

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
30. Juli 2020 (30.07.2020)



(10) Internationale Veröffentlichungsnummer
WO 2020/151987 A1

- (51) Internationale Patentklassifikation:
G07C 1/10 (2006.01) G07C 9/00 (2020.01)
G07C 1/32 (2006.01) E05B 39/04 (2006.01)
- (21) Internationales Aktenzeichen: PCT/EP2020/050723
- (22) Internationales Anmeldedatum:
13. Januar 2020 (13.01.2020)
- (25) Einreichungssprache: Deutsch
- (26) Veröffentlichungssprache: Deutsch
- (30) Angaben zur Priorität:
10 2019 000 559.7
25. Januar 2019 (25.01.2019) DE
- (71) Anmelder: SMART ACCESS SOLUTIONS UG (HAFTUNGSBESCHRÄNKT) [DE/DE]; c/o: Werk1, Atelierstr. 29, 81671 München (DE).
- (72) Erfinder: STÖTTER, Tobias; Heimeranstr. 49, 80339 München (DE). EPPLE, Anton; Bergmannstr. 52, 80339 München (DE). SCHMIDT, Martin; Margeritenstr. 12b, 85586 Poing (DE).
- (74) Anwalt: KEHL, ASCHERL, LIEBHOFF & ETTMAYR; Emil-Riedel-Str. 18, 80538 Munich (DE).
- (81) Bestimmungsstaaten (soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD,

(54) Title: CONTAINER, METHOD, AND SYSTEM FOR ENABLING OFFLINE ACCESS CONTROL AND FOR ENABLING OFFLINE SENSOR DATA TRANSMISSION

(54) Bezeichnung: BEHÄLTNIS, VERFAHREN UND SYSTEM ZUM ERMÖGLICHEN EINER OFFLINEZUGANGSKONTROLLE UND ZUM ERMÖGLICHEN EINER OFFLINESENSORDATENÜBERMITTLUNG

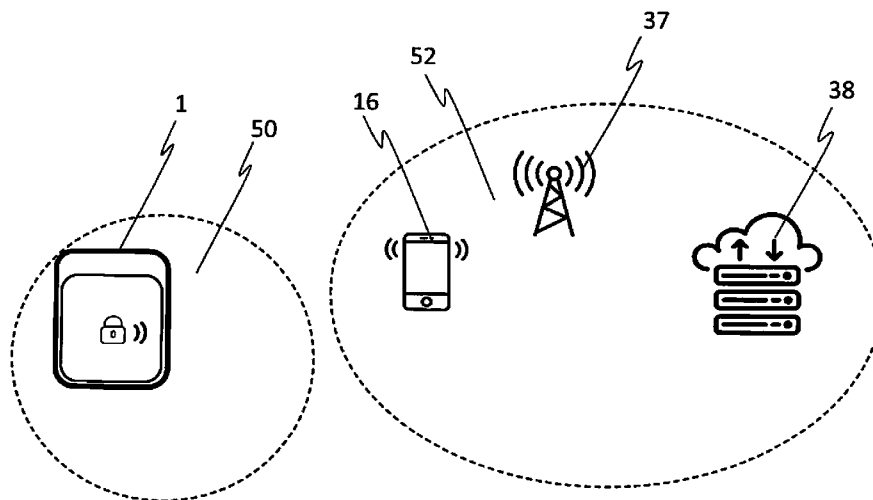


Fig. 7

(57) Abstract: The present invention relates to a method for opening a container. The method comprises at least the following steps: providing a container (1) according to any one of the preceding claims; providing a mobile terminal (16), the mobile terminal (16) having a near-field data transmission means (34) for exchanging data with the near-field data transmission device (14) of the container (1), the mobile terminal (16) having a far-field data transmission means (36), in particular LTE, for exchanging data with a server (38), the mobile terminal (16) having a processor device (40) for executing a control application, the mobile terminal (16) having a memory



WO 2020/151987 A1

ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO,
 NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW,
 SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN,
 TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Bestimmungsstaaten (soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— mit internationalem Recherchenbericht (Artikel 21 Absatz 3)

device (42) for storing container reconfiguration data and container operation data, the container operation data being transmitted by the near-field data transmission device (14) to the near-field data transmission means (34) of the mobile terminal (16) for forwarding to the server device, and the mobile terminal (16) receiving the container reconfiguration data from the server (38) via the far-field data transmission means (36), the container reconfiguration data being generated in response to the container operation data transmitted to the server (38) by means of the near-field data transmission means (34), and the container operation data comprising at least time data and access data.

(57) Zusammenfassung: Die vorliegende Erfindung bezieht sich auf ein Verfahren zum Öffnen eines Behältnisses. Das Verfahren weist dabei mindestens die Schritte auf: Bereitstellen eines Behältnisses (1) nach einem der vorangegangenen Ansprüche, Bereitstellen eines mobilen Endgeräts (16), wobei das mobile Endgerät (16) ein Nahfelddatenübertragungsmittel (34) zum Datenaustausch mit der Nahfelddatenübertragungseinrichtung (14) des Behältnisses (1) aufweist wobei das mobile Endgerät (16) ein Fernfelddatenübertragungsmittel (36), insbesondere LTE, zum Datenaustausch mit einem Server (38) aufweist, wobei das mobile Endgerät (16) eine Prozessoreinrichtung (40) zum Ausführen einer Steuerungsapplikation aufweist, wobei das mobile Endgerät (16) eine Speichereinrichtung (42) zum Speichern von Behältnisneukonfigurationsdaten und von Behältnisbetriebsdaten aufweist, wobei die Behältnisbetriebsdaten durch die Nahfelddatenübertragungseinrichtung (14) zur Weiterleitung an die Servereinrichtung an das Nahfelddatenübertragungsmittel (34) des mobilen Endgeräts (16) übermittelt werden und wobei das mobile Endgerät (16) die Behältnisneukonfigurationsdaten vom Server (38) über das Fernfelddatenübertragungsmittel (36) empfängt, wobei die Behältnisneukonfigurationsdaten in Antwort auf die mittels dem Nahfelddatenübertragungsmittel (34) an den Server (38) übermittelten Behältnisbetriebsdaten erzeugt werden, wobei die Behältnisbetriebsdaten zumindest Zeitdaten und Zugangsdaten aufweisen.

Behältnis, Verfahren und System zum Ermöglichen einer Offlinezugangskontrolle und zum Ermöglichen einer Offlinesensordatenübermittlung

Die vorliegende Erfindung bezieht sich gemäß Anspruch 1 auf ein Behältnis zum Aufnehmen von Objekten, gemäß Anspruch 8 auf ein Verfahren, in dem ein solches Behältnis verwendet wird, und gemäß Anspruch 15 auf ein System.

Es lassen sich Entwicklungen im Bereich der Zugangskontrollsysteme, insbesondere im Bereich der Hausautomatisierung, erkennen, die ein Öffnen eines Schlosses an die Präsenz eines Smartphones koppelt. Dabei können grob zwei Ausprägungen unterschieden werden. Zum einen die Fälle, in denen Daten vom Smartphone über eine App an einen Server und von diesem Server an das Schloss gesendet werden. Zum anderen gibt es Lösungen in denen Schlüsselinformationen bereits im Smartphone hinterlegt sind, so dass eine direkte Kommunikation zwischen Smartphone und Schloss stattfindet (ggf. hat das Schloss keine Verbindung zum Internet). In beiden Ausprägungen wird das Schloss geöffnet, wenn die übermittelten Daten mit den hinterlegten Daten übereinstimmen.

Um jedoch die im Schloss hinterlegten Daten sicher zu verändern (Schlüssel hinzufügen, oder löschen, oder zeitliche Beschränkungen konfigurieren, etc.), benötigt das Schloss zwingend eine Verbindung zum Internet, damit die sichere Übertragung von einer zentralen Stelle erfolgen kann.

Wenn keine Verbindung des Schlosses zum Internet besteht, dann bleibt nur die Möglichkeit, dass die Konfiguration des Schlosses lokal vorgenommen wird, wie dies z.B. bei RFID Schlössern mit „Programmierkarten“ üblich ist. Da dies bei einer sehr hohen Anzahl und weit verteilten oder gar mobilen Schlössern jedoch einerseits unpraktikabel ist, da alle Schlösser einzeln manuell aktualisiert werden müssen – von einer Person, die über entsprechende Programmierertools und Konfigurationsdaten verfügt und auch die Möglichkeit hat Zugriff auf das Schloss zu erhalten. Zum anderen ist die Methode schlichtweg nicht sicher, da nicht zentral überwacht werden kann, ob die Neukonfiguration bei allen Schlössern überhaupt durchgeführt wurde oder diese erfolgreich war.

In Bereichen, in denen keine Internetverbindung vorliegt, oder bei Objekten, die nicht mit einer dauerhaften Datenverbindung ausgestattet werden können, ist eine sichere und zentrale Verwaltung der verteilten Schlösser heute nicht möglich.

Es ist somit eine Aufgabe der vorliegenden Erfindung ein Behältnis, ein Verfahren und ein System bereitzustellen, wodurch eine Verbesserung des Standes der Technik ermöglicht wird. Zusätzlich oder alternativ soll eine Offlinezugangskontrolle und/oder eine Offlinesensordatenübertragung ermöglicht werden. Offline bedeutet hierbei, dass das Objekt selbst zeitweise, insbesondere dauerhaft, keine direkte Verbindung zum Internet aufbauen kann, insbesondere keine Mittel zum Aufbauen einer solchen Verbindung aufweist.

Die zuvor genannte Aufgabe wird erfindungsgemäß durch ein Behältnis, insbesondere nach Anspruch 1, zum Aufnehmen von Objekten, insbesondere von Proben mit biologischem Material, gelöst. Das Behältnis weist dabei bevorzugt zumindest einen Hauptkörper auf, wobei der Hauptkörper ein Aufnahmevolumen mehrseitig umschließt. Ferner weist das Behältnis bevorzugt eine gegenüber dem Hauptkörper beweglich, insbesondere verschließbar, angeordnete Öffnungseinrichtung, insbesondere eine Tür oder Klappe, auf. Weiterhin ist eine Schlossvorrichtung zum Verhindern einer definierten Relativbewegung der Öffnungseinrichtung gegenüber dem Hauptkörper vorgesehen, wobei die Schlossvorrichtung einen elektrisch betriebenen Aktuator aufweist. Ferner ist eine Nahfelddatenübertragungseinrichtung zum Empfangen von Daten von mindestens einem sich in einem definierten Abstandsbereich zu dem Behältnis zeitweise befindenden mobilen Endgerät und zum Senden von Daten an das zumindest eine sich in einem definierten Abstandsbereich zu dem Behältnis zeitweise befindenden mobilen Endgerät vorgesehen. Weiterhin ist eine Speichereinheit zum zeitweisen Speichern von Zeitdaten und Zugangsdaten vorgesehen, wobei die Zeitdaten zumindest Daten zum letzten Öffnungszeitpunkt und/oder zumindest Daten zum letzten Verschlusszeitpunkt aufweist, wobei die Zugangsdaten zumindest Berechtigungsdaten und Identifikationsdaten aufweisen, wobei die Berechtigungsdaten definieren, in Abhängigkeit welcher Identifikationsdaten der Aktuator die Schlossvorrichtung aus einer geschlossenen Konfiguration in eine geöffnete Konfiguration überführt und wobei die Identifikationsdaten eine Zuordnung zu dem mobilen Endgerät, insbesondere zu einer definierten auf dem mobilen Endgerät ausgeführten bzw. ausführbaren Applikation bzw. einem Programm, insbesondere cloudbasiert, vorgeben. Ferner ist eine Prozessoreinrichtung zum Abgleich der Berechtigungsdaten und der Identifikationsdaten vorgesehen, wobei der Aktuator im Falle eines positiven Abgleichs von der Prozessoreinrichtung zum Öffnen der Schlossvorrichtung ansteuerbar ist, wobei ein positiver Abgleich eine definierte Übereinstimmung der abgeglichenen Daten repräsentiert. Weiterhin ist eine von einem Feststromanschluss verschiedene Energiequelle zum Betreiben von zumindest dem Aktuator, der Nahfelddatenübertragungseinrichtung, der Speichereinheit und der Prozessoreinrichtung vorgesehen. Als Festschlussanschluss gelten hiermit bevorzugt nur

solche Anschlüsse, welche mittels einer Kabelverbindung Strom aus einer Versorgerinfrastruktur und somit aus einem besonders bevorzugt zumindest 100m oder 1000m oder 2km oder 3km oder 5km oder 10km entfernten Kraftwerk, wie Kohlekraftwerk, Windkraftwerk, Wasserkraftwerk oder Solarkraftwerk, beziehen. Besonders bevorzugt weist das Objekt zur Datenübermittlung nur die Nahfelddatenübertragungseinrichtung auf und somit besonders bevorzugt keine Fernfelddatenübertragungseinrichtung, insbesondere keine Einrichtung zur Erzeugung einer Mobilfunkdatenverbindung, wie z.B. einer GSM, UMTS oder LTE Verbindung.

Diese Lösung ist vorteilhaft, da das Objekt losgelöst von einer stationären Infrastruktur verwendet bzw. betrieben werden kann. Ferner können eine Vielzahl an Daten bzgl. der Benutzung des Behältnisses erfasst und bereitgestellt werden. Dadurch, dass das Behältnis vorzugsweise keine Fernfelddatenübertragungseinrichtung aufweist, können die Kosten für das Behältnis sehr niedrig sein. Zudem ist dadurch der Gesamtenergiebedarf der elektrischen Komponenten des Behältnisses sehr niedrig. Das Behältnis kann zusätzlich oder alternativ mit IoT Übertragungstechnologien, wie z.B. Narrowband IoT und/oder LORA WAN ausgestattet werden.

Weitere bevorzugte Ausführungsformen der vorliegenden Erfindung sind Gegenstand der Unteransprüche und/oder der nachfolgenden Beschreibungsteile.

Gemäß einer weiteren bevorzugten Ausführungsform der vorliegenden Erfindung sind die Prozessoreinrichtung, die Speichereinheit und die Nahfelddatenübertragungseinrichtung und bevorzugt ebenfalls die Energiequelle als Teil der Schlossvorrichtung ausgebildet, wobei die Prozessoreinrichtung, die Speichereinheit und die Nahfelddatenübertragungseinrichtung in einer geschlossenen Konfiguration des Behälters im Inneren des Behälters angeordnet sind. Diese Ausführungsform ist vorteilhaft, da sehr kurze Datenübertragungswege und sehr kurze Energieübertragungswege vorliegen. Ferner können der Grundkörper des Behältnisses und die Schlossvorrichtung getrennt voneinander hergestellt werden. Weiterhin ist es möglich, dass sich die vorliegende Erfindung alternativ auf eine solche Schlossvorrichtung bezieht. Dies kann vorteilhaft sein, da die Schlossvorrichtung so in unterschiedlichen Behältnissen verwendet werden kann.

