(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
2. Februar 2006 (02.02.2006)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2006/010462 A1

(51) Internationale Patentklassifikation[7]: G06F 1/00

(21) Internationales Aktenzeichen: PCT/EP2005/007507

(22) Internationales Anmeldedatum:
12. Juli 2005 (12.07.2005)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2004 036 374.9 27. Juli 2004 (27.07.2004) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SIEMENS AKTIENGESELLSCHAFT?** [DE/DE]; Wittelsbacherplatz 2, 80333 Munich (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **SCHNEIDER, Werner** [DE/DE]; Josef-Lang-Str. 15, 81245 München (DE).

(74) Anwalt: **BERG, Peter**; Siemens AG, Postfach 22 16 34, 80506 München (DE).

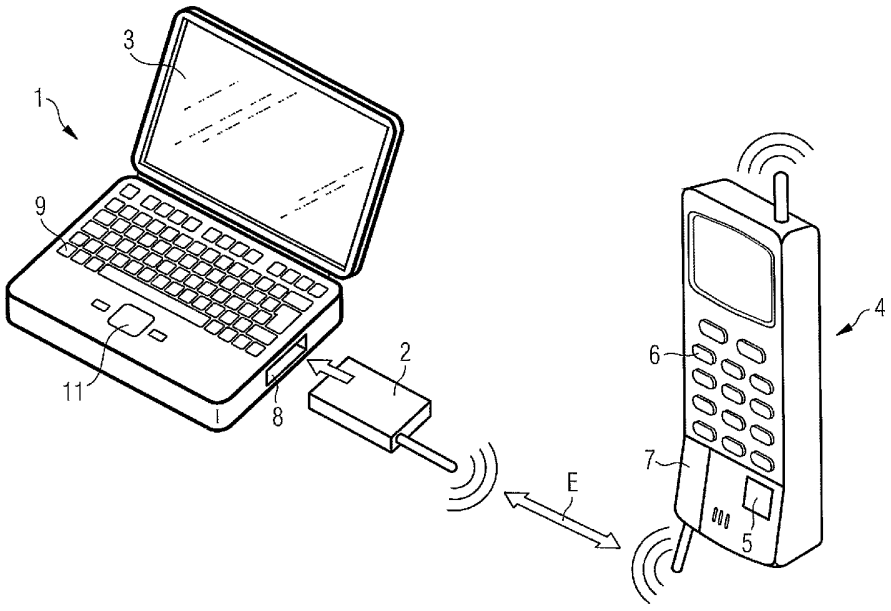
(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, 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).

[Fortsetzung auf der nächsten Seite]

(54) **Title:** METHOD FOR ACCESSING TO A COMPUTER FIRMWARE

(54) **Bezeichnung:** VERFAHREN ZUM ZUGANG ZUR FIRMWARE EINES COMPUTERS



(57) **Abstract:** The invention relates to a method for accessing to a computer firmware. The information carriers of an information carrying and processing device are used also for authenticating a user with respect to the computer. The computer access information is also stored in the memory of said information carrier. During authentication, said access information is wirelessly transmitted from the information carrying and processing device to the computer. A BIOS password is automatically transmitted from said information carrying and processing device to the computer through a wireless communication channel.

[Fortsetzung auf der nächsten Seite]

WO 2006/010462 A1

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.

(57) Zusammenfassung: Verfahren zum Zugang zur Firmware eines Computers Informationsträger eines mobilen, informationstragenden und -verarbeitenden Gerätes werden auch bei der Authentifizierung eines Nutzers gegenüber einem Computer verwendet. Hierzu wird im Speicher dieses Informationsträgers auch die Zugangsinformation zum Computer gespeichert. Während des Authentifizierungsvorgangs wird diese Zugangsinformation drahtlos vom mobilen, informationstragenden und -verarbeitenden Gerät zum Computer übermittelt. Das BIOSPaswort wird automatisch vom mobilen, informationstragenden und -verarbeitenden Gerät über einen drahtlosen Kommunikationskanal an den Computer übermittelt.

Verfahren zum Zugang zur Firmware eines Computers

Technisches Gebiet

Die Erfindung betrifft ein Verfahren zum Zugang zur Firmware in einem Computer, welcher eine Schnittstelleneinrichtung zur leitungsungebundenen Datenübertragung mit einem mobilen, informationstragenden und -verarbeitenden Gerät aufweist.

Stand der Technik

Die Firmware, hier genauer als „BIOS" (BASIC Input Output System) bezeichnet, ist ein Initialisierungsprogramm, das in einem nichtflüchtigen Speicher des Computers gespeichert ist und unmittelbar nach dem Einschalten verschiedene Funktionseinheiten des Computers in einen definierten Ausgangszustand bringt. Diese Firmware fordert den Nutzer beim Hochfahren des Systems auf, ein Passwort einzugeben. Stimmt dieses eingegebene BIOS-Passwort mit einem vorab im System (zum Beispiel in einem CMOS-RAM) gespeicherten Zugangspasswort überein, so wird der Vorgang der Initialisierung fortgeführt und das Betriebssystem in den Arbeitsspeicher des Computers geladen. Eine Fehleingabe hat zur Folge, dass das Hochfahren des Computers unterbrochen wird. Das Betriebssystem wird in diesem Fall nicht geladen und der Nutzer hat somit keinen Zugang zu den Ressourcen im Computer.

