(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 100 40 855 B4** 2005.01.20

(12) # Patentschrift

(21) Aktenzeichen: **100 40 855.9**
(22) Anmeldetag: **21.08.2000**
(43) Offenlegungstag: **14.03.2002**
(45) Veröffentlichungstag
der Patenterteilung: **20.01.2005**

(51) Int Cl.[7]: **G06F 12/14**
G06F 15/173, H04L 9/32

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden.

(71) Patentinhaber:
Infineon Technologies AG, 81669 München, DE

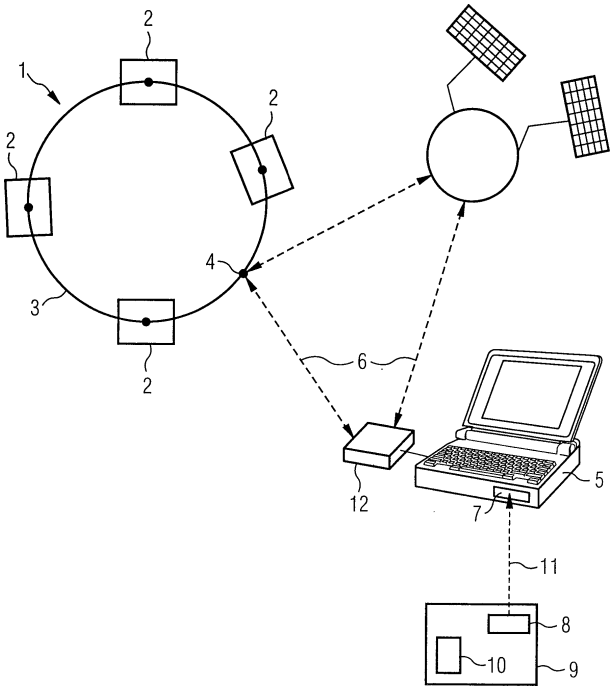
(74) Vertreter:
Epping Hermann Fischer,
Patentanwaltsgesellschaft mbH, 80339 München

(72) Erfinder:
Jung, Peter, 67697 Otterberg, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
DE 195 33 209 A1
US 59 91 807
EP 08 87 774 A2
EP 04 21 409 A2

(54) Bezeichnung: **Netzwerkanordnung**

(57) Hauptanspruch: Netzwerkanordnung mit
– einem lokalen Computernetzwerk (1),
– einem entfernt angeordneten Einzelrechner (5), der Mittel (12) zum Aufbau einer Verbindung (6) zum lokalen Computernetzwerk aufweist, und
– einem von dem lokalen Computernetzwerk unabhängig arbeitenden Identifizierungs-Computer (9), der über eine Kommunikationsschnittstelle (7, 8) mit dem Einzelrechner (5) Daten austauschen kann,
wobei in dem Identifizierungs-Computer (9) Zugangsdaten zu dem lokalen Netzwerk (1) gespeichert oder erzeugbar sind und wobei auf Übermittlung eines Steuerbefehls und der Zugangsdaten von dem Identifizierungs-Computer (9) an den Einzelrechner (5) ein Verbindungsaufbau zwischen dem Einzelrechner (5) und dem lokalen Computernetzwerk (1) und eine Fernregistrierung im lokalen Computernetzwerk (1) mit den Zugangsdaten durchführbar ist.



Beschreibung

[0001] Die Erfindung betrifft eine Netzwerkanordnung zur Verbindung eines Einzelrechners mit einem lokalen Computernetzwerk.

