

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum  
Internationales Büro



(43) Internationales Veröffentlichungsdatum  
16. November 2006 (16.11.2006)

PCT

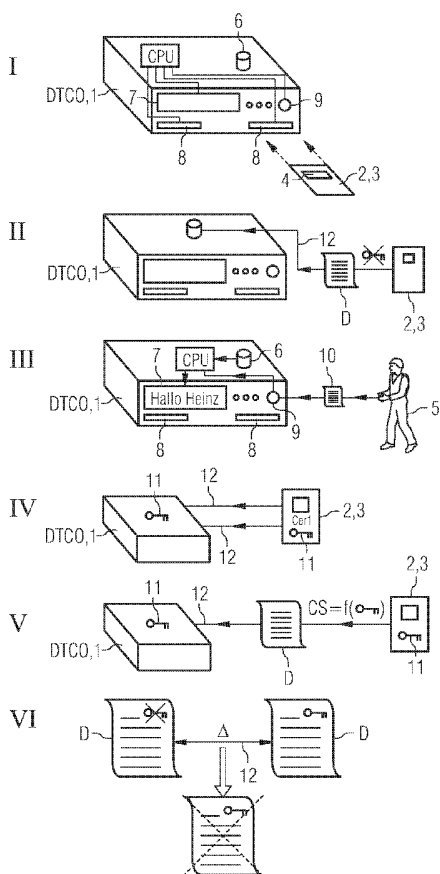
(10) Internationale Veröffentlichungsnummer  
WO 2006/120170 A1

- (51) Internationale Patentklassifikation:  
G07C 5/08 (2006.01) G07F 7/10 (2006.01)  
G06K 7/00 (2006.01) H04L 9/32 (2006.01)  
G06F 21/00 (2006.01)
- (21) Internationales Aktenzeichen: PCT/EP2006/062100
- (22) Internationales Anmeldedatum:  
5. Mai 2006 (05.05.2006)
- (25) Einreichungssprache: Deutsch
- (26) Veröffentlichungssprache: Deutsch
- (30) Angaben zur Priorität:  
10 2005 022 112.2 12. Mai 2005 (12.05.2005) DE
- (71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).
- (72) Erfinder; und  
(75) Erfinder/Anmelder (nur für US): LINDINGER, Andreas [DE/DE]; Im Winkel 12, 78658 Flözlingen (DE). NÄTHER, Horst [DE/DE]; Oderstr. 81/1, 78052 Villingen-Schwenningen (DE).
- (74) Gemeinsamer Vertreter: SIEMENS AKTIENGESELLSCHAFT; Postfach 22 16 34, 80506 München (DE).
- (81) Bestimmungsstaaten (soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES,

[Fortsetzung auf der nächsten Seite]

(54) Title: DATA TRANSFER BETWEEN MODULES

(54) Bezeichnung: DATENÜBERTRAGUNG ZWISCHEN MODULEN



(57) Abstract: The invention relates to a method for transferring data (D) between a first module (1) and a second module (2), whereby data (D) can be transferred from a data memory (4) of the second module (2) to the first module (1) either in a secured or not secured manner. The aim of the invention is to reduce the time required for authentication (IV). The inventive method is characterized by first transferring first data (D) in a not secured and then in a secured manner, said data being used by means of a processor (CPU) of the first module (1) for a first process (III). The data (D) transferred in a not secured manner are compared with those transferred in a secured manner and if there is a difference, results from the first process (III) are discarded. The invention also relates to a system for carrying out the inventive method.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zur Übertragung von Daten (D) zwischen einem ersten Modul (1) und einem zweiten Modul (2), wobei aus einem Datenspeicher (4) des zweiten Moduls (2) Daten (D) an das erste Modul (1) entweder gesichert oder ungesichert übertragbar sind. Der bisher zeitführende Authentisierungsvorgang (IV) dauert mitunter sehr lange. Hier schafft die Erfindung Abhilfe, indem zunächst erste Daten (D) ungesichert und anschließend gesichert übertragen werden, die mittels eines Prozessors (CPU) des ersten Moduls (1) für einen ersten Prozess (III) benutzt werden. Danach werden die ungesichert übertragenen mit den gesichert übertragenen Daten (D) verglichen und bei einem Unterschied Ergebnisse aus dem ersten Prozess (III) verworfen werden. Daneben beschäftigt sich die Erfindung mit einer Anordnung zur Ausführung des erfindungsgemäßen Verfahrens.

