



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11)

EP 1 205 885 A2

(12)

EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
15.05.2002 Patentblatt 2002/20

(51) Int Cl.7: **G07C 9/00**

(21) Anmeldenummer: **01126864.6**

(22) Anmeldetag: **12.11.2001**

(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: **ASTRA Gesellschaft für Asset
Management mbH & Co. KG**
30890 Barsinghausen (DE)

(72) Erfinder: **Stobbe, Anatoli**
30890 Barsinghausen (DE)

(74) Vertreter: **Patentanwälte Thömen & Körner**
Postfach 59 31
30059 Hannover (DE)

(30) Priorität: **13.11.2000 DE 10056119**

(54) **Elektronisch codierbares Schloss-System**

(57) Es wird ein elektronisch codierbares Schloss-System beschrieben.

Dieses umfasst ein Gehäuse mit einem ver- und entriegelbaren Schließorgan, insbesondere eines Vorhängebügels, das durch einen Riegelmechanismus sperr- und entsperrbar ist. Der Riegelungsmechanis-

mus ist mittels eines elektronischen Codeauswerters über eine Steuerleitung bei Auswertung eines gültigen Codes entsperrbar. Dem Codeauswerter ist ein Codeempfänger zugeordnet, der Daten von einem externen Berechtigungsausweis mit einem Codegeber über eine elektromagnetische, optische, akustische oder galvanische Übertragungsstrecke empfängt.

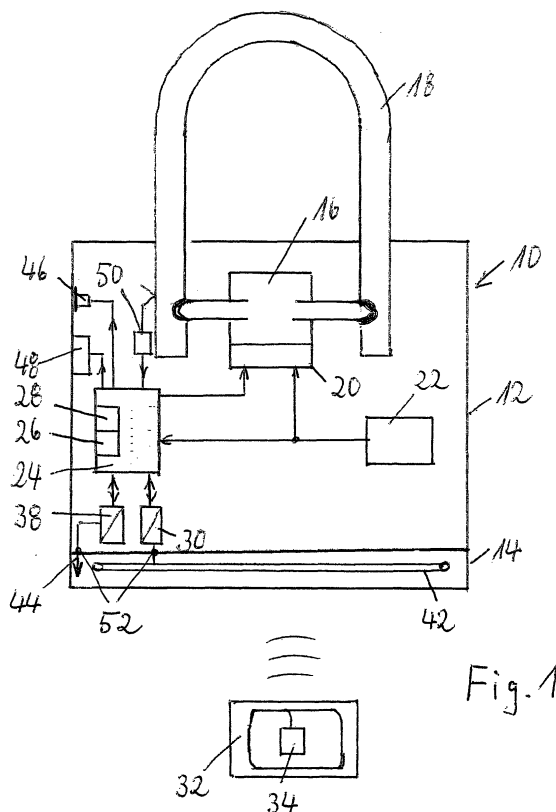


Fig. 1

EP 1 205 885 A2

Beschreibung

[0001] Die Erfindung betrifft ein elektronisch codierbares Schloss-System nach dem Oberbegriff des Anspruchs 1.

[0002] Netzbetreiber der Energieversorgung, Wasser- und Abwasserversorgung sowie der Telekommunikation unterhalten eine Vielzahl von Betriebsstätten, die über das Versorgungsgebiet verteilt sind und häufig ohne ständige Anwesenheit von Personal betrieben werden. Die Betriebsstationen sind gegen unbefugten Zutritt gesichert. Neben Einfriedungen mit verschließbaren Toren sind häufig noch weitere verschließbare Zugänge, Türen und Fenster in Gebäuden vorhanden.

[0003] Bisher benötigte das Wartungs- und Betriebspersonal eine Vielzahl von Schlüsseln, um Zugang zu den Betriebsstätten zu erhalten. Aus Sicherheitsgründen unterscheiden sich die Schlösser, so dass vom berechtigten Betriebspersonal eine Vielzahl von Schlüsseln mitgeführt werden muss, wenn unterschiedliche Betriebsstätten aufgesucht werden.

[0004] Der Erfindung liegt die Aufgabe zugrunde, ein Schloss-System für derartige Betriebsstätten zu schaffen, das vom Wartungs- und Betriebspersonal jeweils mit einem einzigen Berechtigungsausweis zu öffnen ist und es ermöglicht, die Berechtigungen individuell zu vergeben, zu ändern oder zu löschen.

[0005] Diese Aufgabe wird bei einem elektronisch codierten Schloss-System nach dem Oberbegriff des Anspruchs 1 durch die im kennzeichnenden Teil angegebenen Merkmale gelöst.

[0006] Weiterbildungen und vorteilhafte Ausgestaltungen ergeben sich aus den Unteransprüchen.

[0007] Bei dem erfindungsgemäßen Schloss-System wird ein Code eines vom Wartungs- und Betriebspersonal mitgeführten Berechtigungsausweises über einen Codegeber zum Schloss-System übermittelt und mittels eines Codeauswerters ausgewertet, der bei Gültigkeit einen Riegelmechanismus entsperrt. Zusätzlich zu einem Grundcode kann auch ein ergänzender Code verwendet werden, der Systemnummer, Lokalität, Kundennummer, Kundengruppe und Hierarchiestufe umfasst.

