



(11)

EP 4 099 282 B1

(12)

EUROPÄISCHE PATENTSCHRIFT

(45) Veröffentlichungstag und Bekanntmachung des Hinweises auf die Patenterteilung:
17.01.2024 Patentblatt 2024/03

(51) Internationale Patentklassifikation (IPC):
G07C 9/00 (2020.01)

(21) Anmeldenummer: **21177176.1**

(52) Gemeinsame Patentklassifikation (CPC):
G07C 9/00309; G07C 2009/00555;
G07C 2009/00793; G07C 2009/00801;
G07C 2009/00865

(22) Anmeldetag: **01.06.2021**

(54) **SCHLIESSSYSTEM UND VERFAHREN ZUR FREIGABE EINER VERBINDUNG ZWISCHEN EINER MOBILEINHEIT UND EINEM HAUPTSCHLÜSSEL**

LOCKING SYSTEM AND METHOD FOR RELEASING A CONNECTION BETWEEN A MOBILE UNIT AND A MAIN KEY

SYSTÈME DE FERMETURE ET PROCÉDÉ DE LIBÉRATION D'UNE LIAISON ENTRE UNE UNITÉ MOBILE ET UNE CLÉ PRINCIPALE

(84) Benannte Vertragsstaaten:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

• **Lelie, Christoph**
45136 Essen (DE)

(43) Veröffentlichungstag der Anmeldung:
07.12.2022 Patentblatt 2022/49

(74) Vertreter: **DREISS Patentanwälte PartG mbB**
Friedrichstraße 6
70174 Stuttgart (DE)

(73) Patentinhaber: **BKS GmbH**
42549 Velbert (DE)

(56) Entgegenhaltungen:
DE-A1-102015 009 199 DE-A1-102019 008 962
US-A1- 2021 037 099

(72) Erfinder:
• **Braam, Reinhold**
46414 Rhede (DE)

EP 4 099 282 B1

Anmerkung: Innerhalb von neun Monaten nach Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents im Europäischen Patentblatt kann jedermann nach Maßgabe der Ausführungsordnung beim Europäischen Patentamt gegen dieses Patent Einspruch einlegen. Der Einspruch gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist. (Art. 99(1) Europäisches Patentübereinkommen).

Beschreibung

[0001] Die Erfindung betrifft ein Schließsystem, mit einem Hauptschlüssel zur Programmierung und Betätigung einer Schließeinrichtung, mit einer Mobileinheit zur Programmierung des Hauptschlüssels, mit einer Datenübertragungseinrichtung zur Datenübertragung zwischen der Mobileinheit und dem Hauptschlüssel im Zuge der Programmierung, gemäß US 2021/037099 A1.

[0002] Schließsysteme der vorstehend genannten Art ermöglichen eine komfortable Programmierung eines Hauptschlüssels unter Verwendung einer Mobileinheit. Der Hauptschlüssel wiederum dient dazu, eine Schließeinrichtung des Schließsystems zu programmieren, wobei beispielsweise Daten zu Zutrittsberechtigungen weiterer Schlüssel des Schließsystems an eine Schließeinrichtung übermittelt werden.

[0003] Die Verwendung einer Datenübertragungseinrichtung zwischen der Mobileinheit und dem Hauptschlüssel ermöglicht eine komfortable Übertragung von Daten, welche insbesondere berührungslos erfolgen kann.

[0004] Diese berührungslose Datenübertragung geht aber mit dem Risiko einher, dass eine Kommunikation zwischen einer (berechtigten) Mobileinheit und dem Hauptschlüssel potentiell abgehört werden kann, und dass anschließend eine (unberechtigte) Mobileinheit zur Umprogrammierung des Hauptschlüssels verwendet werden könnte.

[0005] Ein Hauptschlüssel weist üblicherweise keine Bedienelemente, also keine Quittierungstaste oder Ähnliches auf. Demnach könnte eine (unberechtigte) Programmierung des Hauptschlüssels auch aus weiterer Entfernung, beispielsweise aus einem Nachbarraum heraus, erfolgen.

[0006] Aus der DE 10 2015 009 199 A1 ist es bekannt, eine Bluetooth-Kommunikation zwischen einer Mobileinheit und einem Schließsystem dadurch zu sichern, dass ein von einem Benutzer der Mobileinheit generiertes akustisches Signal (Stimme, Sprachcode) von dem Schließsystem oder der Mobileinheit empfangen und auf eine Berechtigung dieses Benutzers hin analysiert wird.

[0007] Hiervon ausgehend liegt der vorliegenden Erfindung die Aufgabe zugrunde, ein Schließsystem bereitzustellen, dass einen höheren Manipulationsschutz aufweist.

