(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 699 019 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
06.09.2006 Patentblatt 2006/36

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

(21) Anmeldenummer: **06004327.0**

(22) Anmeldetag: **03.03.2006**

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

(30) Priorität: **03.03.2005 AT 3702005**

(71) Anmelder: **EVVA Sicherheitssysteme GmbH**
2721 Bad Fischau (AT)

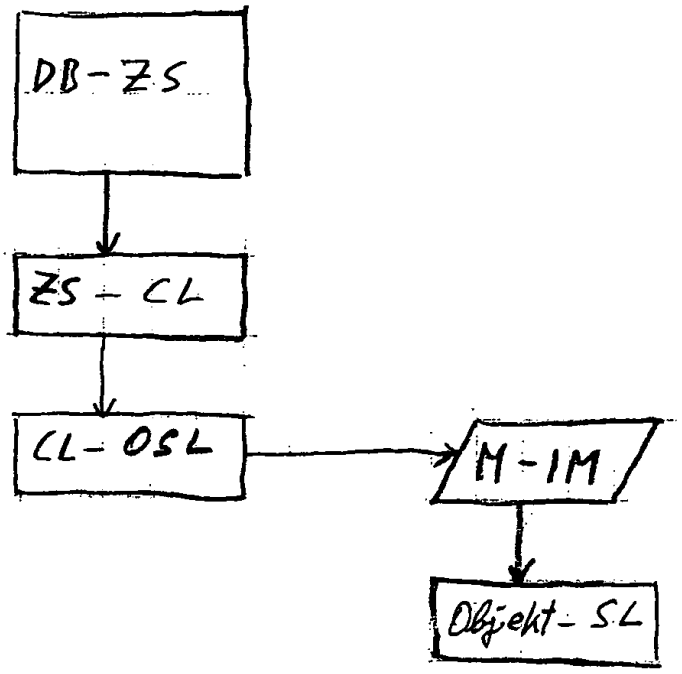
(72) Erfinder: **Zehetner, Peter**
2721 Bad Fischau (AT)

(74) Vertreter: **Puchberger, Peter**
Puchberger, Berger & Partner
Reichsratsstrasse 13
1010 Wien (AT)

(54) Zutrittskontrollanlage

(57) Die Erfindung beschreibt eine Zutrittskontrollanlage mit mindestens einem Datenbankzentralserver (DB-ZS), mindestens einem an DB-ZS angeschlossenen Zentralserver-Client (ZS-CL) mit wenigstens einem Client-Online-Schreib-Lesegerät (CL-OSL), mindestens einem mobilen Ident-Medium (M-IM) und mindestens einem Objekt-Schreib-Lesegerät (Objekt-SL) in Verbindung mit einem Objekt-Verschlusssystem.

Fig. 1



EP 1 699 019 A2

Beschreibung

[0001] Die Erfindung betrifft eine Zutrittskontrollanlage. Derartige Anlagen dienen beispielsweise der Kontrolle und dem Betätigen von Stiegenhauszugängen.

[0002] Ein Großteil der Stiegenhauszugängen in Wohnhäusern mit zentralem Zugang sind mit einem Schloss ausgerüstet, welches für alle solche Zugänge gleich sperrend ist und mit einem sogenannten BEGEH- oder BG-Schlüssel gesperrt werden kann. Diese BG-Schlösser sind im Tableau der Gegensprechanlage oder in deren unmittelbaren Nähe installiert bzw. eingebaut. Diese für alle Zugänge gleichen Schlösser und Schlüssel dienen beispielsweise dazu, den Postzustellern der Post aber auch anderen Personengruppen einen einfach zu bedienenden Zutritt zu den Stiegenhäusern und den Brieffächern, die sich meist innerhalb der Stiegenhäuser befinden, zu bieten.

