

(19)



(11)

EP 2 958 083 A1

(12)

EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
23.12.2015 Patentblatt 2015/52

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

(21) Anmeldenummer: **14173032.5**

(22) Anmeldetag: **18.06.2014**

(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
Benannte Erstreckungsstaaten:
BA ME

(72) Erfinder:
• **Lüling, Harald**
58540 Meinerzhagen (DE)
• **Bagheri, Hossein**
58135 Hagen (DE)

(30) Priorität: **17.06.2014 EP 14172806**

(74) Vertreter: **Stenger Watzke Ring**
Intellectual Property
Am Seestern 8
40547 Düsseldorf (DE)

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

(54) Verfahren zur Konfiguration elektronischer Schlösser

(57) Die Erfindung betrifft ein Verfahren zur Konfiguration elektronischer Schlösser (1, 2, 3, 4), mit einer Vielzahl elektronischer Schlösser (1, 2, 3, 4), welche durch einen Administrator (5) konfigurierbar und durch einen Benutzer (6, 7) unter Verwendung eines elektronischen Schlüssels (10) betätigbar sind, bei welchem neue Konfigurationsdaten für zumindest einen Teil der elektronischen Schlösser (1, 2, 3, 4) auf zumindest einen elektro-

nischen Schlüssel (10) übertragen werden, wobei diese Konfigurationsdaten im Falle einer datentechnischen Kommunikationsverbindung (15, 16, 17, 28, 19) zwischen einem noch nicht neu konfigurierten Schloss (1, 2, 3, 4) und dem elektronischen Schlüssel (10) zum Zwecke der Konfiguration auf das noch nicht konfigurierte Schloss (1, 2, 3, 4) übertragen werden.

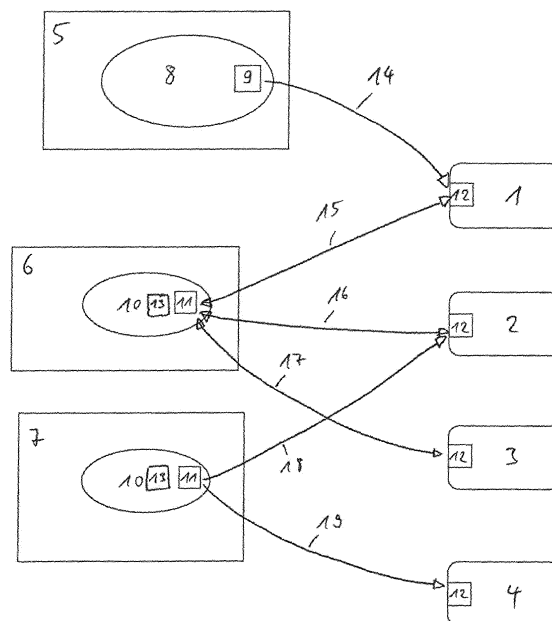


Figure 1

EP 2 958 083 A1

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Konfiguration elektronischer Schlösser, mit einer Vielzahl elektronischer Schlösser, welche durch einen Administrator konfigurierbar und durch einen Benutzer unter Verwendung eines elektronischen Schlüssels betätigbar sind.

[0002] Derartige Verfahren sind aus dem Stand der Technik bekannt. Es handelt sich hierbei oftmals um Verfahren, welche zur Konfiguration umfangreicher Schließanlagen eingesetzt werden, beispielsweise in mehrstöckigen Bürogebäuden und/oder dergleichen.

[0003] Die elektronischen Schlösser können miteinander vernetzt sein. Der Administrator kann dann zentral, beispielsweise mittels eines Computers, alle miteinander vernetzten Schlösser erreichen und konfigurieren.

[0004] Es sind jedoch auch Schließsysteme bekannt, bei denen die einzelnen elektronischen Schlösser nicht miteinander vernetzt sind. Es handelt sich vielmehr bei jedem elektronischen Schloss um ein autark betreibbares System. Dies hat den erheblichen Vorteil, dass der gesamte Aufwand zur Vernetzung vollständig wegfällt.

[0005] Der Nachteil solcher autarken elektronischen Schlösser besteht jedoch darin, dass der Administrator jedes elektronische Schloss eines Schließsystems einzeln quasi von Hand programmieren muss. Hierzu muss er jedes elektronische Schloss aufsuchen und beispielsweise einen Laptop anschließen, um dann neue Konfigurationsdaten auf das elektronische Schloss zu übertragen.

[0006] Vor diesem Hintergrund ist es die Aufgabe der vorliegenden Erfindung, ein gattungsgemäßes Verfahren, insbesondere bei der Verwendung autarker Schlösser, hinsichtlich der Handhabung zu verbessern, hinsichtlich des Aufwands einfacher zu gestalten und darüber hinaus die Kosten zu verringern.

[0007] Zur Lösung schlägt die Erfindung vor, dass neue Konfigurationsdaten für zumindest einen Teil der elektronischen Schlösser auf zumindest einen elektronischen Schlüssel übertragen werden, wobei diese Konfigurationsdaten im Falle einer datentechnischen Kommunikationsverbindung zwischen einem noch nicht neu konfigurierten Schloss und dem elektronischen Schlüssel zum Zwecke der Konfiguration auf das insbesondere neu zu konfigurierende Schloss übertragen werden.