WO 2006/120170 A1



FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

**(84) Bestimmungsstaaten** (soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK,

EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Veröffentlicht:**

— mit internationalem Recherchenbericht

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

## Beschreibung

## Datenübertragung zwischen Modulen

5 Die Erfindung betrifft ein Verfahren zur Übertragung von Daten zwischen einem ersten Modul und einem zweiten Modul, insbesondere zwischen einem Fahrtschreiber und einem an diesen anschließbaren Datenträger, wobei das zweite Modul einen Datenspeicher aufweist, aus welchem Daten an das erste Modul  
10 entweder nach einem Authentisierungsvorgang gesichert oder ungesichert übertragbar sind. Daneben ist eine Anordnung mit einem ersten Modul und einem zweiten Modul bzw. einem Fahrtschreiber und einem anschließbaren Datenträger Gegenstand der Erfindung, wobei die Anordnung zur Ausführung des vorgenannten Verfahrens ausgebildet ist.  
15

Bevorzugtes Anwendungsgebiet der Erfindung ist der Betrieb von Fahrtschreibern bzw. Tachographen, bei welchen stets ein erstes Modul bzw. der Fahrtschreiber in dem Nutzfahrzeug fest  
20 installiert ist und ein zweites Modul bzw. der meist als Datenkarte ausgebildete Datenträger dem Führer des Nutzfahrzeuges zugeordnet ist und in eine Daten übertragende Verbindung mit dem Fahrtschreiber gebracht werden kann. Die personenbezogenen Betriebsdaten werden beim Einstecken der Datenkarte  
25 in den Fahrtschreiber von einem Speicher der Datenkarte zu einem Teil ausgelesen und von dem Fahrtschreiber einer ersten Auswertung unterzogen. Hierbei wird unter anderem festgestellt, wie lange der Fahrzeugführer unter Berücksichtigung der kumulativen Lenkzeitunterbrechung lenken darf. Nach Ste-  
30 cken der Karte bzw. Herstellung der Daten übertragenden Verbindung sind Eingaben des Fahrzeugführers an eine Eingabevorrichtung des Fahrtschreibers zur Aufnahme der Arbeit erforderlich. Hierzu zählen unter anderem das Land des aktuellen Standortes und die beabsichtigte auszuübende Tätigkeit des  
35 Karteninhabers. Nach der EWG-Verordnung Nr. 3821/85 ist die Datenübertragung zwischen dem ersten Modul und dem zweiten Modul bzw. dem Fahrtschreiber und der Datenkarte gesichert

durchzuführen. Hierzu ist eingangs der Datenübertragung eine Authentisierung erforderlich, während derer unter anderem ein Sitzungsschlüssel erzeugt wird, mittels dessen die Übertragung von Daten abgesichert wird. Der Zeitaufwand für den  
5 vollständigen Authentisierungsvorgang übersteigt jedoch unter bestimmten Umständen eine vernünftigerweise zu akzeptierende Dauer.

Ausgehend von diesem Problem liegt der Erfindung die Aufgabe zugrunde, den Zeitraum vom Herstellen einer Daten übertragenden Verbindung zwischen dem ersten Modul und dem zweiten Modul ohne Einbuße an Sicherheit gegen etwaige Manipulationen bis zur Aufnahme eines auf der Datenübertragung basierenden Prozesses auf ein vernünftiges Maß zu verkürzen.

15 Hierzu schlägt die Erfindung ein Verfahren mit den Merkmalen des Anspruchs 1 und eine Anordnung mit den Merkmalen des Anspruchs 11 vor. Die jeweils rückbezogenen Unteransprüche beinhalten vorteilhafte Weiterbildungen der Erfindung.

20 Der besondere Vorteil der Erfindung liegt darin, dass auf Grund des zunächst stattfindenden ungesicherten Lesens bzw. Übertragens von Daten von dem zweiten Modul bzw. der Datenkarte des Fahrschreibers auf das erste Modul bzw. den Fahrschreiber der zeitliche Aufwand des Authentisierens bzw. der Absicherung der Datenübertragung vorab eingespart werden kann. Dies ist insbesondere dann von besonderem Vorteil, wenn erfindungsgemäß die zu übertragenden Daten für einen ersten Prozess benutzt werden. In diesem Fall ist die Datenübertragung also zeitkritisch für den Beginn des ersten Prozesses  
25 bzw. den Gesamtvorgang. Am konkreten Beispiel des Fahrschreibers kann der Fahrzeugführer mit seiner Eingabe bereits früher beginnen ohne auf die Ergebnisse des Authentisierungsvorganges warten zu müssen. Es kommt dennoch nicht zu einer  
30 Einbuße an Sicherheit gegen Manipulation, da im Nachgang die Authentisierung und das gesicherte Übertragen von Daten nachgeholt werden und ein Vergleich der gesichert übertragenen  
35