[0008] Der Code wird dem Codeauswerter über eine erste drahtlose Schnittstelle übermittelt, die als elektromagnetische oder optische Schnittstelle ausgebildet sein kann. Durch eine zweite drahtlose Schnittstelle kann der Codeauswerter eine Verbindung zu einem externen Zugangskontrollsystem oder einer externen Datenbank herstellen und die Gültigkeit des Berechtigungsausweises prüfen lassen. Nach Prüfung wird eine Gültigkeitsantwort rückübertragen, die bei gültigem Berechtigungsausweis den Riegelmechanismus entsperrt oder bei ungültigem Berechtigungsausweis den Riegelmechanismus gesperrt lässt.

[0009] Eine externe Datenbank kann über ein öffentliches oder betriebsinternes Telekommunikationsnetz erreichbar sein und ist wesentlich einfacher und schnell-

ler zu pflegen. Sie ist dann für eine praktisch unbegrenzte Zahl von Klienten, also in diesem Fall von elektronischen Schloss-Systemen verfügbar. Außerdem spielt der Speicherplatz der Datenbank gerade bei einer Vielzahl unterschiedlicher Berechtigungscodes eine geringere Rolle als wenn unterschiedliche Berechtigungscodes in jedem einzelnen Schloss-System abgelegt werden müssten und hierfür lokal Speicherplatz benötigten.

[0010] Alternativ können auch im Codeauswerter Berechtigungsdaten gespeichert werden, die über die zweite drahtlose Schnittstelle aktualisiert werden. In diesem Fall findet dann eine Prüfung der Zugangsberechtigung intern durch den elektronischen Codeauswerter des Schloss-Systems statt. Dies kann entweder generell erfolgen oder im Falle einer gestörten Verbindung zum externen Zugangskontrollsystem oder der externen Datenbank als vorübergehender Notbetrieb zur Gewährleistung der Funktionsbereitschaft des Schloss-Systems.

[0011] Der Vorteil der zweiten drahtlosen Schnittstelle besteht darin, dass das Schloss-System ohne galvanische Verbindung zum externen Zugangskontrollsystem oder zur externen Datenbank autark arbeiten kann, also z. B. im Freien als Vorhängeschloss oder auch als Einbauschloss an Gebäuden ohne eigene Datenleitungen oder Stromversorgungsleitungen. Dennoch ist eine hohe Sicherheit gegen Manipulation gegeben, und es besteht darüber hinaus die Möglichkeit, Neuzuweisungen, Änderungen oder Löschungen von Berechtigungen ohne mechanische Eingriffe bzw. Austausch des Schloss-Systems durchzuführen.

[0012] Dadurch ergibt sich eine erhebliche Vereinfachung in der Verwaltung der Zugänge und der Berechtigungsausweise und für das Wartungs- und Betriebspersonal der Vorteil, dass es mit einem einzigen Berechtigungsausweis Zugang zu unterschiedlichen Schloss-Systemen erhalten kann.

[0013] Vorzugsweise ist die erste Schnittstelle eine Transponderschnittstelle für den Frequenzbereich zwischen 100 kHz und 15 MHz.

[0014] Dieser Frequenzbereich ermöglicht eine Datenübertragung auch dann, wenn keine direkte Sicht zwischen dem Codegeber und dem schlossseitigen Empfänger der ersten drahtlosen Schnittstelle besteht. Es besteht so die Möglichkeit, das Schloss-System ohne Beeinträchtigung der ersten drahtlosen Schnittstelle gegen Witterungseinflüsse oder Vandalismus zu schützen.

[0015] Bei einer Weiterbildung überträgt die Transponderschnittstelle induktiv oder elektromagnetisch Energie zur Speisung eines Transponders im Berechtigungsausweis, und zwischen dem Transponder des Berechtigungsausweises und dem Codeauswerter werden Daten zur Prüfung der Berechtigung übertragen.

[0016] Bei dieser Lösung können kleine, handliche passive Transponder eingesetzt werden, was für das Wartungs- und Betriebspersonal einen Bedienungs-komfort bedeutet. Außerdem lassen sich übliche Kom-

ponenten für Zugangskontrollsysteme verwenden, insbesondere Ausweiskarten mit Codegeber, die auch bereits für Zugänge an anderen Gebäuden mit Anschluss an das elektrische Versorgungsnetz eingesetzt werden.

[0017] Alternativ kann die erste Schnittstelle als Schnittstelle für ein Mobilfunknetz ausgebildet sein.

[0018] In diesem Fall ist es möglich, statt eines zusätzlichen Berechtigungsausweises ein Mobiltelefon als Codegeber zu verwenden. So kann das von Wartungs- und Betriebspersonal üblicherweise mitgeführte Mobiltelefon zusätzlich zu seiner eigentlichen Bestimmung als Kommunikationsgerät auch als Codegeber mit Berechtigungsausweis eingesetzt werden, so dass dann ein zusätzlicher Berechtigungsausweis entbehrlich ist.