Ein oder mindestens ein Temperatursensor ist gemäß einer weiteren bevorzugten Ausführungsform der vorliegenden Erfindung im Inneren des Behältnisses oder an einer Wandung des Behältnisses angeordnet, wobei der Temperatursensor Temperaturwerte oder Temperaturdaten ausgibt, wobei durch die Prozessoreinrichtung die Temperaturwerte in Form von Daten oder die Temperaturdaten zusammen mit Zeitdaten und/oder Zugangsdaten in der

Speichereinheit abspeicherbar sind. Diese Ausführungsform ist vorteilhaft, da z.B. in Abhängigkeit von der Zeit bestimmt werden kann, welchen Temperaturen die im Behältnis angeordneten Objekte ausgesetzt waren. Somit lassen sich z.B. bei Proben von biologischem Material unmittelbar Aussagen treffen, ob diese Proben noch untersucht werden können oder als Ausschuss gelten müssen. Dies hat den Vorteil, dass Proben, die als Ausschuss gelten, nicht unnötig analysiert werden, wodurch Kapazitäten verbessert werden und Kosten reduziert werden.

Gemäß einer weiteren bevorzugten Ausführungsform der vorliegenden Erfindung ist ein oder mindestens ein Feuchtigkeitssensor im Inneren des Behältnisses oder an einer Wandung des Behältnisses angeordnet ist, wobei der Feuchtigkeitssensor Feuchtigkeitswerte oder Feuchtigkeitsdaten ausgibt, wobei durch die Prozessoreinrichtung die Feuchtigkeitswerte in Form von Daten oder die Feuchtigkeitsdaten zusammen mit Zeitdaten und/oder Zugangsdaten und/oder Temperaturdaten in der Speichereinheit abspeicherbar sind. Diese Ausführungsform ist vorteilhaft, da dadurch Effekte auf die im Behältnis vorgehaltenen Objekte bestimmbar sind. Der Feuchtigkeitssensor oder die Feuchtigkeitssensoren, können z.B. auch zur Detektion von aus dem Objekt austretender, insbesondere auslaufender oder verdampfender, Flüssigkeit dienen. Somit können z.B. Konzentrationsveränderungen der im Objekt vorgehaltenen Flüssigkeit bestimmt werden. Zusätzlich oder alternativ können Defekte des Objekts und somit Leckage detektiert werden.

Gemäß einer weiteren bevorzugten Ausführungsform der vorliegenden Erfindung ist ein oder mindestens ein Gewichtssensor in einer den Boden des Behältnisses bildenden Wandung oder auf der den Boden bildenden Wandung angeordnet, wobei der Gewichtssensor Gewichtswerte oder Gewichtsdaten ausgibt. Die Prozessoreinrichtung speichert die Gewichtswerte bevorzugt in Form von Daten und/oder die Gewichtsdaten zusammen mit Zeitdaten und/oder Zugangsdaten und/oder Temperaturdaten und/oder Feuchtigkeitsdaten in der Speichereinheit ab. Diese Ausführungsform ist vorteilhaft, da durch die Gewichtsdaten erfasst werden kann, ob ein Objekt in dem Behältnis angeordnet ist. Zusätzlich oder alternativ lässt sich dadurch bestimmen, ob das Objekt das richtige Objekt ist, d.h. das richtige Objekt oder ein anderes in dem Behältnis abgestellt wurde. Daten zum Objekt werden bevorzugt mittels einer Registriereinrichtung, die bevorzugt nicht Teil des Behältnisses ist, vor der Positionierung des Objekts im Behältnis erfasst. Die Registriereinrichtung kann hierbei zeitweise oder dauerhaft eine Verbindung zum Internet aufweisen und übermittelt bevorzugt objektspezifische Daten und/oder behälterspezifische Daten an die Servereinrichtung. Die Servereinrichtung übermittelt bevorzugt die objektspezifischen Daten und/oder die behälterspezifischen Daten an das mobile Endgerät. Das Behältnis übermittelt dann die

Sensordaten an das mobile Endgerät und das mobile Endgerät führt bevorzugt einen Abgleich der registrierten Daten mit den Ist-Daten des Behältnisses durch. Je nach Objekt kann dieser Abgleich dazu verwendet werden, dass Öffnungsdaten zum Öffnen des Behältnisses überschrieben oder ersetzt werden und das Behältnis verschlossen bleibt, sollte der Abgleich Abweichungen, die über einem definierten Schwellenwert liegen, ergeben. Dies kann z.B. bei Objekten wichtig sein, die Gefahrstoffe, wie Gift, Viren, Bakterien, Sporen, etc. aufweisen.

Durch die Prozessoreinrichtung sind gemäß einer weiteren bevorzugten Ausführungsform Energiequellendaten erzeugbar, wobei die Energiequellendaten Daten zum Ladestand und/oder zum Grad der Entladung über einen definierten Zeitraum und/oder zur Veränderung der Spannung über einen definierten Zeitraum aufweisen. Diese Ausführungsform ist vorteilhaft, da in Abhängigkeit dieser Daten z.B. ein Austausch der Energiequelle vorgenommen werden kann.

Gemäß einer noch weiteren bevorzugten Ausführungsform der vorliegenden Erfindung begrenzt das Behältnis in der geschlossenen Konfiguration ein Volumen von weniger als 10m^3 , insbesondere von weniger als 5m^3 oder von weniger als 2m^3 oder von weniger als 1m^3 oder von weniger als $0,5\text{m}^3$ oder von weniger als $0,1\text{m}^3$, bzw. haust dieses ein bzw. umschließt dieses. Zusätzlich oder alternativ ist die mittlere Wandstärke der Wandungen des Behältnisses bevorzugt weniger als 30mm dick, insbesondere weniger als 20mm oder weniger als 10mm dick ist oder zwischen 20mm und 8mm dick ist oder weniger als 5mm dick ist oder weniger als 3mm dick ist. Zusätzlich oder alternativ überlagert die Öffnungseinrichtung eine in der geschlossenen Konfiguration zur Öffnungseinrichtung parallel erstreckenden Wandung zu zumindest 50% (der Wandungsfläche), insbesondere zu zumindest 60% (der Wandungsfläche) oder zu zumindest 80% (der Wandungsfläche) oder zu zumindest 90% (der Wandungsfläche). Zusätzlich oder alternativ weist die Wandungen ein oder mindestens ein Metall oder ein oder mindestens ein Polymerwerkstoff oder ein oder mindestens ein Kompositwerkstoff auf oder besteht zu zumindest 50% (massemäßig), insbesondere zu zumindest 60% (massemäßig) oder zu zumindest 70% (massemäßig) oder zu zumindest 80% (massemäßig) oder zu zumindest 90% (massemäßig), daraus. Zusätzlich oder alternativ die Energiequelle eine Batterie ist, wobei die Batterie eine Mindestkapazität bzw. elektrische Ladung von mindesten oder genau oder bis zu 500 mAh oder von mindesten oder genau oder bis zu 1400 mAh oder von mindesten oder genau oder bis zu 2000 mAh oder von mindesten oder genau oder bis zu 3000 mAh oder von mindesten oder genau oder bis zu 10000 mAh oder von mindesten oder genau oder bis zu 15000 mAh oder von mindesten oder genau oder bis zu 25000 mAh oder von mindesten oder genau oder bis zu 50000 mAh oder von mindesten oder genau oder bis zu 100000 mAh aufweist. Zusätzlich oder alternativ kann die

Nahfelddatenübertragungseinrichtung eine RFID, Bluetooth, WLAN, ZigBee und/oder Z-Wave Datenübertragungseinrichtung sein.

Die oben genannte Aufgabe wird erfindungsgemäß durch ein Verfahren nach Anspruch 8 gelöst. Dieses Verfahren dient zum Öffnen eines hierin beschriebenen Behältnisses, insbesondere nach einem der Ansprüche 1 bis 7. Das Verfahren weist dabei bevorzugt die nachfolgenden Schritte auf: Bereitstellen eines Behältnisses, insbesondere einem hierin beschriebenen Behältnis, Bereitstellen eines mobilen Endgeräts, wobei das mobile Endgerät ein Nahfelddatenübertragungsmittel zum Datenaustausch mit der Nahfelddatenübertragungseinrichtung des Behältnisses aufweist, wobei das mobile Endgerät ein Fernfelddatenübertragungsmittel, insbesondere LTE, zum Datenaustausch mit einem Server aufweist, wobei das mobile Endgerät eine Prozessoreinrichtung zum Ausführen einer Steuerungsapplikation aufweist, wobei das mobile Endgerät eine Speichereinrichtung zum Speichern von Behältnisneukonfigurationsdaten und von Behältnisbetriebsdaten aufweist, wobei die Behältnisbetriebsdaten durch die Nahfelddatenübertragungseinrichtung zur Weiterleitung an die Servereinrichtung an das Nahfelddatenübertragungsmittel des mobilen Endgeräts übermittelt werden und wobei das mobile Endgerät die Behältnisneukonfigurationsdaten vom Server über das Fernfelddatenübertragungsmittel empfängt, wobei die Behältnisneukonfigurationsdaten in Antwort auf die mittels dem Nahfelddatenübertragungsmittel an den Server übermittelten Behältnisbetriebsdaten erzeugt werden, wobei die Behältnisbetriebsdaten zumindest Zeitdaten und Zugangsdaten aufweisen.

Das erfindungsgemäße Verfahren ist vorteilhaft, da es eine sichere Vergabe eindeutiger Zugriffsrechte (z.B. Key für ein elektronisches Schloss) ohne Verwendung spezialisierter Hardware (z.B. RFID Token oder mechanischer Schlüssel), sowie ohne bestehende Internetverbindung (zum Zeitpunkt der Öffnung / keine „realtime“ Abfrage bei einem Server) möglich.

Besonders vorteilhaft ist hierbei, dass verschiedene (wechselnden) Personen bzw. mobile Endgeräte Zugriff auf einen speziell geschützten Bereich erhalten können. Der Zugriff wird bevorzugt elektronisch verwaltet und die Gewährung wird bevorzugt granular konfiguriert, d.h. es kann z.B. zeitpunkt- oder zeitbereichabhängig und/oder userabhängig und/oder ortsabhängig und/oder prioritätsabhängig eine Zugangsberechtigung erteilt und/oder widerrufen werden. Somit kann z.B. das Öffnen eines bestimmten Behältnisses nur ein einem bestimmten Tag in einem genau festgelegten Zeitfenster ermöglicht werden. Prioritätsabhängig bedeutet hierbei bevorzugt, dass ein User und/oder ein Endgerät mit einer höheren Berechtigung das Behältnis auch dann öffnen kann, wenn ein anderer User/Nutzer und/oder ein anderes Endgerät das Behältnis bereits registriert hat.

Verfügt das Endgerät eines Users über keine bestehende Internetverbindung, so kann er zum Zeitpunkt, zu dem er das Schloss bzw. die Schlossvorrichtung öffnen möchte auch nicht bei einem „Key-Server“, z.B. unter Eingabe der Schloss-ID nachfragen ob er die Berechtigung hat das Schloss zu öffnen, bzw. den notwendigen Key abzufragen. Anwendungsfälle hierbei sind neben anderen Zugriffsrechten auf elektronische Schlösser in nicht mit mobilem Internet versorgten Bereichen (Funklöcher, Naturschutzgebiete, unter Tage, unter Wasser, etc.).

Gemäß einer bevorzugten Ausführungsform der vorliegenden Erfindung weisen die Zeitdaten zumindest Daten zum letzten Öffnungszeitpunkt und/oder zumindest Daten zum letzten Verschlusszeitpunkt auf. Die Zugangsdaten weisen dabei bevorzugt Berechtigungsdaten und Identifikationsdaten auf, wobei die Berechtigungsdaten definieren, in Abhängigkeit welcher Identifikationsdaten der Aktuator die Schlossvorrichtung aus einer geschlossenen Konfiguration in eine geöffnete Konfiguration überführt und wobei die Identifikationsdaten eine Zuordnung zu dem mobilen Endgerät vorgeben.

Diese Lösung ist ferner vorteilhaft, da der „Schlüsselträger“ bzw. der User über ein Mobilgerät verfügt, das grundsätzlich mit einer permanenten Internetverbindung, ausgestattet ist. Auf dem Mobilgerät ist bevorzugt eine Applikation installiert, die sich regelmäßig und/oder zu definierten Zeitpunkten und/oder in Abhängigkeit von definierten Ereignissen, insbesondere Positionsdaten, mit einem Key-Server synchronisiert, auf dem die Zugriffsrechte für den „Schlüsselträger“ verwaltet werden, bzw. Änderungen an den Rechten aktiv an die Applikation überträgt.

Die Übertragung erfolgt bevorzugt verschlüsselt, so dass der eigentliche Key nicht im Klartext erscheint. Darüber hinaus werden bevorzugt die Systemzeiten synchronisiert, so dass Abweichungen der lokalen Zeit des Schlüsselträgers kompensiert werden können (falls Zugriff nur in einem Zeitfenster gewährt werden soll). Erreicht der „Schlüsselträger“ nun das Behältnis, das geöffnet werden soll, muss die eindeutige Schloss-ID an die Applikation übermittelt werden (z.B. eintippen, über Barcode, Übermittlung via Bluetooth, oder eine andere Funktechnologie). Die Applikation des mobilen Endgeräts prüft nun lokal ob Zugriffsrechte bestehen. Bei positiver Prüfung erhält der „Schlüsselträger“ Zugriff (in dem ihm der Code angezeigt wird, oder das Signal zur Öffnung des Schlosses von der Applikation per Funk (z.B. Bluetooth) übertragen wird).

Mit dem vorgestellten Verfahren können unter Verwendung definierter Geräte und Technologien (Mobiltelefon, mobiler Internetzugang, mobile Applikation, Key Server, Verschlüsselung, gesicherte Übertragungstechnologien) und bevorzugt ohne Einsatz spezialisierter Hardware, unterschiedliche Zugriffe für multiple Nutzer online verwaltet werden, auch wenn nicht sichergestellt werden kann, dass zum Zeitpunkt des Zugriffs auf den geschützten Bereich eine Onlineverbindung besteht.