Daten mit den ungesichert übertragenen Daten erfolgt. Fällt dieser Vergleich negativ aus bzw. ist eine Differenz feststellbar, werden die Ergebnisse aus dem ersten Prozess verworfen. Am konkreten Beispiel des Fahrtschreibers bedeutet  
5 das Verwerfen, dass die Eingaben des Fahrzeugführers verworfen werden. Darüber hinaus kann mit Vorteil die Karte von dem Fahrtschreiber nicht akzeptiert werden. Das Authentisieren und das Vergleichen läuft zweckmäßig von dem Prozessor gesteuert in Hintergrund ab, so dass im Sinne eines Multitaskings das Gerät einerseits beispielsweise Eingaben des Benutzers akzeptiert und im konkreten Fall des Fahrtschreibers auch mit der Registrierung von Betriebsdaten, die von einem im Betrieb des Nutzfahrzeuges im Getriebe angeordneten Sensor übermittelt werden, durchführt. Die provisorisch bzw. ungesichert eingelesenen Daten werden sinnvoll in einem Speicher  
10 des ersten Moduls bzw. des Fahrtschreibers abgelegt und während oder nach dem gesicherten Auslesen der Daten mit den letzteren verglichen.

20 Eine vorteilhafte Weiterbildung der Erfindung sieht vor, dass die ungesichert eingelesenen Daten eine Eingabe von zusätzlichen Daten mittels eines dritten Moduls bzw. einer Eingabevorrichtung des Fahrtschreibers während des ersten Prozesses unterstützen. Beispielsweise kann hierbei eine Sprachkennung  
25 aus dem zweiten Modul ausgelesen werden, die angibt, welche Sprache auf einer Anzeigeeinheit des ersten Moduls zur Darstellung von Schrift bzw. Klartext benutzt wird.

Die Zeitersparnis bei dem erfindungsgemäßen Verfahren bzw.  
30 einer Benutzung der erfindungsgemäßen Anordnung ist besonders hoch, wenn die Daten in einem Datenspeicher des zweiten Moduls unverschlüsselt abgelegt sind und von dem ersten Modul auslesbar sind. Dieser Vorgang bzw. eine derartige Ausbildung der Anordnung muss keine Einbuße an Sicherheit bedeuten, wenn  
35 für die gesicherte Übertragung während des Authentisierungsvorganges ein Schlüssel zur gesicherten Datenübertragung von dem ersten Modul erzeugt wird, unter dessen Einbeziehung aus

den übertragenen Daten von dem zweiten Modul mindestens ein  
Kontrolldatum erzeugt wird, so dass das erste Modul aus einer  
Auswertung des mit den zu übermittelnden Daten übersendeten  
Kontrolldatums und den übertragenen Daten die Authentizität  
5 der übertragenen Daten ermitteln kann. Die Abhängigkeit des  
Kontrolldatums einerseits von dem erzeugten geheimen Schlüssel  
und andererseits von den sonstigen übertragenen Daten  
schließt eine unbemerkte Manipulation sicher aus.

10 Erfindungsgemäß kann nur die Authentisierung oder nur die ge-  
sicherte Übertragung von dem Prozessor gesteuert im Hinter-  
grund erfolgen, was bereits zu erheblichen Zeiteinsparungen  
führt. Besonders groß werden die erfindungsgemäßen Vorteile,  
wenn sowohl die Authentisierung als auch die Übertragung im  
15 Hintergrund stattfinden.

Obgleich eine Ausbildung der erfindungsgemäßen gesicherten  
Übertragung und Ermittlung der Authentizität der übertragenen  
Daten als Hardware-Bauelement einen verhältnismäßig geringen  
20 Rechenaufwand und gegenüber der Software-Alternative im Be-  
trieb weniger zeitintensiv ist, ist aus Kostengründen eine  
Implementierung der Vorgänge des Authentisierens und der Er-  
mittlung der Authentizität der übertragenen Daten als aus-  
führbare Programme, die veränderbar zumindest teilweise in  
25 einem Speicher des ersten Moduls abgelegt sind, zu bevorzu-  
gen. Hierbei kommen die Vorteile der erfindungsgemäßen ein-  
gangs des Vorganges der Datenübertragung stattfindenden Be-  
schleunigung besonders zum tragen. Damit die ungesicherte  
Übertragung während des Normalbetriebes nicht unbemerkt zur  
30 Regel wird, ist es sinnvoll, wenn das System diesen Zustand  
normalerweise als Fehler meldet. Derartige Fehlermeldungen  
können mit Vorteil unterdrückt werden, während des ungesi-  
cherten Betriebes von Daten und der Verarbeitung dieser Da-  
ten, insbesondere im zeitlichen Umfeld des Anschließens des  
35 ersten Moduls an das zweite Modul bzw. eingangs der Daten-  
übertragung zwischen dem Fahrtschreiber und dem Datenträger.