Die Eingabe eines Zugangscode ist aber nicht nur bei einem Computer sondern auch bei anderen mobilen, informationstragenden und -verarbeitenden Geräten, wie beispielsweise Mobiltelefone oder PDA's (Personal Digital Assistant) erforderlich. Viele dieser tragbaren Geräte, insbesondere Mobiltelefone, sind heutzutage weit verbreitet. Moderne Ausführungen dieser kleinformatigen Geräte besitzen häufig eine Schnitt-

stellenvorrichtung zur drahtlosen Datenübertragung mit anderen mobilen oder fest installierten Geräten.

Eine international standardisierte Schnittstelleneinrichtung im Kurzstreckendatenfunk (bis zu 100 m) ist Bluetooth, bei der die Daten per Funk im ISM-Band (Industrial Scientific Medical Band) übertragen werden.

Vor diesem Hintergrund wird von vielen Nutzern, die sich beispielsweise bereits gegenüber ihrem Mobiltelefon authentifiziert haben und im Begriff sind ihren Computer in Betrieb zu nehmen, es als umständlich empfunden, wenn sie von der Firmware des Computers erneut zur Eingabe eines Passwortes aufgefordert werden.

Darstellung der Erfindung

Der vorliegenden Erfindung liegt die Aufgabe zu Grunde, ein Verfahren und eine Einrichtung zu schaffen, so dass der Vorgang zur Authentifizierung eines Nutzers gegenüber einem Computer einfacher möglich ist.

Diese Aufgabe wird für ein Verfahren durch die Merkmale des Patentanspruchs 1 und für eine Einrichtung durch die Merkmale des Patentanspruchs 11 gelöst. Vorteilhafte Ausgestaltungen, Aspekte und Einzelheiten der Erfindung ergeben sich aus den abhängigen Ansprüchen, der Beschreibung und der beigefügten Zeichnung.

Die Erfindung geht davon aus, den Informationsträger eines mobilen, informationstragenden und -verarbeitenden Gerätes auch bei der Authentifizierung eines Nutzers gegenüber einem Computer zu verwenden. Hierzu wird im Speicher dieses Informationsträgers auch die Zugangsinformation zum Computer gespeichert. Während des Authentifizierungsvorgangs wird diese Zugangsinformation drahtlos vom mobilen, informationstragen-

den und -verarbeitenden Gerät zum Computer übermittelt. Ein Nutzer, der sich beispielsweise bereits gegenüber seinem Mobiltelefon authentifiziert hat, muss sich Dank der Erfindung nicht mehr das Passwort für den Computer merken. Das BIOS-Passwort wird automatisch von seinem Mobiltelefon über einen drahtlosen Kommunikationskanal an den Computer übermittelt.

Die Übertragung kann über Kurzstreckendatenfunk oder optoelektronisch erfolgen. Das erfindungsgemäße Verfahren ist durch folgende Verfahrensschritte gekennzeichnet:

a) Bereithalten von Daten, die einen Nutzer gegenüber dem mobilen, informationstragenden und -verarbeitenden Gerät und gegenüber dem Computer authentifizieren, auf einem Informationsträger des mobilen, informationstragenden und -verarbeitenden Gerätes;
b) Einbringen des mobilen, informationstragenden und -verarbeitenden Gerätes in den Erfassungsbereich der Schnittstelleneinrichtung;
c) Herstellen eines Kommunikationskanals zwischen dem mobilen, informationstragenden und -verarbeitenden Gerät und dem Computer;
d) Übermitteln der Daten zur Authentifizierung eines Nutzers vom mobilen, informationstragenden und -verarbeitenden Gerät an den Computer über den Kommunikationskanal;
e) Auswerten der vom Computer empfangenen Daten zur Authentifizierung eines Nutzers durch die Firmware des Computers, so dass anhand dieser Daten entschieden wird, ob ein Betriebssystem in den Computer geladen, oder das Hochfahren des Computers unterbrochen wird.

Mit Vorteil wird als mobiles, informationstragendes und -verarbeitendes Gerät ein Mobiltelefon verwendet, in dessen Subscriber Identity Modul (SIM) die Daten zur Authentifizierung des Nutzers gegenüber dem Computer bereit gehalten werden.

Als Schnittstelleneinrichtung wird bevorzugt eine Funkschnittstelle verwendet. Diese kann z.B. als im Computer fest eingebaute Bluetooth Schnittstelle realisiert sein, oder als Zusatzgerät in Form eines Adapters der an die USB-Schnittstelle des Computers angeschlossen ist. Bluetooth ist ein Quasi-Standard nicht nur für Mobiltelefone, sondern auch für PDAs und Organizer. Mit einer Bluetooth-Schnittstelle ist ein Kurzstrecken-Datenfunk, je nach Leistungsklasse, von etwa 10 cm, etwa 10 Meter, oder mit speziellen Varianten bis zu etwa 100 m möglich.

