



(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
27.11.2002 Patentblatt 2002/48

(51) Int Cl.7: **E05B 49/00**, G07C 9/00,
E05B 43/00

(21) Anmeldenummer: **02011312.2**

(22) Anmeldetag: **23.05.2002**

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

(71) Anmelder: **BURG-WÄCHTER KG**
58540 Meinerzhagen -Valbert (DE)

(72) Erfinder:
• **Der Erfinder hat auf seine Nennung verzichtet.**

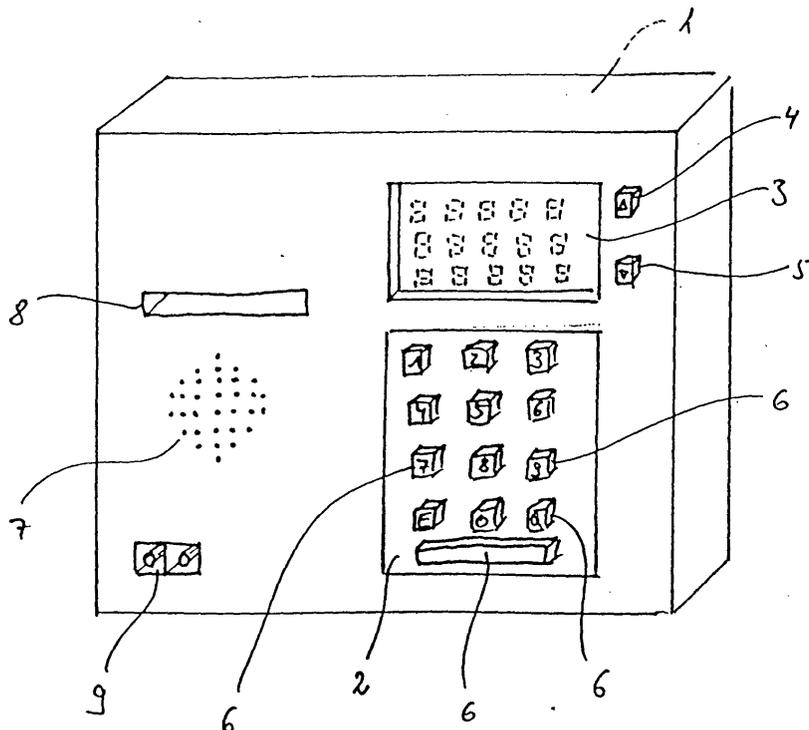
(30) Priorität: **23.05.2001 DE 10125502**
25.05.2001 DE 10125866
30.05.2001 DE 10126235
09.06.2001 DE 10128146

(74) Vertreter: **Wanischeck-Bergmann, Axel**
Köhne & Wanischeck-Bergmann & Schwarz,
Rondorfer Strasse 5a
50968 Köln (DE)

(54) **Verfahren zur Steuerung eines elektronischen Schlosses**

(57) Die Erfindung betrifft ein Verfahren zur Steuerung eines elektronischen Schlosses, bei dem das Schloss über ein Eingabeelement zumindest hinsichtlich des Öffnens und Schließens gesteuert wird, indem Daten, beispielsweise ein Zugangsberechtigungscode eingegeben und mit einem abgespeicherten Code verglichen werden, bevor das Schloss geöffnet oder geschlossen wird. Um ein Verfahren zur Steuerung eines Schlosses derart weiterzubilden, dass das Schloss in

einfacher Weise auf die Anforderungen des Anwenders eingestellt werden kann, ohne dass eine Einzelfertigung der entsprechenden Schlösser erforderlich ist, ist vorgesehen, dass optionale Funktionen des Schlosses, wie beispielsweise zeitliche Zugangsberechtigungen, personenbezogene Zugangsberechtigungen, Öffnungsverzögerungen oder dergleichen nach Eingabe eines Berechtigungscode aktiviert oder deaktiviert werden.



Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Steuerung eines elektronischen Schlosses, bei dem das Schloss über ein Eingabeelement zumindest hinsichtlich des Öffnens und Schließens gesteuert wird, indem Daten, beispielsweise ein Zugangsberechtigungscode eingegeben und mit einem abgespeicherten Code verglichen werden, bevor das Schloss geöffnet oder geschlossen wird.

[0002] Elektronische Schlösser, insbesondere elektronische Türschlösser sind aus dem Stand der Technik bekannt. Beispielsweise offenbart die DE 196 03 200 C2 ein elektronisches Türschloss für Einsteckschlösser, das einen Türinnenbeschlag mit einem Drehknopf, einen Türaußenbeschlag mit einer Einheit für die Eingabe eines Codes sowie mit einem Drehknopf, und eine innenliegende, mit der Eingabeeinheit elektrisch verbundene Elektronik aufweist, in der ein Code gespeichert und über die der Drehknopf im Türaußenbeschlag bei Übereinstimmung des gespeicherten Codes mit dem eingegebenen Code entsperrt ist. Bei diesem vorbekannten elektronischen Türschloss, das sich insgesamt bewährt hat, ist vorgesehen, dass als Eingabeeinheit für den Code ein Tastenfeld verwendet ist und dass die Drehknöpfe jeweils an der Außen- und Innenseite der Tür zusammen mit dem als Adapter ausgebildeten Schließwerk auf einer Achse liegen.