Im Folgenden ist die Erfindung anhand eines speziellen Ausführungsbeispiels zur Verdeutlichung näher erläutert. Es zeigt:

- 5   Figur 1   Schritte 1 bis 6 eines erfindungsgemäßen Datenübertragungsverfahrens mit einer erfindungsgemäßen Anordnung.

In Figur 1 sind Schritte I bis VI eines erfindungsgemäßen Verfahrens dargestellt. In Figur 1 ist ein erstes Modul 1 bzw. ein Fahrtschreiber DTCO im Zusammenwirken mit einem zweiten Modul 2 bzw. einem als Datenkarte ausgebildeten Datenträger 3 dargestellt. Das zweite Modul 2 weist einen Datenspeicher 4 auf, welcher personen-bezogene Betriebsdaten für einen Benutzer 5 speichert. Der Fahrtschreiber DTCO weist einen Prozessor CPU auf, der mit einem Datenspeicher 6 des Fahrtschreibers DTCO in Daten übertragender Verbindung steht. Daneben ist der Prozessor CPU zur Ansteuerung mit einer Anzeige 7, zwei Datenkartenaufnahmen 8 und einer Eingabevorrichtung 9 verbunden. Der Datenträger 3 lässt sich in die Datenkartenaufnahme 8 einführen gemäß dem abgebildeten Schritt I, so dass er von außen unzugänglich ist. Sobald der Datenträger 3 in dem Fahrtschreiber DTCO mit diesem in eine Datenübertragende Verbindung 12 eintritt, werden Daten D von dem Datenträger 3 in den Datenspeicher 6 ungesichert übertragen.

Während des anschließend dargestellten Schrittes III gibt der Benutzer mittels der Eingabevorrichtung 9 Eingabedaten 10 ein, unterstützt von der Anzeige 7, auf der unter Verwendung der während des Schrittes II übertragenen Daten D Vorgaben zu der Eingabe angezeigt werden. Dieser erste Prozess (III) wird unter Zugriff auf den Datenspeicher 6 von dem Prozessor CPU gesteuert.

35 Mit Eingabe der Eingabedaten 10 kann der Benutzer 5 in dem konkreten Ausführungsbeispiel seine Arbeit beginnen bzw. den

Fahrbetrieb aufnehmen, und der Fahrtschreiber DTCO kann die Registrierung der Betriebsdaten personenspezifisch beginnen.

Der mit IV bezeichnete Schritt ist ein Authentisierungsvorgang, während dessen ein Schlüssel 11 zur Sicherung der Datenübertragung zwischen dem Fahrtschreiber DTCO und dem Datenträger 3 erzeugt wird. Dieser Vorgang läuft ebenso wie der nachfolgende im Hintergrund des Multitasking-fähigen Fahrtschreibers DTCO ab. Während des anschließenden Schrittes V findet eine mittels des Schlüssels 11 gesicherte Übertragung der Daten D von dem Datenträger 3 auf den Fahrtschreiber DTCO statt. Die Sicherung der Übertragung erfolgt in der Weise, dass unverschlüsselte Daten D gemeinsam mit einem Kontrolldatum CS übertragen werden, wobei das Kontrolldatum CS sowohl als von dem Schlüssel 11 sowie auch von den Daten D abhängig erzeugt ist. Eine Auswertung des Kontrolldatums CS durch den Fahrtschreiber DTCO unter Berücksichtigung des Schlüssels 11 und der Daten D zeigt, ob die übermittelten Daten D authentisch sind oder eine Manipulation vorliegt. Wird die Authentizität bejaht, gilt die gesicherte Übertragung der Daten D als erfolgreich. Während des anschließenden Schrittes VI werden die erfolgreich gesichert übertragenen Daten D mit den ungesichert übertragenen Daten D, die zwischenzeitlich in dem Speicher 6 des Fahrtschreibers DTCO abgelegt wurden, verglichen. Wird eine Differenz  $\Delta$  festgestellt, werden die Eingabedaten 10 verworfen, und der Datenträger 3 bzw. die Datenkarte wird abgelehnt.