Da bei einer Bluetooth Schnittstelle ein Abhören und eine Manipulation des Datenstroms, wenn überhaupt, insbesondere bei den zwei unteren Leistungsklassen nur aus unmittelbarer Nähe möglich ist, kann diese Form der drahtlosen Übermittlung der Authentifizierungsdaten als beschränkt sicher eingestuft werden. Um die Sicherheit zu erhöhen ist in einer bevorzugten Ausführungsform der Erfindung eine verschlüsselte Datenübertragung vorgesehen. Günstig ist hierbei, dass bei einer Bluetooth-Funkübertragung die Authentifizierungsdaten z.B. mit einem bis zu 128 Bit langen Schlüssel chiffriert werden können. Zudem kann ein asymmetrisches Schlüsselverfahren eingesetzt werden. Dadurch ist eine Manipulation des Datenstroms weitgehend ausgeschlossen, zumal die Reichweite ohnedies auf eine vorgegebene Grenze festgelegt ist.

Um die Sicherheit bei der Übertragung des Passwortes noch weiter zu erhöhen ist vorgesehen, dass in Abhängigkeit einer, dem Computer zugeordneten Sicherheitsklasse der Nutzer vor der Übermittlung des Passwortes zur Eingabe eines PIN gefordert wird. Die Sicherheitsklasse ergibt sich aus der Bluetooth Kommunikation. Bevorzugt wird hierbei ein PIN verwendet, der den Nutzer aus der Verwendung des mobilen, informationsverarbeitenden Gerätes bereits vertraut ist. Dadurch braucht sich der Nutzer nicht eine Vielzahl von unterschiedlichen Zugangsberechtigungen merken.

Eine spezielle Ausführungsvariante des erfindungsgemäßen Verfahrens zeichnet sich dadurch aus, dass der Computer durch den Empfang eines Passwortes an der Bluetooth-Schnittstelle aus einem Sleep-Modus, in welchem die Energieaufnahme des Computers auf einen minimalen Wert eingestellt ist, in einen normalen Betriebszustand hochgefahren wird. Dadurch entfällt das Einschalten des Gerätes.

In einer weiteren Ausgestaltung der Erfindung enthält der Informationsträger des mobilen, informationstragenden und -verarbeitenden Gerätes neben den enthaltenen Daten zur Authentifizierung des Nutzers gegenüber dem Computer nicht nur das für die Firmware erforderliche BIOS-Passwort, sondern auch die in weiterer Folge beim Hochfahren des Betriebssystems erforderliche Eingabe der Benutzerkennung (User Account) sowie das persönliche Passwort für das Betriebssystem. Dadurch ist ein komfortabler Zugang auch zum Betriebssystem und somit auch zu weiteren Sicherheitseinrichtungen, wie beispielsweise Bildschirmschonern gewährleistet.

In einer Variante der Erfindung ist der Computer mit einem Chipkartenlesegerät verbunden und die Firmware so eingerichtet, dass das Passwort alternativ über die Bloetooth-Schnittstelle oder über das Einlegen einer Chipkarte in das Lesegerät eingegeben werden kann.

Kurzbeschreibung der Zeichnung

Zur weiteren Erläuterung der Erfindung wird auf die Zeichnungen Bezug genommen, in denen an Hand eines Ausführungsbeispiels weitere vorteilhafte Ausgestaltungen und Einzelheiten der Erfindung zu entnehmen sind. Es zeigen:

Figur 1 eine schematische Darstellung eines Ausführungsbeispiels der Erfindung, bei dem Daten, die einen Nut-

zer gegenüber einem Computer identifizieren, und die in einer modifizierten SIM-Karte eines Mobiltelefons gespeichert sind, über eine leitungsungebundene Übertragungsstrecke an einen Computer übermittelt werden;

Figur 2 ein Blockschaltbild der erfindungsgemäß modifizierten SIM-Karte des Mobiltelefons, mit einem ersten Speicherbereich, in welchem Daten zur Authentifizierung des Nutzers gegenüber dem Mobiltelefon gespeichert sind und mit einem zweiten Speicherbereich, in welchem Daten zur Authentifizierung des Nutzers gegenüber dem Computer gespeichert sind.

Ausführung der Erfindung

In Figur 1 ist ein Computer 1 mit üblichen Bedieneinrichtungen wie Tastatur 9, Bildschirm 10 und einer Zeigevorrichtung, ausgeführt als Trackball 11, zu sehen.
Der Computer 1 verfügt über eine Universial Serial Bus (USB) -Schnittstelle 8. Die USB-Schnittstelle 8 dient zum Anschluss eines Adapters 2, im Ausführungsbeispiel eine Bluetooth-Funkschnittstelle. Die Bluetooth-Funkschnittstelle weist einen Erfassungsbereich E auf, in welchem sich ein Mobiltelefon 4, das ebenfalls mit einer entsprechenden Bluetooth-Funkschnittstelle 7 ausgerüstet ist, befindet. Die Bluetooth-Adresse des Computers 1 ist am Handy 4 als bekanntes Bluetooth- Gerät konfiguriert. Der Erfassungsbereich einer Bluetooth Schnittstelle beträgt üblicherweise etwa 10 m. Je nach Leistungsklasse kann auch eine Reichweite von etwa 10 cm bzw. etwa 100 m erreicht werden.