[0003] Weiterhin ist aus der US 5 040 391 ein elektronisches Türschloss bekannt, bei dem als Einheit für die Eingabe des Codes eine Codekarte verwendet wird. Die Steuerungselektronik ist außen auf der Codekarte vorgesehen. Diese Ausführung genügt elektrisch nicht den Anforderungen für den Einbruchschutz im Schlossbereich. Hierbei ist zu berücksichtigen, dass elektronische Türschlösser der genannten Art dazu dienen, den Einbruchschutz im Schloßbereich zu erhöhen. Ohne Eingabe des mit dem gespeicherten Code übereinstimmenden Codes, beispielsweise bei Eingabe einer mit einem Schlüsselgeheimnis nicht übereinstimmenden Ziffernfolge für ein Zahlencodeschloss, ist es nicht möglich, das Schloss von außen gewaltfrei zu öffnen. Die Verwendung eines unbefugt angefertigten Nachschlüssels entfällt grundsätzlich bei derartigen elektronischen Türschlössern. Auch ist es hier in der Regel nicht möglich, den Code zu knacken, da beispielsweise bei einem üblichen zehnziffrigen Tastenfeld als Eingabeeinheit die Variationsmöglichkeiten nahezu unbegrenzt sind. Überdies kann von einem Befugten der Code bei Bedarf geändert werden. Derartige Schlösser sind darüber hinaus auch im Bereich von Sicherheitsschranken, insbesondere bei der Verwendung in Hotels bekannt, bei denen der Hotelgast den Zugangscode ändern kann.

[0004] Aus der WO 00/40829 ist darüber hinaus ein Schließsystem bekannt, welches aus einem Masterschloss und mehreren untergeordneten Schlössern besteht. Über ein codierbares Schlüsselsystem kann das Masterschloss und zumindest ein dem codierten

Schlüssel zugeordnetes Schloss geöffnet werden. Ein derartiges Schließsystem ist beispielsweise sinnvoll im Bereich von Wertschrankanlagen in Geldinstituten einsetzbar, bei denen das Masterschloss mit jedem ausgegebenen Schlüssel geöffnet werden kann, dieser Schlüssel aber nur für die Öffnung eines einzigen untergeordneten Schlosses geeignet ist. Hierdurch erhalten sämtliche Inhaber eines Schlüssels den Zugang in einen Raum mit mehreren Wertfächern, von denen mit jedem Schlüssel aber lediglich eines geöffnet werden kann.

[0005] Ausgehend von dem voranstehend beschriebenen Stand der Technik liegt der Erfindung die Aufgabe zugrunde, ein Verfahren zur Steuerung eines Schlosses derart weiterzubilden, dass das Schloss in einfacher Weise auf die Anforderungen des Anwenders eingestellt werden kann, ohne das eine Einzelfertigung der entsprechenden Schlösser erforderlich ist.

[0006] Die Lösung dieser Aufgabenstellung sieht erfindungsgemäß vor, dass optionale Funktionen des Schlosses, wie beispielsweise zeitliche Zugangsberechtigungen, personenbezogene Zugangsberechtigungen, Öffnungsverzögerungen oder dergleichen nach Eingabe eines Berechtigungscode aktiviert oder deaktiviert werden.

[0007] Durch ein erfindungsgemäßes Verfahren können elektronische Schlösser werksseitig konfiguriert werden, um beispielsweise lediglich die einfachste Funktion des Öffnens und Schließens aufzuweisen. Die individuelle Konfiguration des Schlosses kann dann seitens des Anwenders vorgenommen werden. Beispielsweise kann der Anwender eine Öffnungsverzögerung des Schlosses, eine Alarmcodierung, eine zeitliche Limitierung der Öffnungszeiten oder dergleichen entsprechend seinen Anforderungen programmieren. Hierzu kann der Anwender vom Hersteller eine Zugangsberechtigung anfordern, mit der er die erforderlichen Daten in den Speicher des Schlosses eingeben kann, um das Schloss auf seine individuellen Erfordernisse anzupassen. In der Regel kann der Hersteller für jede zusätzliche individuelle Funktion, die mit einer zusätzlich Programmierung des Schlosses verbunden ist, eine ergänzende Lizenzgebühr in Rechnung stellen, so dass dem Hersteller mit dem erfindungsgemäßen Verfahren auch die Möglichkeit gegeben ist, ein elektronisches Schloss relativ preiswert anzubieten, um einen großen Kundenkreis zu erschließen.

[0008] Neben den voranstehend genannten optionalen Funktionen sind weitere Funktionen möglich, die der Anwender ebenfalls zusätzlich, nämlich optional aktivieren oder deaktivieren kann. Beispielsweise können feste oder bewegliche Feiertage programmiert werden, um ein Öffnen des Schlosses an diesen Tagen zu verhindern, wenn der Zugang zu Schließfächern in einem Tresorraum versperrt bleiben soll. Weiterhin können zusätzliche Zugangsberechtigungen ausgegeben oder gesperrt werden. Der Zugangsberechtigungscode kann beispielsweise auf Magnetstreifenkarten, Transpon-

dem oder Smartkarten gespeichert sein, wobei dem Schloss ein Datensatz übermittelt wird, der die Freischaltung des Schlosses für gespeicherte Zugangsberechtigungen ermöglicht. Es besteht aber auch die Möglichkeit, die entsprechenden Datenträger über ein notwendigerweise im Schloss integriertes Lesegerät zu konfigurieren, sobald die entsprechende optionale Funktion aktiviert ist. Sämtliche optionalen Funktionen können zeitlich befristet sein. Beispielsweise kann mit der Übermittlung eines neuen Datensatzes auch die Freigabe der bisherigen optionalen Funktionen beendet werden, um konkurrierende Datenübermittlungen auszuschließen.

[0009] Mit dem Schloss erhält der Anwender einen individuellen Zugangsberechtigungscode, mit dem das Schloss aktivierbar und im weiteren hinsichtlich seiner Grundfunktionen Öffnen und Schließen betätigbar ist. Der individuelle Zugangsberechtigungscode ist derart im Datenspeicher abgelegt, dass er nicht manipulierbar ist oder eine Manipulation nur nach einer umfangreichen Prüfung einer Manipulationsberechtigung durchgeführt werden kann.