## Patentansprüche

1. Verfahren zur Übertragung von Daten (D) zwischen einem  
ersten Modul (1) und einem zweiten Modul (2), insbeson-  
5 dere zwischen einem Fahrtschreiber (DTCO) und einem an  
diesen anschließbaren Datenträger (3),  
wobei das zweite Modul einen Datenspeicher (4) aufweist,  
aus welchem Daten (D) an das erste Modul (1)  
entweder nach einem Authentisierungsvorgang gesichert  
10 oder ungesichert übertragbar sind,  
wobei nach dem Anschluss des zweiten Moduls (2) an das  
erste Modul (1) zunächst Daten (D) ungesichert übertra-  
gen werden, die mittels eines Prozessors (CPU) des ers-  
ten Moduls (1) für einen ersten Prozess (III) benutzt  
15 werden,  
wobei nach Beginn der ungesicherten Übertragung eine ge-  
sicherte Übertragung der Daten (D) von dem zweiten Mo-  
dul (2) auf das erste Modul (1) erfolgt,  
wobei anschließend die ungesichert übertragenen Daten  
20 (D) mit den gesichert übertragenen Daten (D) verglichen  
werden und bei einem Unterschied zwischen den gesichert  
und den ungesichert übertragenen Daten (D) Ergebnisse  
aus dem ersten Prozess (III) verworfen werden.
- 25 2. Verfahren nach Anspruch 1, d a d u r c h g e k e n n -  
z e i c h n e t , dass die ungesichert übertragenen Da-  
ten (D) für eine Eingabe von zusätzlichen Eingabeda-  
ten (10) mittels eines dritten Moduls (Eingabevorrich-  
tung 9) während des ersten Prozesses (III) verwendet  
30 werden.
3. Verfahren nach Anspruch 2, d a d u r c h g e k e n n -  
z e i c h n e t , dass das dritte Modul als Eingabevor-  
richtung (9) ausgebildet ist, an der ein Benutzer (5)  
35 Eingaben machen kann.

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Daten (D) in einem Datenspeicher (4) des zweiten Moduls (2) unverschlüsselt abgelegt sind und von dem ersten Modul (1) auslesbar sind.
- 5
5. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die ungesichert übertragenen Daten (D) in einem ersten Bereich eines Speichers (6) des ersten Moduls (1) abgespeichert werden.
- 10
6. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass für die gesicherte Übertragung während des Authentisierungsvorgangs (IV) ein Schlüssel (11) zur gesicherten Datenübertragung erzeugt wird, unter dessen Einbeziehung aus den übertragenen Daten (D) von dem zweiten Modul (2) mindestens ein Kontrolldatum (CS) erzeugt wird, so dass das erste Modul (1) aus einer Auswertung des Kontrolldatums (CS) und der übertragenen Daten (D) die Authentizität der Daten (D) ermitteln kann.
- 15
- 20
7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, dass der Schlüssel (11) zur gesicherten Datenübertragung von dem ersten Modul (1) erzeugt wird.
- 25
8. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Authentisierungsvorgang (IV) als Prozess im Hintergrund abläuft.
- 30
9. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die gesicherte Übertragung und die Ermittlung der Authentizität der übertragenen Daten (D) als Prozesse im Hintergrund erfolgen.
- 35
10. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Authentisierungsvorgang (IV)

und derjenige der Ermittlung der Authentizität der übertragenen Daten (D) als ausführbare Programme veränderbar zumindest teilweise in einem Speicher (6) des ersten Moduls (1) abgelegt sind.

5

11. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass während des ungesicherten Übertragens von Daten (D) und der Verarbeitung dieser Daten (D) bestimmte Fehlermeldungen des Systems unterdrückt werden, die auf die ungesicherte Übertragung zurückzuführen sind.
12. Anordnung mit einem ersten Modul und einem zweiten Modul, insbesondere mit einem Fahrtschreiber (DTCO) und einem anschließbaren Datenträger (3), wobei zwischen dem ersten Modul (1) und dem zweiten Modul (2) Daten (D) übertragen werden, wobei die Anordnung derart ausgebildet ist,
- dass das zweite Modul (2) einen Datenspeicher (4) aufweist,
  - dass Daten (D) von dem zweiten Modul (2) an das erste Modul (1) entweder nach einem Authentisierungsvorgang (IV) gesichert oder ungesichert übertragbar sind,
  - dass nach dem Anschluss des zweiten Moduls (2) an das erste Modul (1) zunächst Daten (D) ungesichert übertragen werden, die mittels eines Prozessors (CPU) des ersten Moduls (1) für einen ersten Prozess (III) benutzt werden,
  - dass nach Beginn der ungesicherten Übertragung eine gesicherte Übertragung der Daten (D) von dem zweiten Modul (2) auf das erste Modul (1) erfolgt,
  - dass die ungesichert übertragenen Daten (D) mit den gesichert übertragenen Daten (D) verglichen werden und bei einem ermittelten Unterschied zwischen den gesichert und den ungesichert übertragenen Daten (D) Ergebnisse aus dem ersten Prozess (III) verworfen werden.