Das Mobiltelefon 4 besitzt ein Identifikations Modul, die SIM-Karte 5 (SIM-Subscriber Identity Modul). Auf der SIM-Karte sind - wie bislang auch - die nutzerspezifischen Daten, wie die Kundennummer des Nutzers gespeichert, wodurch sich

der Nutzer des Mobiltelefons 4 gegenüber dem Netz identifiziert. Ebenso ist auf der SIM-Karte der kryptographische Algorithmus für die Authentisierung und Nutzdatenverschlüsselung implementiert.

Gemäß der Erfindung ist die SIM-Karte nun so ausgebildet, dass sie auch als Informationsträger für den Zugangscode zu einem Computer verwendet wird. Das heißt, im Speicher 10 (Figur 2) der SIM-Karte 5 sind neben den oben genannten Zugangsinformationen und Funktionalitäten für das Mobilfunknetz auch Authentifizierungsdaten, wie das Boot- Passwort für den Zugang zur Firmware zu einem Computer abgelegt. Diese modifizierte SIM-Karte wird in Verbindung mit am Handy 4 vorhandenen der Funktionalität der leitungsungebundenen, kryptographischen Datenübertragung beim Hochfahren des Computers verwendet.

Im Einzelnen erfolgt der Zugang zur Firmware des Computers nun so, dass nach dem Einschalten des Computers 1 zunächst das Boot-Programm in üblicher Weise startet, an einer definierten Stelle stoppt und auf die korrekte Eingabe des Boot-Passwortes wartet. Im Unterschied zum Stand der Technik ist aber die Firmware des Computers 1 so eingerichtet, dass diese Eingabe nicht von der Tastatur 9 erwartet wird, sondern es wird zusätzlich die Schnittstelleneinrichtung (Adapter 2 in USB-Port 8) abgefragt. Damit ist die umständliche Eingabe des Passwortes über die Tastatur 9 des Computers 1 durch ein drahtloses Übertragungsverfahren ersetzt.

Stimmt das BIOS-Passwort an der Schnittstelleneinrichtung mit dem vom BIOS erwarteten Zugangscode überein, dann lädt die Firmware das auf dem Computer installierte Betriebssystem in den Arbeitsspeicher und startet es.

Unterscheidet sich das an der Schnittstelleneinrichtung bereitgestellte BIOS-Passwort vom Zugangscode der Boot-Software, so stockt der Hochlauf an dieser Stelle und der Zugang zu Ressourcen auf den Computer ist gesperrt.

Die Bluetooth-Schnittstelle kann vorteilhaft so eingerichtet sein, dass nach dem Herstellen des Übertragungskanals die an der Kommunikation beteiligten Geräte identifiziert und einer Sicherheitsklasse zugeordnet werden. In Abhängigkeit dieser Sicherheitsklasse, entscheidet die Funkschnittstelle, ob das BIOS-Passwort automatisch übermittelt wird, oder von der Eingabe eines PIN an der Tastatur 6 am Mobiltelefon 4 abhängig gemacht wird.

Bei Systemen mit geringeren sicherheitstechnischen Anforderungen wird das BIOS-Passwort automatisch vom Mobiltelefon 4 an den Computer 1 übermittelt und von der Schnittstelle 8 eingelesen, so dass die bislang erforderliche manuelle Eingabe des BIOS-Passwortes vollständig wegfällt. Der Zugang zur Firmware des Computers setzt also die bloße Anwesenheit des Nutzermobiltelefons voraus. Für einen Computer, der zu Hause benutzt wird, ist dieser Zugang besonders komfortabel.

Wenn eine höhere Sicherheit gefordert wird, wird der Benutzer zur Eingabe eines PIN aufgefordert, den er entweder an der Tastatur 6 des Mobiltelefons 4 oder an der Tastatur 9 des Computers eingibt. Der PIN ist vorteilhaft der PIN für den Zugang zum Mobiltelefon 4. Dies bedeutet, dass auch im vorliegenden Fall erhöhter Sicherheitsanforderungen der Nutzer nicht das BIOS-Passwort auswendig wissen muss, sondern nur den Zugangscode zu seinem Mobiltelefon, der ihm aus der Nutzung des Mobiltelefons vertraut ist.