[0003] Die BG-Schlösser weisen üblicherweise an der Rückseite einen elektrischen Kontakt auf der durch Drehen des Schlüssels ausgelöst wird und den elektrischen Türöffner betätigt, der Bestandteil der Gegensprechanlage des Wohnhauses ist. Die BG-Schlösser und die zugehörigen Schlüssel sind von relativ einfacher Bauart und unterliegen keinem Patentschutz. Ein Problem liegt darin, dass BG-Schlüssel nicht nur im Besitz der autorisierten Postzusteller sind, sondern auch im Besitz von vielen anderen unerwünschten Personenkreisen, darunter auch Kriminellen, die sich so unerlaubten Zutritt zu den Häusern verschaffen können. Die autorisierten Personen sind nicht bloß Postbedienstete, sondern können auch anderen Personenkreisen wie z. B. Handwerker, Rauchfangkehrer, etc sein.

[0004] Weiters ist es bekannt, Zutrittskontrollanlagen vorzusehen, bei denen die Türschlösser der Anlage über ein Datennetzwerk mit einem Zentralrechner verbunden sind. Eine solche Anlage ist jedoch in der Praxis nur in einem zusammengehörigen Baukomplex wie z. B. Hotel möglich. Ein Nachrüsten vieler Gebäude mit vielen Schlössern ist in der Praxis nicht durchführbar.

[0005] Aufgabe der vorliegenden Erfindung ist es, eine Zutrittskontrollanlage vorzusehen, bei der der Zutritt und die Schlüssel und Schlösser besser kontrollierbar sind. Das Sperren von Schlüsseln für einzelne Objekte oder Objektgruppen soll möglich sein. Die Zutritte für die Objektgruppen sollen durch die Eigentümer oder Verwalter der Objekte selbst verwaltet werden können, wobei aber dennoch übergreifende Sperrungen von Personenkreisen wie Postzustellern, Rauchfangkehrer, Energieversorger, Feuerwehr etc möglich sein müssen. Aber auch bei den systemübergreifenden Sperrautorisierungen sollen Beschränkungen möglich sein, sodass z. B. ein Briefträger nur einen Schlüssel für sein Rayon in Händen hält, unabhängig davon, welche Eigentümer hinter dem zu sperrenden Haus stehen.

[0006] Weiters soll die Zutrittskontrollanlage unabhängig von der sonstigen Schließanlage für die Hausbewohner sein. Diese sollen den zentralen Hauszugang weiterhin über die zentrale mechanische Schließanlage oder über das Zentralschloss im Hausportal schließen. Bei all diesen gewünschten Vorteilen soll aber vermieden werden, dass die Schlösser online über ein Datennetz mit einem Zentralrechner verbunden sein müssen.

[0007] Die erfindungsgemäße Zutrittskontrollanlage weist mindestens einen Datenbankzentralserver DB-ZS, mindestens einen daran angeschlossenen Zentralserver-Client ZS-CL mit wenigstens einem Client-Lese-Schreiber CL-LS, mindestens ein mobiles Ident-Medium M-EM und mindestens einen Objektleseschreiber O-LS in Verbindung mit einem Objektschloss auf.

[0008] Weitere vorteilhafte Merkmale sind den Patentansprüchen, der nachfolgenden Beschreibung und den Zeichnungen zu entnehmen.

[0009] Wesentlicher Bestandteil der Erfindung ist, dass jedes Objektschloss, also jedes Haustor, einen Objekt-Lese-Schreiber O-LS aufweist, der mit einem mobilen Ident-Medium M-IM zusammenarbeitet. Das M-IM weist in bevorzugter Weise einen Microchip mit entsprechenden Speicher- und Verrechnungsmodulen auf. Bevorzugt weist das M-IM keine eigene Batterie auf, sondern wird bei Annäherung oder bei Kontakt mit dem O-LS von diesem gelesen. Die Datenübertragung ist in beiden Richtungen möglich, nämlich vom O-LS zum M-IM und umgekehrt. Dies bedeutet, dass Informationen des O-LS im M-IM gespeichert werden können und im Gegenzug lassen sich Informationen des M-IM auf den O-LS übertragen. Eine Online-Anbindung der Objekt-Schreib-Lesegeräte ist nicht erforderlich.