10

15

20

25

30

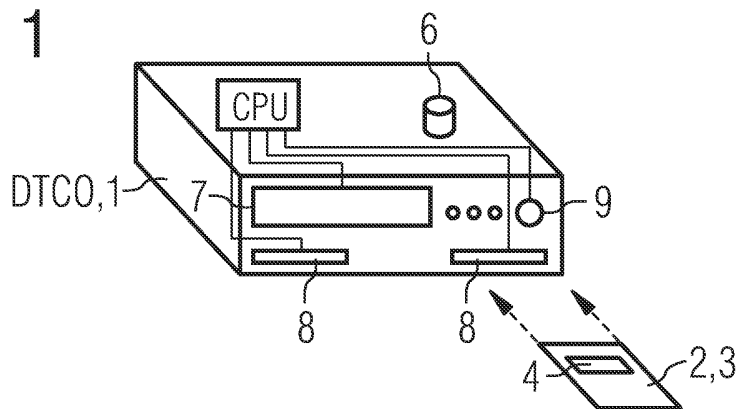
35

13. Anordnung nach Anspruch 12, d a d u r c h g e k e n n -  
z e i c h n e t , dass sie derart ausgebildet ist, dass  
mittels der ungesichert gelesenen Daten (D) eine Eingabe  
von zusätzlichen Daten (D) mittels eines dritten Moduls  
5 (Eingabevorrichtung 9) während des ersten Prozesses  
(III) unterstützt wird.
14. Anordnung nach Anspruch 13, d a d u r c h g e k e n n -  
z e i c h n e t , dass das dritte Modul als Eingabevor-  
10 richtung (9) ausgebildet ist, an der ein Benutzer (5)  
Eingaben machen kann.
15. Anordnung nach Anspruch 12, d a d u r c h g e k e n n -  
z e i c h n e t , dass das zweite Modul (2) einen Daten-  
15 speicher (4) aufweist, in dem die Daten (D) unverschlüs-  
selt abgelegt sind und die Anordnung derart ausgebildet  
ist, dass die Daten (D) von dem ersten Modul (1) ausles-  
bar sind.
- 20 16. Anordnung nach Anspruch 12, d a d u r c h g e k e n n -  
z e i c h n e t , dass das erste Modul (1) einen Spei-  
cher (6) mit einem ersten Bereich aufweist, und die An-  
ordnung derart ausgebildet ist, dass in dem ersten Be-  
reich die ungesichert übertragenen Daten (D) abgespei-  
25 chert werden.
17. Anordnung nach Anspruch 12, d a d u r c h g e k e n n -  
z e i c h n e t , dass sie derart ausgebildet ist, dass  
für die gesicherte Übertragung während des Authentisie-  
30 rungsvorgangs (IV) ein Schlüssel (11) zur gesicherten  
Datenübertragung von dem ersten Modul (1) erzeugt wird,  
unter dessen Einbeziehung aus den übertragenen Daten (D)  
von dem zweiten Modul (2) mindestens ein Kontrolldatum  
(CS) erzeugt wird, so dass das erste Modul (1) aus einer  
35 Auswertung des Kontrolldatum (CS) und der übertragenen  
Daten (D) die Authentizität der Daten (D) ermitteln  
kann.