Das Behältnis weist gemäß einer weiteren bevorzugten Ausführungsform der vorliegenden Erfindung mindestens einen Sensor auf, wobei der Sensor Daten und/oder Signale an der Prozessoreinrichtung des Behältnisses bereitstellt und die Nahfelddatenübertragungseinrichtung des Behältnisses übermittle Signale und/oder Daten, welche die Sensordaten oder Sensorsignale repräsentieren oder darstellen, als Bestandteil der Behältnisbetriebsdaten an das Nahfelddatenübertragungsmittel des mobilen Endgeräts. In der Speichereinrichtung des mobilen Endgeräts werden bevorzugt vom Server bzw. der Servereinrichtung bereitgestellte Identifikationsdaten bereitgestellt, wobei die Identifikationsdaten zusammen mit den Behältnisneukonfigurationsdaten oder als separater Datensatz an das mobile Endgerät übermittle werden. Bevorzugt werden die Identifikationsdaten zusammen mit spezifischen Gerätedaten des mobilen Endgeräts infolge einer Zugangsberechtigungsanfrage mittels dem Nahfelddatenübertragungsmittel an die Nahfelddatenübertragungseinrichtung übermittle. Besonders bevorzugt werden zumindest die Identifikationsdaten in der Speichereinheit abgespeichert und mit in der Speichereinheit vorhandenen Berechtigungsdaten abgeglichen. In Abhängigkeit eines sich aus dem Abgleich ergebenden Abgleichergebnisses verbleibt die Schlossvorrichtung im verschlossenen Zustand oder wird in einen geöffneten Zustand überführt. Ein konkreter Satz an Behältnisbetriebsdaten wird von der Prozessoreinrichtung des Behältnisses bevorzugt in der Speichereinheit modifiziert vorgehalten bzw. hinterlegt bzw. abgespeichert, zumindest nachdem dieser Satz an Behältnisbetriebsdaten an das mobile Endgerät übermittle wurde. Die Behältnisneukonfigurationsdaten der Prozessoreinrichtung des Behältnisses geben dabei bevorzugt vor, welche Daten, insbesondere welcher konkrete Satz an Behältnisdaten, aus der Speichereinheit gelöscht wird, wobei die Prozessoreinrichtung des Behältnisses in Abhängigkeit der Behältnisneukonfigurationsdaten die Daten aus der Speichereinheit löscht. Die Behältnisneukonfigurationsdaten weisen dabei bevorzugt Berechtigungsdaten und eine Anweisung an die Prozessoreinrichtung des Behältnisses auf, die in der Speichereinheit vorgehaltenen Berechtigungsdaten durch die Berechtigungsdaten der Behältnisneukonfigurationsdaten zu ersetzen und/oder zu erweitern.

Die oben genannte Aufgabe wird erfindungsgemäß zudem durch ein Computerprogrammprodukt zum Ausführen eines hierin genannten Verfahrens gelöst.

Weiterhin wird die oben genannte Aufgabe ebenfalls durch ein System gemäß Anspruch 15 gelöst.

Das erfindungsgemäße System weist dabei bevorzugt zumindest eine Vielzahl an Behältnisse, insbesondere hierin beschriebene Behältnisse, und eine Vielzahl an mobilen Endgeräten auf, wobei jedes mobile Endgerät ein Nahfelddatenübertragungsmittel zum Datenaustausch mit der Nahfelddatenübertragungseinrichtungen der Behältnisse aufweist und ein

Fernfelddatenübertragungsmittel, insbesondere LTE, zum Datenaustausch mit einem Server aufweist und eine Prozessoreinrichtung zum Ausführen einer Steuerungsapplikation aufweist und eine Speichereinrichtung zum Speichern von Behältnisneukonfigurationsdaten und von Behältnisbetriebsdaten aufweist. Die Behältnisbetriebsdaten werden dabei bevorzugt durch die Nahfelddatenübertragungseinrichtung zur Weiterleitung an die Servereinrichtung an das Nahfelddatenübertragungsmittel des jeweiligen mobilen Endgeräts übermittelt. Die Behältnisbetriebsdaten weisen dabei zumindest Zeitdaten und Zugangsdaten auf, wobei die Zeitdaten bevorzugt zumindest Daten zum letzten Öffnungszeitpunkt und/oder zumindest Daten zum letzten Verschlusszeitpunkt aufweisen. Weiterhin weist das System bevorzugt eine oder mindestens eine Servereinrichtung, insbesondere eine Cloud-Servereinrichtung, auf. Die Servereinrichtung empfängt dabei bevorzugt vom jeweiligen mobilen Endgerät die Behältnisbetriebsdaten und nach dem Empfang der Behältnisbetriebsdaten erzeugt die Servereinrichtung Behältnisneukonfigurationsdaten. Diese Behältnisneukonfigurationsdaten werden von der Servereinrichtung an das mobile Endgerät oder an mehrere mobile Endgeräte oder an definierte mobile Endgeräte gesendet. Bevorzugt sendet die Servereinrichtung die Behältnisneukonfigurationsdaten an das mobile Endgerät von dem es die Behältnisbetriebsdaten empfangen hat oder sie sendet die Behältnisneukonfigurationsdaten an ein anderes mobiles Endgerät, das dem Behältnis zugeordnet ist, oder sie sendet die Behältnisneukonfigurationsdaten an eine Gruppe von mobilen Endgeräten, wobei bevorzugt einzelne, mehrere, die Mehrzahl oder alle der Gruppe zugeordneten mobilen Endgeräte dem Behältnis zugeordnet sind.

Weitere Vorteile, Ziele und Eigenschaften der vorliegenden Erfindung werden anhand nachfolgender Beschreibung anliegender Zeichnungen erläutert, in welchen beispielhaft das erfindungsgemäße Verfahren dargestellt ist. Bauteile oder Elemente, die in dem erfindungsgemäßen Verfahren bevorzugt eingesetzt werden und/oder welche in den Figuren wenigstens im Wesentlichen hinsichtlich ihrer Funktion übereinstimmen, können hierbei mit gleichen Bezugszeichen gekennzeichnet sein, wobei diese Bauteile oder Elemente nicht in allen Figuren beziffert oder erläutert sein müssen.

Darin zeigen:

- Fig. 1 bis 6 rein schematisch ein Beispiel für ein erfindungsgemäßes Behältnis;
- Fig. 7 bis 10 rein schematisch ein Beispiel für die Datenübertragung gemäß dem erfindungsgemäßen Verfahren oder System; und
- Fig. 11 rein beispielsweise ein bevorzugter Verfahrensablauf gemäß der vorliegenden Erfindung, wobei einzelne oder mehrere der gezeigten Schritte nicht oder auch in einer anderen Abfolge oder auch mehrfach durchgeführt werden können.

Die Figuren 1a bis 3 zeigen dabei schematisch eine Schlossvorrichtung 10 zum Verhindern einer definierten Relativbewegung einer Öffnungseinrichtung 8 gegenüber dem Hauptkörper 4.

Die Schlossvorrichtung 10 weist dabei bevorzugt einen elektrisch betriebenen Aktuator 12 auf.

Ferner ist in der Schlossvorrichtung 10 zumindest oder genau eine Sensoreinrichtung bzw. ein Sensor angeordnet.

Der Sensor bzw. die Sensoren sind dabei bevorzugt direkt in der Schlosseinheit bzw. Schlossvorrichtung 10 verbaut. Zusätzlich oder alternativ kann aber die Möglichkeit bestehen einen oder mehrere Sensoren (insbesondere weitere Sensor/en) über Anschlusskabel oder eine geeignete Nahfeldfunktechnologie (dann benötigt der Sensor bzw. die Sensoren eine eigene Stromversorgung) direkt mit der Schlossvorrichtung 10 zu verbinden um z.B. an geeigneterer Stelle Sensordaten zu erfassen (z.B. Temperaturmessung an unterschiedlichen Stellen in der Box). Bei manchen Sensoren ist eine Erfassung direkt in der Schlosseinheit auch nicht sinnvoll möglich (z.B. Wiegesensor).

Das Behältnis 1 weist einen Innenraum und mindestens eine den Innenraum von der Umgebung abgrenzende Wandung auf. Die Schlossvorrichtung 10 ist an der Wandung oder einer gegenüber der Wandung bewegbaren Öffnungseinrichtung 8, insbesondere einer verschiebbaren oder schwenkbaren Klappe, Fenster oder Tür, angeordnet. Die Seite der Schlossvorrichtung 10, die an der Wandung angeordnet ist, wird hierbei bevorzugt als Außenseite der Schlossvorrichtung 10 angesehen, die im Wesentlichen dazu parallele bzw. gegenüberliegende Seite der Schlossvorrichtung 10 wird dabei als innenliegende Seite angesehen. Ein, mehrere oder alle Sensor/en in der Schlossvorrichtung 10 sind näher zur innenliegenden Seite der Schlossvorrichtung 10 angeordnet als zur außenliegenden Seite. Bevorzugt besteht somit zwischen dem Sensor bzw. der Sensoreinrichtung oder den Sensoren und der Wandung, insbesondere der Kontaktstelle der Schlossvorrichtung mit der Wandung, ein Abstand zwischen 3mm und 50mm, insbesondere zwischen 5mm und 20mm oder zwischen 8mm und 18mm oder von mindestens 5mm oder von mindestens 10mm, zur Außenwand des Behälters. Dies ist vorteilhaft, da dadurch eine thermische Entkopplung (gilt insbesondere für Temperatursensor 24 und/oder Feuchtigkeitssensor bzw. Luftfeuchtigkeitssensor 29) geschaffen wird.

Es besteht die Möglichkeit, dass einer oder mehrere der Sensoren als analoger Sensor vorgesehen bzw. verbaut werden. Eine A/D Wandlung kann dann bevorzugt über eine

entsprechende Funktion bzw. Einrichtung, insbesondere die Prozessoreinrichtung oder eine A/D Wandlereinheit, in der Schlosseinheit bzw. in der Schlossvorrichtung 10 umgesetzt werden. Zusätzlich oder alternativ kann ein digitaler Sensor oder können mehrere digitale Sensoren vorgesehen bzw. angeschlossen bzw. verbaut werden. Ein oder mehrere solcher digitaler Sensoren liefern bereits digitale Messgrößen, so dass die Signale von der Schlosseinheit ohne weitere Wandlung verarbeitet werden können.

Auch können an die Schlossvorrichtung 10 ein oder mindestens ein oder mehrere Fingerabdrucksensoren angeschlossen werden, so dass sich Personen, die den Behälter bzw. das Behältnis 1 öffnen wollen sich mit ihrem Fingerabdruck identifizieren können (z.B. bei höchsten Sicherheitsanforderungen). Der Fingerabdrucksensor kann hierbei aber zusätzlich oder alternativ im mobilen Endgerät 16 befinden und die erfassten Daten können zum Abgleich durch die Prozessoreinrichtung 20 der Schlossvorrichtung 10 über das Nahfelddatenübertragungsmittel 34 des mobilen Endgeräts 16 an die Nahfelddatenübertragungseinrichtung 14 der Schlossvorrichtung 10 übermittelt werden.

Ferner können Leuchtdioden (nicht gezeigt) an die Schlossvorrichtung 10 angeschlossen werden. Zusätzlich oder alternativ können, insbesondere an der Außenseite des Behältnisses 1, durch unterschiedliche Farben und oder „Blink Codes“ unterschiedliche Informationen nach außen mitgeteilt bzw. gestreut werden. Zusätzlich oder alternativ besteht die Möglichkeit graphische Displays an die Schlosseinheit anzuschließen. Hier werden aufgrund des geringen Strombedarfs bevorzugt ePaper, bzw. elektronisches Papier, verwendet. Insbesondere für den Fall von einer nur kurzzeitigen Darstellung von Informationen können auch alle anderen üblichen Displaytechnologien eingesetzt werden (insb. LED Segmentanzeigen, LCD Anzeigen und/oder graphische LCD oder TFT oder OLED Anzeigen).

Fig. 2 zeigt eine an einer Außenwandung 26 des Behältnis 1 angeordnete Schlossvorrichtung 10. Die Schlossvorrichtung 10 weist dabei bevorzugt eine Energiequelle 22, insbesondere eine Batterie, eine Elektronikeinheit 19, eine Aktuatoreinheit 12 und einen mittels der Aktuatoreinheit 12, insbesondere einem Elektromotor, verfahrbaren Riegel 17 auf. Die Elektronikeinheit 18 weist dabei bevorzugt eine Prozessoreinrichtung 20, eine Speichereinheit 18, ein Nahfelddatenübertragungsmittel 14, eine Antenneneinheit 15 und eine Sensoreinrichtung 23 auf. Bevorzugt sind die zuvor genannten Einrichtungen der Elektronikeinheit zumindest indirekt mit der Prozessoreinrichtung 20 verbunden. Die Sensoreinrichtung 23 kann hierbei einen oder mehrere Sensoren aufweisen, insbesondere einen Feuchtigkeitssensor 29 und/oder einen Temperatursensor 24. Die Sensoreinrichtung 23 ist im Gehäuse der Schlossvorrichtung 10 angeordnet, wobei die Schlossvorrichtung 10 bevorzugt eine Ausnehmung bzw. Öffnung 11 in Richtung Behältnisinnere bzw. abgewandt zur nächsten Behältniswandung aufweist, welche bevorzugt offen oder mit einer Membran

abgedeckt sein kann. Die Sensoreinrichtung 23 ist dabei bevorzugt in einem durch das Bezugszeichen 25 dargestellten Abstand von mindesten 2mm, insbesondere mindestens 4mm oder mindestens oder genau oder bis zu 5mm oder mindestens oder genau oder bis zu 8mm oder mindestens oder genau oder bis zu 10mm oder mindestens oder genau oder bis zu 15mm, gegenüber der Außenwandung 26, an der die Schlossvorrichtung 1 angeordnet oder ausgebildet ist, beabstandet.

Die Figuren 4 und 5 zeigen schematisch unterschiedliche Bauformen des Behältnisses 1. Gemäß Fig. 4 ist die Schlossvorrichtung 10 an der Tür angeordnet und das Behältnis 1 bzw. die Behältniswandung weist einen Aufnahmeanteil 5 auf oder bildet diesen aus. Gemäß der Fig. 5 bildet die Tür bzw. die Öffnungseinrichtung 8 den Aufnahmeanteil 5 aus und die Schlossvorrichtung 10 ist an oder in der Behältniswandung angeordnet.

Fig. 6 zeigt rein schematisch, dass das Behältnis ebenfalls mit einem Sensor oder mit mehreren Sensoren ausgestattet sein kann.

Ein oder mehrere Wiegesensoren 30, 31 sind je nach Größe und Beschaffenheit des Behältnisses 1 mittels eines „doppelten Bodens“ so am Boden des Behälters 1 zu verbauen, dass das Gewicht eines abgelegten Gegenstands sicher erfasst werden kann, insbesondere bevorzugt unabhängig von der Form oder Größe des Gegenstands, und/oder unabhängig von der Stelle im Behälter 1, an der der Gegenstand bzw. das Objekt 2 abgelegt wird. Der Anschluss des Wiegesensors bzw. der Wiegesensoren an die Schlossvorrichtung, insbesondere die signal- und/oder datentechnische Kopplung mit der Prozesseinrichtung 20 der Schlossvorrichtung 10, kann drahtgebunden oder platinengebunden oder durch eine geeignete Nahfeldfunktechnologie erfolgen.

Es kann ein Erschütterungssensor oder es können mehrere Erschütterungssensoren, insbesondere Beschleunigungssensor 46, in dem Behältnis 1, insbesondere im Bereich der Wandung, insbesondere am Boden, oder in der Schlossvorrichtung 10 verbaut sein, welche die Beschleunigungswerte aufzeichnen, denen das Behältnis 1 ausgesetzt ist. Ferner kann das Behältnis 1, insbesondere im oberen Bereich, d.h. oberhalb des Zentrums des Behältnisses 1, oder im unteren Bereich, d.h. unterhalb des Zentrums des Behältnisses 1, oder im Bereich des Zentrums des Behältnisses 1 einen weiteren Temperatursensor 240 aufweisen. „Im Bereich des Zentrums“ ist hierbei höhenmäßig als +/- 10% oder +/- 20% oder +/- 30% oder +/- 40% oberhalb und/oder unterhalb des (vertikalen) Zentrums bzw. der vertikalen Mitte zu verstehen. Die Höhenprozente beziehen sich dabei auf die maximale Höhe des Aufnahmebereichs.