Das Boot-Programm ist üblicherweise auf einem Flash-ROM auf dem Motherboard des Computers untergebracht. Das Boot-Programm ist nicht Teil des Betriebssystems, kann mit Betriebssystemen unterschiedlicher Hersteller zusammenarbeiten und unterschiedlich konfiguriert werden. So kann beispielsweise in den sogenannten Powermanagement-Einstellungen die Art und Weise justiert werden, wie sich der PC bei längerer Wartezeit verhält. Der Computer kann bis zum völligen Still-

stand deaktiviert werden. Festplatten können heruntergefahren und der Monitor ausgestalten werden. So lässt sich in einer BIOS-Konfiguration ein eingeschalteter Computer vor der Eingabe eines BIOS-Passwortes in einen so-genannten Sleep-Modus bringen, in welchem er nur geringe Leistung aufnimmt. In diesem Betriebszustand verharrt der Computer bis er durch ein entsprechendes Signal aufgeweckt wird. Dieses Aufwecken kann so erfolgen, dass das Mobiltelefon 4 in den Erfassungsbereich der Schnittstelleneinrichtung gebracht und das BIOS-Passwort übertragen wird. Der Adapter 2 der Bluetooth-Schnittstelle am USB-Port 8 ist gemäß der Erfindung so eingerichtet, dass er ein Interrupt-Signal erzeugt. Die Firmware (BIOS) erfasst dieses Interrupt-Signal und setzt den Hochlaufvorgang fort. In der Folge wird der Computer aus dem Ruhezustand aufgeweckt und das System erwartet in üblicher Weise an einer bestimmten Stelle des Boot-Programms ein BIOS-Passwort. Dieses wird in der oben beschriebenen Weise über Bluetooth übermittelt und von der Firmware ausgewertet. Da das BIOS-Programm nicht Teil des Betriebssystems ist, erfordert die Implementierung der Erfindung keine Anpassung des Betriebssystems.

In Figur 2 ist die erfindungsgemäß modifizierte SIM-Karte 5 als Blockschaltbild näher gezeigt. Die SIM-Karte 5 weist einen Systembus 14 auf, der einen Prozessor 12, eine Ein-Ausgabeeinheit 11, einen Controller 13 und den Speicher 10 verbindet. Der Speicher 10 beinhaltet verschiedene flüchtige (RAM) und nichtflüchtige Speicher (ROM, EPROM, EPROM) und ist im zweiten Speicherbereich 8 und 9 gegliedert. Im ersten Speicherbereich 8 werden - wie bisher auch - jene Daten gespeichert und verwaltet, durch die sich der Nutzer gegenüber dem Mobiltelefon 4 und dem Netzbetreiber des Mobilfunknetzes als berechtigt ausweist. In einem zweiten Speicherbereich 9 sind jene Authentifizierungsdaten abgelegt, die den Nutzer gegenüber dem Computer als berechtigten Nutzer ausweisen.

Selbstverständlich kann die leitungsungebundene Schnittstelleneinrichtung auch als Infrarot-Schnittstelle ausgebildet sein.

Der Begriff Computer steht synonym für einen PC, einen Laptop oder eine andere stationäre datenverarbeitende Einrichtung. Das erfindungsgemäße Zugangskontrollsystem kann auch für andere Zugangssysteme, wie beispielsweise Parkplatzschranken oder Türöffner eingesetzt werden. In diesem Fall kann das mobile Gerät ein entsprechend ausgestattetes Fahrzeug sein.

Wie bereits eingangs dargestellt, erfasst der Begriff "mobiles, informationstragendes und -verarbeitendes Gerät" Geräte unterschiedlicher Ausführung, wie beispielsweise PDAs und Organizer, aber auch Fahrzeuge verschiedenster Art. Entscheidend im Sinne der Erfindung ist lediglich, dass der Informationsträger eines derartigen Gerätes sowohl zum Speichern und Verwalten von Daten verwendet wird, durch die sich ein Nutzer gegenüber diesem Gerät als berechtigt ausweist, als auch zum Speichern und Verwalten einer Zugangsinformation, durch die sich der Nutzer gegenüber der Firmware bzw. dem Betriebssystem eines Computers authentifiziert.

Patentansprüche

1. Verfahren zum Zugang zur Firmware eines Computers, der sich in einem Sleep-Modus mit reduzierter Energieaufnahme befindet, der eine Schnittstellenvorrichtung aufweist, um mit einem in einem Erfassungsbereich befindlichen mobilen, insbesondere informationstragenden und -verarbeitenden Gerät einen Kommunikationskanal zur leitungsungebundenen Datenübertragung aufzubauen, gekennzeichnet durch folgende Schritte:
   a) Bereithalten von Daten, um einen Nutzer gegenüber dem mobilen, informationstragenden und -verabeitenden Gerät und gegenüber dem Computer zu authentifizieren, auf einem Informationsträger des mobilen, informationstragenden und -verarbeitenden Gerätes;
   b) Einbringen des mobilen, informationstragenden und -verarbeitenden Gerätes in den Erfassungsbereich der Schnittstelleneinrichtung;
   c) Herstellen eines Kommunikationskanals zwischen dem mobilen, informationstragenden und -verarbeitenden Gerät und dem Computer, wobei die Schnittstelleneinrichtung ein Signal erzeugt, welches den Computer aus dem Sleep-Modus in einen Betriebsmodus hochfährt;
   d) Übermitteln der Daten zur Authentifizierung des Nutzers gegenüber dem Computer vom mobilen, informationstragenden und -verarbeitenden Gerät an den Computer über den Kommunikationskanal;
   e) Auswerten der vom Computer empfangenen Daten durch die Firmware des Computers, so dass anhand dieser Daten entschieden wird, ob ein Betriebssystem in den Computer geladen, oder das Hochfahren des Computers unterbrochen wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das Signal ein Interrupt-Signal ist.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass als mobiles, informationstragendes und -verarbeitendes Gerät ein Mobiltelefon verwendet wird, und die Daten zur Authentifizierung des Nutzers gegenüber dem Computer im Subscriber-Identity-Module des Mobiltelefons bereit gehalten werden.