[0019] Der Code kann der SIM-Kartennummer entsprechen oder auch gesondert aus einem Speicher oder über die Tastatur, gegebenenfalls in Verknüpfung mit der SIM-Kartennummer, übermittelt werden.

[0020] Gemäß einer Weiterbildung kann die erste Schnittstelle zusätzlich einen Nahfeldsensor zur Erfassung der Aussendung eines als Codegeber dienenden Mobiltelefons umfassen.

[0021] Bei dieser Ausführung wird sichergestellt, dass der Code über das Mobiltelefon nur dann wirksam eingegeben werden kann, wenn der Mitarbeiter sich vor Ort in unmittelbarer Nähe des Schloss-Systems aufhält und damit nur das unmittelbar benachbarte Schloss-System entriegelt wird, nicht aber gleichzeitig alle mit demselben Code programmierten Schloss-Systeme.

[0022] Alternativ kann vorgesehen sein, dass der ersten Schnittstelle zusätzlich ein Display zur Anzeige eines ständig wechselnden Codes zugeordnet ist, der über die Tastatur des als Codegeber dienenden Mobiltelefons vom Wartungs- und Betriebspersonal einzugeben ist.

[0023] Auch diese Maßnahme stellt sicher, dass nur das in der Nähe befindliche Schloss-System entriegelt werden kann, dessen Display sichtbar ist, denn durch den ständig wechselnden Code werden einzelne Schloss-Systeme individualisiert.

[0024] Vorzugsweise umfasst die zweite Schnittstelle einen Empfänger oder einen Transceiver für eine Funkstrecke kleiner Leistung in einem zugelassenen Frequenzbereich, insbesondere 433 MHz oder 868 MHz, oder für ein Mobilfunknetz.

[0025] Dadurch ist es möglich, eine Datenkommunikation über eine kurze Entfernung zu einem stationären Schnittstellensender oder -transceiver herzustellen, der dann seinerseits über Datenleitungen mit dem externen Zugangskontrollsystem oder der externen Datenbank verbunden ist. Möglich sind hier bei Funkstrecken kleiner Leistung Entfernungen von einigen zehn Metern oder bei einem Mobilfunknetz auch von einigen hundert Metern bis Kilometern zur nächsten Kopfstation.

[0026] Durch die Funkstrecke kleiner Leistung können mehrere benachbarte Schloss-Systeme untereinander und/oder mit einer Relaisstation kommunizieren.

Eines der Schloss-Systeme oder die Relaisstation übernimmt dann die Verbindung zu einem externen Zugangskontrollsystem oder einer Datenbank. Hierfür ist dann nur eine gemeinsame Schnittstelle erforderlich. Da im praktischen Betrieb nur jeweils ein Schloss-System aktiv ist, besteht keine Gefahr einer Datenkollision durch gleichzeitigen Übertragungswunsch mehrerer Schloss-Systeme.

[0027] Der Codeauswerter kann einen Speicher für unterschiedliche Codes von Berechtigungsausweisen umfassen, die über die zweite drahtlose Schnittstelle aktualisierbar sind. Bei Ausbildung der zweiten Schnittstelle als unidirektional zwischen dem externen Zugangskontrollsystem oder der externen Datenbank und dem Codeauswerter des Riegelmechanismus erfolgt die Zugangsprüfung durch den Codeauswerter generell mit dem lokal gespeicherten Code. Bei Ausbildung der zweiten Schnittstelle als bidirektional zwischen dem externen Zugangskontrollsystem oder der externen Datenbank und dem Codeauswerter des Riegelmechanismus erfolgt die Zugangsprüfung durch den Codeauswerter nur bei Ausfall dieser Schnittstelle mit dem lokal gespeicherten Code.

[0028] Hierdurch wird jederzeit eine Zugangsmöglichkeit mit unterschiedlichen Berechtigungsausweisen durch unterschiedliches Wartungs- und Betriebspersonal ermöglicht, wobei eine ferngesteuerte Verwaltung der Berechtigungen möglich ist und außerdem ein Notbetrieb während des Ausfalls der zweiten Schnittstelle aufrechterhalten werden kann.

[0029] Ferner kann der Codeauswerter auch einen Zeitmesser umfassen, welcher als Echtzeituhr, gegebenenfalls mit Tageszeit und zusätzlich Datum oder als Zähler ausgebildet ist. Zusätzlich kann eine Zugangsprüfung mit einer generellen oder temporären Berechtigung des Berechtigungsausweises verknüpft werden.

[0030] Es ist dann möglich, den Zugang von einem Datum, einer Uhrzeit oder einem Zählerstand abhängig zu machen. Dadurch kann ein Berechtigungsausweis mit unverändertem Code dennoch zeitselektiv eingesetzt werden. Eine temporäre Berechtigung kann auch Dauer oder Häufigkeit des Zugangs umfassen. Sie kann intern oder extern vergeben und auch nach ein- oder mehrmaliger Benutzung verändert oder gelöscht werden.