[0008] Diese Aufgabe wird durch ein Schließsystem mit den Merkmalen des Patentanspruchs 1 gelöst.

[0009] Bei dem erfindungsgemäßen Schließsystem ist zusätzlich zu einer Zweiwegekommunikation zwischen der Mobileinheit und dem Hauptschlüssel über die Datenübertragungseinrichtung ein zusätzlicher Kommunikationsweg bereitgestellt, und zwar in Form eines akustischen Kommunikationswegs von dem Hauptschlüssel ausgehend in Richtung auf die Mobileinheit.

[0010] Der Hauptschlüssel weist also einen akustischen Sender zur Übermittlung eines akustischen Signals auf, das die Mobileinheit empfängt. Die Mobileinheit

berücksichtigt dieses akustische Signal bei seiner Authentifizierung gegenüber dem Hauptschlüssel.

[0011] Der akustische Sender ist vorzugsweise ein piezokeramischer Lautsprecher, der besonders kompakt baut und dennoch ein modulationsfähiges akustisches Signal erzeugen kann. Ein solcher Lautsprecher kann in einfacher Weise in einen Hauptschlüssel integriert werden. Der Hauptschlüssel ist beispielsweise kartenförmig oder weist einen Schließbart auf.

[0012] Die Mobileinheit ist vorzugsweise durch ein Smartphone gebildet, wobei der akustische Empfänger der akustischen Zusatzeinrichtung durch ein Mikrofon des Smartphones gebildet ist. Auf diese Weise kann ein Teil der akustischen Zusatzeinrichtung durch ein handelsübliches Smartphone bereitgehalten werden.

[0013] Besonders bevorzugt ist es, wenn der akustische Sender, das akustische Signal und der akustische Empfänger derart aufeinander abgestimmt sind, dass ein Empfang des akustischen Signals nur möglich ist, wenn der akustische Sender und der akustische Empfänger maximal 1 m, vorzugsweise maximal 0,5 m, insbesondere maximal 0,2 m, zueinander beabstandet sind. Dies bedeutet, dass ein Nutzer der Mobileinheit zumindest die Mobileinheit selbst in unmittelbarer Nähe zu dem Hauptschlüssel positionieren muss, damit die Mobileinheit ein von dem Hauptschlüssel erzeugtes akustisches Signal überhaupt empfangen kann. Auf diese Weise wird der Manipulationsschutz weiter verbessert.

[0014] Insbesondere wird vorgeschlagen, dass das akustische Signal - gemessen in einem zu einer Schallabstrahlfläche des akustischen Senders senkrechten Abstand von 10 cm - einen maximalen Schalldruckpegel von 30 dB, vorzugsweise von maximal 20 dB, insbesondere von maximal 10 dB, aufweist. Die Verwendung solch niedriger Schalldruckpegel hat den Vorteil, dass ein Empfang des akustischen Signals durch die Mobileinheit nur dann möglich ist, wenn die Mobileinheit in unmittelbarer Nähe des Hauptschlüssels angeordnet wird. Zusätzlich bewirken die genannten niedrigen Schalldruckpegel, dass ein Empfang des akustischen Signals des Hauptschlüssels nur in einer geräuschfreien oder zumindest geräuscharmen Umgebung möglich ist. Zu diesem Zweck muss ein Nutzer der Mobileinheit unmittelbaren Zugriff zu dem Hauptschlüssel haben, um diesen und die Mobileinheit in einer akustisch geeigneten Umgebung positionieren zu können. Auch dieser Zugriffsschutz erhöht die Manipulationssicherheit des Schließsystems.

[0015] Bei der Datenübertragungseinrichtung handelt es sich in vorteilhafter Weise um eine Bluetooth-Einrichtung. Diese hat den Vorteil einer vergleichsweise niedrigen Reichweite von beispielsweise maximal 10 m, so dass auch während der Nutzung des freigegebenen Datenübertragungssystems eine räumliche Nähe zwischen der Mobileinheit und dem Hauptschlüssel beibehalten werden muss. Hierdurch wird eine weitere Verbesserung der Manipulationssicherheit erzielt.

[0016] Die eingangs genannte Aufgabe wird auch ge-

löst durch ein Verfahren zur Freigabe einer Verbindung zwischen einer Mobileinheit und einem Hauptschlüssel, wobei die Verbindung zur Datenübertragung zwischen der Mobileinheit und dem Hauptschlüssel dient, unter Verwendung eines vorstehend beschriebenen Schließsystems. Das Verfahren umfasst:

- Senden einer Verbindungsanfrage von der Mobileinheit an den Hauptschlüssel,
- Empfangen der Verbindungsanfrage durch den Hauptschlüssel, Erzeugen einer Authentifizierungsaufforderung und Übersenden der Authentifizierungsaufforderung an die Mobileinheit unter Verwendung der akustischen Zusatzeinrichtung,
- Empfangen der Authentifizierungsaufforderung durch die Mobileinheit, Erzeugen einer Authentifizierungsantwort und Übersenden an den Hauptschlüssel,
- Empfangen der Authentifizierungsantwort durch den Hauptschlüssel, Prüfen der Authentifizierungsantwort auf Identität mit der Authentifizierungsaufforderung, und im Falle der Identität: Freigeben der Verbindung zwischen Mobileinheit und Hauptschlüssel.