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass als mobiles Gerät ein Fahrzeug zu Land, zu Wasser, und in der Luft dient, das ein informationstragendes und -verarbeitendes Gerät beinhaltet, und die Daten zur Authentifizierung des Nutzers gegenüber dem Computer in dem Subscriber-Identity-Module des informationstragenden und -verarbeitenden Geräts bereit gehalten werden.

5. Verfahren nach Anspruch 1, 2, 3 oder 4, dadurch gekennzeichnet, dass als Schnittstelleneinrichtung eine Funkschnittstelle verwendet wird.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, dass als Funkschnittstelle eine im Computer fest eingebaute Bluetooth-Schnittstelle verwendet wird.

7. Verfahren nach Anspruch 5, dadurch gekennzeichnet, dass als Funkschnittstelle ein an einem USB-Port oder einem anderen, ähnlichen Zwecken dienenden Port des Computers steckbar aufgenommener Adapter einer Bluetooth-Schnittstelle verwendet wird.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass die Übermittlung der Daten zur Authentifizierung des Nutzers gegenüber dem Computer verschlüsselt erfolgt.

9. Verfahren nach Anspruch 6 bis 8, dadurch gekennzeichnet, dass vor der Übermittlung der Daten zur Authentifizierung des Nutzers gegenüber dem Computer in Abhängigkeit einer, dem Computer zugeordneten Sicherheitsklasse, der Nutzer zur Eingabe eines PIN aufgefordert wird.

10. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass die Daten für die Authentifizierung des Nutzers gegenüber dem Computer das BIOS-Passwort für die Firmware, die Benutzerkennung und das persönliche Passwort für das Betriebssystem des Computers umfassen.

11. Zugangskontrolleinrichtung für einen Computer, der sich in einem Sleep-Modus mit reduzierter Energieaufnahme befindet, der eine Schnittstelleneinrichtung zur leitungsungebundenen Datenübertragung mit einem in einem Erfassungsbereich befindlichen mobilen, informationstragenden und
-verarbeitenden Gerät aufweist, dadurch gekennzeichnet, dass die Schnittstelleneinrichtung vom mobilen, informationstragenden und -verarbeitenden Gerät Authentifizierungsdaten empfängt, dass die Schnittstelleneinrichtung nach Empfang der Authentifizierungsdaten ein Signal erzeugt, welches den Computer aus dem Sleep-Modus in einen Betriebsmodus hochfährt und die Authentifizierungsdaten der Firmware des Computers beim Hochfahren bereitstellt.

12. Zugangskontrolleinrichtung nach Anspruch 11, dadurch gekennzeichnet, dass das Signal ein Interrupt-Signal ist.

13. Verfahren nach Anspruch 11 oder 12, dadurch gekennzeichnet, dass das mobile, informationstragende und -verarbeitende Gerät ein Mobiltelefon ist, das ein

Subscriber Identity Modul aufweist, in welchem Daten zur Authentifizierung des Nutzers gegenüber dem Mobilfunknetz sowie Daten zur Authentifizierung des Nutzers gegenüber dem Computer gespeichert sind.

14. Zugangskontrolleinrichtung nach Anspruch 11, dadurch gekennzeichnet, dass als mobiles Gerät ein Fahrzeug zu Land, zu Wasser, und in der Luft dient, das ein informationstragendes und -verarbeitendes Gerät beinhaltet, und ein Subscriber-Identity-Module aufweist, in welchem Daten zur Authentifizierung des Nutzers gegenüber dem mobilen Gerät enthält sowie Daten zur Authentifizierung des Nutzers gegenüber dem Computer gespeichert sind.

15. Zugangskontrolleinrichtung nach Anspruch 11, 12, 13 oder 14, dadurch gekennzeichnet, dass die Schnittstelleneinrichtung eine im Computer fest eingebaute Bluetooth-Schnittstelle ist.

16. Zugangskontrolleinrichtung nach Anspruch 11, 12, 13 oder 14, dadurch gekennzeichnet, dass die Schnittstelleneinrichtung durch einen an einem USB-Port oder einem anderen, ähnlichen Zwecken dienenden Port des Computers steckbar aufgenommen Adapter einer Bluetooth- Schnittstelle gebildet ist.

17. Zugangskontrolleinrichtung nach einem der Ansprüche 11, 15 oder 16, dadurch gekennzeichnet, dass der Computer mit einer Chipkarten-Leseeinrichtung verbunden ist und die Firmware des Computers so eingerichtet ist, dass die Daten zur Authentifizierung des Nutzers gegenüber dem Computer alternativ von der Bluetooth-Schnittstelle oder vom Chipkarten-Lesegerät ausgewertet werden.

18. Zugangskontrolleinrichtung nach Anspruch 11, 12, 13 oder 14, dadurch gekennzeichnet, dass die Schnittstel-

leneinrichtung als Infrarot-Schnittstellen-Einrichtung ausgebildet ist.