Es kann ein Luftdrucksensor (nicht gezeigt) oder es können mehrere Luftdrucksensoren, in dem Behältnis 1, insbesondere im Bereich der Wandung, insbesondere am Boden, oder in der

Schlossvorrichtung 10 verbaut sein, welche die Luftdruckveränderungen aufzeichnen, denen das Behältnis 1 ausgesetzt ist. Zusätzlich oder alternativ kann ein oder können mehrere Gassensoren im Behältnis 1, insbesondere im Bereich einer Wandung, insbesondere am Boden oder an der Decke des Behältnisses 1, vorgesehen sein. Diese Ausführungsformen sind vorteilhaft, da dadurch sehr präzise die Umweltbedingungen im Bereich des Behältnisses 1 erfasst werden können, z.B. in Transportbehältern, die mit Flugzeugen transportiert werden.

Darüber hinaus kann ein Bewegungssensor oder können unterschiedliche Bewegungssensoren mit der Schlossvorrichtung 10 verbunden werden, um z.B. - sollte das Behältnis 1 als Briefkasten oder briefkastenartig ausgebildet sein - zu erkennen, dass ein Einwurf bzw. eine Bestückung stattgefunden hat. Hier kommen je nach Anwendungsfall ein oder mehrere Lichtsensor/en, Infrarot-, Ultraschall- und/oder Magnetfeldsensor/en in Betracht.

Ein weiterer Sensortyp der in Betracht kommt wäre ein Feuchtesensor bzw. ein Flüssigkeitssensor, der z.B. analog zum Wiegesensor/en sinnvollerweise am Boden des Behälters 1 zu verbauen ist um festzustellen, ob Flüssigkeiten im Behältnis 1 ausgelaufen sind.

Um festzustellen, ob z.B. eine mobile Transportkiste umgestürzt ist oder eine vorgeschriebene Höchstneigung überschritten wurde, kann ein Gyroskop Sensor (Kreiselinstrument) mit der Schlossvorrichtung gekoppelt, insbesondere verbunden, sein bzw. in dieser verbaut sein.

Ferner besteht zusätzlich oder alternativ die Möglichkeit einen GPS Empfänger an die Schlossvorrichtung 10 anzuschließen, bzw. diesen zu integrieren.

Die Figuren 7 bis 10 zeigen rein schematisch ein Beispiel für einen Ablauf des erfindungsgemäßen Verfahrens zum Öffnen eines Behältnisses.

Es ist erkennbar, dass ein Behältnisses 1, insbesondere ein geschützter Behälter ohne permanente Internetverbindung, bereitgestellt ist, wobei das Behältnis eine Nahfeldkommunikationseinrichtung aufweist und dadurch einen Nahfeldkommunikationsbereich vorgibt.

Ferner erfolgt die Bereitstellung von zumindest einem mobilen Endgeräts 16, insbesondere von einer Vielzahl an mobilen Endgeräten, insbesondere mehr als 5 pro 100km² oder mehr als oder bis zu 10 pro 100km² oder mehr als oder bis zu 15 pro 100km² oder mehr als oder bis zu 25 pro 100km² oder mehr als oder bis zu 50 pro 100km² oder mehr als oder bis zu 100 pro 100km² oder mehr als oder bis zu 200 pro 100km² oder mehr als oder bis zu 500 pro 100km².

Das mobile Endgerät 16 weist hierbei ein Nahfelddatenübertragungsmittel 34 zum Datenaustausch mit der Nahfelddatenübertragungseinrichtung 14 des Behältnisses 1 auf und

ferner weist es bevorzugt ein besonders bevorzugt kabelloses Fernfelddatenübertragungsmittel 36, insbesondere GSM, UMTS, LTE, etc., zum Datenaustausch mit einem Server 38 auf.

Ferner wird erfindungsgemäß eine Sendeinfrastruktur, insbesondere ein oder mehrere Sendestationen, insbesondere Sendemasten, genutzt. Das Fernfelddatenübertragungsmittel sendet und bevorzugt empfängt zeitgleich oder zeitversetzt oder zeitweise zeitgleich Daten. Die empfangenen Daten empfängt das Fernfelddatenübertragungsmittel von über die Sendeinfrastruktur, wobei die Sendeinfrastruktur Daten von einem Server bzw. einer Servereinrichtung, insbesondere einem Cloudserver, erhält. Die gesendeten Daten werden von der Fernfelddatenübertragungseinrichtung an die Sendeinfrastruktur zur Weiterleitung an den Server bzw. die Servereinrichtung übermittelt.

Das mobile Endgerät 16 weist dabei eine Prozessoreinrichtung 40 zum Ausführen einer Steuerungsapplikation auf, ferner weist das mobile Endgerät 16 eine Speichereinrichtung 42 zum Speichern von Behältnisneukonfigurationsdaten und von Behältnisbetriebsdaten auf. Bevorzugt alle Daten, die von der zentralen Servereinheit, bzw. von der Schlosseinheit an die mobile Applikation übermittelt und dort (zwischen-)gespeichert werden, werden durch eine Verschlüsselung, insbesondere durch eine lokale Verschlüsselung, vor einem Zugriff von außen geschützt. D.h., dass weder der Nutzer der Applikation selbst, noch ein Dritter direkt auf die in der mobilen Applikation abgelegten Daten Zugriff nehmen können, insbesondere auch nicht durch Auslesen des physikalischen Speichers des mobilen Geräts. Die Verschlüsselungsmethode und/oder die genauen Parameter der Verschlüsselung werden bevorzugt vom Administrator der Servereinheit zentral konfiguriert und von dort an die mobile Applikation übertragen.

In Fig. 8 ist schematisch dargestellt, dass das mobile Endgerät Zugangsdaten von einem Server bzw. einer Servereinrichtung empfängt, wobei die Zugangsdaten über die Sendeinfrastruktur übermittelt werden.

Die Nutzerrechte und/oder die Schlosskonfigurationen, sowie bevorzugt die Übertragungen aller relevanten Sensordaten, bzw. sonstiger Daten der Schlosseinheiten wird/werden durch einen oder mehrere Operatoren/Administratoren verwaltet.

In Fig. 9 ist schematisch gezeigt, dass das mobile Endgerät 16 die Zugangsdaten über die Nahfelddatenübertragungseinrichtung an das Behältnis übermittelt. Daraufhin werden die Behältnisbetriebsdaten durch die Nahfelddatenübertragungseinrichtung 14 zur Weiterleitung an die Servereinrichtung an das Nahfelddatenübertragungsmittel 34 des mobilen Endgeräts 16 übermittelt. Es ist rein schematisch erkennbar, dass das mobile Endgerät 16 außerhalb der

Reichweite der Sendefunkinfrastruktur ist bzw. keine mobile Datenverbindung zum Internet aufbauen kann.

Fig. 10 zeigt schematisch, dass das mobile Endgerät 16, sobald es wieder im Abdeckungsbereich der Sendefunkinfrastruktur oder infolge eines definierten Auslöseevents (nur bei bestehender Datenverbindung ins Internet), insbesondere einer Tastenbetätigung und/oder eines Ortsdatenabgleichs und/oder eines Zeitabgleichs, Behältnisbetriebsdaten an den Server bzw. die Servereinrichtung übermittelt.

Das mobile Endgerät 16 empfängt die Behältnisneukonfigurationsdaten vom Server 38 über das Fernfelddatenübertragungsmittel 36, wobei die Behältnisneukonfigurationsdaten in Antwort auf die mittels dem Nahfelddatenübertragungsmittel 34 an den Server 38 übermittelten Behältnisbetriebsdaten erzeugt werden, wobei die Behältnisbetriebsdaten zumindest Zeitdaten und Zugangsdaten aufweisen.

Die Figuren 7 bis 10 zeigen somit ein Verfahren zum Öffnen eines Behältnisses 1. Das Verfahren weist dabei mindestens die Schritte auf: Bereitstellen eines Behältnisses 1, Bereitstellen mindestens eines mobilen Endgeräts 16, wobei das mobile Endgerät 16 ein Nahfelddatenübertragungsmittel 34 zum Datenaustausch mit der Nahfelddatenübertragungseinrichtung 14 des Behältnisses 1 aufweist, wobei das mobile Endgerät 16 ein Fernfelddatenübertragungsmittel 36, insbesondere LTE, zum Datenaustausch mit einem Server 38 aufweist, wobei das mobile Endgerät 16 eine Prozessoreinrichtung 40 zum Ausführen einer Steuerungsapplikation aufweist, wobei das mobile Endgerät 16 eine Speichereinrichtung 42 zum Speichern von Behältnisneukonfigurationsdaten und von Behältnisbetriebsdaten aufweist, wobei die Behältnisbetriebsdaten durch die Nahfelddatenübertragungseinrichtung 14 zur Weiterleitung an die Servereinrichtung an das Nahfelddatenübertragungsmittel 34 des mobilen Endgeräts 16 übermittelt werden und wobei das mobile Endgerät 16 die Behältnisneukonfigurationsdaten vom Server 38 über das Fernfelddatenübertragungsmittel 36 empfängt, wobei die Behältnisneukonfigurationsdaten in Antwort auf die mittels dem Nahfelddatenübertragungsmittel 34 an den Server 38 übermittelten Behältnisbetriebsdaten erzeugt werden, wobei die Behältnisbetriebsdaten zumindest Zeitdaten und Zugangsdaten aufweisen.

Fig. 11 zeigt einen schematischen Ablauf des erfindungsgemäßen Verfahrens, wobei dieser Ablauf eine Vielzahl zusätzlicher oder alternativer Schritte aufweist. Die gezeigten Schritte S1-S25 umfassen dabei:

S1. Operator/Administrator legt auf der zentralen Servereinheit eine Schlosseinheit mit einer eindeutigen Kennung an und verknüpft diese ggf. mit einer Schlossgruppe.

S2. Operator/Administrator legt auf der zentralen Servereinheit einen Nutzer an, bzw. stellt einer definierten Nutzergruppe die Möglichkeit bereit sich selbst an der zentralen Servereinheit zu registrieren (Self Service).

S3. Nutzer lädt die notwendige Software aus einem Appstore oder einem anderen online zugreifbaren Speicherort auf sein mobiles Device (z.B. Smartphone). Das kann prinzipiell von jedem Ort der Welt erfolgen.

S4. Der Nutzer meldet sich über seine App an der zentralen Servereinheit an. Dazu verwendet er ihm bekannte Zugangsdaten (wie vom Operator/Administrator in Schritt 1 angelegt) oder er registriert sich im Falle des Self Service und wählt seine Zugangsdaten entsprechend selbst.

S5. Die zentrale Servereinheit prüft ob für diesen Nutzer, bzw. die Gruppe(n) in die der Nutzer eingeordnet ist Zugriffsrechte auf ein oder mehrere Schlösser, bzw. Schlossgruppen vorliegen. Sind Zugriffsrechte vorhanden werden diese an die mobile Einheit verschlüsselt übertragen (ggf. mit vorhandenen Zusatzinformationen). Dabei können die Zugriffsrechte auch zeitlichen Beschränkungen unterliegen. Z.B. kann ein Zugriffsrecht automatisch nach 24 Stunden ablaufen, sofern in dieser Zeitspanne keine weitere Synchronisation zwischen mobiler Einheit und zentraler Servereinheit mehr stattfindet.

Bei jeder Synchronisation zwischen der mobilen Einheit und der zentralen Servereinheit werden neben den Zugriffsrechten und weiterer Informationen insbesondere auch die Systemuhren abgeglichen, so dass Abweichungen der Uhren jeweils berücksichtigt werden können.

S6. Die von der mobilen Einheit empfangenen Zugriffsdaten und Zusatzinformationen werden lokal in einem „virtuellen Schlüsselbund“ verschlüsselt zwischengespeichert. Dabei prüft die Mobile Einheit regelmäßig ob ein Zugriffsrecht noch besteht und löscht ggf. alle Zugriffsrechte, die bereits abgelaufen sind.

S7. Möchte der Nutzer nun eine Schlosseinheit öffnen und befindet sich mit seiner mobilen Einheit in deren Reichweite, so wird die mobile Einheit entweder automatisch (im Hintergrund) eine Verbindung zur Schlosseinheit herstellen, oder nach manueller Eingabe in der mobilen Einheit („Connect Knopf“). Die Verbindung zwischen mobiler Einheit und Schlosseinheit kann dabei über die im Übertragungsstandard enthaltene Verschlüsselung hinaus weiter verschlüsselt werden.

S8. Die Schlosseinheit überträgt beim Aufbau der Verbindung zur mobilen Einheit eine Eindeutige Kennung an die mobile Einheit. Ggf. können auch weitere Informationen übertragen werden (z.B. Zugehörigkeit zu einer bestimmten Schlossgruppe)

S9. Die mobile Einheit prüft ob für dieses Schloss, bzw. die Schlossgruppe Zugriffsrechte im lokalen Speicher bestehen. Eine Verbindung zur zentralen Servereinheit wird dabei nicht aufgebaut.

S10. Wenn ein Zugriffsrecht besteht kann es (ja nach Konfiguration durch den Operator/Administrator) notwendig sein, dass weitere Schlüssel zur Bedienung der Schlosseinheit notwendig sind (z.B. Pineingabe, Scannen eines Barcodes, etc.) die in der mobilen Einheit eingegeben und an die Schlosseinheit übertragen werden müssen. Außerdem kann es notwendig sein, dass eine Verbindung zur zentralen Servereinheit aufgebaut werden muss, da die Konfiguration vorgibt, dass das Schloss nur bei bestehen einer Verbindung zwischen mobiler Einheit und zentraler Servereinheit zu öffnen ist um die Sicherheit weiter zu erhöhen, da über eine aktive Verbindung immer auch die Zugriffsrechte zwischen mobiler und zentraler Einheit synchronisiert werden.

S11. Die mobile Einheit sendet der Schlosseinheit (nach positiver Prüfung) ein Signal zum Öffnen und überträgt den entsprechenden Schlüssel.

S12. Die Schlosseinheit prüft den Schlüssel und wird sowohl den Verbindungsversuch, als auch das Ergebnis der Prüfung, sowie alle übertragenen Informationen zum Nutzer, bzw. der mobilen Einheit im internen temporären Speicher ablegen.

S13. Nach positiver Prüfung gibt die Schlosseinheit den Verriegelungsmechanismus frei und wird auch dieses Event im temporären Speicher ablegen.

S14. Die mobile Einheit überträgt nun Daten an die Schlosseinheit, die in der zentralen Servereinheit mit dem Zugriffsrecht verknüpft wurden. Insbesondere die Informationen, dass von der Schlosseinheit bereitgestellte Daten dort empfangen und nun lokal gelöscht werden können. Es können aber auch Änderungen an der lokalen Konfiguration der Software der Schlosseinheit übertragen werden.

S15. Die Schlosseinheit wir die von der zentralen Einheit empfangenen Daten aus dem lokalen Speicher löschen und alle weiteren notwendigen Operationen durchführen.

S16. Das Löschen, bzw. die Ausführung der Operationen wird quittiert.