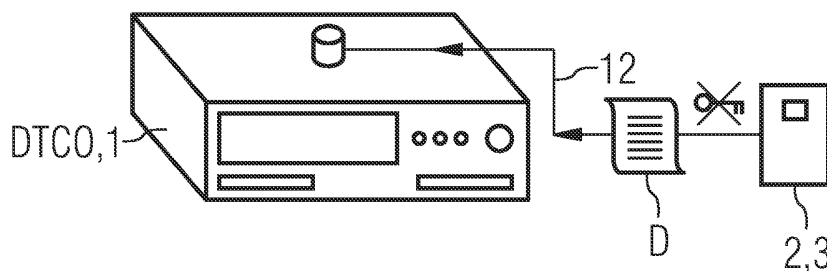
18. Anordnung nach Anspruch 12, d a d u r c h g e k e n n -  
z e i c h n e t , dass sie derart ausgebildet ist, dass  
die Authentisierung als Prozess im Hintergrund erfolgt.
- 5 19. Anordnung nach Anspruch 12, d a d u r c h g e k e n n -  
z e i c h n e t , dass sie derart ausgebildet ist, dass  
die gesicherte Übertragung und die Ermittlung der Au-  
thentizität der übertragenen Daten (D) als Prozesse im  
Hintergrund erfolgen.
- 10 20. Anordnung nach Anspruch 12, d a d u r c h g e k e n n -  
z e i c h n e t , dass sie derart ausgebildet ist, dass  
der Vorgang der Authentisierung und derjenige der Er-  
mittlung der Authentizität der übertragenen Daten als  
15 ausführbares Programm veränderbar zumindest teilweise in  
einem Speicher (6) des ersten Moduls (1) abgelegt sind.
- 20 21. Anordnung nach Anspruch 12, d a d u r c h g e k e n n -  
z e i c h n e t , dass sie derart ausgebildet ist, dass  
während des ungesicherten Übertragens von Daten (D) und  
der Verarbeitung dieser Daten (D) bestimmte Fehlermel-  
dungen des Systems unterdrückt werden, die auf die unge-  
sicherte Übertragung zurückzuführen sind.