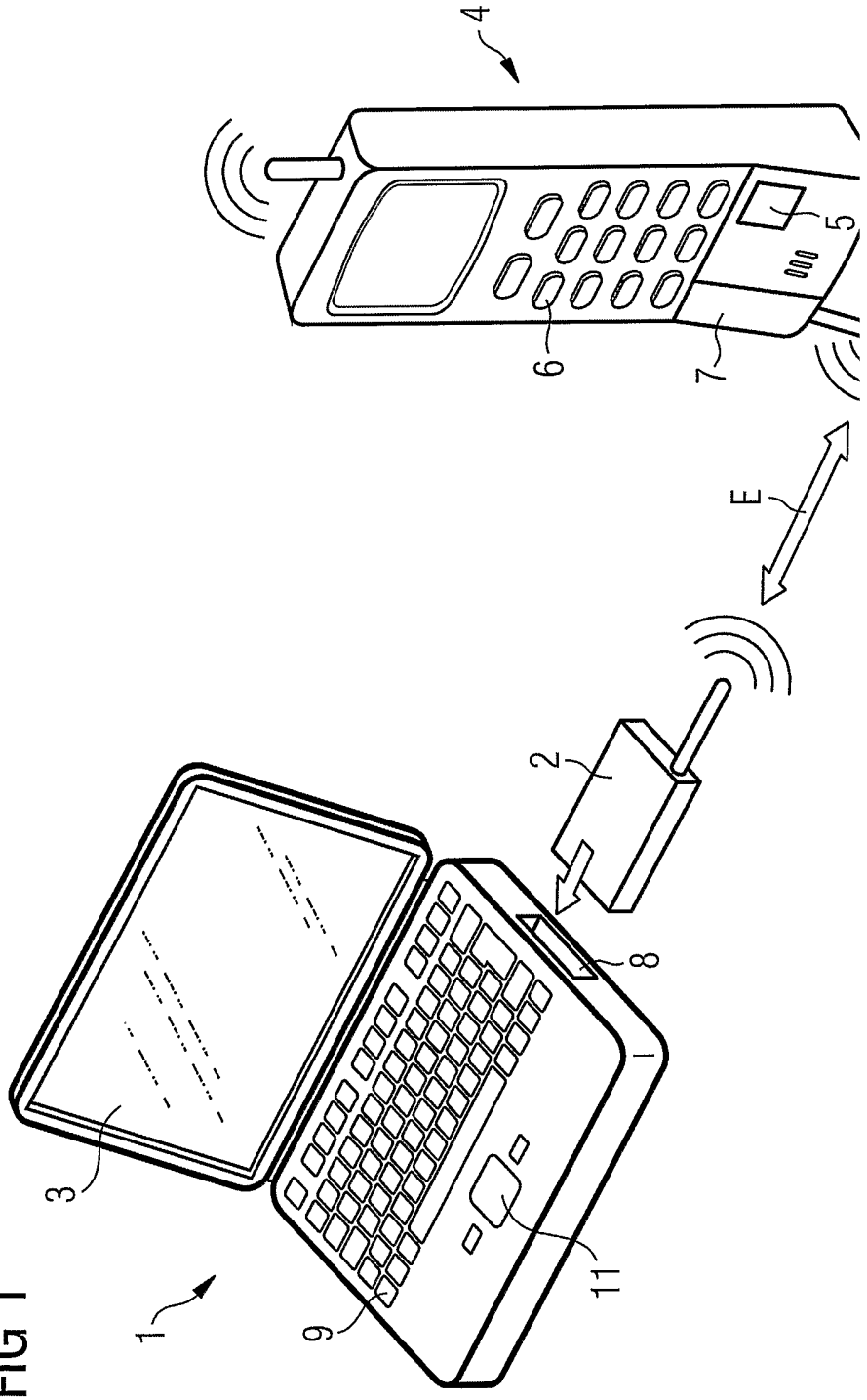
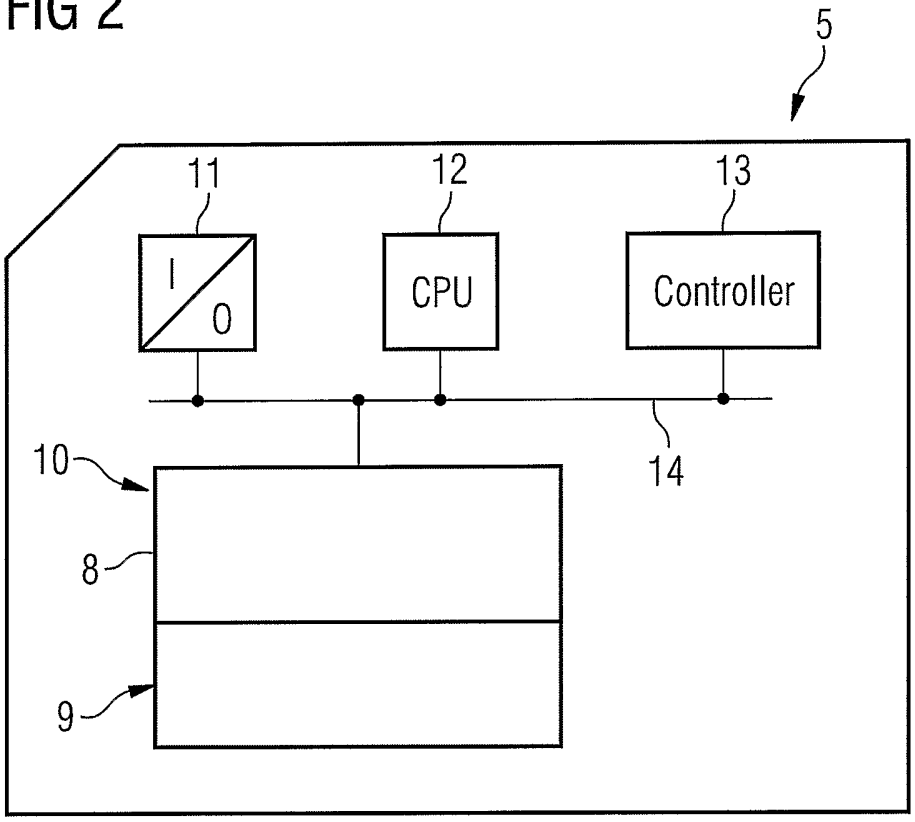


