

(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11)

EP 1 650 716 A1

(12)

EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
26.04.2006 Patentblatt 2006/17

(51) Int Cl.:
G07C 9/00 (2006.01)

(21) Anmeldenummer: **04025175.3**

(22) Anmeldetag: **25.10.2004**

(84) Benannte Vertragsstaaten:
**AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
HU IE IT LI LU MC NL PL PT RO SE SI SK TR**
Benannte Erstreckungsstaaten:
AL HR LT LV MK

(71) Anmelder: **Leicher Projekt GmbH**
85551 Kirchheim (DE)

(72) Erfinder:
• **Wentzlig, Eduard**
82515 Wolfratshausen (DE)

• **Kisser, Olaf**
38539 Müden/Aller (DE)

(74) Vertreter: **Lang, Friedrich et al**
Patentanwälte,
Lang & Tomerius,
Bavariaring 29
80336 München (DE)

(54) **Verfahren zur Verwaltung von Benutzerrechten für ein codesicheres Objekt**

(57) Die Erfindung betrifft ein Verfahren zur Verwaltung von Benutzerrechten für ein codesicheres Objekt (1), wie z.B. Einem Bankautomaten, bei dem ein Code (6) mit einer Objektkennung (7) und einer Berechtigungszeit (8) von einer Benutzerrechteverwaltung (5) erzeugt wird, der einem berechtigten Benutzer (9) für einen Zugriff auf das Objekt (1) übermittelt wird und den der Berechtigte (9) einer Kontrollvorrichtung (3) mitteilt, wobei die Kontrollvorrichtung (3) den Code (6) anhand der ihr vorgegebenen Objektkennung (11) und einer von der

Kontrollvorrichtung (3) ermittelten Zeit (12) überprüft. Dabei muss der Benutzer (9) den Code (6) der Kontrollvorrichtung (3) dann übermitteln, wenn die von ihr ermittelte Zeit (12) mit der im Code (6) enthaltenen Berechtigungszeit (8) zumindest etwa übereinstimmt. Bei Vorliegen eines ordnungsgemäßen Codes (6) ermöglicht die Kontrollvorrichtung (3) dem Berechtigten (9) dann den Zugriff auf das Objekt (1).

EP 1 650 716 A1

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Verwaltung von Benutzerrechten für ein codegesichertes Objekt gemäß dem Oberbegriff des Anspruchs 1.

[0002] Dabei erfolgt durch die Verwaltung von Benutzerrechten zumindest die Vergabe und die Kontrolle von Rechten sowie die anschließende Freigabe des Objektes zur Benutzung durch den Berechtigten. Es wird daher einem begrenzten Personenkreis ermöglicht, ein entsprechend verwaltetes Objekt exklusiv zu benutzen. Hierbei werden unter gesicherten Objekten Sicherheitschlosser, Tresorräume, Geldausgabeautomaten (GAA), Geldeinzahlungsautomaten (GEA), Schlüsselausgabeautomaten, gegen Zugriff von Unbefugten gesicherte Maschinen, Geräte und Räumlichkeiten, wie z.B. Hotelzimmer und Ähnliches verstanden. Die Benutzerrechte können dem berechtigten Benutzer allgemein den Zugriff, den Zutritt oder sonstige Nutzungsmöglichkeiten in Abhängigkeit seiner Rechte verschaffen.

[0003] In letzter Zeit sind die Anforderungen an Verfahren zur Verwaltung von Benutzerrechten für gesicherte Objekte immer größer geworden. Insbesondere bei der Verwaltung von Benutzerrechten für die Wartung, Pflege und Bestückung von Geldausgabeautomaten (GAA) hat sich das Problem herauskristallisiert, dass eine ganze Reihe unterschiedlicher Dienstleister Zugriff auf die auch als Geldautomaten bezeichneten Geräte bekommen sollen, ohne dass die Sicherheit der Automaten darunter leiden darf. Üblicherweise erhalten so neben Bankangestellten auch Mitarbeiter von Werttransportunternehmen (WTU) und Kundendienstunternehmen (KDU) Zugriff auf die gesicherten Objekte.

[0004] In der Vergangenheit wurden den einzelnen Benutzern von der Verwaltung der Benutzerrechte Schlüssel für jedes gesicherte Objekt ausgehändigt, die diese nach Vollendung ihrer Zugriffe auf die Objekte wieder dort abgeben mussten. Da insbesondere in der Werttransport- und Sicherungsbranche die Mitarbeiter in der Regel eine Vielzahl von gesicherten Objekten betreuen, führen sie im Einsatz oft eine große Zahl von Schlüsseln mit sich. Dies ist sehr unhandlich, die Schlüsselverwaltung sehr aufwendig und nicht zuletzt sind auch Schlüssel mit den verbundenen Sicherheitsrisiken verloren gegangen.

[0005] Als Alternative bieten sich Nummernschlösser und auch elektronisch gesicherte Codeschlösser an, bei denen der Zugriffsberechtigte nur eine Nummern- und/oder Zeichenfolge von der Verwaltung ausgehändigt bekommt, die ihm den Zugriff auf das gesicherte Objekt ermöglicht. Der Code wird üblicherweise von den Zugriffsberechtigten über eine Eingabevorrichtung an eine Kontrolleinrichtung des Objektes übermittelt, die diesen eingegeben Code (Eingabecode) mit einem ihm vorgegebenen Code (Norgabecode) vergleicht. Sind beide Codes identisch, ermöglicht die Kontrollvorrichtung den Zugriff auf das Objekt, z.B. indem ein Schloss freigeschaltet wird. Vorteilhaft an dieser Lösung ist, dass die Verwal-

tung inklusive der Erzeugung, Ausgabe und Handhabung von Codes in der Regel weniger aufwendig ist als die von Schlüsseln.

[0006] Allerdings besteht das Problem bei dieser bekannten Lösung, dass der für die Hinterlegung von Vorgabecodes notwendige Speicherplatz im Codeschloss begrenzt ist und nur eine feste und begrenzte Anzahl von Codes für jedes Codeschloss ausgegeben und verwaltet werden kann. Deshalb werden bei steigender Zahl zugriffsberechtigter Personen, die jedem Codeschloss individuell zugewiesenen Codes üblicherweise einer Vielzahl von Personen ausgehändigt. Oftmals können dies mehrere Dutzend Personen sein, was die Objektsicherheit empfindlich verringert. Dieses Problem verstärkt sich teilweise noch wenn die Service- und Werttransportunternehmen eine hohe Mitarbeiterfluktuation aufweisen. Dann ist es oft nur schwer nachvollziehbar, wer tatsächlich im Besitz eines Codes für ein spezifisches Codeschloss war oder ist.

[0007] Um dieses Problem zu lösen, wurden Verfahren zur Verwaltung von Benutzerrechten entwickelt, bei denen die von der Verwaltung vergebenen Codes nach einer gewissen Zeit ungültig werden oder von der Verwaltung per Datenübertragung im Codeschloss verändert werden können. Bei diesen veränderlichen oder alternden Codes entfällt das Aufbewahrungsrisiko, d.h. der Verlust eines Codes ist zumindest nach dem Bekanntwerden des Verlustes oder nach einer gewissen Zeitspanne kein unmittelbares Sicherheitsrisiko mehr. Allerdings ist es notwendig, das Codeschloss mit einer Datenübertragungsvorrichtung wie z.B. einer Datenleitung oder einer Funkverbindung zu versehen, um einen entwerteten Code durch einen neuen Code zu ersetzen. Datenübertragungsvorrichtungen weisen naturgemäß wiederum neue Sicherheitsrisiken auf und sind aufwendig und kostenintensiv zu unterhalten. Zudem können bereits vorhandene Codeschlösser oftmals nicht mit einer Datenübertragungsvorrichtung versehen werden. Das macht das Umstellen der Verwaltung von Benutzerrechten auf ein per Datenübertragungsvorrichtung kommunizierendes Verfahren bei einer großen Anzahl von zu verwaltenden Codegesicherten Objekten, wie z.B. bei einem flächendeckenden Geldautomatennetz einer Bank, oftmals zu teuer.