[0031] Das Gehäuse des Schloss-Systems kann aus zwei Teilen bestehen, von denen ein erstes Teil aus Metall besteht und den Riegelmechanismus umfasst und ein zweites Teil aus Kunststoff besteht und eine Antenne des Codeempfängers oder -senders sowie gegebenenfalls des Transceivers oder der Transceiver für eine Funkstrecke kleiner Leistung und/oder ein Mobilfunknetz umfassen. Dabei können die übrigen Komponenten ganz oder teilweise im ersten oder zweiten Teil des Gehäuses angeordnet sein.

[0032] Dieser Aufbau ermöglicht es, besonders sicherheitsrelevante Teile im Gehäuse aus Metall unterzubringen und so gegen Sabotage zu schützen. Dage-

gen könnte die Antenne, welche zur Erzielung guter Strahlungseigenschaften abgesetzt aber geschützt angebracht sein muss, im Gehäuseteil aus Kunststoff angeordnet werden. Dort können aber auch andere weniger sicherheitsrelevante Teile, zum Beispiel Batterien, angeordnet sein, um deren Austausch zu vereinfachen.

[0033] Bei Anordnung von elektrischen Komponenten in beiden Teilen des Gehäuses können diese durch Kontakte untereinander verbunden sein.

[0034] Dadurch ist es im Prinzip weitgehend freigestellt, in welchem der beiden Teile die elektrischen und elektronischen Komponenten untergebracht sind, soweit dies nicht durch sicherheitsrelevante Erfordernisse vorgegeben ist.

[0035] Zur Erhöhung der Sicherheit der Datenkommunikation zwischen trennbaren Teilen des Gehäuses können auch interne Verschlüsselungseinrichtungen mit Authentitätsprüfung in beiden Teilen des Gehäuses vorgesehen sein.

[0036] Diese stellen nur dann die Funktion der beiden Teile des Gehäuses her, wenn zusammengehörende Teile verwendet werden. Ein missbräuchlicher Austausch unterschiedlicher Teile des Gehäuses z. B. unterschiedlicher Schloss-Systeme wird so erkannt und eine Funktion verhindert. Nur bei passenden Teilen des Gehäuses wird nach Zusammenfügen automatisch wieder die Funktionsbereitschaft hergestellt.

[0037] Weiterhin ist vorgesehen, dass bei Ausbildung als Vorhängeschloss ein Positionsgeber für den Riegel oder Vorhängebügel mit dem Codeauswerter verbunden ist.

[0038] Hierdurch kann erkannt werden, ob der Riegel oder Vorhängebügel nach dem Schließen wieder in die richtige Position gelangt und auch ob das Schloss gewaltsam geöffnet wird.

[0039] Nachfolgend wird die Erfindung anhand eines Ausführungsbeispiels beschrieben, das in der Zeichnung dargestellt ist.

[0040] In der Zeichnung zeigen:

Fig. 1 eine Prinzipdarstellung eines elektronisch codierten Schloss-Systems mit einem Vorhängeschlosses in einer ersten Ausführung,

Fig. 2 eine Prinzipdarstellung eines elektronisch codierten Schloss-Systems mit einem Vorhängeschloss in einer zweiten Ausgestaltung und

Fig. 3 eine Prinzipdarstellung der Integration eines elektronisch codierten Schloss-Systems in einem Zugangskontrollsystem

[0041] Die Figuren 1 und 2 zeigen unterschiedliche Ausführungsformen eines elektronisch codierten Schloss-Systems mit einem Vorhängeschloss 10. Das Schloss-System umfasst ein Gehäuse, welches aus einem ersten Gehäuseteil 12 aus Metall und einem zweiten Gehäuseteil 14 aus Kunststoff besteht. In dem Ge-

häuseteil 12 aus Metall ist ein Riegelmechanismus 16 angeordnet, der einen Vorhängebügel 18 sperrt oder entsperrt.

[0042] Der Riegelmechanismus 16 umfasst einen Antrieb 20 zur Betätigung. Dieser ist bei der Darstellung in Figur 1 durch einen elektrischen Antrieb gebildet, zum Beispiel durch einen Motor, einen Magneten oder ein Piezoelement.

[0043] Der Antrieb 20 sowie weitere elektronische Bauelemente wird durch eine Energieversorgung 22 mit elektrischer Energie versorgt. Bei der Energieversorgung kann es sich um eine Batterie, einen Akku oder auch um eine externe Energiequelle mit oder ohne Pufferelement, zum Beispiel in Form eines Kondensators, handeln.

[0044] Der Antrieb 20 wird durch einen Codeauswerter 24 gesteuert. Diesem Codeauswerter 24 kann ein interner Speicher 26 zur Speicherung von zugelassenen Codes und eine Uhr 28 oder ein externes Zugangskontrollsystem oder eine externe Datenbank zugeordnet sein. Der Codeauswerter 24 ist ferner mit einem Codetransceiver 30 verbunden, dem der zu prüfende und bei Gültigkeit eine Freigabe ermöglichende Code über einen Berechtigungsausweis 32 mit einem Codegeber 34 zugeführt wird. Zur Übertragung des Codes vom Codegeber 34 zum Codetransceiver 30 kann die Übertragungsstrecke eine elektromagnetische, optische, akustische oder galvanische Schnittstelle sein. Als elektromagnetische Schnittstelle ist eine Transponderschnittstelle oder ein Mobilfunknetz geeignet.