S17. Die Schlosseinheit überträgt nun alle Daten aus dem temporären Speicher (Logdaten über Zugriffe, Zugriffsversuche, sowie alle gespeicherten Sensordaten an die mobile Einheit. Es werden auch alle Daten übertragen die bereits zur Löschung vorgemerkt sind, jedoch der Empfang durch die zentrale Servereinheit noch nicht bestätigt wurde.

S18. Die mobile Einheit empfängt die Daten von der Schlosseinheit und legt diese in einem geschützten Bereich ab. Der Empfang wird quittiert.

S19. Die Schlosseinheit wird nun alle übertragenen Daten mit zusätzlichen Informationen markieren (zum Löschen vormerken), aber noch nicht löschen, da noch nicht sichergestellt ist, dass diese Daten auch auf der Servereinheit empfangen wurden. Ggf. werden mehrfach übertragene Daten mit weiteren Informationen angereichert.

S20. Die Verbindung zwischen der Schlosseinheit und der mobilen Einheit wird wieder abgebaut.

S21. Die mobile Einheit wird nun zum nächst möglichen, bzw. zu einem konfigurierten Zeitpunkt versuchen Kontakt zur zentralen Servereinheit aufzunehmen und die von der Schlosseinheit übertragenen Daten dorthin zu übertragen.

S22. Sobald eine Verbindung zwischen der mobilen Einheit und der zentralen Servereinheit besteht werden die Daten übertragen und von der zentralen Servereinheit quittiert.

S23. Die quittierten Daten werden nun aus dem temporären Speicher der mobilen Einheit gelöscht.

S24. Die zentrale Servereinheit aktualisiert nun das Zugriffsrecht auf das spezifische Schloss um die Information, dass die definierten Daten empfangen wurden und lokal gelöscht werden können (unter Berücksichtigung der Information welche Daten von der Einheit bereits gelöscht wurden).

S25. Das Zugriffsrecht wird nun mit allen mobilen Einheiten synchronisiert, die auf das spezifische Schloss, bzw. auf die zugehörige Schlossgruppe Zugriff haben.

Somit wird ein Verfahren zur asymmetrischen, bzw. indirekten Übertragung von Daten zwischen einem Sender und einem Empfänger offenbart.

Es können somit Sensordaten (z.B.), die an Orten erhoben werden, an denen temporär oder dauerhaft, keine Internetverbindung bzw. keine Verbindung zu einem alternativ geeigneten Übertragungsnetz besteht zu einem zentralen Server übertragen werden. Derartige „Offline-Situationen“ gibt es bei Funklöchern, unter Tage, unter Wasser, etc.

Die erfindungsgemäße Lösung baut inhaltlich bevorzugt auf das ebenfalls hierin beschriebene Verfahren zur sicheren Vergabe eindeutiger Zugriffsrechte ohne Verwendung spezialisierter Hardware sowie ohne bestehende Internetverbindung auf. Bestandteil ist hierbei eine mobile Applikation, die auf einem Gerät, insbesondere Server und/oder mehreren mobilen Endgeräten, läuft, das über eine mobile Datenverbindung mit einer Servereinrichtung, insbesondere einem zentralen Server, verbunden ist und von diesem (analog dem oben beschriebenen Verfahren) Access Keys empfangen und lokal vorhalten kann.

Sollen nun Sensordaten eines (offline) Behältnisses an die Servereinrichtung 38, insbesondere den zentralen Server, übertragen werden, so ist das mobile Gerät bzw. das mobile Endgerät 16 in die Nähe des Behältnisses 1 zu bringen, damit das Nahfeldübertragungsmittel 34 des mobilen Endgeräts 16 rohe oder aufbereitete oder teilweise aufbereitete Sensordaten eines oder mehrerer am oder im Behältnis 1 angeordneter Sensoren empfangen kann. Die Sensordaten werden dabei über die Nahfelddatenübertragungseinrichtung des Behältnisses, insbesondere der Schlossvorrichtung 10, an das Nahfelddatenübertragungsmittel 34 des mobilen Endgeräts 16 übermittelt. Der Sensor ist mit einer elektronischen Vorrichtung, insbesondere der Prozessoreinrichtung 20, versehen oder gekoppelt oder verbunden, welche die vom Sensor zur Verfügung gestellten Daten, insbesondere in konfigurierbarer Weise, lokal, insbesondere in einer Speichereinheit 18, speichert. Kommt das mobile Gerät 16 in Reichweite der Nahfelddatenübertragungseinrichtung 14 authentifiziert es sich bevorzugt mittels des Access Keys beim Behältnis, insbesondere der Prozessoreinrichtung 20, und fordert den Inhalt oder definierte Daten der im lokalen Speicher vorgehaltenen oder zwischengespeicherten Daten, insbesondere Zeit und/oder Sensordaten, an.

Akzeptiert die Prozessoreinrichtung den Zugriff und die Anforderung, so werden die angefragten Daten an das mobile Gerät 16 übertragen (z.B. Bluetooth oder NFC). Nach Prüfung der Vollständigkeit und Korrektheit der übertragenen Daten sendet das mobile Endgerät 16 bevorzugt ein Löschesignal oder Löschesdaten, welche das Löschen zumindest eines Teils der lokal gespeicherten bzw. zwischengespeicherten Daten, insbesondere der Sensordaten und/oder Zeitdaten, auslösen (temporärer Speicher geleert). Anderenfalls wird die Übertragung bevorzugt erneut angefordert. Über den selben Mechanismus können auch Konfigurationsänderungen an das Behältnis übertragen werden und die lokalen Zeiten (Behältnis und Mobilgerät) synchronisiert werden. Nachdem die Verbindung abgebaut ist arbeitet das Behältnis 1 und der oder die darin angeordneten oder vorgesehenen Sensoren bevorzugt vollständig autark und sammelt bzw. sammeln Daten bis zum nächsten Zugriff durch die mobile Applikation.

Die Behältnisdaten, insbesondere die durch den oder die Sensoren erzeugten Daten, können somit auch ohne dauerhafte Internetverbindung, durch die vorgelagerte Übertragung an ein mobiles Endgerät 16, vollständig an eine zentrale Einheit, insbesondere die Servereinrichtung 38, übertragen werden. Somit wird ein Verfahren zur asymmetrischen bzw. indirekten Übertragung von Daten zwischen einem Sender (mobilen Endgerät) und einem Empfänger (Behältnis) bereitgestellt, wobei nach dem Datenaufbau das mobile Endgerät auch Daten vom Behältnis empfängt bzw. das Behältnis Daten an das mobile Endgerät sendet.

Bezugszeichenliste

- 1 Behältnis
- 2 Objekt
- 4 Hauptkörper
- 5 Aufnahmeanteil
- 6 Aufnahmevolumen
- 8 Öffnungseinrichtung
- 10 Schlossvorrichtung
- 11 Öffnung / Membran
- 12 Aktuator
- 14 Nahfelddatenübertragungseinrichtung
- 15 Antenneneinheit
- 16 mobiles Endgerät
- 17 Riegel
- 18 Speichereinheit
- 19 Elektronikeinheit
- 20 Prozessoreinrichtung
- 22 Energiequelle
- 23 Sensoreinrichtung
- 24 Temperatursensor
- 25 Abstand
- 26 Wandung des Behältnisses
- 28 Feuchtigkeitssensor
- 29 Luftfeuchtigkeitssensor
- 30 Gewichtssensor
- 31 weiterer Gewichtssensor
- 32 Boden
- 34 Nahfelddatenübertragungsmittel
- 36 Fernfelddatenübertragungsmittel
- 37 Fernfeldkommunikationsinfrastruktur

- 38 Server oder Servereinrichtung
- 40 Prozessoreinrichtung des mobilen Endgeräts
- 42 Speichereinrichtung
- 44 Bohrung für Befestigungsschraube
- 46 Beschleunigungssensor
- 50 Abdeckungsbereich des Nahfeldkommunikationsmittels des Behältnisses
- 52 Abdeckungsbereich einer Fernfeldkommunikationsinfrastruktur
- 54 Kommunikation zwischen Server und Sendefunkinfrastruktur
- 56 Kommunikation zwischen Sendefunkinfrastruktur und mobilem Endgerät
- 58 Nahfeldkommunikation zwischen Nahfeldkommunikationsmittels und Nahfeldkommunikationseinrichtung
- 240 weiterer Temperatursensor

Ansprüche

1. Behältnis (1) zum Aufnehmen von einem oder mehreren Objekten (2), insbesondere von Proben mit biologischem Material,
mindestens aufweisend
einen Hauptkörper (4),
wobei der Hauptkörper (4) ein Aufnahmevolumen (6) mehrseitig umschließt,
eine gegenüber dem Hauptkörper (4) beweglich angeordnete Öffnungseinrichtung (8), insbesondere eine Tür oder Klappe,
eine Schlossvorrichtung (10) zum Verhindern einer definierten Relativbewegung der Öffnungseinrichtung (8) gegenüber dem Hauptkörper (4),
wobei die Schlossvorrichtung (10) einen elektrisch betriebenen Aktuator (12) aufweist
eine Nahfelddatenübertragungseinrichtung (14) zum Empfangen von Daten von mindestens einem sich in einem definierten Abstandsbereich zu dem Behältnis (1) zeitweise befindenden mobilen Endgerät (16) und zum Senden von Daten an das zumindest eine sich in einem definierten Abstandsbereich zu dem Behältnis (1) zeitweise befindenden mobilen Endgerät (16),
eine Speichereinheit (18) zum zeitweisen Speichern von Zeitdaten und Zugangsdaten,
wobei die Zeitdaten zumindest Daten zum letzten Öffnungszeitpunkt und/oder zumindest Daten zum letzten Verschlusszeitpunkt aufweist,
wobei die Zugangsdaten zumindest Berechtigungsdaten und Identifikationsdaten aufweisen,
wobei die Berechtigungsdaten definieren, in Abhängigkeit welcher Identifikationsdaten der Aktuator die Schlossvorrichtung aus einer geschlossenen Konfiguration in eine geöffnete Konfiguration überführt und
wobei die Identifikationsdaten eine Zuordnung zu dem mobilen Endgerät vorgeben,
eine Prozessoreinrichtung (20) zum Abgleich der Berechtigungsdaten und der Identifikationsdaten,

wobei der Aktuator (12) im Falle eines positiven Abgleichs von der Prozessoreinrichtung (20) zum Öffnen der Schlossvorrichtung (10) ansteuerbar ist, wobei ein positiver Abgleich eine definierte Übereinstimmung der abgeglichenen Daten repräsentiert,

eine von einem Feststromanschluss verschiedene Energiequelle (22) zum Betreiben von zumindest dem Aktuator (12), der Nahfelddatenübertragungseinrichtung (14), der Speichereinheit (18) und der Prozessoreinrichtung (20).

2. Behältnis nach Anspruch 1,

dadurch gekennzeichnet, dass

die Prozessoreinrichtung (20), die Speichereinheit (18) und die Nahfelddatenübertragungseinrichtung (14) und bevorzugt ebenfalls die Energiequelle (22) als Teil der Schlossvorrichtung (10) ausgebildet sind, wobei die Prozessoreinrichtung (20), die Speichereinheit (18) und die Nahfelddatenübertragungseinrichtung (14) in einer geschlossenen Konfiguration des Behälters (1) im Inneren des Behälters (1) angeordnet sind.

3. Behältnis nach Anspruch 2,

dadurch gekennzeichnet, dass

ein oder mindestens ein Temperatursensor (24) im Inneren des Behältnisses (1) oder an einer Wandung (26) des Behältnisses (1) angeordnet ist, wobei der Temperatursensor (24) Temperaturwerte oder Temperaturdaten ausgibt,

wobei durch die Prozessoreinrichtung (20) die Temperaturwerte in Form von Daten oder die Temperaturdaten zusammen mit Zeitdaten und/oder Zugangsdaten in der Speichereinheit (18) abspeicherbar sind.

4. Behältnis nach Anspruch 2 oder Anspruch 3,

dadurch gekennzeichnet, dass

ein oder mindestens ein Feuchtigkeitssensor (28) im Inneren des Behältnisses (1) oder an einer Wandung (26) des Behältnisses (1) angeordnet ist, wobei der Feuchtigkeitssensor (28) Feuchtigkeitswerte oder Feuchtigkeitsdaten ausgibt,

wobei durch die Prozessoreinrichtung (20) die Feuchtigkeitswerte in Form von Daten oder die Feuchtigkeitsdaten zusammen mit Zeitdaten und/oder Zugangsdaten und/oder Temperaturdaten in der Speichereinheit (18) abspeicherbar sind.

5. Behältnis nach einem der Ansprüche 2 bis 4,

dadurch gekennzeichnet, dass

ein oder mindestens ein Gewichtssensor (30) in einer den Boden (32) des Behältnisses (1) bildenden Wandung oder auf der den Boden (32) bildenden Wandung angeordnet ist, wobei der Gewichtssensor (30) Gewichtswerte oder Gewichtsdaten ausgibt,

wobei durch die Prozessoreinrichtung (20) die Gewichtswerte in Form von Daten oder die Gewichtsdaten zusammen mit Zeitdaten und/oder Zugangsdaten und/oder Temperaturdaten und/oder Feuchtigkeitsdaten in der Speichereinheit (18) abspeicherbar sind.

6. Behältnis nach einem der vorangegangenen Ansprüche,

dadurch gekennzeichnet, dass

durch die Prozessoreinrichtung (20) Energiequellendaten erzeugbar sind, wobei die Energiequellendaten Daten zum Ladestand und/oder zum Grad der Entladung über einen definierten Zeitraum und/oder zur Veränderung der Spannung über einen definierten Zeitraum aufweisen.

7. Behältnis nach einem der vorangegangenen Ansprüche,

dadurch gekennzeichnet, dass

das Behältnis (1) in der geschlossenen Konfiguration ein Volumen von weniger als 10m^3 , insbesondere von weniger als 5m^3 oder von weniger als 2m^3 oder von weniger als 1m^3 oder von weniger als $0,5\text{m}^3$ oder von weniger als $0,1\text{m}^3$, einhaust bzw. umschließt bzw. begrenzt, und

die mittlere Wandstärke der Wandungen (26, 30) des Behältnisses (1) weniger als 30mm dick ist, insbesondere weniger als 20mm oder weniger als 10mm dick ist oder zwischen 20mm und 8mm dick ist oder weniger als 5mm dick ist oder weniger als 3mm dick ist

und

die Öffnungseinrichtung (8) eine in der geschlossenen Konfiguration zur Öffnungseinrichtung (8) parallel erstreckenden Wandung zu zumindest 50% (der Wandungsfläche), insbesondere zu zumindest 60% (der Wandungsfläche) oder zu zumindest 80% (der Wandungsfläche) oder zu zumindest 90% (der Wandungsfläche), überlagert

und

die Wandungen (26, 30) ein oder mindestens ein Metall oder ein oder mindestens ein Polymerwerkstoff oder ein oder mindestens ein Kompositwerkstoff aufweisen oder zu zumindest 50% (massemäßig), insbesondere zu zumindest 60% (massemäßig) oder zu zumindest 70% (massemäßig) oder zu zumindest 80% (massemäßig) oder zu zumindest 90% (massemäßig), daraus bestehen

und

die Energiequelle (22) eine Batterie ist, wobei die Batterie eine Mindestkapazität von 1000mAh aufweist

und

die Nahfelddatenübertragungseinrichtung (14) eine RFID, Bluetooth, WLAN, ZigBee und/oder Z-Wave Datenübertragungseinrichtung ist.