[0008] Um dieses Problem zu lösen, ist man in den USA bei der Verwaltung von Benutzerrechten für Geldautomaten wieder dazu übergegangen, den Werttransport- und Serviceunternehmen Transponder mitzugeben, die als elektronische Schlüssel die elektronisch gesicherten Schlösser mit wechselnden Codes schließen. Bei diesem System sind natürlich die bereits von herkömmlichen Schlüsseln bekannten Nachteile vorhanden.

[0009] Die Erfindung stellt sich daher die **Aufgabe**, ein einfaches Verfahren zur Verwaltung von Benutzerrechten von codegesicherten Objekten anzugeben, bei welchem eine unbegrenzte Zahl von Codes vergeben werden kann, ohne dass die Kontrollvorrichtung des code-

gesicherten Objektes über eine Datenübertragungsvorrichtung mit der Benutzerrechteverwaltung verbunden sein muss.

[0010] Die Lösung dieser Aufgabe gelingt mit dem Verfahren zur Verwaltung von Benutzerrechten gemäß Anspruch 1. Bevorzugte Ausführungsformen und Weiterbildungen sind in den Unteransprüchen beschrieben.

[0011] Bei dem erfindungsgemäßen Verfahren wird ein Code von einer Benutzerrechteverwaltung erzeugt, der eine Objektkennung und eine Berechtigungszeit beinhaltet. Dieser Code wird dann einem berechtigten Benutzer für einen Zugriff auf das Objekt übermittelt. Um Zugriff auf das gesicherte Objekt zu erhalten, teilt der Benutzer diesen Code der Kontrollvorrichtung mit. Die Kontrollvorrichtung überprüft den eingegebenen Code anhand einer ihr vorgegebenen Objektkennung und einer von ihr ermittelten Zeit. Daher ist es notwendig, dass der Benutzer den Code der Kontrollvorrichtung dann übermittelt, wenn die von ihr ermittelte Zeit mit der im Code enthaltenen Berechtigungszeit übereinstimmt.

[0012] Dabei kann die Benutzerrechteverwaltung den Code in verschlüsselter oder unverschlüsselter Form dem berechtigten Benutzer übermitteln. Ein verschlüsselter Code erhöht die Sicherheit des Verfahrens noch weiter. Üblicherweise übermittelt der Berechtigte über eine Eingabevorrichtung wie z.B. eine Tastatur oder einen Kartenleser den Code der Kontrollvorrichtung, wobei die Eingabevorrichtung integrierter Bestandteil der Kontrollvorrichtung, oder auch räumlich von dieser getrennt angeordnet sein kann.

[0013] Die im Code enthaltene Objektkennung kann dabei aus einer beliebigen Zeichenfolge bestehen, ein Passwort, eine Objekt-Identifikationsnummer (Objekt-ID), ein Zahlenschlüssel oder ähnliches sein. Wichtig ist nur, dass sie der Kontrollvorrichtung eindeutig und unverwechselbar vorgegeben sein muss. Es ist dabei unerheblich, ob die Kennung unveränderbar oder durch die Benutzerrechteverwaltung veränderbar in der Kontrollvorrichtung hinterlegt ist. Eine besonders bevorzugte Objektkennung ist die unveränderbare und individuelle Produktnummer der jeweiligen Kontrollvorrichtung.

[0014] Wesentlich an dem erfindungsgemäßen Verfahren ist, dass die Kontrolleinrichtung nicht nur die Objektkennung überprüft, sondern auch die im eingegebenen Code enthaltene Berechtigungszeit. Diese Berechtigungszeitangabe im eingegebenen Code wird von der Kontrolleinrichtung gelesen und mit einer von ihr unabhängig ermittelten Zeit verglichen. Stimmt die in der Kontrolleinrichtung ermittelte Zeit mit der Berechtigungszeit des Codes überein, ermöglicht die Kontrollvorrichtung den Zugriff auf das Objekt, zum Beispiel dadurch, dass ein Sperrelement eines Schlosses entriegelt, eine Tür oder ein Schloss geöffnet oder eine Klappe zurückgeschwenkt wird.

[0015] Die Übereinstimmung zwischen der im Code enthaltenen Berechtigungszeit und der von der Kontrollvorrichtung ermittelten Berechtigungszeit wird in vorbestimmter Genauigkeit ermittelt. Die Kontrollvorrichtung

kann eine Übereinstimmung der von ihr ermittelten Zeit mit der im Code enthaltenen Berechtigungszeit im Bereich von Sekunden fordern, oder eine Unschärfe bzw. Abweichung vom Sollwert zulassen, indem eine Übereinstimmungsgenauigkeit im Bereich von Stunden oder Tagen gefordert wird. Letzteres hat den Vorteil, dass auf einfache Weise ein Zeitfenster erzeugt wird, in dem der Berechtigte den Code eingeben muss. Dies ist insbesondere dann von Vorteil, wenn z.B. mit einer abweichenden Eingabe aufgrund von Verkehrsstatus bereits bei der Vergabe des Codes gerechnet werden kann.

[0016] Der besondere Vorteil von diesem Verfahren ist, dass der Kontrollvorrichtung ein ihr vorher unbekannter Code übermittelt wird, den diese anhand einer unabhängigen Zählseinheit wie einer Uhr überprüft. Somit ist es bei diesem Verfahren möglich unendlich viele neue Codes zu generieren, ohne diese vorher der Kontrollvorrichtung mitteilen zu müssen. Dies verringert den notwendigen Speicherplatz zur Vorgabe von Codes oder Kennungen in der Kontrollvorrichtung und es ist auf einfache Weise möglich ein zentral verwaltetes Netz von gesicherten Objekten wie z.B. Bankautomaten zu schaffen, ohne dass alle Objekte mittels Datenübertragungsvorrichtungen mit der Benutzerrechteverwaltung verbunden sein müssen. Zudem weisen die meisten Bankautomaten bereits Zeitermittlungsbausteine auf, wodurch sich der Aufwand bei einer Umrüstung solcher Geräte weiter verringert.

[0017] In einer ersten Weiterbildung des Verfahrens ist die im Code enthaltene Berechtigungszeit eine Zeitspanne, wobei der Benutzer den Code der Kontrollvorrichtung dann übermitteln muss, wenn die von ihr ermittelte Zeit innerhalb der im Code enthaltenen Berechtigungszeit liegt. Hierdurch muss der Berechtigte nur in einem gewissen Zeitfenster den Code eingeben, was ebenfalls die bereits oben geschilderten Vorzüge erzeugt.