[0010] Ein weiteres wesentliches Merkmal ist ein Datenbankzentralserver DB-ZS, der alle notwendigen Zutrittsdaten für die gesamte Anlage also im wesentlichen den Schließplan gespeichert hat. An dem Datenbankzentralserver hängt mindestens ein Zentralserver-Client ZS-CL, wobei in einer Minimalversion der DB-ZS und ZS-CL ein einziger Computer sein können. Üblicherweise wird aber die erfindungsgemäße Anlage nur für einen größeren Anwendungsbereich sinnvoll sein, sodass mehrere Zentralserver-Clients über entsprechende Datenleitungen an einem Datenbankzentralserver angeschlossen sind. Beispielsweise wird es sinnvoll sein, für den Bereich Wien an jeder Postverteilerstelle einen Client anzuordnen. Weitere Clients können beispielsweise bei Hausverwaltungen, Wohnungsgenossenschaften und dergleichen stehen, damit auch diese Verwalter von mehreren Wohnobjekten in das Anlagensystem eingreifen können.

[0011] Von wesentlicher Bedeutung für den organisatorischen Ablauf ist die Anordnung der Benutzerclients bei der Post, die an jeder Postverteilerstelle mit wenigstens einem Client-Lese-Schreiber versehen ist. Jeder Postbote erhält ein mobiles Ident-Medium, welches durch den Client-Lese-Schreiber mit den erforderlichen Daten aufgeladen wird. Somit kann der Postbote durch sein mobiles Ident-Medium täglich neu für den Zutritt zu den Wohnhäusern seines Rayons autorisiert werden. Der Zutritt zu Wohnhäusern außerhalb des Rayons ist ihm dabei verwehrt. Wenn das mobile

Ident-Medium verloren geht, verliert der Schlüssel am nächsten Tag seine Gültigkeit, sodass das Medium nicht unbefugt verwendet werden kann.

[0012] Weiters kann das mobile Ident-Medium des Postboten dazu verwendet werden, die Identifikationsdaten den Objektleseschreibern der einzelnen Häuser zu übergeben, sodass auch nach einiger Zeit nachvollzogen werden kann, durch welches Ident-Medium eine Öffnung des Haustores erfolgt ist. Durch das mobile Ident-Medium können auch beliebige andere Informationen gezielt an einzelne Objekt-Lese-Schreiber übermittelt werden wie z. B. die Sperre eines bestimmten anderen mobilen Ident-Mediums z. B. von einem Handwerker, der sein Ident-Medium verloren hat.

[0013] Wenn also von dem Träger eines übergeordneten mobilen Ident-Mediums, nämlich vom Postboten, täglich jedes Haustor seines Rayons abgegangen und die Information aus seinem Ident-Medium an die jeweiligen Objekt-Lese-Schreiber übergeben wurde und gegebenenfalls Rückmeldungen auf seinem Ident-Medium gespeichert hat, kann das gesamte Zutrittskontrollsystem täglich mit allen Informationen versorgt werden und es ist nicht nötig, diese Informationsübertragung mit teuren Funkanlagen oder on-line Verkabelungen vorzunehmen.

[0014] Andere Zentralserver-Clients sind Anschlüsse z. B. professioneller Hausverwaltungen, die Zutrittsberechtigungen für die eigenen Mitarbeiter und andere Professionisten selbständig vergeben können. Beispielsweise kann dem Hauselektriker für ein bestimmtes Haus oder eine Häusergruppe für den geplanten Zeitraum die allgemeine Zutrittsberechtigung gegeben werden, die nach Ablauf der voreingestellten Zeit wieder abläuft. Bei Verlust des Ident-Mediums kann die Zugangsberechtigung schon einen Tag später gelöscht werden. Alle diese notwendigen Datenflüsse gehen über den Datenbankzentralserver, an dem alle Zentralserver-Clients einschließlich jenem der Post angeschlossen sind. Die Identmedien können bevorzugt auch zeitprotokolliert Informationen speichern und eine Kontrolle bieten, wer wann ein Tor auf diesem Weg geöffnet hat.

[0015] Die Identmedien der Postbeamten dienen als Datenübermittlungsträger nicht nur in Richtung zu den einzelnen Objekten, sondern auch in Gegenrichtung zum Datenbankzentralserver. Dazu wird lediglich das mobile Ident-Medium des Postbeamten an den Client-Lese-Schreiber der Poststation angelegt und der Dateninhalt abgelesen. Somit können alle protokollierten Vorgänge und übermittelten Informationen an den Zentralserver geliefert werden, der daraufhin die notwendigen Maßnahmen trifft.