[0010] Um optionale Funktionen zu aktivieren ist es in der Regel vorgesehen, dass der Anwender nach Eingabe seines individuellen Zugangsberechtigungscode einen weiteren, vom Hersteller erhaltenen Code eingibt, der die gewünschte optionale Funktion freigibt. Hierbei wird grundsätzlich nicht die Programmierung, sondern die Konfiguration des Schlosses geändert. Somit ist bei dem erfindungsgemäßen Verfahren zwischen einem Zugangsberechtigungscode und einem Programmiercode zu unterscheiden, wobei es vorteilhaft ist, die Anwendung des Programmiercodes von der richtigen Eingabe des Zugangsberechtigungscode abhängig zu machen.

[0011] Es besteht aber auch die Möglichkeit, die optionalen Funktionen bereits nach Eingabe des Zugangsberechtigungscode aufzurufen und zu aktivieren bzw. zu deaktivieren. Die Konfiguration des elektronischen Schlosses kann dann durch den Anwender ohne vorherige Rücksprache mit dem Hersteller durchgeführt werden.

[0012] Seitens des Herstellers sind die Schlösser mit einer Seriennummer registriert, so dass für jedes Schloss ein individualisierter Programmiercode vorgesehen ist, um die Programmierung bzw. Aktivierung von optionalen Funktionen auf individuelle Schlösser zu begrenzen und Missbrauch hinsichtlich anderer Schlösser zu vermeiden.

[0013] Nach einem weiteren Merkmal der Erfindung ist vorgesehen, dass der Berechtigungscode über das Eingabeelement, beispielsweise eine Tastatur eingegeben wird. Eine Tastatur stellt ein relativ preiswertes Bauelement dar und ermöglicht eine schnelle und einfache Eingabe von Daten. Darüber hinaus ist eine Tastatur Bestandteil üblicher elektronischer Schlösser, um einen Öffnungscode einzugeben. Daher ist es vorteilhaft, die bereits vorhandenen Bauteile für das erfindungsgemä-

ße Verfahren anzuwenden.

[0014] Es hat sich ferner als vorteilhaft erwiesen, den Berechtigungscode über eine Telekommunikationseinrichtung, insbesondere eine Datenleitung oder ein Telefonfunknetz zu übermitteln. Hierzu können sowohl ein Festnetz als auch ein Funknetz zur Datenübermittlung genutzt werden. In einer einfachsten Ausgestaltung ist vorgesehen, dass Daten aus dem Schloss über ein Mehrfrequenzverfahren (MFV-Technik) ausgelesen werden, wie es beispielsweise auch bei Fernabfragen von Anrufbeantwortern üblich ist. Es können auch andere Verfahren verwendet werden. Hierzu generiert das Schloss bei Abruf der Daten eine bestimmte Tonfolge, die akustisch über eine Telekommunikationsleitung an einen Empfänger, beispielsweise den Hersteller und/oder einen mit Programmierung und/oder Wartung derartiger Schlösser betrauten Händler übermittelt wird. Der Empfänger kann anhand der Tonfolge die wesentlichen Daten und Eigenschaften des Schlosses erkennen und im Gegenzug Daten an das Schloss übermitteln. Die Decodierung der übermittelten Tonfolge kann beispielsweise auch durch einen Rechner erfolgen.

[0015] Mit dieser Vorgehensweise ist insbesondere eine Ferndiagnose von Defekten des Schlosses durchführbar. So kann vorgesehen sein, dass das Schloss unterschiedliche Tonfolgen für verschiedene Defekte und/oder Wartungsanforderungen übermittelt werden. Im Gegenzug können dem Anwender verschiedene Codeeingaben übermittelt werden, die der Ausführung von Wartung und/oder der Beseitigung von Defekten dienen. Die Übermittlung der Codeeingabe kann hierbei fernmündlich erfolgen. Es bestehen aber auch die Möglichkeiten einer Datenübertragung über elektronische Medien, beispielsweise in Form eines Emails, einer SMS oder dergleichen. Diese Daten können beispielsweise auch in Form einer Sequenz aus Steuerzeichen direkt in den Datenspeicher des Schlosses übermittelt werden.

[0016] Ist das Schloss direkt an eine Telekommunikationsleitung angeschlossen, so können die notwendigen Codeeingaben direkt in das Schloss übermittelt und über ein Display angezeigt werden. Im Gegenzug können beispielsweise über bestimmte Anbieter von Telefonleitungen vom Hersteller und/oder Vertriebshändler erbrachte Leistungen direkt bei Inanspruchnahme abgerechnet werden.

[0017] Gleiches gilt hinsichtlich der Freigabe zusätzlicher Lizenz für die Nutzung optionaler Funktionen des Schlosses.

[0018] Nach einem weiteren Merkmal der Erfindung ist vorgesehen, dass für jede optionale Funktion ein eigener Berechtigungscode eingegeben wird. Hierdurch ist eine weitergehende Individualisierung des auf den Anwender angepassten Funktionen des Schlosses möglich.

[0019] Bei dem erfindungsgemäßen Verfahren ist weiterhin vorgesehen, dass nach Eingabe des Berechtigungscode die optionale Funktion des Schlosses pro-

grammiert wird. Hierdurch wird sichergestellt, dass eine Programmierung optionaler Funktionen nur durch berechtigte Personen durchgeführt werden kann. Erfolgt die Programmierung über eine Datenleitung, so ist die vorherige Freischaltung der Programmiermöglichkeit durch Eingabe des Berechtigungscode durch eine berechtigte Person erforderlich. Hierdurch wird auch sichergestellt, dass eine Manipulation von außen nicht erfolgen kann. Die berechtigte Person kann beispielsweise auch eine herstellerseitig einen Rechner zur Wartung und/oder Programmierung bedienende Person sein.