[0018] Die Berechtigungszeit muss nicht unbedingt eine Uhrzeit sein, sondern ist vielmehr ein Maß für eine mit bestimmter Geschwindigkeit gezählte Einheit. Denkbar wäre daher auch ein Verfahren bei dem die Berechtigungszeit einfach eine von einem konstant laufenden Zählwerk ermittelte Zahl ist. Dann sollte zumindest die Benutzerrechteverwaltung einen Schlüssel zum Umrechnen der Zählwerkszahl in eine Uhrzeit haben, oder der Berechtigte verfügt über ein mit dem Zählwerk in der Kontrollvorrichtung gleich zählendes Zählwerk mit dem der Berechtigte ermitteln kann, wann das Zählwerk der Kontrollvorrichtung die vorbestimmte Zahl erreicht und er den Code zum richtigen Zeitpunkt der Kontrollvorrichtung übermittelt.

[0019] In einer vorteilhaften Weiterbildung des Verfahrens beinhaltet der Code zusätzlich eine Berechtigtenkennung. Dadurch ist es der Kontrolleinrichtung möglich einen Berechtigten zu identifizieren, indem sie die im eingegebenen Code enthaltene Berechtigtenkennung anhand einer ihr vorher vorgegebenen Berechtigtenkennung überprüft. Es wird also von der Rechteverwaltung

ein Code mit wenigstens drei von einander unabhängigen Parametern gebildet, wobei ein Parameter dem Berechtigten zugeordnet wird. Die Berechtigtenkennung wird dazu üblicherweise in der Kontrolleinrichtung fest hinterlegt. Wechselt der Berechtigte, z.B. das für einen Automaten zuständige WTU, so erhält der neue Berechtigte diese Berechtigtenkennung zugewiesen. Der nicht mehr Berechtigte erhält dann einfach keinen neuen Code von der Berechtigtenkennung. So hat der nicht mehr Berechtigte nur Codes, die keine gültige Berechtigungszeit haben und erhält daher auch keine Zugriffsmöglichkeit auf das Objekt.

[0020] Die Berechtigtenerkennung ist insbesondere dann von Vorteil, wenn für das gesicherte Objekt eine Vielzahl von Personen oder Unternehmen Zugriff erhalten soll. So können zum Beispiel einem Geldautomaten verschiedene WTU's, Serviceunternehmen und Bankangestellte zugeordnet werden.

[0021] In einer weiteren Ausführungsform des Verfahrens kann die Rechteverwaltung einem Benutzer nur ein beschränktes Benutzungsrecht für das gesicherte Objekt erteilen, wodurch die Kontrollvorrichtung dem identifizierten Benutzer nur eine ihr vorgegebene beschränkte Benutzung ermöglicht. Die verschiedenen Benutzer erhalten jeweils eigene, teilweise auch unterschiedliche Zugriffsebenen für das gesicherte Objekt zugewiesen. Bei einem Geldautomaten ist es sinnvoll, dass ein WTU-Mitarbeiter nur Zugriff auf das Geldfach bekommt, während ein Mitarbeiter eines Serviceunternehmens nur Zugriff auf die von ihm zu wartenden Bauteile erhält und nicht auf das Geldfach. Es ist daher notwendig der Kontrollvorrichtung zu jeder Benutzerkennung eine Freigabeebene vorzugeben.

[0022] In einer weiteren vorteilhaften Weiterbildung umfasst die Berechtigungszeit eine Uhrzeit und ein Datum oder eine Uhrzeit oder ein Datum. Bei diesem Verfahren ist es dann möglich, sowohl die Kontrollvorrichtung wie auch den Zugriffsberechtigten mit handelsüblichen Uhren auszustatten, wobei nur darauf geachtet werden muss, dass beide Uhren synchron zueinander laufen und auf die gleiche Zeit eingestellt werden. Dies kann die normal gültige Ortszeit sein, wie z.B. in Deutschland die Mitteleuropäische Zeit. Wird nur ein Datum vorgegeben, so ist es möglich, dem Zugriffsberechtigten einen ganzen Tag Zeit zu geben, auf das gesicherte Objekt zuzugreifen. Bei Kombination von Uhrzeit und Datum kann der Berechtigte nur an konkreten Tagen und Zeiten auf das Objekt zugreifen, dies ermöglicht. Werden zwei Uhrzeiten im Code angegeben, so definieren diese eine Zeitspanne innerhalb derer der Zugriffsberechtigte auf das gesicherte Objekt zugreifen muss. Erfolgt die Eingabe außerhalb dieses festgelegten Zeitrahmens, so ist der Code nicht mehr gültig und die Kontrollvorrichtung wird einen Zugriff auf das gesicherte Objekt nicht ermöglichen.

[0023] In einer weiteren vorteilhaften Ausführungsform des Verfahrens wird die Berechtigungszeit in der Benutzerrechteverwaltung und in der Kontrollvorrichtung

anhand zweier gleichlaufender Uhren festgelegt und überprüft, wobei die Uhren schneller oder langsamer laufen als eine die normale Uhrzeit ermittelnde Uhr. Zum Beispiel ist es bei doppelt so schnell laufenden Uhren möglich, an einem Tag zwei um 12 Stunden versetzte Berechtigungszeiten festzulegen, wenn die Berechtigungszeit kein konkretes Datum enthält. Dies hat den Vorteil, dass es eine zweite Zugriffszeit gibt, die dem Berechtigten von der Benutzerrechteverwaltung mitgeteilt werden, z.B. wenn er die erste Zugriffszeit an dem Tag verpasst hat.

[0024] Es ist auch denkbar, dass in der Kontrollvorrichtung zwei Berechtigungszeiten ermittelt werden, wobei die eine Berechtigungszeit eine Uhrzeit ist, die zum Beispiel schneller oder langsamer gezählt wird und die andere ein normal ermitteltes Datum ist. Bei dieser Lösung ist es dann sogar möglich, mehrere Berechtigungszeitpunkte für den Zugriff auf das gesicherte Objekt pro Tag an verschiedenen Tagen zu definieren.

[0025] In einer weiteren vorteilhaften Ausführungsform wird der Zugriff eines Berechtigten zusammen mit der Zugriffszeit gespeichert, um den Zugriff zu dokumentieren. Dies ist insbesondere aus versicherungstechnischen Gründen von Vorteil, da so ermittelt wird, wer tatsächlich Zugriff auf das gesicherte Objekt hatte.

[0026] In einer weiteren Ausführungsform des Verfahrens kann die Benutzerrechteverwaltung per Datenübertragung eine Rückmeldung über einen erfolgten Zugriff auf das gesicherte Objekt erhalten. Auch hierbei liegt der Vorteil darin, dass ein Zugriff dokumentiert wird, wobei es dann möglich ist, den Zugriff extern abzuspeichern. Vorteilhafterweise kann ein solches Verfahren derart weitergebildet werden, dass die Benutzerrechteverwaltung der Kontrollvorrichtung per Datenübertragung Codeparameter ändern und/oder neu vorgeben kann. So wird es zum Beispiel möglich, die Objektkennung zu verändern oder eine alternde Objektkennung vorzusehen, wobei dann nach einer Ablaufzeit eine neue Objektkennung der Kontrollvorrichtung übermittelt und vorgegeben wird. Auch ist es dann möglich, über die Datenübertragung zum Beispiel bei elektrischen Uhren die Uhren der Kontrollvorrichtung mit der Uhr der Benutzerrechteverwaltung oder der Uhr des Benutzers synchron zu schalten.

[0027] In besonders bevorzugter Weise wird das Verfahren benutzt, um ein Sperrelement wie z.B. ein Schloss eines Bankautomaten durch die Kontrollvorrichtung anzusteuern.