[0016] Die dargestellten Beispiele sollen die Erfindung nicht einschränken. Die Zutrittskontrollanlage muss nicht mit dem Haustor enden, auch innerhalb der Häuser oder Hausanlagen können allgemein zugängliche Verschlussräume vorhanden sein, z. B. können durch die mobilen Identmedien des Postbeamten auch die Postfächer geöffnet werden und gemäß Erfindung kann sichergestellt sein, dass nicht andere Benutzerkreise wie Handwerker mit ihren Identmedien ebenfalls diese Zutrittsberechtigung haben. Wenn oben von Postverteilstellen und Postbeamten gesprochen wird, dann ist dies nicht einschränkend, sondern nur beispielsweise. Zum Transport des Ident-Mediums eignen sich alle Personengruppen, die mit der erforderlichen Frequenz von zentralen Stellen aus zu den Objekten wie Haustore gelangen.

[0017] Die Fig. 1 und 2 veranschaulichen schematisch zwei Beispiele für erfindungsgemäße Zutrittskontrollanlagen.

[0018] Die Fig. 1 zeigt eine Minimalversion der Anlage. Der Datenbankzentralserver DB-ZS steht über dem Zentralserverclient ZS-CL mit einem Client-Lese-Schreiber CL-LS online in Verbindung. Die Verbindung kann z. B. über Internet VPN-Tunnels erfolgen. Die für das mobile Ident-Medium M-IM bestimmten Daten werden bei Bedarf vom CL-LS übertragen und im Speicherchip des M-IM gespeichert. Die Datenübertragung erfolgt auf bekannte Weise z. B. induktiv oder über Kontakte, wenn der M-IM auf den CL-LS aufgelegt wird. Der M-IM ist tragbar und kann auf Art eines Schlüssels getragen und verwendet werden. Wie eingangs beschrieben kann der Träger des M-IM beispielsweise ein Postbeamter oder ein Angestellter der Hausverwaltung, oder eine sonstige Benutzerperson sein. Der Objekt-Lese-Schreiber O-LS befindet sich fix eingebaut in einem Objekt wie z. B. im Hauseingang eines Wohnhauses an der Türsprechanlage. Die Bedienperson bringt seine M-IM am O-LS in Kontakt oder in entsprechende Lese-Schreib-Stellung und übergibt seine Daten an den O-LS.

[0019] Auf umgekehrten Wege können vorhandene Daten des O-LS auch an den M-IM übergeben werden, und wenn durch die Bedienperson der M-IM wieder zum CL-LS getragen wird, können die zurückerhaltenen Informationen wieder über den ZS-CL zum DB-ZS übertragen werden, sodass die darin verarbeiteten neuen Informationen die Datenbank updaten und somit auf den letzten Stand bringen.

[0020] Die Fig. 2 zeigt eine größere erfindungsgemäße Anlage mit angeschlossenen drei Zentralserverclients und jeweils angeschlossenen Client-Lese-Schreiber. Der Client 1 ist beispielsweise eine erste Hausverwaltung. Der Client 2 eine zweite Hausverwaltung und der Client 3 steht bei einer Postverteilerstelle.

[0021] Dem Client 1 ist ein mobiles Ident-Medium M-IM 1 zugeordnet. In gleicher Weise sind dem Client 2 ein M-IM 2 und dem Client 3 ein mobiles Ident-Medium M-IM 3 zugeordnet.

[0022] Die erste Hausverwaltung verwaltet über den Client 1 drei Objekte also drei Häuser mit den Bezeichnungen CL1-01-LS bis CL1-03-LS. Auch die zweite Hausverwaltung verwaltet über ZS-CL2 drei Objekte, nämlich CL2-01-LS bis CL2-03-LS.