[0020] Vorzugsweise wird die erforderliche Vorgehensweise zur Aktivierung oder Deaktivierung einer optionalen Funktion in einem Display des Schlosses angezeigt. Als vorteilhaft hat es sich erwiesen, dem Anwender bei Bedarf einer zusätzlichen Funktion eine Code zu übermitteln, der über die Eingabeeinheit eingegeben wird. Bei zutreffender Eingabe des Codes, der für jedes Schloss individualisiert sein kann, wird der Anwender über das Display angeleitet, um die gewünschte Funktion zu installieren. Für den Hersteller erübrigt sich hierdurch die Bereitstellung umfangreichen Bedienungsanleitungen in verschiedenen Sprachen, da derartige Produkte in der Regel international eingesetzt werden. Im übrigen erleichtert diese Vorgehensweise die Abrechnung der Schlösser unterschiedlicher Konfiguration, so dass dem Anwender ein Schloss angeboten werden kann, das genau auf seine Bedürfnisse angepasst ist. Der Anwender muss daher nicht benötigte, aber bei üblichen Schlössern vorinstallierte Leistungsmerkmale nicht bezahlen.

[0021] Es ist nach einem weiteren Merkmal der Erfindung vorgesehen, dass die Aktivierung oder Deaktivierung von optionalen Funktionen des Schlosses über Menüs angezeigt und/oder gesteuert werden. Hierzu kann beispielsweise ein vierzeiliges Display vorgesehen sein, das über Texte und/oder Pictogramme die erforderliche Vorgehensweise zur Freischaltung optionaler Funktionen leicht verständlich anzeigt. Andere Anzeigeeinrichtungen, wie LEDs sind alternativ oder zusätzlich möglich und können der Darstellung von Buchstaben, Zahlen oder Pictogrammen dienen. Die Verwendung von Pictogrammen hat insbesondere den Vorteil, dass auf eine detaillierte textliche Beschreibung mit den damit verbundenen Problemen verschiedener Sprachen verzichtet werden kann. Aber auch die Verwendung von Textbausteinen ist unproblematisch, da entsprechende Speicherbausteine mit den erforderlichen Texten in einer Vielzahl von Sprachen hergestellt und verwendet werden können, so dass in einem ersten Schritt die gewünschte Sprache ausgewählt wird. Die Auswahl der Sprache kann sowohl seitens des Herstellers, des Händlers als auch seitens des Anwenders durchgeführt werden und stellt beispielsweise eine Verfahrensschritt bei der ersten Inbetriebnahme des Schlosses dar.

[0022] Es ist weiterhin als vorteilhafte Ausgestaltung des erfindungsgemäßen Verfahrens vorgesehen, dass

die Programmierung und/oder Konfiguration des Schlosses über eine optionale Funktion ausgelesen und als insbesondere verschlüsselter Datensatz übermittelt wird. Diese Funktion ist vorzugsweise über Sperrfunktionen abgesichert, so dass nur mit einem bestimmten Code die Programmierung auslesbar ist. Für die Änderung der Programmierung müssen darüberhinaus weitere Sicherungsstufen vorgesehen werden, um unberechtigte Manipulation auszuschließen.

[0023] Vorzugsweise können bestimmte Daten des Schlosses zu Wartungs- und/oder Kontrollzwecken mittels einer optionalen Funktion ausgelesen werden. Eine Übermittlung ergänzender Daten, beispielsweise eines Öffnungscodes wird hierdurch unterbunden. Durch die Eingabe des Codes für die Wartungs- und/oder Kontrollfunktion werden beispielsweise weitere Funktion und/oder Speicherebenen zumindest für einen bestimmten Zeitraum gesperrt. Alternativ kann vorgesehen sein, dass nach einer Wartung des Schlosses eine weitere Programmierung des Schlosses nur nach Eingabe des Zugangsberechtigungscode vorgenommen werden kann. Es werden somit durch die Eingabe des Codes für die optionale Funktion der Wartung und/oder Kontrolle des Schlosses alle weiteren Programmiermöglichkeiten gesperrt, bis durch Eingabe des zutreffenden Zugangsberechtigungscode signalisiert wird, dass der berechtigte Anwender eine Freischaltung aller Programmiermöglichkeiten wünscht. Es wird hierdurch verhindert, dass beispielsweise bei der Wartung des Schlosses Manipulationen ausgeführt werden, die später für einen unberechtigten Öffnungsvorgang oder eine Umprogrammierung des Datensatzes des Schlosses genutzt werden.

[0024] Nach einem weiteren Merkmal ist vorgesehen, dass die Daten bezüglich der Programmierung des Schlosses über eine Telekommunikationseinrichtung, insbesondere eine Datenleitung oder ein Telefonfunknetz übermittelt werden. Neben den Fernwartungsmöglichkeiten wird hierdurch die Möglichkeit eröffnet, das Schloss in einfacher Weise mit aktualisierten Programmversionen zu versehen, ohne dass hierzu eine Wartung vor Ort durch eine Serviceperson durchgeführt oder das Schloss dem Hersteller zur Verfügung gestellt werden muss. Der Anwender kann auf Wunsch jederzeit aktualisierte, gegebenenfalls weitere optionale Funktionen aufweisende Programme erhalten.

[0025] Es ist weiterhin vorgesehen, dass das Schloss über eine Telekommunikationseinrichtung, insbesondere eine Datenleitung oder ein Telefonfunknetz zu Wartungs- und/oder Instandsetzungsarbeiten angesprochen wird.

[0026] Vorzugsweise wird die Programmierung des Schlosses ausgelesen und die Wartung des Schlosses im Gegenzug über eine bidirektionale Datenübermittlung durchgeführt wird. Die Wartung kann hierdurch sehr weitgehend automatisiert werden und beispielsweise über einen beim Hersteller installierten Rechner insoweit erfolgen, dass eine Kommunikation zwischen

dem Schloss und dem Rechner zu einer Diagnose führt, die als Ergebnis die notwendigen Wartungs- bzw. Instandhaltungsarbeiten festlegt und dem Anwender in Form eines einzugebenden Wartungscode übermittelt. Dieser Wartungscode kann beispielsweise nach seiner Eingabe auch die Aufforderung enthalten, eine berechtigtes Wartungsunternehmen zu beauftragen, dem über einen Codeschlüssel die erforderlichen Wartungsarbeiten übermittelt werden.