[0017] Die Freigabe der Verbindung zur Datenübertragung zwischen der Mobileinheit und dem Hauptschlüssel über die Datenübertragungseinrichtung erfolgt also nur dann, wenn die Authentifizierungsantwort der Mobileinheit zu der Authentifizierungsaufforderung des Hauptschlüssels identisch ist. Die Authentifizierungsaufforderung wird als akustisches Signal von dem Hauptschlüssel an die Mobileinheit gesendet.

[0018] Zur weiteren Erhöhung der Manipulationssicherheit ist es möglich, dass die Authentifizierungsaufforderung einen Zeitstempel enthält. Eine zu einer solchen Aufforderung identische Antwort muss dann innerhalb einer kurzen Zeitdauer von der Mobileinheit erzeugt werden, wodurch eine Manipulation durch Auffangen des akustischen Signals und "Raten" einer Antwort weiter erschwert wird.

[0019] Die Authentifizierungsaufforderung ist vorzugsweise ein akustisch kodierte Zufallsdatum, insbesondere eine Zufallszahl. Ein solches Zufallsdatum oder eine solche Zufallszahl kann als Tonfolge moduliert werden. Hierbei ist es möglich, dass nur eine Tonfrequenz verwendet wird, welche in mehreren Abschnitten und zwischenzeitlichen Unterbrechungen gesendet wird. Zusätzlich oder alternativ hierzu ist die Verwendung unterschiedlicher Tonfrequenzen innerhalb einer Authentifizierungsaufforderung möglich.

[0020] Die Authentifizierungsantwort entspricht in vorteilhafter Weise dem Zufallsdatum, insbesondere der Zufallszahl. Es ist aber auch möglich, dass die Authentifizierungsantwort weitere Daten enthält, beispielsweise zu der Identität der Mobileinheit oder auch ein zusätzliches Passwort, das auch in dem Hauptschlüssel abgelegt ist.

[0021] Weitere Merkmale und Vorteile der Erfindung

sind Gegenstand der nachfolgenden Beschreibung und der zeichnerischen Darstellung bevorzugter Ausführungsbeispiele.

[0022] In der Zeichnung zeigt:

- Fig. 1 eine schematische Darstellung eines Ausführungsbeispiels eines Schließsystems; und
 Fig. 2 eine Darstellung des Ablaufs eines Verfahrens zur Freigabe einer Verbindung zwischen einer Mobileinheit und einem Hauptschlüssel bei einem Schließsystem gemäß Fig. 1.

[0023] Ein Schließsystem ist in der Zeichnung insgesamt mit dem Bezugszeichen 10 bezeichnet. Das Schließsystem umfasst einen Hauptschlüssel 12 und eine Mobileinheit 14, insbesondere in Form eines Smartphones 16.

[0024] Die Mobileinheit 14 weist eine Einrichtung 18 zum Empfangen und Senden von Daten auf. Der Hauptschlüssel 12 weist eine entsprechende Einrichtung 20 zum Empfangen und Senden von Daten auf. Die Einrichtungen 18 und 20 bilden gemeinsam eine Datenübertragungseinrichtung 22. Dies ist insbesondere als Bluetooth-Einrichtung ausgebildet.

[0025] Der Hauptschlüssel 12 kann - aufgrund seiner Fähigkeit, mittels der Einrichtung 20 Daten senden zu können - auch als "aktiver Transponder" bezeichnet werden. Der Hauptschlüssel 12 weist vorzugsweise einen Energiespeicher, insbesondere eine Batterie, auf.

[0026] Der Hauptschlüssel 12 weist eine Programmiereinheit 24 auf, welche in an sich bekannter Weise dazu dient, einen Datenspeicher 26 einer Schließeinrichtung 28 zu programmieren. Bei der Schließeinrichtung 28 kann es sich beispielsweise um einen Schließzylinder 30 handeln. Idealerweise dient der Hauptschlüssel 12 zur Programmierung und Betätigung einer Mehrzahl von Schließeinrichtungen 28, 32, 34.