[0028] In einer weiteren Ausführungsform werden die Benutzerrechte zentral verwaltet. Dies kann zum Beispiel in einem Call Center einer Bank geschehen, wobei dieses dann zentral verwaltete Verfahren die Vorteile der banktypischen Sicherheitsvorrichtungen und -strukturen genießt. Auch hat eine zentrale Benutzerrechteverwaltung den Vorteil, dass die Bank eine zeitliche Kontrolle der Arbeiten der Berechtigten vornehmen kann.

[0029] Es ist aber auch denkbar, dass mit dem Verfahren die Benutzerrechte des gesicherten Objektes de-

zentral verwaltet werden. Dabei kann zum Beispiel ein WTU seine ihm zugeordnete Benutzerebene eines Geldautomaten mit Hilfe einer von der Bank lizenzierten Software verwalten und ein Serviceunternehmen die ihm zugeordneten Berechtigungs- und Zugriffsebenen seiner Mitarbeiter verwalten. Dieses Vorgehen hat den Vorteil, dass die Berechtigten in ihren Benutzer- und Zugriffsebene bzw. Rechten unabhängig von den Vorgaben der Bank den Zugriff auf den Automaten planen und auch abrechnen können.

[0030] In einer weiteren vorteilhaften Ausführungsform des Verfahrens werden die Benutzerrechte unter Berücksichtigung einer Zugriffszeitplanung des Berechtigten vergeben. Wie bereits geschildert, ist es von großer Wichtigkeit, dass der jeweils Berechtigte zu einem bestimmten Zeitpunkt am gesicherten Objekt den Code eingibt. Da die Serviceunternehmen oder WTU's in der Regel eine Vielzahl von gesicherten Objekten an einem Tag bedienen, ist es von Vorteil, wenn die Vergabe der Benutzerrechte und der Zuteilung von Zugriffscodes für die gesicherten Objekte unter Berücksichtigung der Zugriffszeitplanung bzw. des Tourenplans des Mitarbeiters der Unternehmen erfolgt. So kann die Benutzerrechteverwaltung mit der Tourenplanung des Berechtigten vernetzt sein und auf der Basis seiner Tourenplanung Berechtigungscodes erstellen.

[0031] Alternativ kann die Benutzerrechteverwaltung erst dann einen Code vergeben, wenn der Berechtigte die Zugriffsmöglichkeit anfordert, z.B. wenn er unmittelbar vor dem gesicherten Objekt steht. Der Berechtigte kann dann einfach wann er will an das gesicherte Objekt gehen. Ist er vor Ort, meldet er sich bei der Benutzerrechteverwaltung und teilt dieser mit, vor welchem gesicherten Objekt er steht. Diese sendet ihm dann einen für das entsprechende Objekt gültigen Code z.B. per SMS, den er unmittelbar nach Empfang der Kontrollvorrichtung übermitteln muss. Bei dieser Ausführungsform ist es daher notwendig, dass die Benutzerrechteverwaltung eine Uhr hat, die im Einklang zur Uhr des gesicherten Objektes läuft. Vorteilhaft an dieser Ausführungsform ist die große Flexibilität des Benutzers bei seiner Zugriffszeitplanung.

[0032] Die Erfindung wird nachfolgend anhand einer Zeichnung näher erläutert. Es zeigen schematisch:

- Fig. 1 eine Ansicht der Rückseite eines Bankautomaten;
- Fig. 2 ein Blockdiagramm für ein erstes Ausführungsbeispiel des erfindungsgemäßen Verfahrens;
- Fig. 3 ein Blockdiagramm für ein zweites Ausführungsbeispiel des erfindungsgemäßen Verfahrens;
- Fig. 4 ein Blockdiagramm für ein drittes Ausführungsbeispiel des erfindungsgemäßen Verfahrens;
- Fig. 5 ein Blockdiagramm für ein viertes Ausführungsbeispiel des erfindungsgemäßen Verfahrens;
- Fig. 6 ein Blockdiagramm für ein fünftes Ausführungsbeispiel des erfindungsgemäßen Verfahrens;

rens.

[0033] Fig. 1 zeigt in schematischer Darstellung ein codesicheres Objekt 1, dessen Benutzerrechte mit dem erfindungsgemäßen Verfahren verwaltet werden. Das codesichere Objekt 1 ist in diesem ersten Ausführungsbeispiel ein Bankautomat, der zum Erledigen üblicher Funktionsvorgänge oder Transaktionen wie beispielsweise Bargeld abheben, Bargeld einzahlen, Kontostandsabfragen, Kontoauszugsdrucken, Ausführen von Überweisungen und dergleichen dient. Dabei zeigt Fig. 1 die Rückseite des Automaten mit einer Tür 2, die über eine Kontrollvorrichtung 3 verfügt. Die Kontrollvorrichtung 3 weist an ihrer Außenseite eine Eingabevorrichtung 4 auf, die in hier aus einer Tastatur 4a und einer Anzeige 4b besteht.

[0034] In der Fig. 2 wird nun ein erstes Ausführungsbeispiel des Verfahrens zur Verwaltung der Benutzerrechte des in Fig. 1 dargestellten Bankautomaten 1 gezeigt. Erfindungsgemäß generiert die Benutzerrechteverwaltung 5 einen Code 6, der eine Objektkennung 7 und eine Berechtigungszeit 8 beinhaltet. Der Code 6 wird dem Berechtigten 9 zusammen mit einer Zeitvorgabe 10 übermittelt. Die Zeitvorgabe 10 gibt an, wann der Zugriff durch den Berechtigten 9 auf das ihm bekannte gesicherte Objekt 1 erfolgen soll. Die Übermittlung des Codes 6 und der Zeitvorgabe 10 kann dabei auf dem üblichen Wege zum Beispiel in Papierform per Post, per E-Mail, per Funk, per Telefon oder auch per SMS erfolgen.

[0035] Der Berechtigte 9 muss nun zur vorgegebenen Zeit 10 der Kontrollvorrichtung 3 des gesicherten Objektes den Code 6 eingeben. Die Kontrollvorrichtung 3 wird dann den eingegebenen Code 6 überprüfen. Bei der Überprüfung vergleicht die Kontrollvorrichtung 3 den Teil 7 des eingegebenen Codes 6, der die Objektkennung beinhaltet, mit einer ihr vorgegebenen Objektkennung 11. Weiterhin überprüft die Kontrollvorrichtung 3 die im eingegebenen Code 6 enthaltene Berechtigungszeit 8 mit einer von der Kontrollvorrichtung 3 ermittelten Zeit 12.

[0036] Die Kontrollvorrichtung 3 weist ein handelsübliches Speichermedium, in dem die Objektkennung 11 gespeichert werden kann und einen Zeitbaustein oder eine Uhr zur Ermittlung der Berechtigungszeit 12 auf. Stimmt die eingegebene Objektkennung 7 mit der vorgegebenen Objektkennung 11 und die eingegebene Uhrzeit 8 mit der von der Kontrollvorrichtung 3 ermittelten Zeit 12 überein, so wird von der Kontrollvorrichtung 3 das Sperrelement 13 der Tür 2 des Bankautomaten 1 so angesteuert, dass sich die Tür 2 öffnen lässt.