[0002] In vielen Anwendungsfällen sind Einzelrechner einer Benutzergruppe in einem lokalen Computernetzwerk zusammengeschlossen. Dies ermöglicht die Kommunikation der Rechner untereinander sowie den Zugriff auf gemeinsame Ressourcen wie Datenbestände und Drucker. Trotzdem soll in der Regel die Möglichkeit bestehen, sich von außen in das lokale Netzwerk einzuklinken, um so auch von einem entfernt plazierten Einzelrechner die Möglichkeit zu haben, auf die Ressourcen des Netzwerkes zuzugreifen. Gerade durch die zunehmende Verbreitung von tragbaren Computern, den sogenannten Notebooks oder Laptops, kann so beispielsweise auf einer Dienstreise fast unter Bürobedingungen gearbeitet werden. Auch die beginnende Einführung von Arbeitszeitmodellen mit teilweiser Heimarbeit erfordert es, von zu Hause aus auf das lokale Computernetzwerk der Firma zugreifen zu können.

[0003] Allerdings muß sichergestellt werden, daß sich nur berechtigte Benutzer in das lokale Computernetzwerk einwählen. Außerdem ist eine Vielzahl von Zugangsdaten notwendig, um auf technischer Ebene die Kommunikation zwischen dem Einzelrechner und dem Computernetzwerk herzustellen. Die sogenannte Fernregistrierung wird bisher von Hand durchgeführt. Dieses Vorgehen ist aber zum einen langwierig und zum anderen fehlerträchtig. Des weiteren ist es anfällig für unautorisierte Verwendung durch Dritte, da oft das Paßwort auf der Festplatte gespeichert oder schriftlich notiert wird. Auch der Einsatz spezieller Software zum Ausprobieren oder Erraten des Paßwortes führt oft zum unberechtigten Zugriff Dritter auf das Computernetzwerk unter Ausnutzung der Möglichkeit der Fernregistrierung.

Stand der Technik

[0004] Aus der DE 195 33 209 ist eine Vorrichtung zur Zuordnung von Benutzern in einem Computernetzwerk beschrieben, wobei Computer in dem Computernetzwerk über eine Identifikationsnummer indentifzierbar ist. Zur einfacheren Vergabe von Benutzerrechten ist die Identifikationsnummer auf einem separaten Datenträger gespeichert, der einem Benutzer, zugeordnet ist und der in Verbindung mit unterschiedlichen Computern verwendet werden kann.

[0005] Die US 5 991 807 offenbart eine lokales Computernetzwerk mit einem LAN-Server, der Verbindungs- und Zugangsdaten verschiedener Benutzer in dem Netzwerk zu einem globalen Netzwerk bereitstellt. Dadurch wird die Nutzung einer Zugangsvorrichtung zu dem globalen Netzwerk optimiert.

[0006] Die EP 0 887 774 beschreibt eine Identifizierung an einem lokalen Netzwerk mit Hilfe einer IC-Karte. Auf der Karte sind Zugangsdaten gespeichert, die von einem lokalen Rechner abgerufen werden, der dann mit Hilfe der Zugangsdaten auf ein Netzwerk zugreift.

[0007] Letztlich offenbart die EP 0766472 ein Verfahren zum anonymen Zugriff auf einen Informationsdienst. Ein Benutzer fordert dabei von einem Authentifizierungsserver einen zufälliges Passwort an, mit der er sich in einem zweiten Schritt an den Informationsserver anmeldet. Das Passwort, das zwischen Informationsserver und Authentifizierungsserver ausgetauscht wurde, erlaubt keine Rückschlüsse auf den Benutzer.

Aufgabenstellung

[0008] Aufgabe der Erfindung ist es, eine Netzwerkanordnung vorzuschlagen, bei der die Fernregistrierung vereinfacht und die Sicherheit gegen unautorisierte Verwendung durch Dritte erhöht wird.

[0009] Dieses Ziel wird durch eine Netzwerkanordnung erreicht mit

- einem lokalen Computernetzwerk,
- einem entfernt angeordneten Einzelrechner, der Mittel zum Aufbau einer Verbindung zum lokalen Computernetzwerk aufweist, und
- einem von dem lokalen Computernetzwerk unabhängig arbeitenden Identifizierungs-Computer, der über eine Kommunikationsschnittstelle mit dem Einzelrechner Daten austauschen kann,

wobei in dem Identifizierungs-Computer Zugangsdaten zu dem lokalen Netzwerk gespeichert oder erzeugbar sind und wobei auf Übermittlung eines Steuerbefehls und der Zugangsdaten von dem Identifizierungs-Computer an den Einzelrechner ein Verbindungsaufbau zwischen dem Einzelrechner und dem lokalen Computernetzwerk und eine Fernregistrierung im lokalen Computernetzwerk mit den Zugangsdaten durchführbar ist.