8. Verfahren zum Öffnen eines Behältnisses nach einem der vorangegangenen Ansprüche,

mindestens aufweisend die Schritte:

Bereitstellen eines Behältnisses (1) nach einem der vorangegangenen Ansprüche,

Bereitstellen eines mobilen Endgeräts (16),

wobei das mobile Endgerät (16) ein Nahfelddatenübertragungsmittel (34) zum Datenaustausch mit der Nahfelddatenübertragungseinrichtung (14) des Behältnisses (1) aufweist

wobei das mobile Endgerät (16) ein Fernfelddatenübertragungsmittel (36), insbesondere LTE, zum Datenaustausch mit einem Server (38) aufweist,

wobei das mobile Endgerät (16) eine Prozessoreinrichtung (40) zum Ausführen einer Steuerungsapplikation aufweist,

wobei das mobile Endgerät (16) eine Speichereinrichtung (42) zum Speichern von Behältnisneukonfigurationsdaten und von Behältnisbetriebsdaten aufweist,

wobei die Behältnisbetriebsdaten durch die Nahfelddatenübertragungseinrichtung (14) zur Weiterleitung an die Servereinrichtung an das Nahfelddatenübertragungsmittel (34) des mobilen Endgeräts (16) übermittelt werden und

wobei das mobile Endgerät (16) die Behältnisneukonfigurationsdaten vom Server (38) über das Fernfelddatenübertragungsmittel (36) empfängt,

wobei die Behältnisneukonfigurationsdaten in Antwort auf die mittels dem Nahfelddatenübertragungsmittel (34) an den Server (38) übermittelten Behältnisbetriebsdaten erzeugt werden,

wobei die Behältnisbetriebsdaten zumindest Zeitdaten und Zugangsdaten aufweisen.

9. Verfahren nach Anspruch 8,

dadurch gekennzeichnet, dass

das Behältnis (1) mindestens einen Sensor (24, 28, 30) aufweist, wobei der Sensor (24, 28, 30) Daten und/oder Signale an der Prozessoreinrichtung (20) des Behältnisses (1) bereitstellt und

die Nahfelddatenübertragungseinrichtung (14) des Behältnisses (1) Signale und/oder Daten, welche die Sensordaten oder Sensorsignale repräsentieren oder darstellen, als Bestandteil der Behältnisbetriebsdaten an das Nahfelddatenübertragungsmittel (34) des mobilen Endgeräts (16) übermittelt.

10. Verfahren nach einem der Ansprüche 8 oder 9,

dadurch gekennzeichnet, dass

in der Speichereinrichtung (42) des mobilen Endgeräts (16) vom Server (38) bereitgestellte Identifikationsdaten bereitgestellt werden, wobei die Identifikationsdaten zusammen mit den Behältnisneukonfigurationsdaten oder als separater Datensatz an das mobile Endgerät (16) übermittelt werden,

wobei die Identifikationsdaten zusammen mit spezifischen Gerätedaten des mobilen Endgeräts (16) infolge einer Zugangsberechtigungsanfrage mittels dem Nahfelddatenübertragungsmittel (34) an die Nahfelddatenübertragungseinrichtung (14) übermittelt werden, wobei zumindest die Identifikationsdaten in der Speichereinheit (18) abgespeichert werden und mit in der Speichereinheit (18) vorhandenen Berechtigungsdaten abgeglichen werden,

wobei in Abhängigkeit eines sich aus dem Abgleich ergebenden Abgleichergebnisses die Schlossvorrichtung (10) im verschlossenen Zustand verbleibt oder in einen geöffneten Zustand überführt wird.

11. Verfahren nach einem der vorangegangenen Ansprüche 8 bis 10

dadurch gekennzeichnet, dass

ein konkreter Satz an Behältnisbetriebsdaten von der Prozessoreinrichtung (20) des Behältnisses (1) in der Speichereinheit (18) modifiziert vorgehalten wird, zumindest nachdem dieser Satz an Behältnisbetriebsdaten an das mobile Endgerät (16) übermittelt wurde.

12. Verfahren nach einem der Ansprüche 8 bis 11,

dadurch gekennzeichnet, dass

die Behältnisneukonfigurationsdaten der Prozessoreinrichtung (20) des Behältnisses (1) vorgeben, welche Daten, insbesondere welcher konkrete Satz an Behältnisdaten, aus der Speichereinheit (18) gelöscht wird, wobei die Prozessoreinrichtung (20) des Behältnisses (1) in Abhängigkeit der Behältnisneukonfigurationsdaten die Daten aus der Speichereinheit (18) löscht.

13. Verfahren nach Anspruch 12,

dadurch gekennzeichnet, dass

die Behältnisneukonfigurationsdaten Berechtigungsdaten aufweisen und eine Anweisung an die Prozessoreinrichtung (20) des Behältnisses (1) aufweist die in der Speichereinheit (18) vorgehaltenen Berechtigungsdaten durch die Berechtigungsdaten der Behältnisneukonfigurationsdaten zu ersetzen und/oder zu erweitern.

14. Computerprogrammprodukt zum Ausführen eines zuvor genannten Verfahrens.

15. System,

mindestens aufweisend

eine Vielzahl an Behältnissen (1) gemäß einem der Ansprüche 1 bis 7,

eine Vielzahl an mobilen Endgeräten (16),

wobei jedes mobile Endgerät (16)

ein Nahfelddatenübertragungsmittel (34) zum Datenaustausch mit der Nahfelddatenübertragungseinrichtungen (14) der Behältnisse (1) aufweist und

ein Fernfelddatenübertragungsmittel (36), insbesondere LTE, zum Datenaustausch mit einem Server (38) aufweist und

eine Prozessoreinrichtung (40) zum Ausführen einer Steuerungsapplikation aufweist und

eine Speichereinrichtung (42) zum Speichern von Behältnisneukonfigurationsdaten und von Behältnisbetriebsdaten aufweist,

wobei die Behältnisbetriebsdaten durch die Nahfelddatenübertragungseinrichtung (14) zur Weiterleitung an die Servereinrichtung (38) an das Nahfelddatenübertragungsmittel (34) des jeweiligen mobilen Endgeräts (16) übermittelt werden und

wobei die Behältnisbetriebsdaten zumindest Zeitdaten und Zugangsdaten aufweisen,

wobei die Zeitdaten zumindest Daten zum letzten Öffnungszeitpunkt und/oder zumindest Daten zum letzten Verschlusszeitpunkt aufweisen,

mindestens eine Servereinrichtung (38), insbesondere eine Cloud-Servereinrichtung,

wobei die Servereinrichtung (38) vom jeweiligen mobilen Endgerät (16) die Behältnisbetriebsdaten empfängt und nach dem Empfang der Behältnisbetriebsdaten Behältnisneukonfigurationsdaten erzeugt und diese an das mobile Endgerät (16) sendet, von

dem es die Behältnisbetriebsdaten empfangen hat oder an ein anderes mobiles Endgerät (16) sendet, das dem Behältnis (1) zugeordnet ist, oder an eine Gruppe von mobilen Endgeräten (16) sendet, wobei alle der Gruppe zugeordneten mobilen Endgeräte (16) dem Behältnis (1) zugeordnet sind.