FIG 1

FIG 2



INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2005/007507

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 189 105 B1 (LOPES ROBERT JOSEPH) 13 February 2001 (2001-02-13) column 4, lines 19-64	1-18
X	US 6 137 480 A (SHINTANI ET AL) 24 October 2000 (2000-10-24) column 3, lines 11-22 column 3, line 59 - column 4, line 3	1-18
A	WO 00/16179 A (MARANDI, MART) 23 March 2000 (2000-03-23) page 3, line 26 - page 4, line 29	
A	US 5 892 906 A (CHOU ET AL) 6 April 1999 (1999-04-06) abstract	

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in 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
31 October 2005	11/11/2005

Name and mailing address of the ISA	Authorized officer
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	Mezödi, S

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2005/007507

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2002/148895 A1 (CECIL KENNETH B ET AL) 17 October 2002 (2002-10-17) abstract	
A	US 2002/097876 A1 (HARRISON KEITH ALEXANDER) 25 July 2002 (2002-07-25) abstract	
A	BLUETOOTHSHAREWARE: "LockItNow"'Online! 6 December 2003 (2003-12-06), XP002344675 Retrieved from the Internet: URL:http://web.archive.org/web/20031206035838/http://www.bluetoothshareware.com/lockitnow.asp> 'retrieved on 2005-09-13! the whole document	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2005/007507

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6189105 B1	13-02-2001	NONE	
US 6137480 A	24-10-2000	ID 19303 A	02-07-1998
WO 0016179 A	23-03-2000	AU 5728199 A	03-04-2000
		EE 9800237 A	17-04-2000
US 5892906 A	06-04-1999	NONE	
US 2002148895 A1	17-10-2002	US 6340116 B1	22-01-2002
US 2002097876 A1	25-07-2002	GB 2370383 A	26-06-2002
		GB 2372178 A	14-08-2002

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2005/007507

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F1/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F

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

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 6 189 105 B1 (LOPES ROBERT JOSEPH) 13. Februar 2001 (2001-02-13) Spalte 4, Zeilen 19-64	1-18
X	US 6 137 480 A (SHINTANI ET AL) 24. Oktober 2000 (2000-10-24) Spalte 3, Zeilen 11-22 Spalte 3, Zeile 59 - Spalte 4, Zeile 3	1-18
A	WO 00/16179 A (MARANDI, MART) 23. März 2000 (2000-03-23) Seite 3, Zeile 26 - Seite 4, Zeile 29	
A	US 5 892 906 A (CHOU ET AL) 6. April 1999 (1999-04-06) Zusammenfassung	

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] 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 naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
31. Oktober 2005	11/11/2005

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
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	Mezödi, S

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 2002/148895 A1 (CECIL KENNETH B ET AL) 17. Oktober 2002 (2002-10-17) Zusammenfassung	
A	US 2002/097876 A1 (HARRISON KEITH ALEXANDER) 25. Juli 2002 (2002-07-25) Zusammenfassung	
A	BLUETOOTHSHAREWARE: "LockItNow"'Online! 6. Dezember 2003 (2003-12-06), XP002344675 Gefunden im Internet: URL:http://web.archive.org/web/20031206035838/http://www.bluetoothshareware.com/lockitnow.asp> 'gefunden am 2005-09-13! das ganze Dokument	

INTERNATIONALE RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2005/007507

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
US 6189105	B1	13-02-2001	KEINE		
US 6137480	A	24-10-2000	ID	19303 A	02-07-1998
WO 0016179	A	23-03-2000	AU	5728199 A	03-04-2000
			EE	9800237 A	17-04-2000
US 5892906	A	06-04-1999	KEINE		
US 2002148895	A1	17-10-2002	US	6340116 B1	22-01-2002
US 2002097876	A1	25-07-2002	GB	2370383 A	26-06-2002
			GB	2372178 A	14-08-2002