[0045] Die Transponderschnittstelle kann bidirektional ausgebildet sein. Die Mobilfunkschnittstelle umfasst einen Mobilfunktransceiver 38. Alternativ kann auch ein Transceiver für eine Funkstrecke kleiner Leistung verwendet werden, zum Beispiel im 433 oder 868 MHz-Bereich.

[0046] Zur Kommunikation mit einem externen Zugangskontrollsystem oder einer externen Datenbank kann ebenfalls die Mobilfunkschnittstelle dienen oder eine HF- oder NF-Schnittstelle mit einem Transceiver. Als HF- Schnittstelle kann eine Funkstrecke kleiner Leistung dienen, zum Beispiel im 433 oder 868 MHz-Bereich.

[0047] Die beiden Transceiver 30 und 38 umfassen auch Antennen 42 und 44. Diese sind im Gehäuseteil 14 aus Kunststoff angeordnet.

[0048] Ergänzend können auch noch ein akustischer Alarmgeber 46 und eine optische Anzeige 48, die auch als Display für numerische oder alphanumerische Zeichen ausgebildet sein kann, vorhanden sein. Diese können einer Quittierung einer richtigen Funktion oder einer Fehlfunktion dienen oder auch zur Eingabe eines sich in Abständen fortlaufend ändernden Codes auffordern, der nur durch Ablesen erkannt werden kann.

[0049] Darüber hinaus kann auch noch ein Sensor 50 vorgesehen sein, der eine korrekte Verriegelung oder aber auch eine gewaltsame Öffnung signalisieren kann.

[0050] Die Bestandteile der elektrischen und elektro-

nischen Komponenten im Gehäuseteil 12 und im Gehäuseteil 14 werden durch Kontakte 52 untereinander verbunden.

[0051] Bei der Ausgestaltung nach Fig. 2 wird statt eines elektrischen Antriebs ein mechanischer Antrieb 54 verwendet, der mit dem Riegelmechanismus 16 über eine Kupplung 56 verbunden ist. Im übrigen entspricht der weitere Aufbau weitgehend dem in Fig. 1, wobei jedoch bei Fig. 2 einige der elektronischen Baugruppen anders in den beiden Gehäuseteilen 12 und 14 verteilt sind.

[0052] Zur Sicherung eines zulässigen Datentransfers zwischen den Gehäuseteilen 12 und 14 und Verhinderung eines unzulässigen Austausches der Gehäuseteile erfolgt der Datentransfer zwischen den Gehäuseteilen mittels Codiervorrichtungen 36 und 40. Diese prüfen die Daten auf Autentität und verhindert gleichzeitig Datenmanipulationen an der Schnittstelle.

[0053] Fig. 3 zeigt die Integration eines elektronisch codierten Schloss-Systems in ein Zugangskontrollsystem. Das Zugangskontrollsystem umfasst hier einen Datenbus 58, der zu einer externen Datenbank führt. Daran angeschlossen ist ein in einem Gebäude an einer Tür angebrachtes Schreib-/Lesegerät 62, das mit üblichen Transpondern kommunizieren kann. Ein solcher Transponder kann auch ein Berechtigungsausweis 32 mit einem Codegeber 34 sein, der dadurch universell einsetzbar ist.

[0054] Mit dem Schreib-/Lesegerät 62 ist eine Türsteuereinheit 60 mit einem Transceiver 64 gekoppelt, die über eine Antenne 66 mit einem oder mehreren der elektronischen Schlösser über eine Funkverbindung kleiner Leistung kommuniziert. Dadurch kann von den Schlössern eine Abfrage extern gespeicherter Zugangsdaten erfolgen. Es kann sich dabei um die gleichen Zugangsdaten handeln, die auch vom Schreib-/Lesegerät 62 abgefragt werden, also um Daten im Speicher eines örtlichen Zugangskontrollsystems oder einer externen Datenbank. Jedes mobile oder stationäre Schloss entspricht dann einem weiteren in das Zugangskontrollsystem integrierten Schreib-/Lesegerät für eine Zugangskontrolle. Die Türsteuereinheit mit dem Transceiver kann aber auch als Relaisstelle für eine Kommunikation der Schlösser 10 in der beschriebenen Ausgestaltung für eine Zugangsdatenabfrage oder eine Datenaktualisierung dienen.

[0055] Falls zur Prüfung der Zugangsdaten auf eine externen Datenbank zugegriffen werden muss, kann dies gemeinsam über ein Bussystem 58 und/oder ein zwischengeschaltetes Kommunikationsnetz erfolgen.

Patentansprüche

1. Elektronisch codierbares Schloss-System, bestehend aus einem Gehäuse mit einem durch einen Riegelmechanismus ver- und entriegelbaren Schließorgan, wobei der Riegelmechanismus mittels eines elektronischen Codeauswerter bei Aus-

wertung eines gültigen Codes entsperrbar ist und der Codeauswerter eine erste drahtlose Schnittstelle umfasst, über die Daten von einem externen Berechtigungsausweis mit einem Codegeber übertragbar sind, **dadurch gekennzeichnet, dass** der Codeauswerter eine zweite drahtlose Schnittstelle zur Datenkommunikation mit einem externen Zugangskontrollsystem oder einer externen Datenbank umfasst, über die im Codeauswerter speicherbare Berechtigungsdaten aktualisierbar sind und/oder über die eine Gültigkeitsanfrage des Berechtigungsausweises übertragbar und eine Gültigkeitsantwort rückübertragbar ist.