[0010] Die Zugangsdaten zu dem lokalen Computernetzwerk sind also nicht von Hand einzugeben, sondern sind auf dem Identifizierungs-Computer, der die Form einer Chipkarte haben kann, gespeichert. Fehler bei der Eingabe der Zugangsdaten sind somit ausgeschlossen. Der Aufbau einer Verbindung zwischen dem Einzelrechner und dem Computernetzwerk kann auf Knopfdruck geschehen, da der Einzelrechner durch den Identifizierungs-Computer fernsteuerbar ist, nämlich durch Übermittlung eines Steuerbefehls eine Verbindung herstellt.

[0011] Der Benutzer und Besitzer des Identifizie-

rungs-Computers ist auch nicht darauf angewiesen, immer denselben Einzelrechner zu verwenden. Unter der Voraussetzung, daß die entsprechende Datenfernübertragungssoftware installiert ist und eine Schnittstelle zur Kommunikation mit dem Identifizierungs-Computer besteht, kann die Verbindung von jedem beliebigen Einzelrechner aus aufgebaut werden.

[0012] Zur Erhöhung der Zugangssicherheit ist in einer Weiterbildung der Identifizierungs-Computer um eine Benutzerauthentisierungseinheit erweitert. In einer besonders vorteilhaften Ausgestaltung ist dies ein biometrischer Sensor, vorzugsweise ein Sensor zur Erkennung eines Fingerabdrucks.

[0013] Die Verbindung zwischen dem Identifizierungs-Computer und dem Einzelrechner erfolgt in besonders einfacher Weise durch eine Blue Tooth-Schnittstelle.

Ausführungsbeispiel

[0014] Die Erfindung wird nachfolgend anhand eines Ausführungsbeispieles näher erläutert. Die Figur zeigt schematisch die Elemente der Netzwerkanordnung und die Kommunikationspfade zwischen den Elementen.

[0015] In dem Ausführungsbeispiel gemäß der Figur sind mehrere Computer **2** über eine Datenleitung **3** zu einem lokalen Computernetzwerk **1** zusammengeschlossen. Außerdem ist ein zusätzlicher Knoten **4** vorgesehen, über den sich weitere Computer von außen in das lokale Computernetzwerk **1** einwählen können. Dies ist möglich mit einem Einzelrechner **5**, der Mittel zum Aufbau einer Verbindung **6** zu dem lokalen Computernetzwerk **1** aufweist. Dazu notwendig ist eine Kommunikationsschnittstelle, beispielsweise ein Modem **12**. Die Verbindung kann dabei sowohl über das Festnetz als auch über Mobilfunk erfolgen. Der Einzelrechner weist darüber hinaus eine weitere Kommunikationsschnittstelle **7** auf, über die Daten und Steuerbefehle entgegen genommen werden können. Der Einzelrechner ist so ausgerüstet, daß der Verbindungsaufbau zwischen dem Einzelrechner **5** und dem lokalen Computernetzwerk **1**, also die Verbindung **6**, über einen Steuerbefehl und einer auf dem Einzelrechner **5** installierten Software automatisch hergestellt werden kann. Erfindungsgemäß wird dieser Steuerbefehl von einem Identifizierungs-Computer **9** gesendet. Dazu weist der Identifizierungs-Computer **9** ebenfalls eine Kommunikationsschnittstelle **8** auf, über die er mit der Kommunikationsschnittstelle **7** des Einzelrechners **5** kommunizieren kann. In dem Identifizierungs-Computer **9** sind die Zugangsdaten zu dem Computernetzwerk **1** hinterlegt.