[0037] Wie sich an diesem Beispiel erkennen lässt, ist es also von herausgehobener Bedeutung, dass der Berechtigte 9 den Code 6 genau dann eingibt, wenn die in der Kontrollvorrichtung 3 ermittelte Zeit 12 mit der Berechtigungszeit 8 übereinstimmt. Um hier eine möglichst gute Übereinstimmung zwischen dem Zeitpunkt der Codeeingabe und der von der Kontrollvorrichtung ermittelten Zeit 12 zu erreichen, ist es zum Beispiel denkbar, dass an der Kontrollvorrichtung 3 die von der Kontroll-

vorrichtung 3 ermittelte Uhrzeit 12 in einem Display 4b angegeben wird. Dann kann der Berechtigte 9 so lange warten, bis er genau die Zeit 12 angezeigt bekommt, die mit seiner von der Benutzerrechteverwaltung 5 vorgegebenen Zeitvorgabe 10 übereinstimmt und kann dann seinen Code 6 eingeben. Alternativ kann die Uhr der Kontrollvorrichtung 3 verdeckt, also nicht sichtbar, die Zeit ermitteln, dann muss allerdings der Berechtigte 9 über eine Uhr verfügen, die genau im Einklang mit der Uhr der Kontrollvorrichtung 3 die Zeit ermittelt. Zusammen mit der von der Benutzerrechteverwaltung 5 erhaltenen Zeitvorgabe 10 kann er dann den Code 6 eingeben.

[0038] In diesem Beispiel berücksichtigt die Kontrollvorrichtung 3 bei der Überprüfung der Berechtigungszeit 8 eine gewisse Zeitüber- und -unterschreitung bzw. Toleranzzeit. So wird bei der Überprüfung der Berechtigungszeit 8 ein Zeitraum von einer Stunde als Toleranzzeit akzeptiert. Genauso gut ist es auch möglich, den Codeparameter Berechtigungszeit 8 als Zeitraum mit Anfangs- und Endzeit zu definieren. Dann müsste die Kontrollvorrichtung 3 lediglich überprüfen, ob die von ihr ermittelte Zeit 12 innerhalb oder auch außerhalb des Berechtigungszeitraumes 8 liegt und könnte entsprechend den Zugriff ermöglichen oder verhindern.

[0039] Fig. 3 zeigt eine zweite Ausführungsform des Verfahrens bei dem von einer zentralen Rechteverwaltung 5 aus drei verschiedene Codes 61, 62, 63 vergeben werden. Diese werden an drei unterschiedliche Berechtigte z. B. Geldtransportunternehmen 91, 92, 93 weitergeleitet, so dass drei verschiedene Berechtigte auf den Geldautomaten 1 Zugriff haben, indem jeder seinen eigenen individuellen Code eingibt.

[0040] In Fig. 4 wird eine dritte Ausführungsform des erfindungsgemäßen Verfahrens zur Verwaltung von Benutzerrechten dargestellt, bei dem in der Rechteverwaltung 5 ein Code 6 aus einer Datenbank 15 heraus erstellt wird. Der Code 6 enthält eine Objektkennung 7, eine Berechtigungszeit 8 und eine Berechtigtenkennung 14 und wird nach der Erstellung in der Benutzerrechteverwaltung verschlüsselt und an den Berechtigten 9, der in diesem Beispiel ein Werttransportunternehmen (WTU) ist, übermittelt. Zusammen mit dem Code 6 erhält der Berechtigte 9 eine Vorgabe 10, wann er auf das gesicherte Objekt "A" zugreifen muss. In diesem Beispiel lautet die Objektkennung 12345678, die Berechtigungszeit 12.15 Uhr und die Berechtigtenkennung 02. Der Berechtigte 9 gibt den verschlüsselten Code 6 in die Kontrollvorrichtung 3 des gesicherten Objektes "A" ein, welches in diesem Ausführungsbeispiel ein Geldautomat 1 ist.

[0041] Der Code 6 ist in diesem Ausführungsbeispiel zehnstellig, wobei auch mehr- oder wenigerstellige Codes denkbar sind. Die Kontrollvorrichtung 3 entschlüsselt den eingegebenen Code 16 und prüft die im Code 16 enthaltenen Parameter Objektkennung, Berechtigungszeit und Berechtigtenkennung.

[0042] Die der Kontrollvorrichtung 3 vorgegebene Objektkennung 11 lautet 12345678 und stimmt daher mit der eingegebenen Objektkennung überein. Die Uhrzeit,

zu der der Code 6 in die Kontrollvorrichtung eingegeben worden ist, wird von der Kontrollvorrichtung 3 mit 12.15 Uhr ermittelt und stimmt daher auch mit der Berechtigungszeit überein. Als letzter Parameter wird die Berechtigtenkennung des eingegebenen Codes 16 anhand einer der Kontrollvorrichtung vorgegebenen Berechtigtenkennung 17 verglichen. Auch die eingegebene Berechtigtenkennung stimmt mit der der Kontrollvorrichtung vorgegebenen Berechtigtenkennung 17 überein. Alle drei Codeparameter sind korrekt und die Kontrollvorrichtung 3 öffnet das Schloss 13 des Geldautomaten 1.

[0043] Gleichzeitig übermittelt die Kontrollvorrichtung 3 der Benutzerrechteverwaltung 5 mit einer Rückmeldung 19, dass der Berechtigte 9 um 12.15 Uhr Zugriff auf den Geldautomaten 1 hatte. So ist es der Benutzerrechteverwaltung möglich, online z. B. über eine Standleitung zu ermitteln, welche Berechtigten Zugriff auf den gesicherten Geldautomaten 1 hatten. Die Datenübertragungsvorrichtung kann dabei auch ein Speicher sein, der erst mit einer gewissen Zeitverzögerung z. B. durch einen Servicemitarbeiter ausgelesen wird.

[0044] In Fig. 5 ist ebenfalls in Blockdiagrammdarstellung gezeigt, wie das erfindungsgemäße Verfahren in einer dezentralen Organisationsstruktur ablaufen kann. Bei dieser Ausgestaltungsform vergibt eine Bank 100 wie hier dargestellt zwei Lizenzen 101, 102 an zwei Berechtigte 91 und 92. Mit diesen Lizenzen 101, 102 können sie eine Rechteverwaltung 51 und eine Rechteverwaltung 52 betreiben. Dabei vergibt jeweils die Rechteverwaltung 51 einen Code 61 und die Rechteverwaltung 52 einen Code 62, wobei die Codes in Bezug auf ihre Berechtigungszeit stets unterschiedlich und unbegrenzt sind, aber die Objektkennung und die Berechtigtenkennung fest vorgegeben sind. So enthält Code 61 die Berechtigtenkennung des Berechtigten 91 und die spezifische Objektkennung zum Geldautomaten 1. Die von Rechteverwaltung 52 erstellten Codes 62 enthalten grundsätzlich ebenfalls die Objektkennung für den Geldautomaten 1, aber grundsätzlich die Berechtigtenkennung des Berechtigten 92, und stets veränderliche Berechtigungszeiten. Somit unterscheiden sich die beiden von der Rechteverwaltung 91 und von der Rechteverwaltung 92 erzeugten Codes 61 und 62 stets voneinander.