[0023] Wie dem Datenflussschema zu entnehmen ist, kann die erste Hausverwaltung über das mobile Ident-Medium M-IM 1 auf die zugehörigen drei Objekte direkt zugreifen und entsprechende Informationen austauschen. Gleiches gilt auch für die zweite Hausverwaltung mit Hilfe des mobilen Ident-Mediums M-IM 2.

[0024] Das der Postverteilerstelle zugeordnete mobile Ident-Medium M-IM 3 greift auf sämtliche Objekte zu und kann sowohl Daten auf die jeweiligen Leser-Schreiber übertragen als auch Daten dieser Objekte speichern und über den Client Leser-Schreiber CL3-LS die Daten zentral an den Datenbankzentralserver DB-ZS übertragen.

[0025] Bei diesem System stellt das mobile Ident-Medium M-IM 3 ein übergeordnetes M-IM 3 dar, weil damit der Datenfluss zwischen sämtlichen Objekten zum Datenbankzentralserver herstellbar ist. Dem gegenüber sind die beiden anderen mobilen Identmedien M-IM 1 und M-IM 2 untergeordnet, da sie nur für die jeweiligen zugehörigen Objekte verwendbar sind.

[0026] Durch die Anordnung und entsprechende Programmierung weiterer mobiler Ident-Medien kann eine beliebige Auswahl der Zutrittsberechtigung getroffen werden, so kann z. B. ein für einen Installateur bestimmtes mobiles Ident-Medium den Zutritt nur zu dem Objekt CL1-03-LS gewähren. Alle denkbaren Berechtigungsmodalitäten sind frei wählbar und einstellbar. Die programmtechnische Umsetzung ist bereits Stand der Technik und liegt im Belieben des Fachmannes. Die bekannten Informationstechnologien bieten dafür viele Beispiele. Weiter ist die Erfindung auch auf andere Verteiler- und Logistiksysteme anwendbar, wie z. B. Logistik-Behälter, Schließfächer etc.

[0027] Der Objekt-Lese-Schreiber kann durch ein Programmiergerät die Grundprogrammierung erhalten, womit er in das bestehende System eingebunden wird. Mit diesem Programmiergerät können aber auch die in Objekt-Lese-Schreiber O-LS gespeicherten Bewegungsdaten ausgelesen werden. Damit lässt sich ein lückenloses historisches Protokoll anfertigen.

Patentansprüche

1. Zutrittskontrollanlage mit mindestens einem Datenbankzentralserver (DB-ZS), mindestens einem an DB-ZS angeschlossenen Zentralserver-Client (ZS-CL) mit wenigstens einem Client-Lese-Schreiber (CL-LS), mindestens einem mobilen Ident-Medium (M-IM) und mindestens einem Objekt-Lese-Schreiber (O-LS) in Verbindung mit einem Objekt-Schloss.

2. Zutrittskontrollanlage nach Anspruch 1, **dadurch gekennzeichnet, dass** der DB-ZS alle Zutrittsdaten für alle Objekt-Schlösser und alle Informationsdaten für alle CL-LS und M-IM enthält.

3. Zutrittskontrollanlage nach Anspruch 1, **dadurch gekennzeichnet, dass** die Zutrittsdaten für die Objekt-Schlösser und die Informationsdaten für die CL-LS und M-IM auf den DB-ZS und ein oder mehrere ZS-CL aufgeteilt sind.

4. Zutrittskontrollanlage nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet, dass** das M-IM zur gegenseitigen Datenübertragung mit dem O-LS eingerichtet ist.

5. Zutrittskontrollanlage nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet, dass** eine Mehrzahl von mobilen Ident-Medien (M-IM) vorgesehen sind, die zur Übertragung und Speicherung von Daten eingerichtet sind, wobei wenigstens eines der M-IM als übergeordnetes M-IM für sämtliche Client-Objekt-Lese-Schreiber (CL-O-LS) der Anlage autorisiert ist.

6. Zutrittskontrollanlage nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet, dass** die Zutrittsberechtigung zeitgesteuert ist.

7. Zutrittskontrollanlage nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet, dass** das mobile Ident-Medium (M-IM) ein tragbarer Datenspeicher ist.