[0027] Wie bereits ausgeführt kann ergänzend vorgesehen werden, dass die Programmierung des Schlosses über die Telekommunikationseinrichtung durchgeführt wird, wobei insbesondere eine Aktualisierung der Datensätze für den Betrieb des Schlosses durchgeführt wird. Eine Programmierung bzw. Konfiguration kann aber auch über eine Schnittstelle im Schloss vorgesehen sein, an die ein Rechner, beispielsweise ein Laptop, ein Pocket-Computer und/oder ein anderes elektronisches Werkzeug anschließbar ist, um Daten aus dem Schloss auszulesen und/oder in das Schloss einzuspeisen.

[0028] Schließlich ist vorgesehen, dass die Datenübermittlung über einen im Schloss angeordneten GSM-, DECT- o. ä. Baustein oder ein Lesegerät für ein zum Zwecke der Datenübermittlung eingesetzten GSM-, DECT- o. ä. Baustein durchgeführt wird. Bei dieser Weiterbildung des Verfahrens kann jedem Schloss eine Telefonnummer zugeordnet werden, die es ermöglicht, das Schloss unmittelbar anzuwählen, um die notwendigen Daten für eine Wartung und/oder ergänzende Programmierung optionaler Funktionen auszulesen bzw. zu übermitteln. Weist das Schloss ein Lesegerät für GSM-, DECT- o. ä. Chips auf, so kann der berechnigte Anwender eine individualisierte und auf seinen Namen registrierte Telefonnummer verwenden. Der Zugang zum Datensatz des Schlosses ist dann nur möglich, wenn der entsprechende GSM-, DECT- o. ä. Chip eingesetzt und dem Wartungs- und/oder Herstellungsunternehmen die Zugangsnummer bekannt gegeben ist. Es liegt somit in der Hand des berechtigten Anwenders die Zugangsvoraussetzungen für eine Fernwartung und/oder Ergänzung des Datensatzes zu schaffen.

[0029] Vorzugsweise kann der GSM-, DECT- o. ä. Chip nur eingesetzt oder entnommen werden, wenn zuvor der Zugangsberechtigungscode eingegeben wurde. Es hat sich somit als sinnvoll erwiesen, das Lesegerät derart anzuordnen, dass es nur in der geöffneten Stellung des Schlosses zugänglich ist.

[0030] Die optionale Funktion kann auch eine zeitliche Limitierung der Bedienbarkeit des Schlosses vorgesehen. Derartige Schlösser können beispielsweise im Hotelbereich für Zimmertüren eingesetzt werden. Ein Hotelgast erhält gegen Entrichtung des Zimmerpreises einen zeitlich limitierten individuellen Zugangsberechtigungscode, mit dem er die Zimmertür öffnen und ggfs. auch weitere Einrichtungen, wie beispielsweise Minibar und/oder vorausbezahlte Fernsehprogramme (Pay-TV) freischalten und nutzen kann. Nach Ablauf der voraus-

bezahlten Mietzeit wird der individuelle Zugangsberechtigungscode ungültig, so dass eine weitere oder neue Nutzung des Hotelzimmers nur nach Erwerb eines neuen individuellen Zugangsberechtigungscode möglich ist. Bei dieser Anwendung der Erfindung ist eine Fernüberwachung und Wartung des Schlosses besonders vorteilhaft, um beispielsweise eine direkte Abrechnung der mit Bankkarten (Kreditkarten) vorausbezahlten Zimmer vornehmen zu können.

[0031] Weitere Merkmale und Vorteile der Erfindung ergeben sich aus der nachfolgenden Beschreibung der zugehörigen Zeichnung, in der ein Gehäuse eines elektronischen Schlosses dargestellt ist, mit dem das erfindungsgemäße Verfahren durchführbar ist.

[0032] Ein elektronisches Schloss weist ein Gehäuse 1 auf, welches eine numerische Tastatur 2 und ein dreizeiliges Display 3 hat. Neben dem Display 3 sind zwei Taste 4, 5 angeordnet, die der sogenannten "Scroll"-Funktion dienen. Demzufolge dienen die Taste 4, 5 der Aufund Abbewegung eines auf dem Display 3 dargestellten Textes oder dergleichen.

[0033] Die Tastatur 2 weist dreizehn Tasten 6 auf, von denen zehn Tasten zur Eingabe einzelner Ziffern 0 bis 9 dienen. Ferner ist eine Taste 6 mit dem Symbol "E" vorgesehen, über die ein in dem Gehäuse 1 angeordneter und nicht näher dargestellter Datenspeicher aktivierbar, d.h. einschaltbar ist. Ferner ist eine Taste mit der Bezeichnung "Q" vorgesehen, um Befehle in den Speicher bzw. einen zugehörigen, nicht näher dargestellten Mikroprozessor einzugeben. Eine weiterhin vorgesehene, flächenmäßig größere Taste ist im vorliegenden Ausführungsbeispiel nicht belegt, kann aber beispielsweise dazu verwendet werden, dass zuletzt eingegebene Befehle korrigiert oder gelöscht werden.

[0034] Über die Tastatur 2 wird nach Betätigung der Taste 6 mit dem Buchstaben "E" ein Zugangsberechtigungscode eingegeben, der mit dem im Datenspeicher abgelegten Code übereinstimmt. Nach einem Vergleich des eingegebenen Zugangsberechtigungscode mit dem im Datenspeicher abgelegten Code öffnet das nicht näher dargestellte Schloss, wie es beispielsweise in der DE 196 03 200 C2 detailliert beschrieben ist. Hierzu kann eine motorische Öffnung bzw. Verschiebung der Sperrriegel vorgesehen sein. Alternativ besteht die Möglichkeit, dass nach Eingabe des zutreffenden Zugangsberechtigungscode ein akustisches und/oder optisches Signal erscheint, welches dem Anwender signalisiert, dass das Schloss nunmehr durch Betätigung, beispielsweise eines Drehknafs geöffnet werden kann.