[0045] Der Berechtigte 93 ist in diesem Ausführungsbeispiel ein Bankangestellter, der zum Beispiel in einer Filiale eine Rechteverwaltung 53 zum Beispiel in Form einer Software auf einem üblichen Computer laufen hat. Da er Angestellter der Bank 100 ist, benötigt er für seine Rechteverwaltung 93 daher keine Lizenz. Die Rechteverwaltung 93 wiederum erstellt in bereits erwähnter Weise einen Code 53, wobei hier die Berechtigtenkennung 93 hinzugefügt wird. Bei dieser Ausführungsform ist es daher möglich, dass die unterschiedlichen Berechtigtenkennungen im Geldautomaten 1 erschiedene Zugriffsebenen öffnen. So kann Code 93 alle Schlösser des Automaten 1 öffnen, während Code 91 nur Zugang zum Geldfach ermöglicht und Code 92 nur Zugang zur Geld-

zählmaschine im aber nicht zu den Geldfächern ermöglicht

[0046] In Fig. 6 ist eine schematische Darstellung der Organisationsstruktur, der an die Rechteverwaltung angeschlossenen Berechtigten dargestellt. Hier übermittelt die Rechteverwaltung 5 per TCP/IP einen Code 61 an eine Serviceagentur 91, den diese mit einem handelsüblichen Browser empfangen kann. Serviceagentur 91 ist dabei eine bundesweite operierende Servicezentrale. Die bundesweite Servicezentrale 91 übermittelt nun ebenfalls über TCP/IP an einen Servicemitarbeiter 95 den Code 65 und den konkreten Auftrag zur Wartung eines Geldautomaten 1. Auf der anderen Seite sind drei Werttransportunternehmen 92, 93, 94 zu erkennen, die alle drei direkt von der Rechteverwaltung einen Code 62, 63, 64 per TCP/IP erhalten.

Patentansprüche

1. Verfahren zur Verwaltung von Benutzerrechten für ein codegesichertes Objekt (1), bei dem ein Code (6) mit einer Objektkennung (7) von einer Benutzerrechteverwaltung (5) erzeugt wird, der einem berechtigten Benutzer (9) für einen Zugriff auf das Objekt (1) übermittelt wird und den der Berechtigte (9) einer Kontrollvorrichtung (3) mitteilt, wobei die Kontrollvorrichtung (3) den Code (6) anhand der ihr vorgegebenen Objektkennung (11) überprüft und bei Vorliegen eines ordnungsgemäßen Codes (6) dem Berechtigten (9) den Zugriff auf das Objekt (1) ermöglicht,
dadurch gekennzeichnet,
dass der von der Benutzerrechteverwaltung (5) erzeugte Code (6) auch eine Berechtigungszeit (8) beinhaltet, so dass die Kontrollvorrichtung (3) die im eingegebenen Code (6) enthaltene Berechtigungszeit (8) anhand einer von der Kontrollvorrichtung (3) ermittelten Zeit (12) überprüft, wobei der Benutzer (9) den Code (6) der Kontrollvorrichtung (3) dann übermitteln muss, wenn die von ihr ermittelte Zeit (12) mit der im Code (6) enthaltenen Berechtigungszeit (8) übereinstimmt.
2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,
dass die im Code (6) enthaltene Berechtigungszeit (8) eine Zeitspanne ist, wobei der Benutzer (9) den Code (6) der Kontrollvorrichtung (3) dann übermitteln muss, wenn die von ihr ermittelte Zeit (12) innerhalb der im Code (6) enthaltenen Berechtigungszeit (8) liegt.
3. Verfahren nach einem der Ansprüche 1 oder 2,
dadurch gekennzeichnet,
dass der Code (6) zusätzlich eine Berechtigtenkennung (14) beinhaltet, und dass die Kontrollvorrichtung (3) einen Berechtigten (9) identifiziert, indem

sie die im eingegeben Code (6) enthaltene Berechtigtenkennung (14) anhand einer ihr vorgegebenen Berechtigtenkennung (17) überprüft.

4. Verfahren nach Anspruch 3,
dadurch gekennzeichnet,
dass die Benutzerrechteverwaltung (5) einem Benutzer (9) nur ein beschränktes Benutzungsrecht für das gesicherte Objekt (1) erteilt, wodurch die Kontrollvorrichtung (3) dem identifizierten Benutzer (9) nur eine ihr vorgegebene beschränkte Benutzung ermöglicht.
5. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass die Berechtigungszeit (8) eine Uhrzeit und/oder ein Datum umfasst.
6. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass die Berechtigungszeit (8) in der Benutzerrechteverwaltung (5) und in der Kontrollvorrichtung (3) anhand zweier gleich eingestellter und gleich laufender Uhren festgelegt und überprüft wird, wobei die Uhren schneller oder langsamer laufen als eine die normale Uhrzeit ermittelnde Uhr.
7. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass der Zugriff eines Berechtigten (9) zusammen mit der Zugriffszeit gespeichert wird, um den Zugriff zu dokumentieren.
8. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass die Benutzerrechteverwaltung (5) per Datenübertragung eine Rückmeldung über einen erfolgten Zugriff auf das gesicherte Objekt (1) erhält.
9. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass die Benutzerrechteverwaltung (5) der Kontrollvorrichtung (3) per Datenübertragung zu kontrollierende Codeparameter ändern und/oder neu vorgeben kann.
10. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass die Kontrollvorrichtung (3) ein Sperrelement (13) eines Bankautomaten (1) ansteuert.
11. Verfahren nach einem der vorhergehenden Ansprüche

che,
dadurchgekennzeichnet,
dass die Benutzerrechte zentral verwaltet werden.

12. Verfahren nach einem der Ansprüche 1 bis 10, 5
dadurchgekennzeichnet,
dass die Benutzerrechte dezentral verwaltet werden.
13. Verfahren nach einem der vorhergehenden Ansprüche 10
che, 10
dadurchgekennzeichnet,
dass die Benutzerrechte unter Berücksichtigung einer Zugriffszeitplanung des Berechtigten vergeben werden. 15