8. Zutrittskontrollanlage nach einem der Ansprüche 1 bis 7, **dadurch gekennzeichnet, dass** die Objekt-Schreib-Lesegeräte (Objekt-SL) gegenüber dem Client-Online-Schreib-Lesegerät (CL-OSL) und dem Datenbankzentralserver (DB-ZS) Offline sind und ihre Information oder Informationsänderung über das Ident-Medium entnehmen oder auf dieses übertragen.

Fig. 1

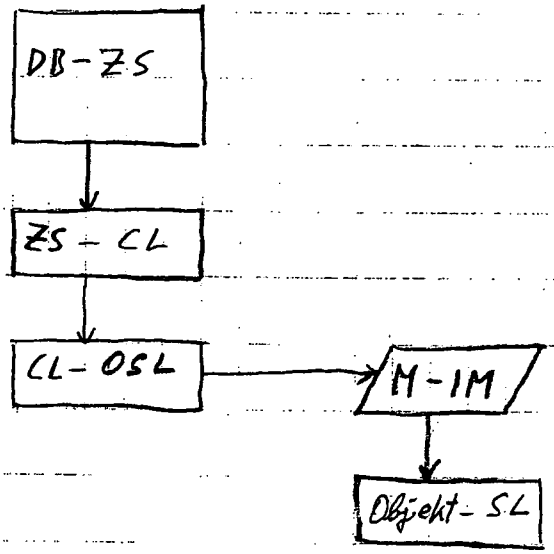
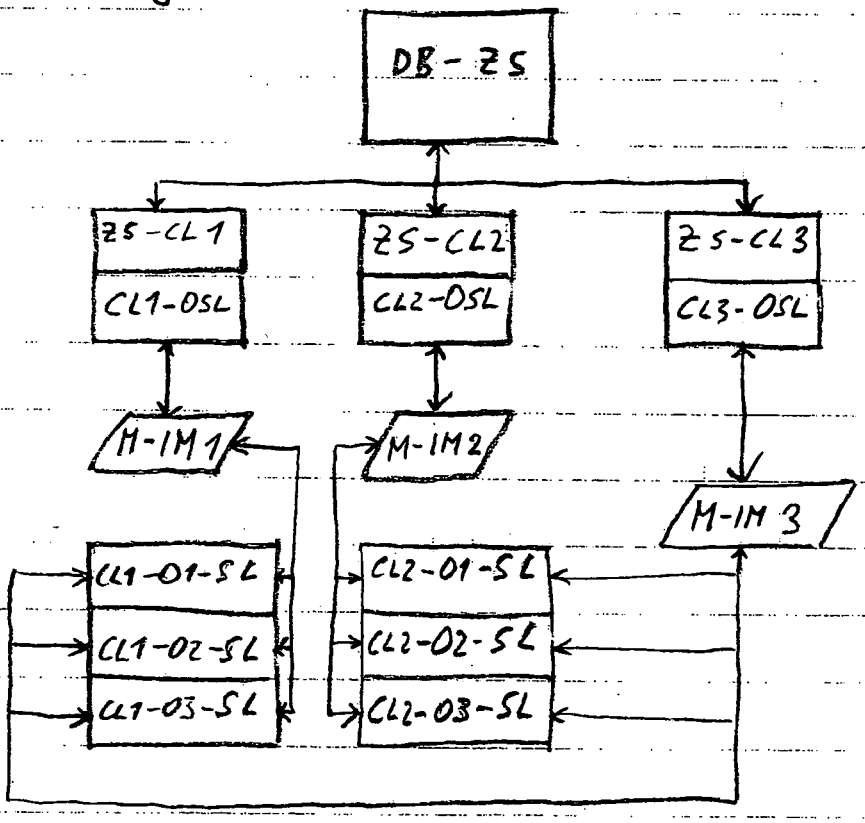

DB-ZS
ZS-CL
CL-OSL
M-IM
Objekt-SL

Fig 2


DB-ZS
ZS-CL1
CL1-OSL
ZS-CL2
CL2-OSL
ZS-CL3
CL3-OSL
M-IM1
M-IM2
M-IM3
CL1-01-SL
CL1-02-SL
CL1-03-SL
CL2-01-SL
CL2-02-SL
CL2-03-SL