[0027] Die Programmierung des Hauptschlüssels 12 erfolgt mittels der Mobileinheit 14, und zwar unter Verwendung der Datenübertragungseinrichtung 22. Zur Freigabe einer Kommunikation über die Datenübertragungseinrichtung 22 umfasst das Schließsystem 10 eine insgesamt mit dem Bezugszeichen 36 bezeichnete akustische Zusatzeinrichtung. Diese umfasst einen an dem Hauptschlüssel 12 angeordneten akustischen Sender 38 und einen an der Mobileinheit 14 angeordneten akustischen Empfänger 40.

[0028] Der akustische Sender ist vorzugsweise in Form eines piezokeramischen Lautsprechers 42 ausgebildet.

[0029] Bei dem akustischen Empfänger 40 handelt es sich insbesondere um ein Mikrofon 44 des Smartphones 16.

[0030] Zur Freigabe einer Verbindung über die Datenübertragungseinrichtung 22 zwischen der Mobileinheit 14 und dem Hauptschlüssel 12 wird ein nachfolgend unter Bezugnahme auf Figur 2 beschriebenes Authentifizierungsverfahren durchgeführt.

[0031] Verfahrensschritte, die der Mobileinheit 14 zugeordnet sind, sind in dem Diagramm gemäß Figur 2 linker Hand dargestellt; Verfahrensschritte, die dem Hauptschlüssel 12 zugeordnet sind, sind in dem Diagramm gemäß Figur 2 rechter Hand dargestellt. Ein zeitlicher Ablauf des Verfahrens korrespondiert mit einer Leserichtung von oben nach unten der Darstellung gemäß Figur 2.

[0032] In einem ersten Schritt des Verfahrens erzeugt die Mobileinheit 14 eine Verbindungsanfrage 46 und übersendet diese mittels der Einrichtung 18 an die Einrichtung 20 des Hauptschlüssels 12. Der Hauptschlüssel 12 empfängt die Verbindungsanfrage 46 und erzeugt daraufhin ein Zufallsdatum 48 und wandelt dieses in ein akustisches Signal 50 um, das der akustische Sender 38 in die unmittelbare Umgebung des Hauptschlüssels 12 abstrahlt und das von dem akustischen Empfänger 40 der Mobileinheit 14 empfangen wird. Das akustische Signal 50 verkörpert eine Authentifizierungsaufforderung 52 des Hauptschlüssels 12 an die Mobileinheit 14.

[0033] Die Mobileinheit 14 verarbeitet das akustische Signal 50 / die Authentifizierungsaufforderung 52 und erzeugt (in Abhängigkeit eines in der Mobileinheit 14 abgelegten "Geheimnisses") eine Authentifizierungsantwort 54 und sendet diese an den Hauptschlüssel 12. Für die Übermittlung der Authentifizierungsantwort 54 wird die Datenübertragungseinrichtung 22 verwendet.

[0034] Der Hauptschlüssel 12 empfängt die Authentifizierungsantwort 54 und führt eine Prüfung 56 auf Identität der Authentifizierungsantwort 54 zu der Authentifizierungsaufforderung 52 durch.

[0035] Im Falle einer Identität (in Figur 2 durch "y" = englisch "yes" verbildlicht), erfolgt in einem Schritt 58 eine Freigabe der Verbindung zur Datenübertragung zwischen der Mobileinheit 14 und dem Hauptschlüssel 12 unter Verwendung der Datenübertragungseinrichtung 22 und zwecks Programmierung des Hauptschlüssels 12.

[0036] Im Falle der Nichtidentität (in Figur 2 durch "n" = englisch "no" verbildlicht) wird in einem Schritt 60 die Freigabe einer Verbindung zwischen den Einrichtungen 18 und 20 der Datenübertragungseinrichtung 22 verweigert. Der Schritt 60 kann mit weiteren Maßnahmen einhergehen, beispielsweise mit einer grundsätzlichen Sperrung der Programmiermöglichkeit des Hauptschlüssels 12 für einen bestimmten Zeitraum.

Patentansprüche

1. Schließsystem (10), mit einem Hauptschlüssel (12) zur Programmierung und Betätigung einer Schließeinrichtung (28), mit einer Mobileinheit (14) zur Programmierung des Hauptschlüssels (12), mit einer Datenübertragungseinrichtung (22) zur Datenübertragung zwischen der Mobileinheit (14) und dem Hauptschlüssel (12) im Zuge der Programmierung, **gekennzeichnet durch** eine akustische Zusatzein-

richtung (36), umfassend einen an dem Hauptschlüssel (12) angeordneten akustischen Sender (38) zur Übersendung eines akustischen Signals (50) an einen der Mobileinheit (14) zugeordneten akustischen Empfänger (40), wobei der Hauptschlüssel (12) und die Mobileinheit (14) dazu eingerichtet sind, eine Verbindung über die Datenübertragungseinrichtung (22) zwischen Mobileinheit (14) und Hauptschlüssel (12) nur unter der Bedingung freizugeben, dass sich die Mobileinheit (14) unter Berücksichtigung des von dem Hauptschlüssel (12) übersandten akustischen Signals (50) gegenüber dem Hauptschlüssel (12) authentifiziert.