20

25

30

35

40

45

50

55

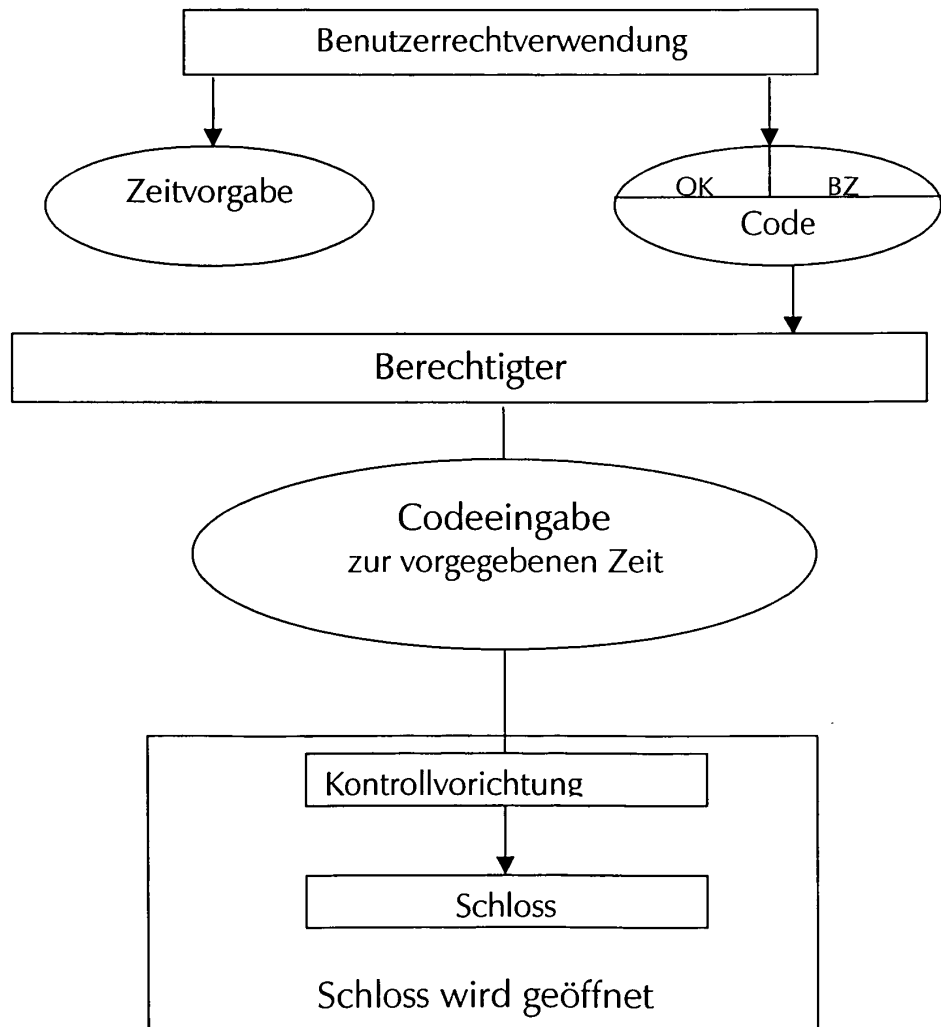
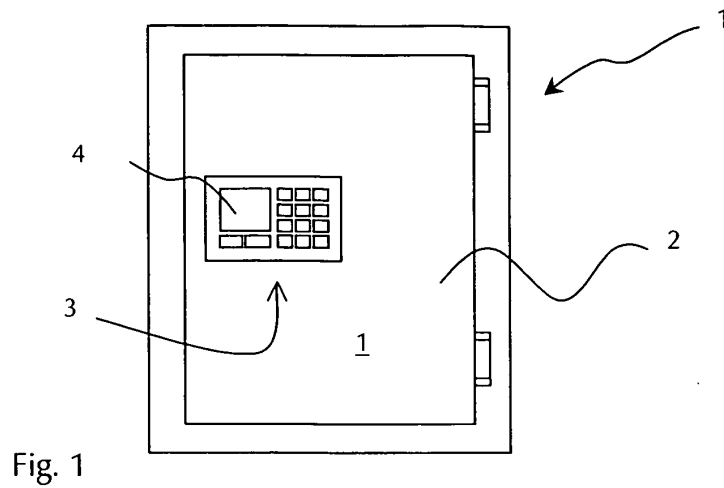