[0035] In einfachster Weise ist das Schloss lediglich mit der voranstehend genannten Funktion ausgestattet. Im Datenspeicher sind weitere Funktionen vorgesehen, die vom Anwender optional ausgewählt und aktiviert werden können. Zu diesem Zweck kann über eine Menüsteuerung im Display 3 jede optionale Funktion angezeigt werden. Beispielsweise kann durch zweimaliges Betätigen der Taste "E" die Menüsteuerung aufgerufen werden, wobei beispielsweise im Display die op-

tionale Funktion "Zeitverzögerung" angezeigt wird. Eine solche Zeitverzögerung sieht vor, dass das Schloss erst ein vorbestimmtes Zeitintervall nach Eingabe des Zugangsberechtigungscode öffnet.

[0036] Wird nun in der mittleren Zeile des Displays 3 die optionale Funktion "Zeitverzögerung" angezeigt, so kann der oberen Zeile des Displays 3 das Wort "ja" und in der unteren Zeile das Wort "nein" erscheinen. Mit den Tasten 4 und 5 kann der Anwender nun auswählen, ob er die Funktion "Zeitverzögerung" bei seinem Schloss einstellen möchte. Drückt er zu diesem Zweck die Taste 4 erscheint die Mitteilung, dass sich der Anwender beispielsweise unter Angabe eines bestimmten Codes an den Hersteller des Schlosses oder seinen Vertrieb wenden möge.

[0037] Gibt der Anwender dort den erhaltenen Code an, so erhält er vom Hersteller bzw. Vertrieb einen Berechtigungscode, mit dem die Funktion "Zeitverzögerung" aktivierbar ist. Im Gegenzug bezahlt der Anwender für diese zusätzliche Funktion eine Lizenzgebühr an den Hersteller.

[0038] Wählt der Anwender über die Taste 5 hinsichtlich der optionalen Funktion "Zeitverzögerung" die Antwort "nein", so gelangt er zur nächsten optionalen Funktion, beispielsweise einer Funktion "Alarm", bei der ein Alarm ausgelöst wird, sobald ein bestimmter Code eingegeben wird. Ein solcher Code kann beispielsweise die Eingabe des Zugangsberechtigungscode in umgekehrter Reihenfolge sein.

[0039] Über diese Vorgehensweise kann das elektronische Schloss eine Vielzahl von optionalen Funktionen aufweisen, die seitens des Anwenders hinsichtlich seiner Anforderungen ausgewählt und installiert werden können. Sämtliche optionalen Funktionen sind hierbei in der Ursprungsprogrammierung des Datenspeichers enthalten und können über die voranstehend beschriebene Vorgehensweise aktiviert oder deaktiviert werden.

[0040] Das Schloss weist ferner einen Lautsprecher 7 und/oder ein Kartenlesegerät 8 und/oder einen Anschluß 9 für eine Datenleitung auf, mit der Daten des Datenspeichers über ein Telefonfestnetz übertragen werden können.

[0041] Die voranstehend genannten Bauteile des Schlosses denen insbesondere der Datenübertragung. Zusammen mit dem Kartenlesegerät 8 ist eine Sende- und Empfangseinheit vorgesehen, mit der Daten über ein Telefonfunknetz im GSM-, DECT- o. ä. Standard übermittelt werden können.

[0042] In der einfachsten und damit preisgünstigsten Ausführung des Schlosses ist ein Lautsprecher 7 vorgesehen. Bei dieser Ausführungsform werden Daten aus dem Schloss über ein Mehrfrequenzverfahren (MFV) ausgelesen. Hierzu generiert das Schloss bei Abruf der Daten eine bestimmte Tonfolge, die akustisch über eine Telekommunikationsleitung an einen Empfänger, beispielsweise den Hersteller und/oder einen mit der Programmierung und/oder Wartung derartiger Schlösser betrauten Händler übermittelt wird. Der Emp-

fänger kann anhand der Tonfolge die wesentlichen Daten und Eigenschaften des Schlosses erkennen und im Gegenzug Daten an das Schloss übermitteln. Beispielsweise können auf diese Weise Daten übermittelt werden, die erkennbar machen, wann das Schloss geöffnet und geschlossen wurde. Darüber hinaus können auch Fehler des Schlosses, beispielsweise Tastaturfehler, schwergängige Sperrglieder und/oder Sperrelement, elektrische oder mechanische Fehler, Riegelwerksfehler, Korrosionsschäden, Batterieprobleme, Spannungseinbrüche, Bedienungsfehler, Ureinstellungsfehler oder dergleichen erkannt und im Zuge einer Wartung beseitigt werden. Zu diesem Zweck ist es erforderlich, dass die generierten Töne über den Lautsprecher in eine Telekommunikationseinrichtung, beispielsweise ein Telefon übermittelt werden. Die Auswertung der generierten Töne kann seitens des Empfängers mittels eines Rechners erfolgen, der mittels eines Rechners die übermittelten Daten dekodiert und ein entsprechendes Konzept zur Beseitigung des Fehlers bereitstellt.

[0043] Alternativ zu einer voranstehend beschriebenen Übermittlung der Daten kann eine Datenübermittlung auch über den Anschluß 9 erfolgen. Hierzu wird das Schloss über den Anschluß 9 mit einem Datenkabel mit einem Telekommunikationsnetz, insbesondere einem Festnetz verbunden. Vorteil dieser Ausführungsform ist, dass eine wesentliche zuverlässigere Datenübermittlung erfolgt. Dieser Vorteil kann auch dahingehend genutzt werden, dass ergänzend Daten an den Datenspeicher des Schlosses übermittelt werden, so dass zum einen auch optionale Funktionen über die Datenleitung eingegeben werden können und zum anderen Störungen erkannt und beseitigt werden, soweit diese Störungen nicht durch den Einsatz eines Servicemitarbeiters beseitigt werden müssen.