2. Elektronisch codierbares Schloss-System nach Anspruch 1, **dadurch gekennzeichnet, dass** die erste Schnittstelle eine Transponderschnittstelle für den Frequenzbereich zwischen 100 KHz und 15 MHz ist.

3. Elektronisch codierbares Schloss-System nach Anspruch 2, **dadurch gekennzeichnet, dass** die Transponderschnittstelle induktiv oder elektromagnetisch Energie zur Speisung eines Transponders im externen Berechtigungsausweis überträgt und zwischen dem Transponder des Berechtigungsausweises und dem Codeauswerter Daten zur Prüfung der Berechtigung übertragen werden.

4. Elektronisch codierbares Schloss-System nach Anspruch 1, **dadurch gekennzeichnet, dass** die erste Schnittstelle als Schnittstelle für ein Mobilfunknetz ausgebildet ist.

5. Elektronisch codierbares Schloss-System nach Anspruch 4, **dadurch gekennzeichnet, dass** die erste Schnittstelle zusätzlich einen Nahfeldsensor zur Erfassung der Aussendung eines als Codegeber dienenden Mobiltelefons umfasst.

6. Elektronisch codierbares Schloss-System nach Anspruch 4 oder 5, **dadurch gekennzeichnet, dass** die erste Schnittstelle zusätzlich ein Display zur Anzeige eines ständig wechselnden Codes umfasst, der über die Tastatur des als Codegeber dienenden Mobiltelefons vom Betriebspersonal einzugeben ist.

7. Elektronisch codierbares Schloss-System nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet, dass** die zweite Schnittstelle einen Empfänger oder einen Transceiver für eine Funkstrecke kleiner Leistung in einem zugelassenen Frequenzbereich, insbesondere 433 MHz oder 868 MHz, oder für ein Mobilfunknetz umfasst.

8. Elektronisch codierbares Schloss-System nach einem der Ansprüche 1 bis 7, **dadurch gekennzeichnet,**

net, dass der Codeauswerter einen Speicher für unterschiedliche Codes von Berechtigungsausweisen umfasst, der über die zweite drahtlose Schnittstelle aktualisierbar ist und bei Ausbildung der zweiten Schnittstelle unidirektional vom externen Zugangskontrollsystem oder der externen Datenbank zum Codeauswerter des Riegelmechanismus generell oder bei Ausbildung der zweiten Schnittstelle bidirektional zwischen dem externen Zugangskontrollsystem oder der externen Datenbank und dem Codeauswerter des Riegelmechanismus nur bei Ausfall dieser Schnittstelle die Zugangsprüfung mit den lokal gespeicherten Codes erfolgt.

9. Elektronisch codierbares Schloss-System nach einem der Ansprüche 1 bis 8, **dadurch gekennzeichnet, dass** der Codeauswerter eine Uhr umfasst, welche als Echtzeituhr oder als Zähler ausgebildet ist und zusätzlich eine generelle oder individuelle temporäre Berechtigung des Berechtigungsausweises mit der Zugangsprüfung verknüpft. 5