Fig. 2

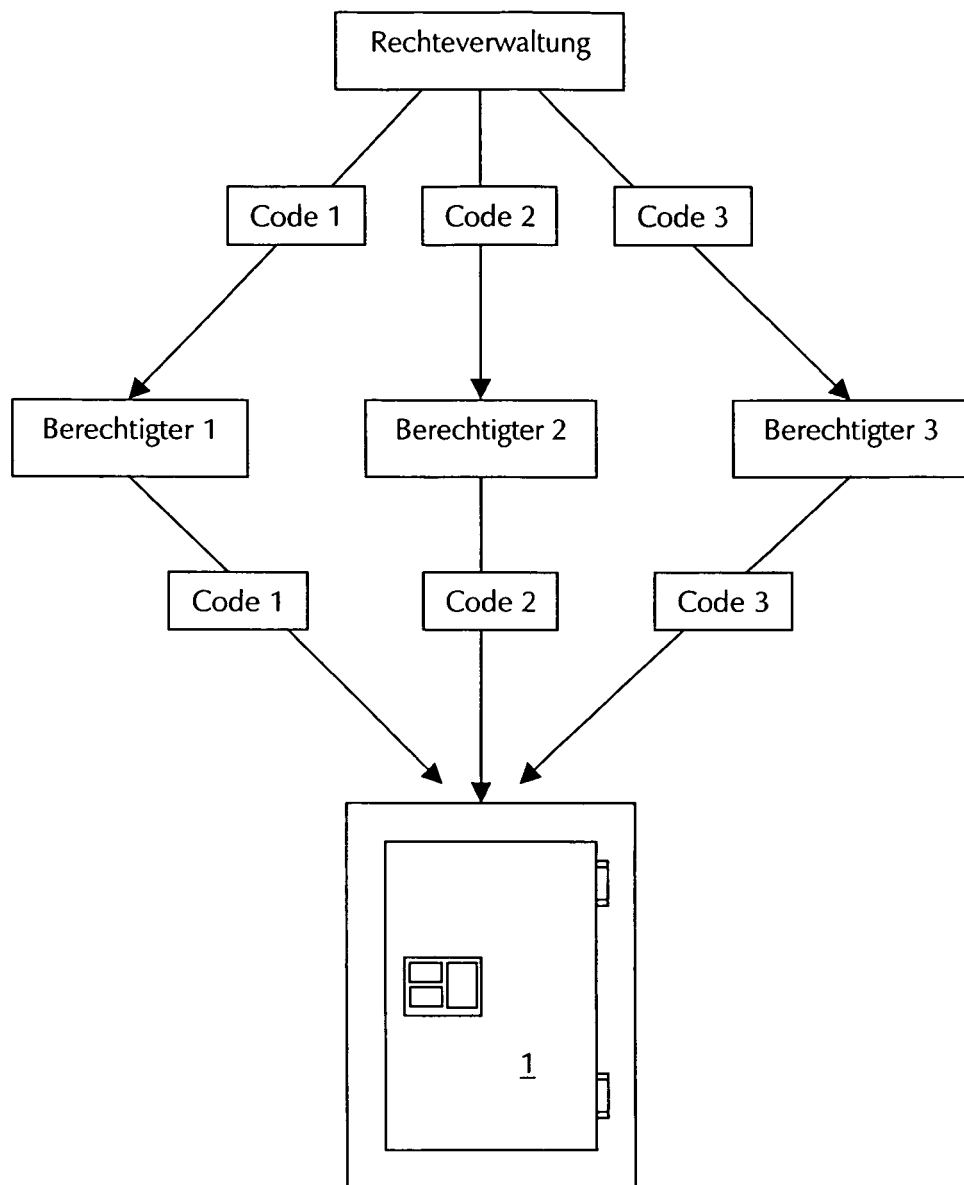


Fig. 3

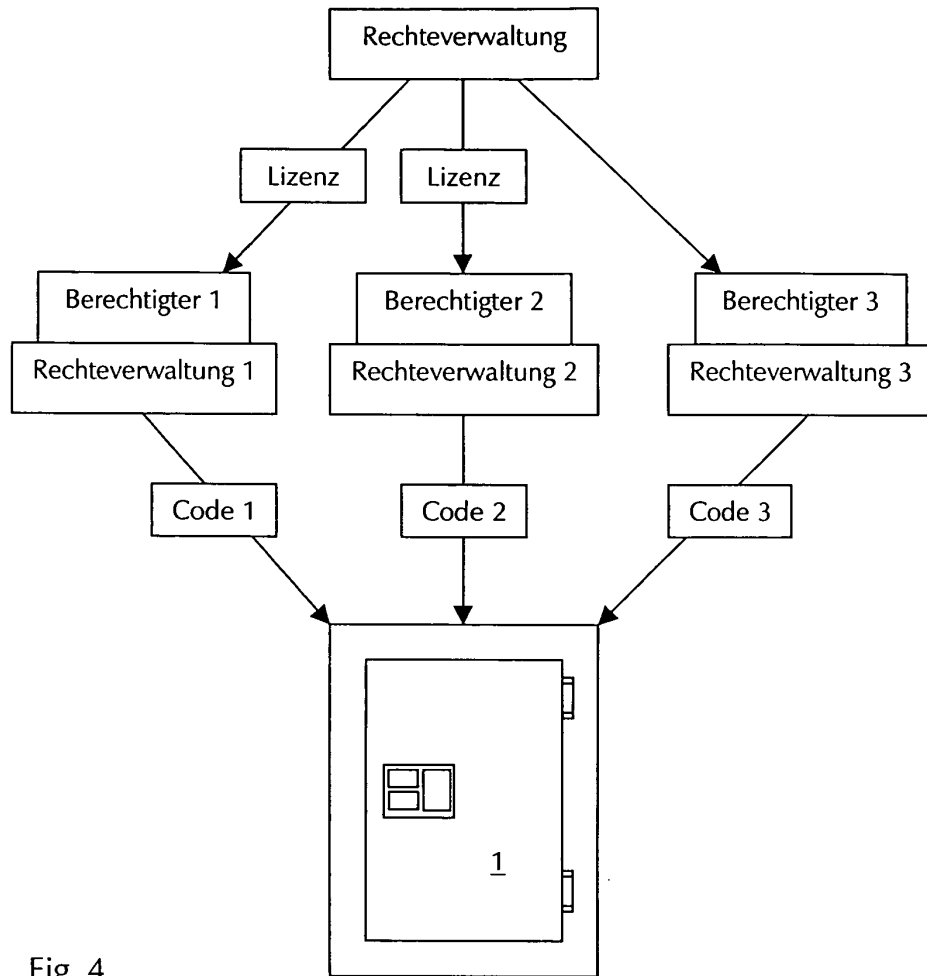


Fig. 4

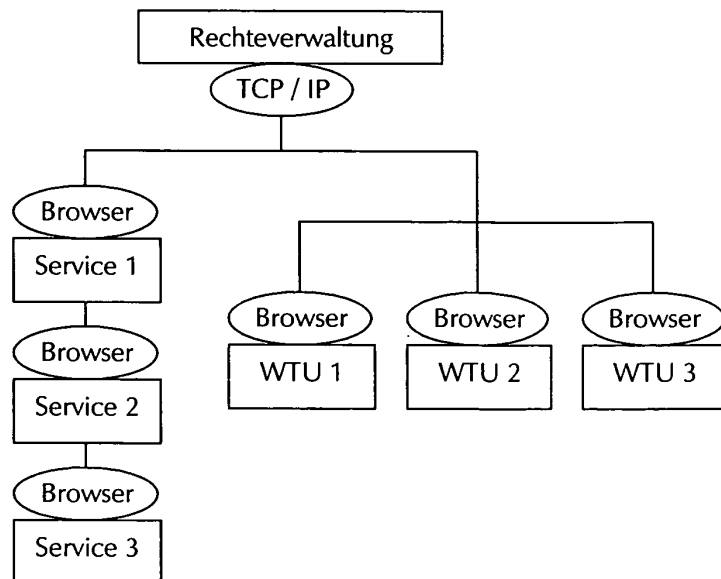


Fig. 5



Europäisches
Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 04 02 5175

EINSCHLÄGIGE DOKUMENTE			
Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.7)
X	FR 2 819 085 A (SAY PATRICK) 5. Juli 2002 (2002-07-05) * Zusammenfassung * * Seite 4, Zeile 11 - Seite 6, Zeile 5 * * Seite 7, Zeile 8 - Seite 12, Zeile 22 * * Abbildungen 1,2 * -----	1-13	G07C9/00
X	WO 02/18733 A (GLOBALOCK CORPORATION LIMITED; NEWBY, ROBERT, MATTHEW; HAMLING, CHRIST) 7. März 2002 (2002-03-07) * Zusammenfassung * * Seite 4, Zeile 11 - Seite 9, Zeile 20 * * Seite 10, Zeile 5 - Seite 18, Zeile 30 * * Abbildungen 1-5 * -----	1-13	
X	US 2003/179075 A1 (GREENMAN HERBERT A) 25. September 2003 (2003-09-25) * Zusammenfassung * * Seite 1, Absatz 8 - Absatz 10 * * Seite 2, Absatz 14 - Absatz 15 * * Seite 2, Absatz 28 - Seite 3, Absatz 30 * * Seite 3, Absatz 35 - Absatz 36 * * Abbildungen 2-5 * -----	1-13	
X	WO 02/08551 A (CODESMART ACCESS SYSTEMS PTY LTD; ROCHFORD, CRAIG, JOHN; MARSHALL, RIC) 31. Januar 2002 (2002-01-31) * Seite 3, Zeile 1 - Zeile 10 * * Seite 4, Zeile 26 - Seite 9, Zeile 16 * * Abbildungen 1-6 * -----	1,2,5, 10-13	
X	US 4 805 722 A (KEATING ET AL) 21. Februar 1989 (1989-02-21) * Zusammenfassung * * Spalte 2, Zeile 8 - Zeile 33 * * Abbildungen 1-3 * ----- -/-	1,2,5, 11-13	
Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt			
Recherchenort Den Haag		Abschlußdatum der Recherche 23. März 2005	Prüfer Van Der Haegen, D
KATEGORIE DER GENANNTEN DOKUMENTE X : von besonderer Bedeutung allein betrachtet Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie A : technologischer Hintergrund O : mündliche Offenbarung P : Zwischenliteratur T : der Erfindung zugrunde liegende Theorien oder Grundsätze E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist D : in der Anmeldung angeführtes Dokument L : aus anderen Gründen angeführtes Dokument & : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument			

1
EPO FORM 1503 03 82 (P04C03)



Europäisches
Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 04 02 5175

EINSCHLÄGIGE DOKUMENTE			
Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.7)
A	WO 93/03246 A (SUPRA PRODUCTS, INC) 18. Februar 1993 (1993-02-18) * Seite 21, Zeile 10 - Zeile 37 * * Seite 46, Zeile 8 - Seite 50, Zeile 9 * -----	1-13	
			RECHERCHIERTE SACHGEBIETE (Int.Cl.7)
Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt			
Recherchenort Den Haag		Abschlußdatum der Recherche 23. März 2005	Prüfer Van Der Haegen, D
KATEGORIE DER GENANNTEN DOKUMENTE X : von besonderer Bedeutung allein betrachtet Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie A : technologischer Hintergrund O : mündliche Offenbarung P : Zwischenliteratur		T : der Erfindung zugrunde liegende Theorien oder Grundsätze E : älteres Patentedokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist D : in der Anmeldung angeführtes Dokument L : aus anderen Gründen angeführtes Dokument & : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument	

1
EPO FORM 1503 03.82 (P04C03)

**ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT
 ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR.**

EP 04 02 5175

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.

Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
 Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

23-03-2005

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
FR 2819085 A	05-07-2002	FR 2819089 A1	05-07-2002
		FR 2819085 A1	05-07-2002
		EP 1350226 A2	08-10-2003
		WO 02054352 A2	11-07-2002
-----		-----	
WO 0218733 A	07-03-2002	AU 9036901 A	13-03-2002
		WO 0218733 A1	07-03-2002
		US 2004103287 A1	27-05-2004
-----		-----	
US 2003179075 A1	25-09-2003	KEINE	
-----		-----	
WO 0208551 A	31-01-2002	WO 0208551 A1	31-01-2002
		AU 7222501 A	05-02-2002
-----		-----	
US 4805722 A	21-02-1989	KEINE	
-----		-----	
WO 9303246 A	18-02-1993	US 5280518 A	18-01-1994
		AU 2271792 A	02-03-1993
		WO 9303246 A1	18-02-1993
-----		-----	

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82