[0044] Der Anschluß 9 kann aber auch ein Zugang zu einer Schnittstelle des in das Schloss integrierten Prozessors sein. Über diese Schnittstelle können Daten aus dem Schloss ausgelesen und/oder in das Schloss gespeichert werden, um beispielsweise die Art der Nutzung und/oder Wartungsanforderungen festzustellen. Ferner können aktualisierte Programme gespeichert und/oder optionale Funktion freigeschaltet werden.

[0045] Selbstverständlich können die Daten auch über ein Telefonfunknetz übermittelt werden, wobei zum einen der Anschluß 9 zum Anschluß eines üblichen Funktelefons (Handy) genutzt werden kann. Andererseits kann aber bereits im Gehäuse 1 eine entsprechende Sende- und/oder Empfangseinheit angeordnet sein, die entweder eine eigene Chipkarte im GSM-, DECT- o. ä. Modus aufweist oder das Kartenlesegerät hat, in welches der Anwender des Schlosses beispielsweise eine Karte mit einem GSM-, DECT- o. ä. Chip einsteckt. Auf diese Weise kann das Schloss mit einem beim Hersteller installierten Rechner kommunizieren und Daten übermitteln. Entfernt der Anwender die Karte mit dem

GSM-, DECT- o. ä. Chip, so ist ein unberechtigter Zugang durch Anwahl des Schlosses nicht möglich. Um einen unberechtigten Datentransfer über eine nicht dem Anwender zuzuordnende Karte mit GSM-, DECT- o. ä. Chip zu vermeiden kann vorgesehen sein, dass nach Eingeben der Karte mit dem GSM-, DECT- o. ä. Chip zuerst der Zugangsberechtigungscode eingegeben werden muss, bevor die Sende-/Empfangseinheit des Schlosses für den Datenaustausch aktiviert wird.

[0046] Weiterhin kann hierbei auch vorgesehen sein, dass ein Vertriebshändler die Serviceleistungen erbringt und zu diesem Zweck mit einer Chipkarte im GSM-, DECT- o. ä. Modus ausgerüstet ist, mit der er mit dem Rechner des Herstellers in Kontakt treten kann.

[0047] Vorteil des erfindungsgemäßen Verfahrens ist insbesondere, dass derartige elektronische Schlösser werkseitig als Serienprodukt mit immer gleicher Konfiguration hinsichtlich der Leistungsfähigkeit hergestellt werden können. Für optional gewünschte Funktionen besteht dann die Möglichkeit, vom Hersteller ergänzende Lizenzen zu erwerben, so dass die voranstehend beschriebenen Funktionen und weitere Funktionen eines elektronischen Schlosses genutzt werden können. Ein derartiges elektronisches Schloss in einfachster Konfiguration kann demzufolge kostengünstig angeboten werden. Andererseits besteht der Vorteil, dass über ein erfindungsgemäßes Verfahren auch eine Vielzahl von Wartungs- und/oder Instandsetzungsarbeiten ausgeführt werden können, ohne dass hierfür Wartungspersonal vorgehalten werden muss. Die einfache Ausgestaltung des Schlosses mit einer Menüsteuerung ermöglicht es, ein solches Schloss annähernd ohne umfangreiche Bedienungsanleitung bedienen zu können. Unterschiedliche Sprachen, in denen derartige Bedienungsanleitungen bei internationalem Vertrieb vorgehalten werden müssen, können im Datenspeicher abgelegt und seitens des Herstellers oder seines Zentralvertriebs im jeweiligen Land bzw. durch den Anwender aktiviert werden. Ergänzende Informationen können über Datenleitungen in das Display 3 des Gehäuses 1 übermittelt werden.

[0048] Erkennt der im Schloss integrierte Prozessor einen Fehler, beispielsweise eine Verringerung der Batterieleistung, so kann ein derartiger Fehler rechtzeitig im Display 3 angezeigt werden, woraufhin der Anwender entsprechende Informationen zur Beseitigung dieses Fehlers schnell und problemlos über bestimmte Kodierungen mitgeteilt bekommt. Darüber hinaus sind auch sogenannte Notöffnungen seitens des Herstellers möglich, sollte der Zugangsberechtigungscode nicht mehr zur Verfügung stehen.

[0049] Ein erfindungsgemäßes Verfahren kann beispielsweise bei einer Schließanlage mit einer Vielzahl von Schlössern angewendet werden, wobei jedes Schloss den Zugang zu einem Raum verschließt, in dem eine Sende-/Empfangseinheit mit einer Antenne angeordnet ist. Eine derartige Sende-/Empfangseinheit kann beispielsweise für Funktelefonnetze vorgesehen

sein.

[0050] Die Antenne ist über die Sende-/Empfangseinheit mit dem Schloss verbunden, um Daten aus einem Zentralrechner in den Datenspeicher übermitteln zu können. Jedes Schloss ist mit einem jeweils einen Zugangsberechtigungscode aufweisenden Datenträger in Form einer sogenannten Smartkarten zu öffnen. Als optionale Funktion können dem Schloss Daten übermittelt werden, um weitere Zugangsberechtigungen mit weiteren Smartkarten zu ermöglichen. Somit können Wartungen der Sende-/Empfangseinheiten dadurch schnell und zuverlässig durchgeführt werden, dass einer Vielzahl von Wartungsmitarbeitern entsprechende Smartkarten ausgehändigt werden, die den Zugang zu einzelnen Räumen ermöglicht.