2. Schließsystem (10) nach Anspruch 1, **dadurch gekennzeichnet, dass** der akustische Sender (38) ein piezokeramischer Lautsprecher (42) ist.

3. Schließsystem (10) nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet, dass** die Mobileinheit (14) durch ein Smartphone (16) gebildet ist und dass der akustische Empfänger (40) durch ein Mikrofon (44) des Smartphones (16) gebildet ist.

4. Schließsystem (10) nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet, dass** der akustische Sender (38), das akustische Signal (50) und der akustische Empfänger (42) derart auf einander abgestimmt sind, dass ein Empfang des akustischen Signals (50) nur möglich ist, wenn der akustische Sender (38) und der akustische Empfänger (42) maximal 1 m, vorzugsweise maximal 0,5 m, insbesondere maximal 0,2 m, zueinander beabstandet sind.

5. Schließsystem (10) nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet, dass** das akustische Signal (50) - gemessen in einem zu einer Schallabstrahlfläche des akustischen Senders (38) senkrechten Abstand von 10 cm - einen maximalen Schalldruckpegel von 30 dB, vorzugsweise von maximal 20 dB, insbesondere von maximal 10 dB, aufweist.

6. Schließsystem (10) nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet, dass** die Datenübertragungseinrichtung (22) eine Bluetooth-Einrichtung ist.

7. Verfahren zur Freigabe einer Verbindung zwischen einer Mobileinheit (14) und einem Hauptschlüssel (12), wobei die Verbindung zur Datenübertragung zwischen der Mobileinheit (14) und dem Hauptschlüssel (12) dient, unter Verwendung eines Schließsystems (10) nach Anspruch 1, **gekennzeichnet durch:**

- Senden einer Verbindungsanfrage (46) von der Mobileinheit (14) an den Hauptschlüssel (12),
 - Empfangen der Verbindungsanfrage (46) durch den Hauptschlüssel (12), Erzeugen einer Authentifizierungsaufforderung (52) und Über-senden der Authentifizierungsaufforderung (52) an die Mobileinheit (14) unter Verwendung der akustischen Zusatzeinrichtung (36),
 - Empfangen der Authentifizierungsaufforde-rung (52) durch die Mobileinheit (14), Erzeugen einer Authentifizierungsantwort (54) und Über-senden an den Hauptschlüssel (12),
 - Empfangen der Authentifizierungsantwort (54) durch den Hauptschlüssel (12), Prüfen der Au-thentifizierungsantwort (54) auf Identität mit der Authentifizierungsaufforderung (52), und im Falle der Identität: Freigeben der Verbindung zwischen Mobileinheit (14) und Hauptschlüssel (12).
8. Verfahren nach Anspruch 7, **dadurch gekenn-
zeichnet, dass** die Authentifizierungsaufforderung (52) einen Zeitstempel enthält.
9. Verfahren nach Anspruch 7 oder 8, **dadurch ge-
kennzeichnet, dass** die Authentifizierungsauffor-derung (52) ein akustisch kodierte Zufallsdatum, insbesondere eine Zufallszahl, ist.
10. Verfahren nach Anspruch 9, **dadurch gekenn-
zeichnet, dass** die Authentifizierungsantwort (54) dem Zufallsdatum, insbesondere der Zufallszahl, entspricht.

Claims

1. A locking system (10), with a master key (12) for programming and actuating a locking device (28), with a mobile unit (14) for programming the master key (12), with a data-transfer apparatus (22) for transmitting data between the mobile unit (14) and the master key (12) in the course of programming, **characterized by** an acoustic auxiliary apparatus (36) comprising an acoustic transmitter (38) ar-ranged on the master key (12) for transmitting an acoustic signal (50) to an acoustic receiver (40) as-sociated with the mobile unit (14), wherein the mas-ter key (12) and the mobile unit (14) are configured to enable a connection via the data-transfer appa-ratus (22) between the mobile unit (14) and the master key (12) only under the condition that the mobile unit (14) authenticates itself with respect to the master key (12), taking into account the acoustic signal (50) transmitted by the master key (12).
2. The locking system (10) according to claim 1, **char-**

acterized in that the acoustic transmitter (38) is a piezoceramic loudspeaker (42).