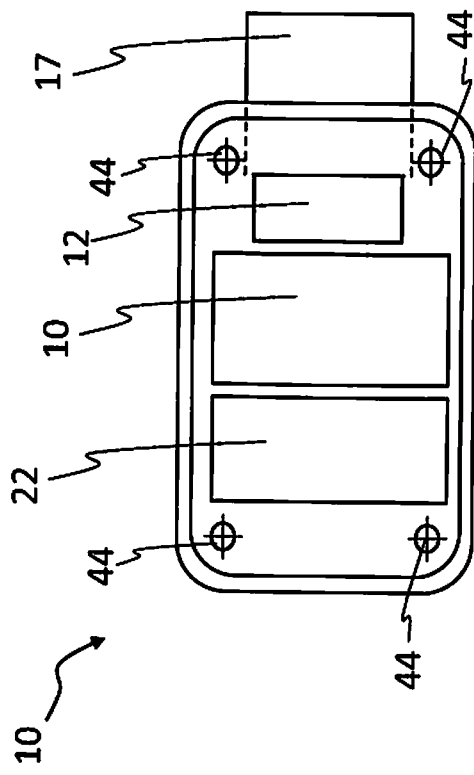


Fig. 1a

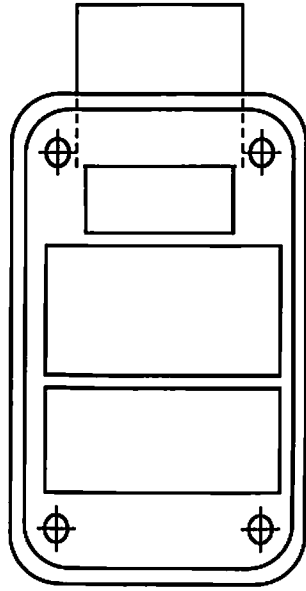


Fig. 1b

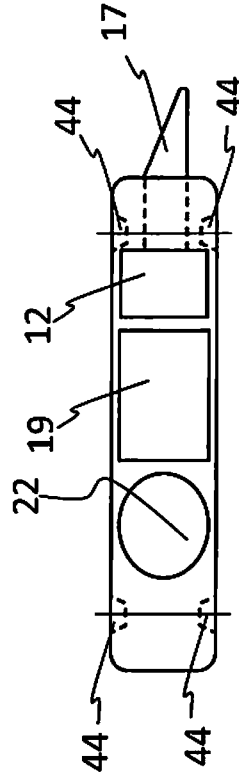


Fig. 1d

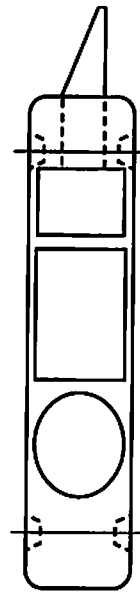


Fig. 1c

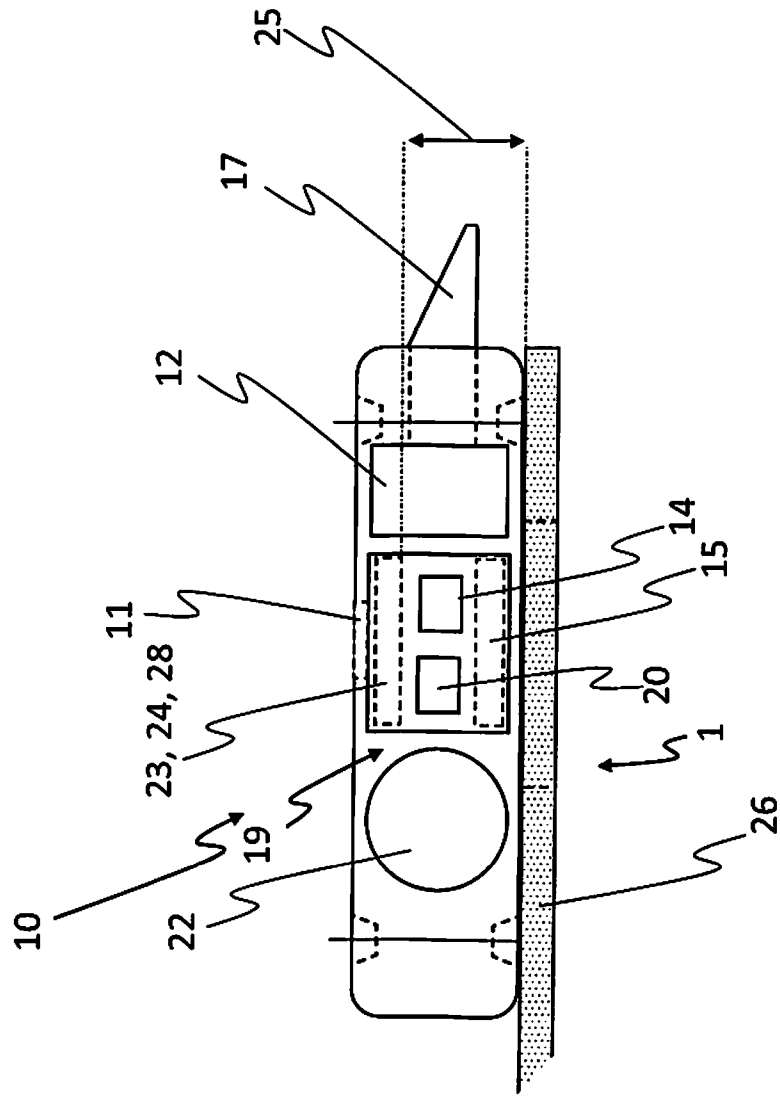


Fig. 2

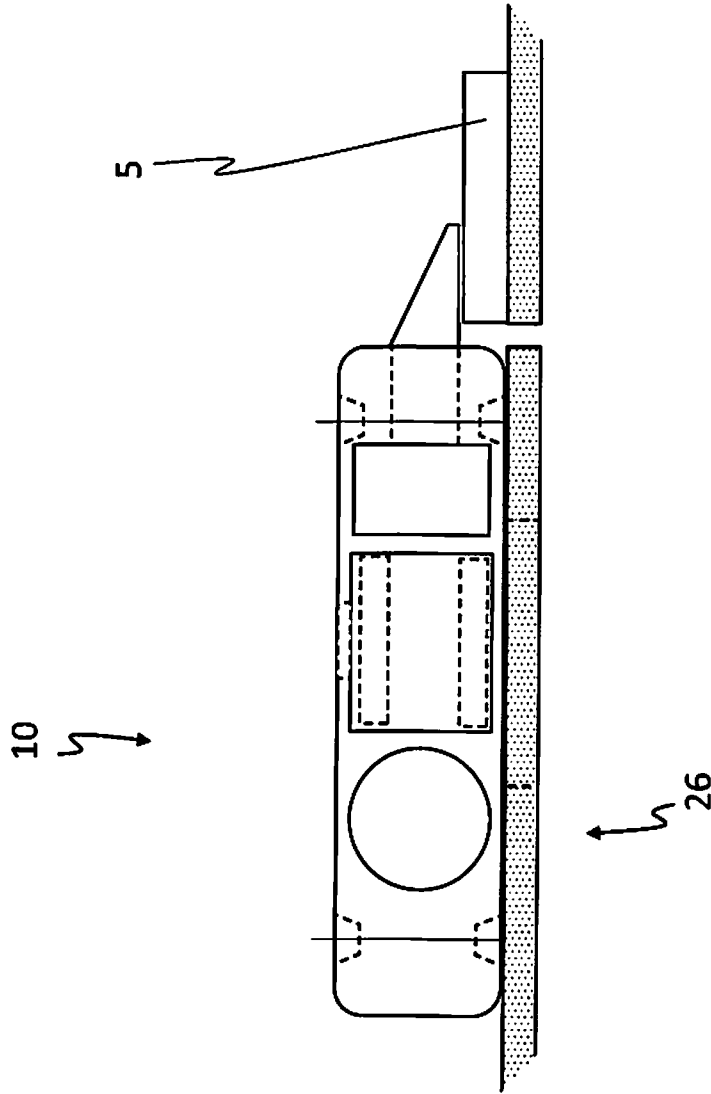


Fig. 3

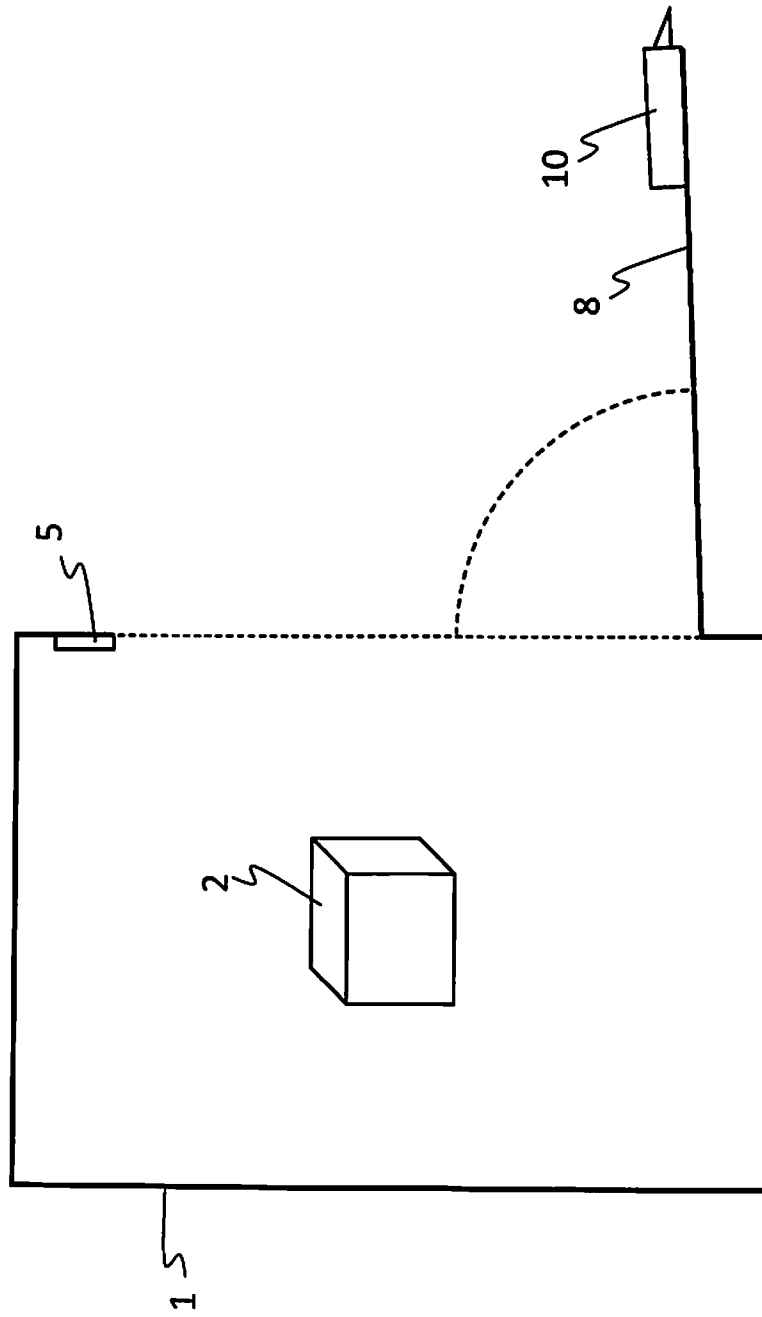


Fig. 4

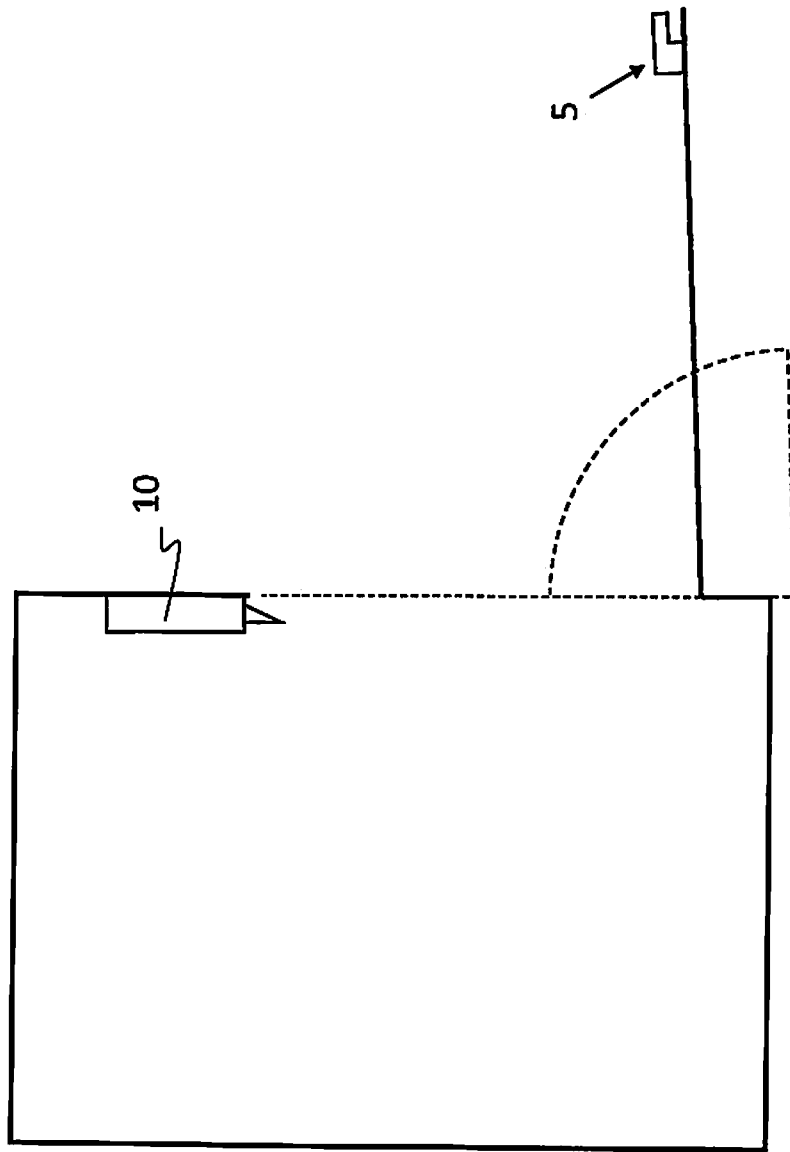


Fig. 5

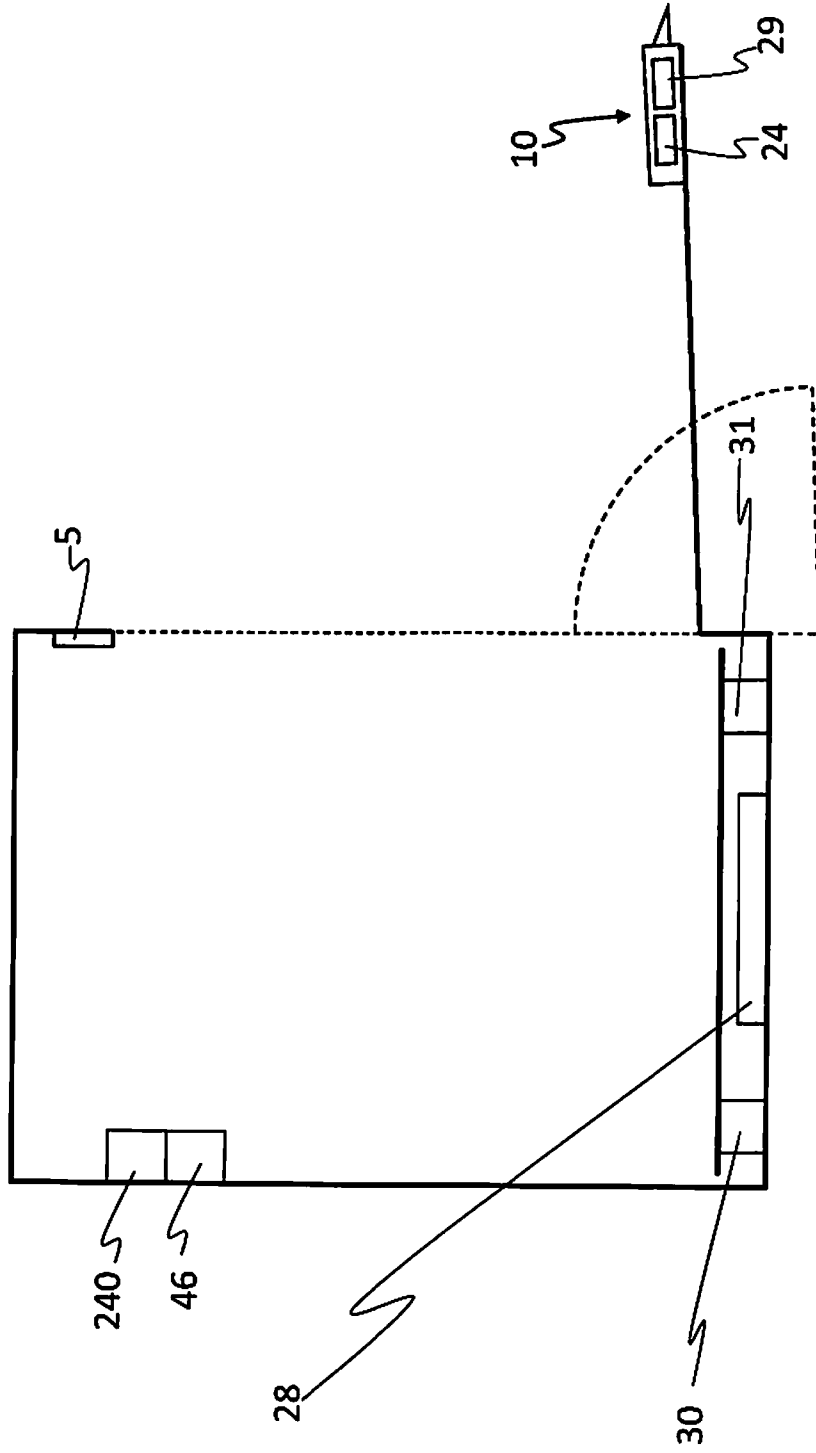


Fig. 6

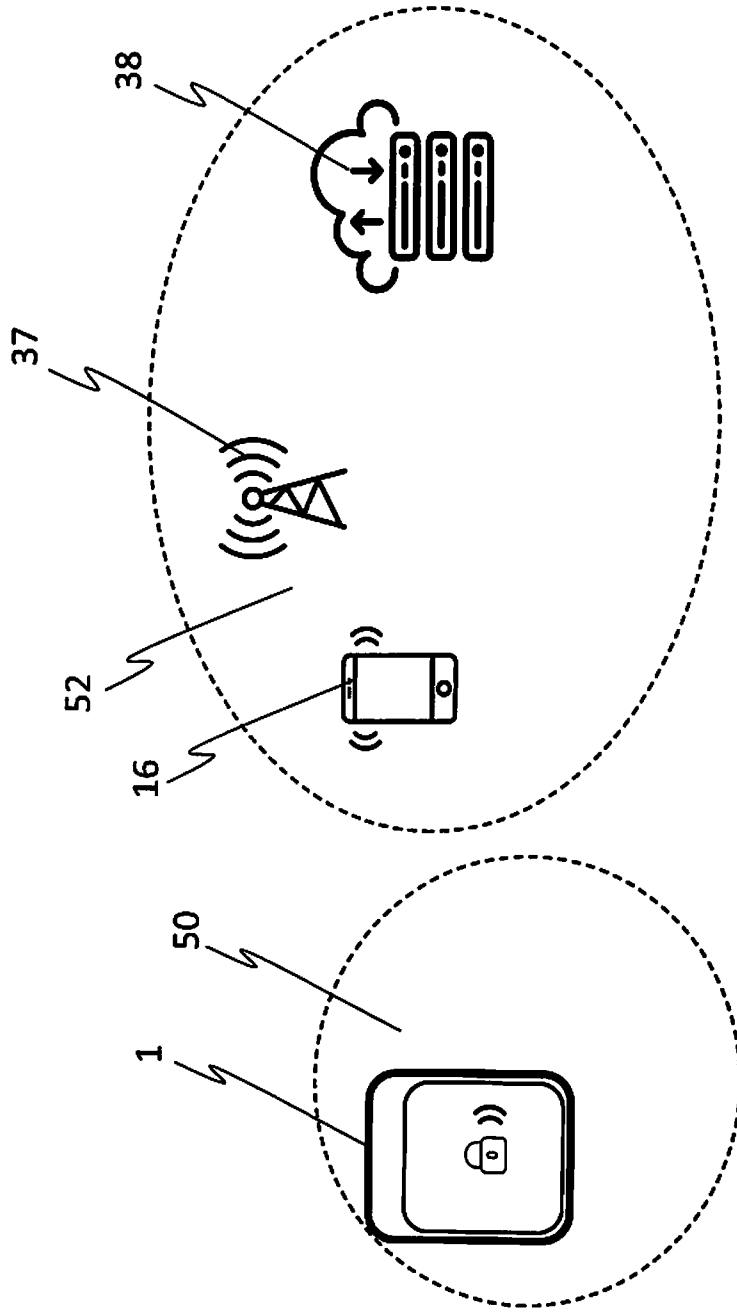


Fig. 7

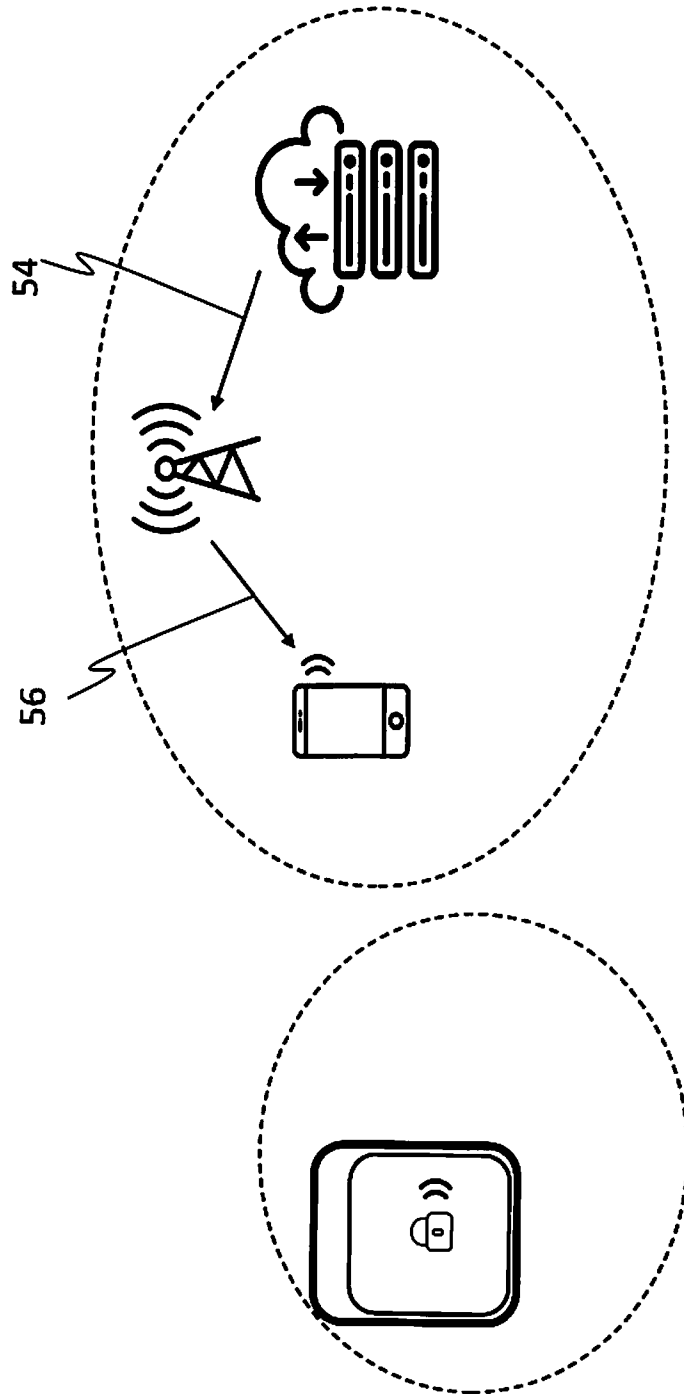


Fig. 8

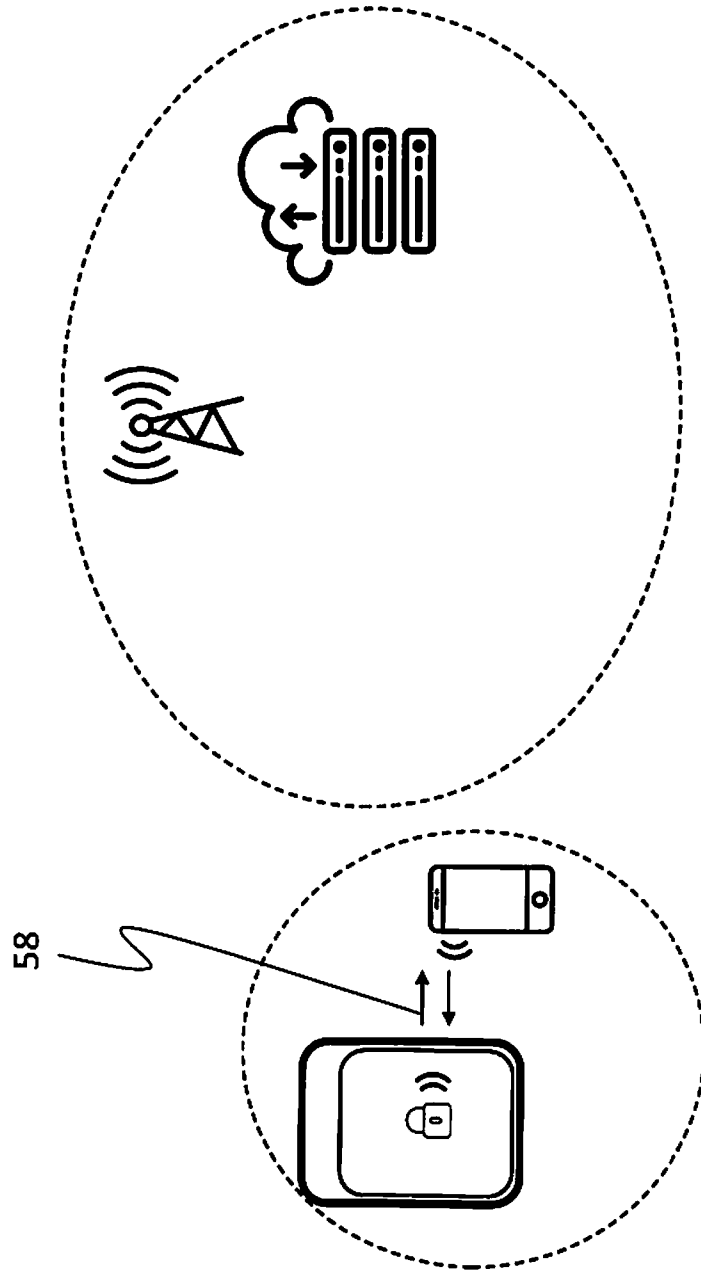


Fig. 9

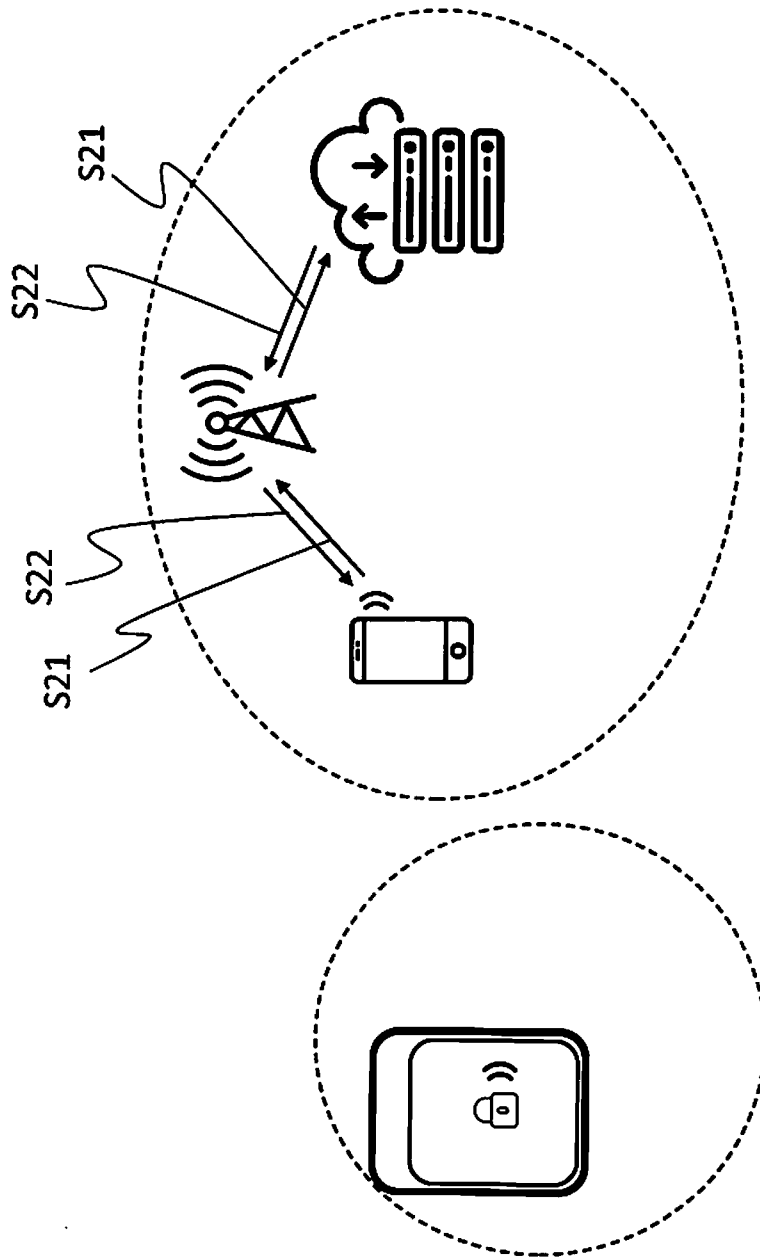


Fig. 10

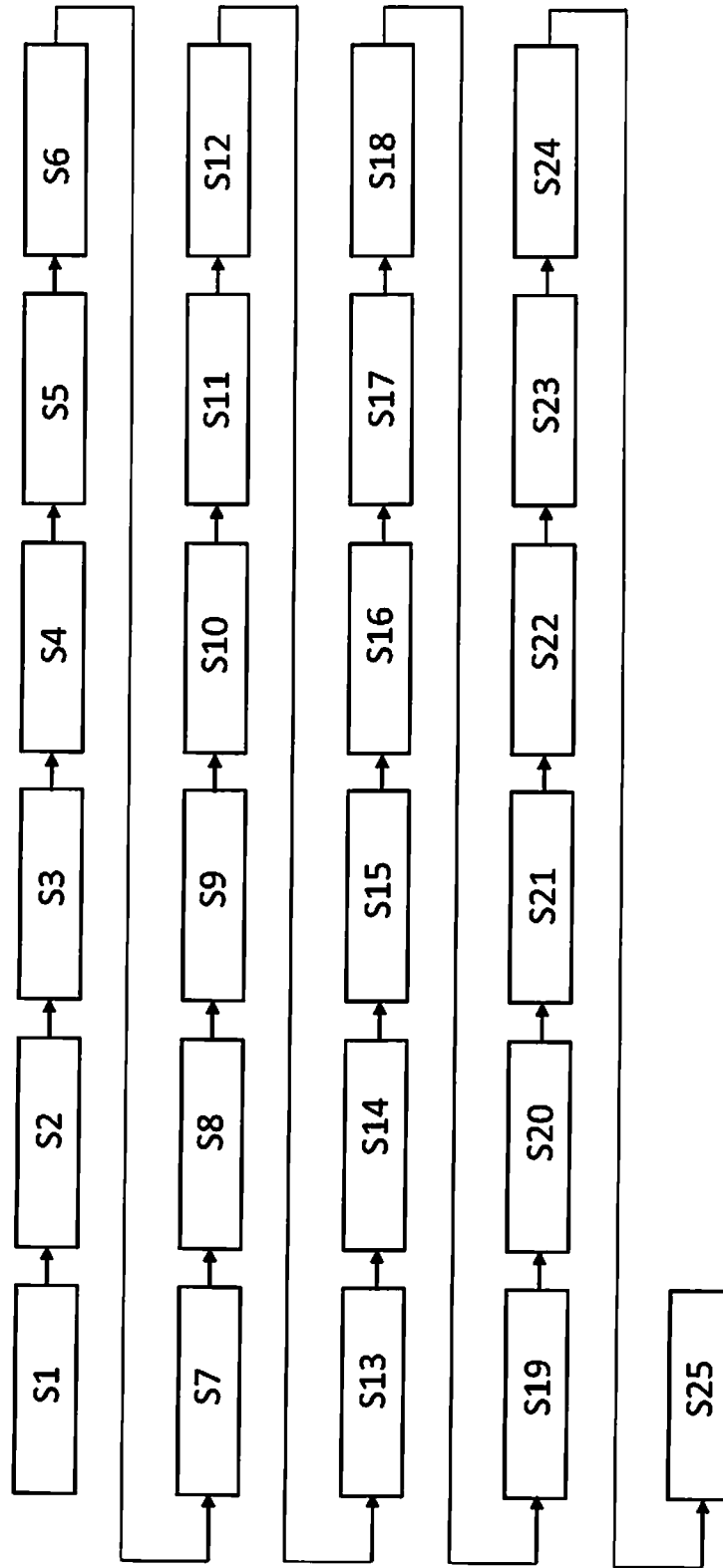


Fig. 11

INTERNATIONAL SEARCH REPORT

International application No.

PCT/EP2020/050723

A. CLASSIFICATION OF SUBJECT MATTER		
<i>G07C 1/10</i> (2006.01)i; <i>G07C 1/32</i> (2006.01)i; <i>G07C 9/00</i> (2020.01)i; <i>E05B 39/04</i> (2006.01)n		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) G07C; H04W; E05C; E05B		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPO-Internal, WPI Data		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 2005232747 A1 (BRACKMANN ROGERS F [US] ET AL) 20 October 2005 (2005-10-20) paragraph [0002] paragraph [0009] - paragraph [0015] paragraph [0026] - paragraph [0031] paragraph [0090] - paragraph [0108]	1-7 8-15
Y A	US 2014051407 A1 (AHEARN JOHN ROBERT [US] ET AL) 20 February 2014 (2014-02-20) paragraph [0012] - paragraph [0020] paragraph [0029] - paragraph [0032]	8-15 6,7
A	DE 102011081207 A1 (CARGOGUARD GMBH [DE]) 21 February 2013 (2013-02-21) paragraph [0017] paragraph [0035]	3-6
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 01 April 2020		Date of mailing of the international search report 14 April 2020
Name and mailing address of the ISA/EP European Patent Office p.b. 5818, Patentlaan 2, 2280 HV Rijswijk Netherlands Telephone No. (+31-70)340-2040 Facsimile No. (+31-70)340-3016		Authorized officer Mechenbier, Bernd Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/EP2020/050723

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2005232747	A1	20 October 2005	NONE			