FIG 1

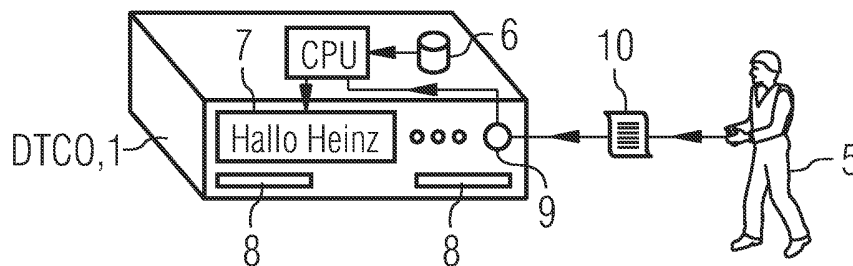
I



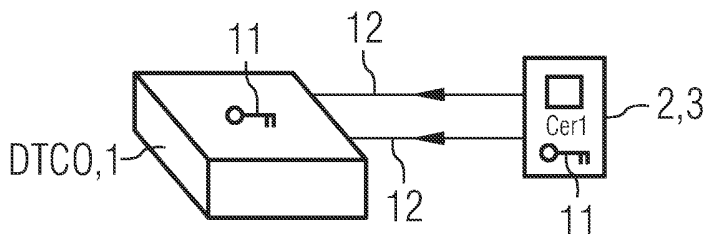
II



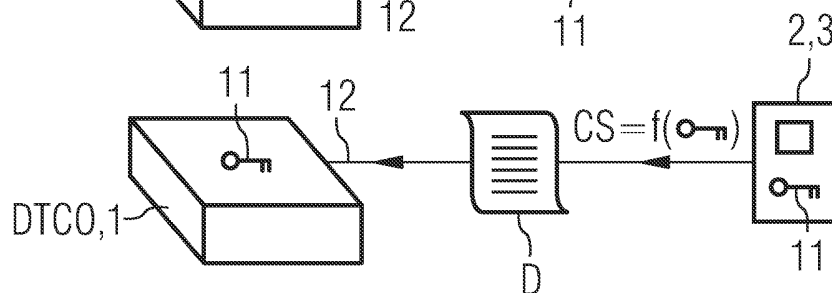
III



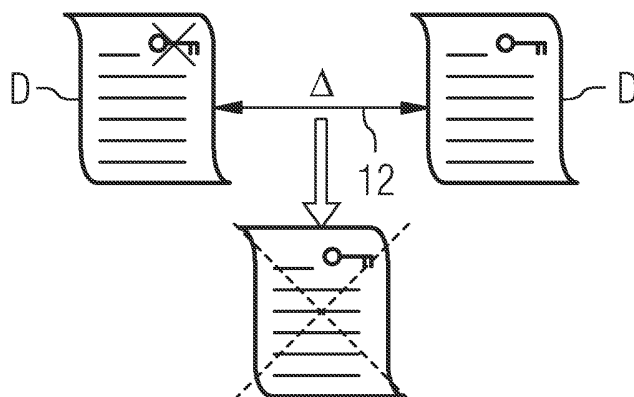
IV



V



VI



# INTERNATIONAL SEARCH REPORT

International application No  
PCT/EP2006/062100

<b>A. CLASSIFICATION OF SUBJECT MATTER</b> INV. G07C5/08      G06K7/00 ADD. G06F21/00      G07F7/10      H04L9/32		
According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b> Minimum documentation searched (classification system followed by classification symbols) G07C G06F G07F G06K		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used) EPO-Internal, WPI Data		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	FR 2 697 929 A (INNOVATRON SA) 13 May 1994 (1994-05-13)  page 6, line 30 - page 8, line 4 page 12, line 12 - page 15, line 24 -----	1-7, 10-17, 20,21
X	US 2004/093507 A1 (COURCAMBECK STEPHAN ET AL) 13 May 2004 (2004-05-13) paragraph [0033] - paragraph [0034] paragraph [0053] paragraph [0068] -----	1,4-12, 15-21
X	FR 2 861 202 A (GRISON PAUL) 22 April 2005 (2005-04-22) figure 2 page 5, line 3 - line 10 page 6, line 18 - page 7, line 5 ----- -/--	1,12
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.		
* Special categories of cited documents :		
*A* document defining the general state of the art which is not considered to be of particular relevance *E* earlier document but published on or after the international filing date *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) *O* document referring to an oral disclosure, use, exhibition or other means *P* document published prior to the international filing date but later than the priority date claimed	*T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art. *&* document member of the same patent family	
Date of the actual completion of the international search	Date of mailing of the international search report	
20 July 2006	31/07/2006	
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer  Buron, E	

INTERNATIONAL SEARCH REPORT

International application No  
PCT/EP2006/062100

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GB 2 404 065 A (* TEMPORAL S) 19 January 2005 (2005-01-19) page 1, line 1 - last line -----	1,12

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No PCT/EP2006/062100
---

Patent document cited in search report	A	Publication date	Patent family member(s)	Publication date
FR 2697929	A	13-05-1994	NONE	
US 2004093507	A1	13-05-2004	EP 1376367 A2	02-01-2004
FR 2861202	A	22-04-2005	AU 2004283353 A1 CA 2543138 A1 WO 2005041133 A1 HR 20060152 A2	06-05-2005 06-05-2005 06-05-2005 30-06-2006
GB 2404065	A	19-01-2005	NONE	

**INTERNATIONALER RECHERCHENBERICHT**

Internationales Aktenzeichen  
PCT/EP2006/062100

<b>A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES</b> INV. G07C5/08 G06K7/00 ADD. G06F21/00 G07F7/10 H04L9/32		
Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC		
<b>B. RECHERCHIERTE GEBIETE</b> Recherchiertes Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole) G07C G06F G07F G06K		
Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen		
Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe) EPO-Internal, WPI Data		
<b>C. ALS WESENTLICH ANGESEHENE UNTERLAGEN</b>		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	FR 2 697 929 A (INNOVATRON SA) 13. Mai 1994 (1994-05-13)  Seite 6, Zeile 30 - Seite 8, Zeile 4 Seite 12, Zeile 12 - Seite 15, Zeile 24 -----	1-7, 10-17, 20,21
X	US 2004/093507 A1 (COURCAMBECK STEPHAN ET AL) 13. Mai 2004 (2004-05-13) Absatz [0033] - Absatz [0034] Absatz [0053] Absatz [0068] -----	1,4-12, 15-21
X	FR 2 861 202 A (GRISON PAUL) 22. April 2005 (2005-04-22) Abbildung 2 *Seite 5, Zeile 3 - Zeile 10 Seite 6, Zeile 18 - Seite 7, Zeile 5 ----- -/--	1,12
<input checked="" type="checkbox"/> Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen <input checked="" type="checkbox"/> Siehe Anhang Patentfamilie		
* Besondere Kategorien von angegebenen Veröffentlichungen : *A* Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist *E* älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist *L* Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt) *O* Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht *P* Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist *T* Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist *X* Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden *Y* Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann nahelegend ist *&* Veröffentlichung, die Mitglied derselben Patentfamilie ist		
Datum des Abschlusses der Internationalen Recherche  20. Juli 2006		Absendedatum des internationalen Recherchenberichts  31/07/2006
Name und Postanschrift der Internationalen Recherchenbehörde Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016		Bevollmächtigter Bediensteter  Buron, E

## INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen  
PCT/EP2006/062100

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	GB 2 404 065 A (* TEMPORAL S) 19. Januar 2005 (2005-01-19) Seite 1, Zeile 1 - letzte Zeile -----	1,12

# INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2006/062100

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
FR 2697929	A	13-05-1994	KEINE	
US 2004093507	A1	13-05-2004	EP 1376367 A2	02-01-2004
FR 2861202	A	22-04-2005	AU 2004283353 A1	06-05-2005
			CA 2543138 A1	06-05-2005
			WO 2005041133 A1	06-05-2005
			HR 20060152 A2	30-06-2006
GB 2404065	A	19-01-2005	KEINE	