3. The locking system (10) according to any of the pre-ceding claims, **characterized in that** the mobile unit (14) is formed by a smartphone (16) **and in that** the acoustic receiver (40) is formed by a microphone (44) of the smartphone (16).
4. The locking system (10) according to any of the pre-ceding claims, **characterized in that** the acoustic transmitter (38), the acoustic signal (50) and the acoustic receiver (42) are tuned to one another such that reception of the acoustic signal (50) is only pos-sible if the acoustic transmitter (38) and the acoustic receiver (42) are at a maximum distance of 1 m, pref-erably at a maximum distance of 0.5 m, particularly at a maximum distance of 0.2 m, from one another.
5. The locking system (10) according to any of the pre-ceding claims, **characterized in that** the acoustic signal (50) - measured at a distance of 10 cm per-pendicular to a sound-emitting surface of the acous-tic transmitter (38) - has a maximum sound pressure level of 30 dB, preferably of at most 20 dB, particu-larly of at most 10 dB.
6. The locking system (10) according to any of the pre-ceding claims, **characterized in that** the data-trans-fer apparatus (22) is a Bluetooth apparatus.
7. A method for enabling a connection between a mo-bile unit (14) and a master key (12), wherein the con-nection is for transmitting data between the mobile unit (14) and the master key (12), using a locking system (10) according to claim 1, **characterized by:**
- sending a connection request (46) from the mo-bile unit (14) to the master key (12),
 - receiving the connection request (46) by the master key (12), generating an authentication request (52) and transmitting the authentication request (52) to the mobile unit (14) using the acoustic auxiliary apparatus (36),
 - receiving the authentication request (52) by the mobile unit (14), generating an authentication response (54) and sending it to the master key (12),
 - receiving the authentication response (54) by the master key (12), checking the authentication response (54) for identity with the authentication request (52), and in case of identity: releasing the connection between the mobile unit (14) and the master key (12).
8. The method according to claim 7, **characterized in that** the authentication request (52) contains a time stamp.

9. The method according to claim 7 or 8, **characterized in that** the authentication request (52) is an acoustically encoded random date, particularly a random number.
10. The method according to claim 9, **characterized in that** the authentication response (54) corresponds to the random date, particularly the random number.

Revendications

1. Système de fermeture (10), avec une clé principale (12) pour la programmation et l'actionnement d'un dispositif de fermeture (28), avec une unité mobile (14) pour la programmation de la clé principale (12), avec un dispositif de transmission de données (22) pour la transmission de données entre l'unité mobile (14) et la clé principale (12) au cours de la programmation, **caractérisé par** un dispositif acoustique supplémentaire (36), comprenant un émetteur acoustique (38) disposé sur la clé principale (12) pour transmettre un signal acoustique (50) à un récepteur acoustique (40) associé à l'unité mobile (14), dans lequel la clé principale (12) et l'unité mobile (14) sont conçues pour ne libérer une connexion via le dispositif de transmission de données (22) entre l'unité mobile (14) et la clé principale (12) qu'à la condition que l'unité mobile (14) s'authentifie vis-à-vis de la clé principale (12) en tenant compte du signal acoustique (50) envoyé par la clé principale (12).
2. Système de fermeture (10) selon la revendication 1, **caractérisé en ce que** l'émetteur acoustique (38) est un haut-parleur piézoélectrique (42).
3. Système de fermeture (10) selon l'une quelconque des revendications précédentes, **caractérisé en ce que** l'unité mobile (14) est formée par un téléphone intelligent (16) et que le récepteur acoustique (40) est formé par un microphone (44) du téléphone intelligent (16).
4. Système de fermeture (10) selon l'une quelconque des revendications précédentes, **caractérisé en ce que** l'émetteur acoustique (38), le signal acoustique (50) et le récepteur acoustique (42) sont accordés les uns aux autres de telle sorte qu'une réception du signal acoustique (50) n'est possible que si l'émetteur acoustique (38) et le récepteur acoustique (42) sont distants l'un de l'autre de 1 m maximum, de préférence de 0,5 m maximum, en particulier de 0,2 m maximum.
5. Système de fermeture (10) selon l'une quelconque des revendications précédentes, **caractérisé en ce que** le signal acoustique (50) - mesuré à une distance

de 10 cm perpendiculairement à une surface d'émission sonore de l'émetteur acoustique (38) - présente un niveau de pression acoustique maximal de 30 dB, de préférence de 20 dB maximum, en particulier de 10 dB maximum.

6. Système de fermeture (10) selon l'une quelconque des revendications précédentes, **caractérisé en ce que** le dispositif de transmission de données (22) est un dispositif Bluetooth.