[0016] Zusätzlich ist in dem Identifizierungs-Computer eine Benutzerauthentisierungseinheit **10** vorgesehen, um zu verhindern, daß ein unbefugter Nutzer, der in den Besitz des Identifizierungs-Computers gelangt ist, sich in das lokale Computernetzwerk **1** einwählen kann. Die Benutzerauthentisierungseinheit **10** ist im vorliegenden Beispiel als Sensor zur Erkennung eines Fingerabdrucks samt der dafür notwendigen Auswerteeinrichtung ausgeführt. In einer vereinfachten Ausführung könnte hier aber auch eine Paßwort-Eingabe erfolgen. Nach Eingabe des Paßwortes bzw. Auflegen eines Fingers und Erkennung des Fingerabdrucks eines berechtigten Benutzers erzeugt der Identifizierungs-Computer **9** einen Paßwortzahlencode. Gemeinsam mit diesem werden in dem Identifizierungs-Computer **9** gespeicherte Zugangsdaten zu dem lokalen Computernetzwerk an den Einzelrechner **5** über die Kommunikationsschnittstelle **8** und **7** übermittelt. Die Verbindung **11** zwischen diesen beiden Kommunikationsschnittstellen **7** und **8** ist in besonders einfacher Weise durch eine Blue Tooth-Schnittstelle realisiert. Schnittstellen nach dem Blue Tooth-Industriestandard können auch für andere Anwendungen verwendet werden, so daß dies in vielen Fällen keinen zusätzlichen Aufwand an dem Einzelrechner bedeutet. Zusammen mit dem Paßwortzahlencode und den Zugangsdaten wird ein Steuerbefehl an den Einzelrechner übermittelt. Eine dafür vorgesehene Software auf dem Einzelrechner **5** startet nun den Verbindungsaufbau zu dem lokalen Computernetzwerk **1** und führt dort die erforderliche Registrierung durch. Dem Benutzer ist es somit möglich, lediglich durch das Auflegen eines Fingers auf den Identifizierungs-Computer einen vollständigen Verbindungsaufbau und die Registrierung beim lokalen Computernetzwerk **1** durchzuführen, wobei die unberechtigte Benutzung durch Dritte verhindert ist.

Patentansprüche

1. Netzwerkanordnung mit
– einem lokalen Computernetzwerk (**1**),
– einem entfernt angeordneten Einzelrechner (**5**), der Mittel (**12**) zum Aufbau einer Verbindung (**6**) zum lokalen Computernetzwerk aufweist, und
– einem von dem lokalen Computernetzwerk unabhängig arbeitenden Identifizierungs-Computer (**9**), der über eine Kommunikationsschnittstelle (**7**, **8**) mit dem Einzelrechner (**5**) Daten austauschen kann,
wobei in dem Identifizierungs-Computer (**9**) Zugangsdaten zu dem lokalen Netzwerk (**1**) gespeichert oder erzeugbar sind und wobei auf Übermittlung eines Steuerbefehls und der Zugangsdaten von dem Identifizierungs-Computer (**9**) an den Einzelrechner (**5**) ein Verbindungsaufbau zwischen dem Einzelrechner (**5**) und dem lokalen Computernetzwerk (**1**) und eine Fernregistrierung im lokalen Computernetzwerk (**1**) mit den Zugangsdaten durchführbar ist.

2. Anordnung nach Anspruch 1, dadurch gekennzeichnet, daß der Identifizierungs-Computer (**9**) eine

Benutzerauthentisierungseinheit (**10**) mit einem biometrischen Sensor, vorzugsweise einem Sensor zur Erkennung eines Fingerabdrucks, aufweist.

3. Anordnung nach Anspruch 1, dadurch gekennzeichnet, daß die Kommunikationsschnittstelle (**7**, **8**) eine Blue Tooth-Schnittstelle ist.

Es folgt ein Blatt Zeichnungen

Anhängende Zeichnungen