfamilie** ist.