[0051] Die Fluktuation der Mitarbeiter und die Sicherheit der Schlösser, beispielsweise bei Verlust und/oder unberechtigter Weitergabe von Smartkarten macht es erforderlich, eine Datenänderung zumindest beim Auftreten entsprechender Vorkommnisse durchzuführen. Hierbei hat es sich als vorteilhaft erwiesen, entsprechende Datenerneuerungen nicht nur Bedarf, sondern regelmäßig, beispielsweise einmal täglich durchzuführen, um neue Zugangsberechtigungen einzulesen oder bestimmten Zugangsberechtigungen zu sperren. Die Datenübermittlung erfolgt in diesem Ausführungsbeispiel über die bereits installierte Sende-/Empfangseinheit und die angebundene Antenne, wobei die Sende-/Empfangseinheit mit dem Schloss über eine Datenleitung verbunden ist.

[0052] Es hat sich als vorteilhaft erwiesen, die Datenerneuerung regelmäßig, beispielsweise zu Zeiten geringer Inanspruchnahme der Sende-/Empfangseinheit durchzuführen, so dass insbesondere die Nachtstunden für dieses Vorgehen geeignet sind. Im Falle eines Defektes der Antenne und/oder der Sende-/Empfangseinheit bleibt die Zugangsberechtigung in ihrem Datensatz vor dem Defekt bestehen, so dass lediglich neue Zugangsberechtigungen und/oder Zugangssperrungen nicht berücksichtigt werden. Die Grundfunktion des Schlosses wird hierdurch aber nicht beeinträchtigt, so dass ein sicheres Öffnen des Schlosses möglich bleibt.

[0053] Ergänzend ist bei einem erfindungsgemäßen Verfahren möglich, dass ein Schloss ohne Zugangsberechtigungscode und damit nicht funktionsfähig ausgeliefert wird. Die optionale Funktion ist dann darin zu sehen, dass das Schloss nach Einbau und Anschluss an eine Datenleitung und Verbindung mit einem Rechner hinsichtlich des Zugangsberechtigungscode konfiguriert wird. In diesem Fall wird lediglich der im Datenspeicher des Schlosses abgelegte Vergleichscode ausgelesen und mit dem externen Code aus dem Rechner verglichen. Nach dieser Konfiguration ist das Schloss betriebs- und funktionsbereit. Die Konfiguration des Schlosses kann beispielsweise durch einen Dialog zwischen dem im Schloss installierten Prozessor und einem Zentralrechner erfolgen.

Patentansprüche

1. Verfahren zur Steuerung eines elektronischen Schlosses, bei dem das Schloss über ein Eingabelement zumindest hinsichtlich des Öffnens und Schließens gesteuert wird, indem Daten, beispielsweise ein Zugangsberechtigungscode eingegeben und mit einem abgespeicherten Code verglichen werden, bevor das Schloss geöffnet oder geschlossen wird,
5
dadurch gekennzeichnet,
dass optionale Funktionen des Schlosses, wie beispielsweise zeitliche Zugangsberechtigungen, personenbezogene Zugangsberechtigungen, Öffnungsverzögerungen oder dergleichen nach Eingabe eines Berechtigungscode aktiviert oder deaktiviert werden.
2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,
dass der Berechtigungscode über das Eingabelement, beispielsweise eine Tastatur eingegeben wird. 20
3. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,
dass der Berechtigungscode über eine Telekommunikationseinrichtung, insbesondere eine Datenleitung oder ein Telefonfunknetz übermittelt wird. 25
4. Verfahren nach Anspruch 3,
dadurch gekennzeichnet,
dass für jede optionale Funktion ein eigener Berechtigungscode eingegeben wird. 30
5. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,
dass nach Eingabe des Zugangsberechtigungscode die optionale Funktion des Schlosses programmiert wird. 35
6. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,
dass die erforderliche Vorgehensweise zur Aktivierung oder Deaktivierung einer optionale Funktion in einem Display des Schlosses angezeigt wird. 40
7. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,
dass die Aktivierung oder Deaktivierung von optionalen Funktionen des Schlosses über Menüs angezeigt und/oder gesteuert werden. 45
8. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,
dass die Programmierung des Schlosses über eine optionale Funktion ausgelesen und als insbesondere verschlüsselter Datensatz übermittelt wird. 50
9. Verfahren nach Anspruch 8,
dadurch gekennzeichnet,
dass bestimmten Daten des Schlosses zu Wartungs- und/oder Kontrollzwecken mittels optionalen Funktion ausgelesen werden können. 55
10. Verfahren nach Anspruch 8,
dadurch gekennzeichnet,
dass die Daten bezüglich der Programmierung des Schlosses über eine Telekommunikationseinrichtung, insbesondere eine Datenleitung oder ein Telefonfunknetz übermittelt werden.
11. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,
dass das Schloss über eine Telekommunikationseinrichtung, insbesondere eine Datenleitung oder ein Telefonfunknetz zu Wartungs- und/oder Instandsetzungsarbeiten angesprochen wird. 15
12. Verfahren nach Anspruch 11,
dadurch gekennzeichnet,
dass die Programmierung des Schlosses ausgelesen und die Wartung des Schlosses im Gegenzug über eine bidirektionale Datenübermittlung durchgeführt wird. 20
13. Verfahren nach Anspruch 11,
dadurch gekennzeichnet,
dass die Programmierung des Schlosses über die Telekommunikationseinrichtung durchgeführt wird, wobei insbesondere eine Aktualisierung der Datensätze für den Betrieb des Schlosses durchgeführt wird. 25
14. Verfahren nach Anspruch 3,
dadurch gekennzeichnet,
dass die Datenübermittlung über einen im Schloss angeordneten GSM-, DECT- o. ä. Baustein oder ein Lesegerät für ein zum Zwecke der Datenübermittlung eingesetzten GSM-, DECT- o. ä. Baustein durchgeführt wird. 30