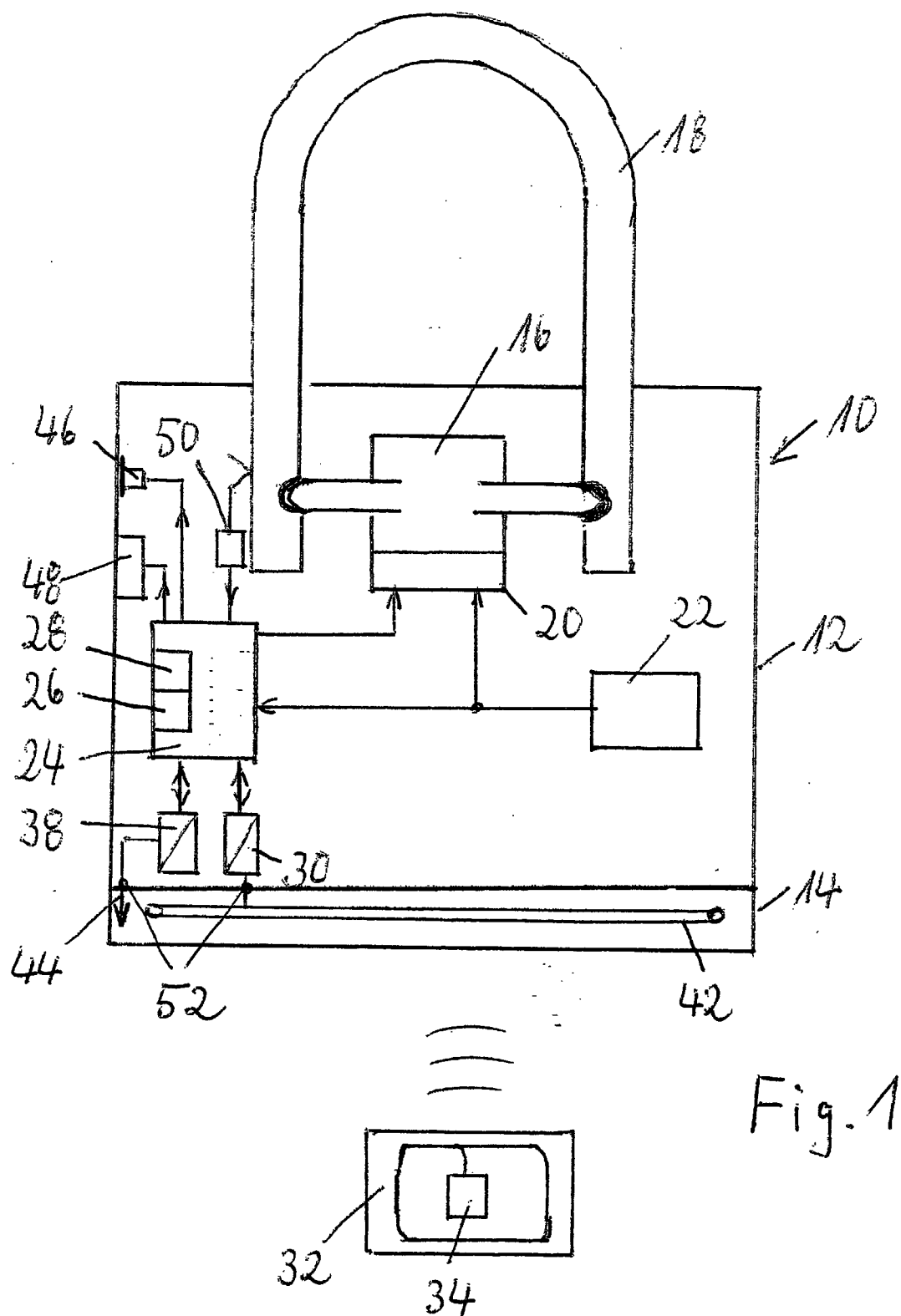
10. Elektronisch codierbares Schloss-System nach einem der Ansprüche 1 bis 9, **dadurch gekennzeichnet, dass** das Gehäuse aus zwei Teilen besteht, von denen ein erstes Teil aus Metall besteht und den Riegelmechanismus umfasst, und ein zweites Teil aus Kunststoff besteht und Antennen der ersten und zweiten Schnittstellen umfasst, wobei die übrigen Komponenten ganz oder teilweise im ersten oder zweiten Teil des Gehäuses angeordnet sind. 10

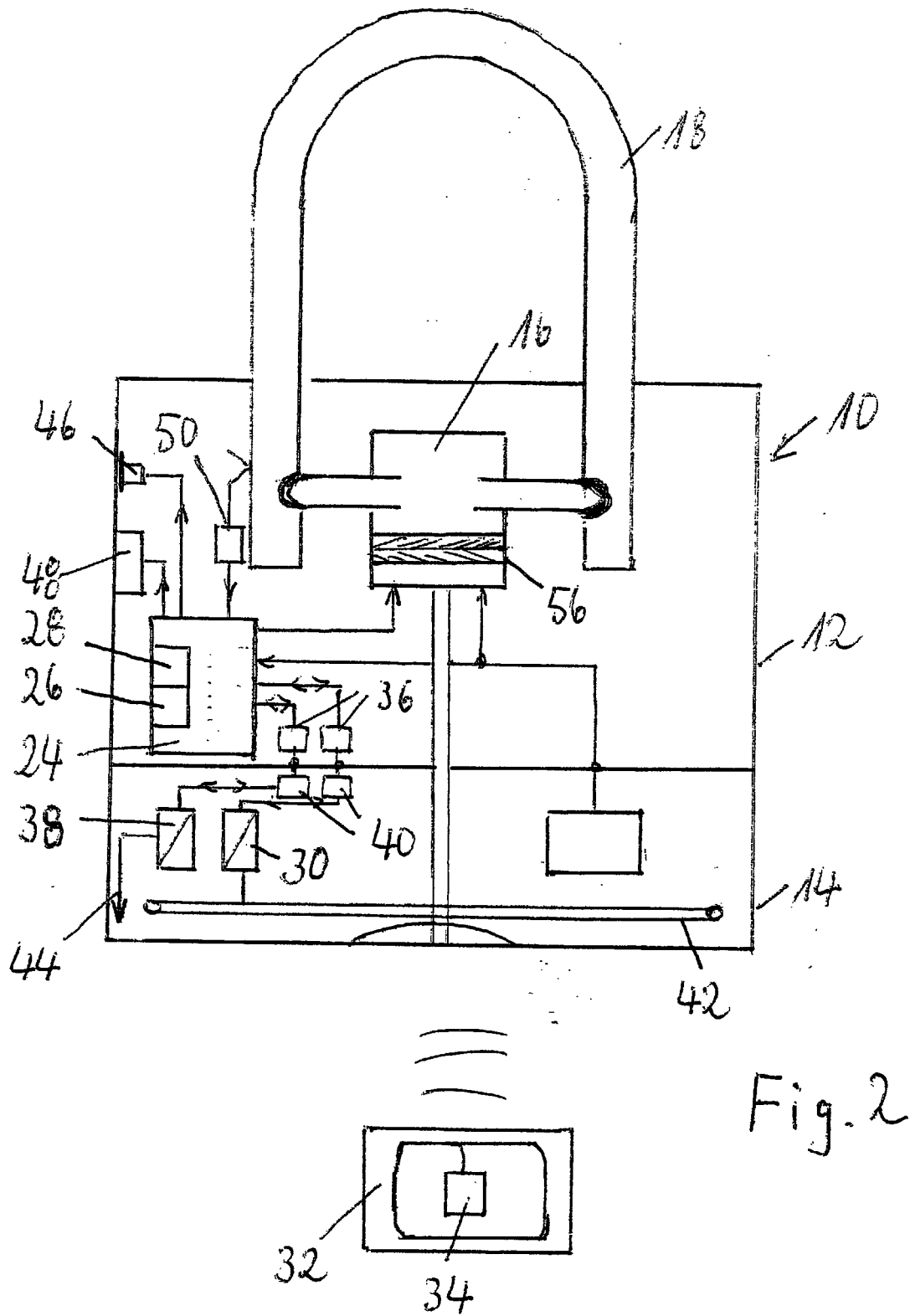
11. Elektronisch codierbares Schloss-System nach Anspruch 10, **dadurch gekennzeichnet, dass** bei Anordnung von elektrischen Komponenten in beiden Teilen des Gehäuses diese Komponenten durch Kontakte untereinander verbunden sind. 15