7. Procédé pour libérer une connexion entre une unité mobile (14) et une clé principale (12), dans lequel la connexion sert à la transmission de données entre l'unité mobile (14) et la clé principale (12), en utilisant un système de fermeture (10) selon la revendication 1, **caractérisé par** :

- l'envoi d'une demande de connexion (46) de l'unité mobile (14) à la clé principale (12),
- la réception de la demande de connexion (46) par la clé principale (12), la génération d'une

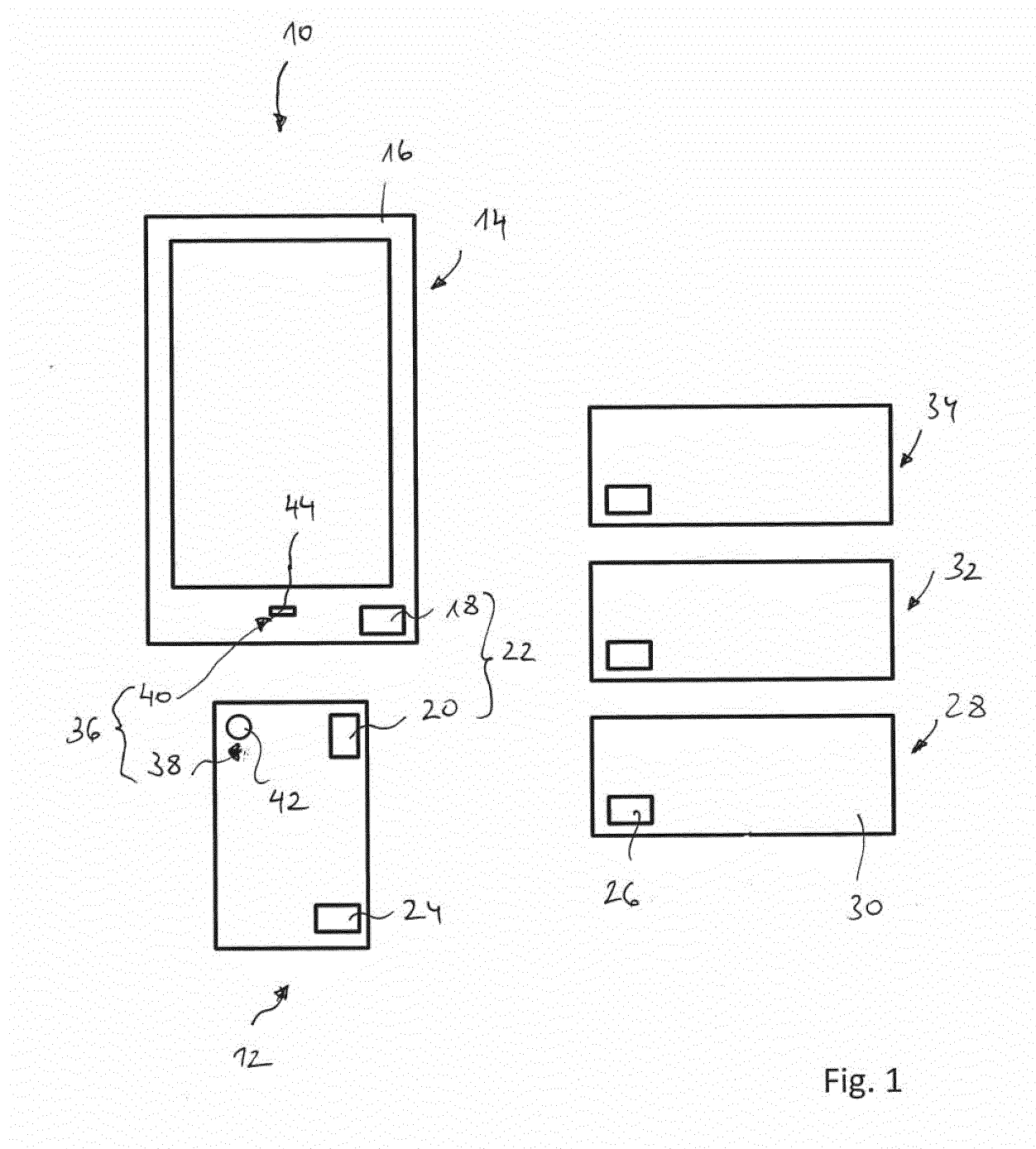
requête d'authentification (52) et l'envoi de la requête d'authentification (52) à l'unité mobile (14) en utilisant le dispositif acoustique supplémentaire (36),

- la réception de la requête d'authentification (52) par l'unité mobile (14), la génération d'une réponse d'authentification (54) et l'envoi à la clé principale (12),
- la réception de la réponse d'authentification (54) par la clé principale (12), le contrôle de la réponse d'authentification (54) en vue d'y détecter l'identité avec la requête d'authentification (52), et dans le cas de l'identité : la libération de la connexion entre l'unité mobile (14) et la clé principale (12).

8. Procédé selon la revendication 7, **caractérisé en ce que** la requête d'authentification (52) contient un horodatage.