US	2014051407	A1	20 February 2014	AU	2013302378	A1	02 April 2015
				EP	2885167	A1	24 June 2015
				MX	361609	B	31 October 2018
				NZ	706026	A	26 February 2016
				US	2014051407	A1	20 February 2014
				US	2014051425	A1	20 February 2014
				US	2017265026	A1	14 September 2017
				US	2019141504	A1	09 May 2019
				WO	2014028897	A1	20 February 2014
DE	102011081207	A1	21 February 2013	DE	102011081207	A1	21 February 2013
				EP	2745275	A2	25 June 2014
				WO	2013023794	A2	21 February 2013

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP2020/050723

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
 INV. G07C1/10 G07C1/32 G07C9/00
 ADD. E05B39/04

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
 G07C H04W E05C E05B

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
 EPO-Internal, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2005/232747 A1 (BRACKMANN ROGERS F [US] ET AL) 20. Oktober 2005 (2005-10-20)	1-7
Y	Absatz [0002] Absatz [0009] - Absatz [0015] Absatz [0026] - Absatz [0031] Absatz [0090] - Absatz [0108] -----	8-15
Y	US 2014/051407 A1 (AHEARN JOHN ROBERT [US] ET AL) 20. Februar 2014 (2014-02-20)	8-15
A	Absatz [0012] - Absatz [0020] Absatz [0029] - Absatz [0032] -----	6,7
A	DE 10 2011 081207 A1 (CARGOGUARD GMBH [DE]) 21. Februar 2013 (2013-02-21) Absatz [0017] Absatz [0035] -----	3-6

Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absenddatum des internationalen Recherchenberichts
1. April 2020	14/04/2020

Name und Postanschrift der Internationalen Recherchenbehörde Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Bevollmächtigter Bediensteter Mechenbier, Bernd
--	--

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2020/050723

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2005232747 A1	20-10-2005	KEINE	

US 2014051407 A1	20-02-2014	AU 2013302378 A1	02-04-2015
		EP 2885167 A1	24-06-2015
		MX 361609 B	31-10-2018
		NZ 706026 A	26-02-2016
		US 2014051407 A1	20-02-2014
		US 2014051425 A1	20-02-2014
		US 2017265026 A1	14-09-2017
		US 2019141504 A1	09-05-2019
		WO 2014028897 A1	20-02-2014

DE 102011081207 A1	21-02-2013	DE 102011081207 A1	21-02-2013
		EP 2745275 A2	25-06-2014
		WO 2013023794 A2	21-02-2013