12. Elektronisch codierbares Schloss-System nach Anspruch 10 oder 11, **dadurch gekennzeichnet, dass** den trennbaren elektronischen Komponenten in den Teilen des Schloss-Systems Codiervorrichtungen für einen gesicherten Datenaustausch untereinander zugeordnet sind. 20

13. Elektronisch codierbares Schloss-System nach einem der Ansprüche 1 bis 12, **dadurch gekennzeichnet, dass** bei Ausbildung als Vorhängeschloß ein Positionsgeber für den Vorhängebügel im Gehäuse angeordnet ist, der vom Codeauswerter ausgewertet wird. 25

55





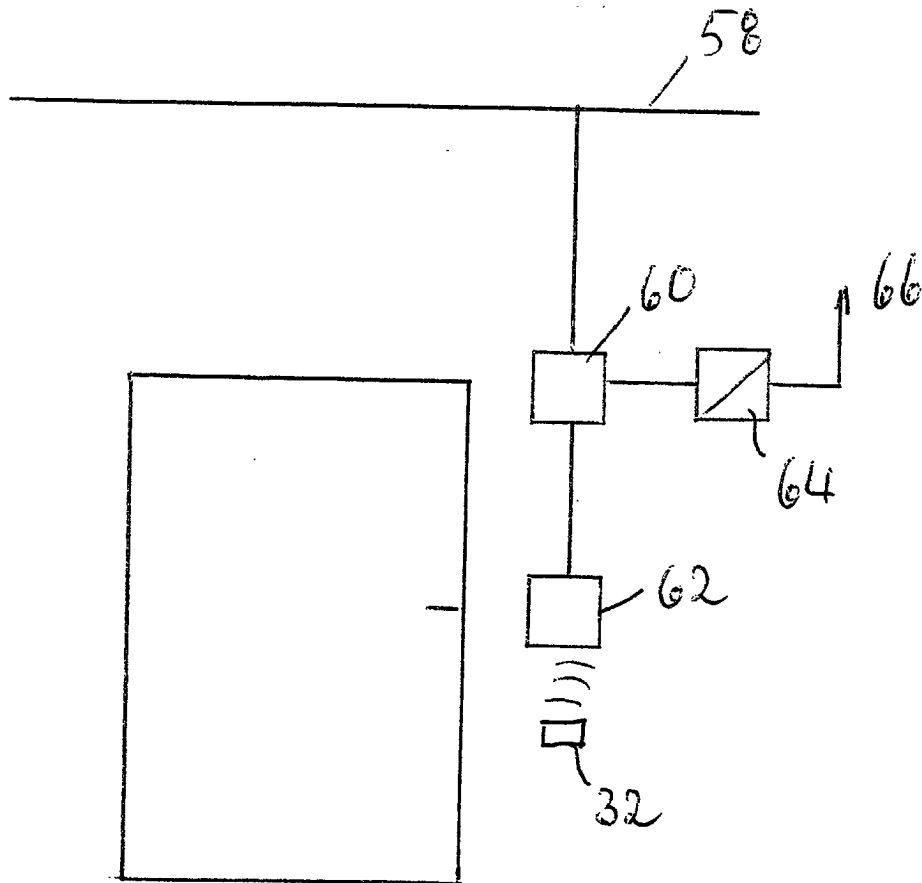


Fig. 3