9. Procédé selon la revendication 7 ou 8, **caractérisé en ce que** la requête d'authentification (52) est une donnée aléatoire codée acoustiquement, en particulier un nombre aléatoire.

10. Procédé selon la revendication 9, **caractérisé en ce que** la réponse d'authentification (54) correspond à la donnée aléatoire, notamment au nombre aléatoire.



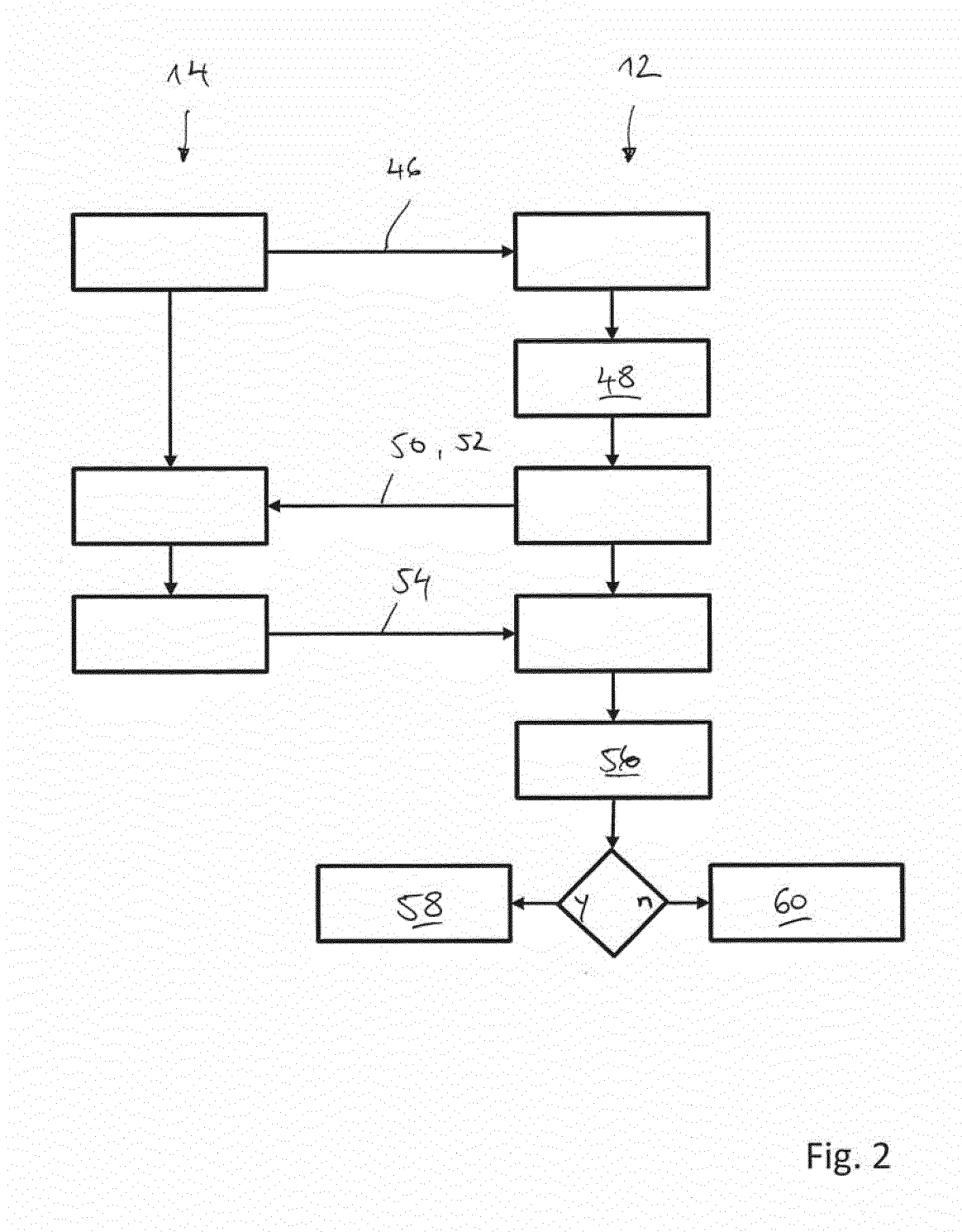


Fig. 2

IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

Diese Liste der vom Anmelder aufgeführten Dokumente wurde ausschließlich zur Information des Lesers aufgenommen und ist nicht Bestandteil des europäischen Patentdokumentes. Sie wurde mit größter Sorgfalt zusammengestellt; das EPA übernimmt jedoch keinerlei Haftung für etwaige Fehler oder Auslassungen.

In der Beschreibung aufgeführte Patentdokumente

- US 2021037099 A1 [0001]
- DE 102015009199 A1 [0006]