[0008] Die Erfindung schlägt mit anderen Worten vor, dass eine Konfiguration eines elektronischen Schlosses nicht mehr durch den Administrator selbst, beispielsweise unter Verwendung eines Notebooks, durchgeführt wird. Es wird vielmehr zumindest einer der ohnehin vorhandenen und auch verwendeten elektronischen Schlüssel eines Benutzers dazu verwendet, zunächst die Konfigurationsdaten zu empfangen und anschließend, im Falle einer entsprechenden Kommunikationsverbindung, die Konfigurationsdaten auf ein noch nicht konfiguriertes Schloss zu übertragen. Der Benutzer beziehungsweise der elektronische Schlüssel des Benutzers wird sozusagen als "Wirt" zweckentfremdet, um nicht nur Öffnungs- und/oder Schließbefehle an die elektronischen Schlösser zu senden, sondern auch Konfigurationsdaten zu übertragen.

[0009] Der Administrator eines Schließsystems muss daher lediglich sicherstellen, dass einer der elektronischen Schlüssel die neuen Konfigurationsdaten empfängt. Je nach der Art der elektronischen Schlüssel kann dies auf unterschiedliche Weisen geschehen. Der Schlüssel kann gegebenenfalls über eine Schnittstelle für ein Wide-Area-Network oder ein Local-Area-Network verfügen. Über dieses können die neuen Konfigurationsdaten, beispielsweise in Form einer Email, auf den Schlüssel übertragen werden. Dort können sie gespeichert und, im Falle der Kommunikationsverbindung, auf das noch nicht konfigurierte Schloss übertragen werden. Die Konfigurationsdaten können auch unmittelbar auf den elektronischen Schlüssel geladen werden. Hierzu wird beispielsweise ein Benutzer im Eingangsbereich eines Gebäudes abgefangen und gebeten, seinen Schlüssel für eine Datenübertragung zur Verfügung zu stellen. Durch eine entsprechende Vorrichtung, beispielsweise ein Computerterminal mit entsprechender Schnittstelle oder dergleichen, können die Konfigurationsdaten auf den elektronischen Schlüssel geladen werden. Eine weitere Alternative besteht darin, dass der Administrator einen Teil, insbesondere nur eines der Schlösser konfiguriert, wobei im Falle einer datentechnischen Kommunikationsverbindung zwischen einem bereits konfigurierten Schloss und dem elektronischen Schlüssel die neuen Konfigurationsdaten auf den elektronischen Schlüssel übertragen werden.

[0010] Sofern der elektronische Schlüssel eines Benutzers die neuen Konfigurationsdaten empfangen hat, können diese bei jeder Kommunikationsverbindung mit einem weiteren, noch nicht neu konfigurierten Schloss auf dieses übertragen werden. Der Administrator muss also nicht jedes elektronische Schloss einzeln konfigurieren, sondern muss lediglich einen Konfigurationsprozess durch einmaliges Konfigurieren eines einzigen elektronischen Schlüssels und/oder eines einzigen elektronischen Schlosses anstoßen. Anschließend verteilen sich die neuen Konfigurationsdaten durch den normalen Gebrauch des Schließsystems nach und nach auf die verschiedenen elektronischen Schlösser. Man kann insofern auch von einer Virus-ähnlichen Ausbreitung der neuen Konfigurationsdaten unter Verwendung der Benutzer beziehungsweise deren elektronischen Schlüsseln als Wirte sprechen. Die Erfindung macht sich eine Art menschliches Netzwerk beziehungsweise eine Form von Schwarmintelligenz zunutze, um elektronische Schlösser zu konfigurieren.

[0011] Der Aufwand für die Konfiguration elektronischer Schlösser wird somit deutlich verringert. Es ist mit dem erfindungsgemäßen Verfahren entbehrlich, jedes elektronische Schloss einzeln durch einen Administrator zu konfigurieren. Die Erfindung ist daher insbesondere bei der Verwendung autarker elektronischer Schlösser von Vorteil. Durch die

Erfindung wird somit die Handhabung eines Schließsystems deutlich verbessert, zudem wird die Konfiguration deutlich vereinfacht. Insgesamt lassen sich durch das erfindungsgemäße Verfahren auch Kosten einsparen, da personeller Aufwand für eine gezielte Konfiguration einzelner Schlösser eingespart werden kann beziehungsweise auf ein kostenintensives System miteinander vernetzter elektronischer Schlösser verzichtet werden kann.

[0012] Ein elektronisches Schloss im Sinne der Erfindung ist eine insbesondere mechanische Verriegelungseinrichtung für beispielsweise Türen, welche durch einen elektrischen Antrieb geschaltet wird, welcher wiederum durch ein elektrisches Signal angesteuert wird. Es handelt sich somit um ein mechatronisches System.

[0013] Die Konfigurationsdaten können Zugriffsrechte für einzelne elektronische Schlüssel, Zeiträume für eine dauerhafte Öffnung bestimmter elektronischer Schlösser, eine Zeitdauer für eine Öffnung des elektronischen Schlosses nach Betätigung mit einem elektronischen Schlüssel und/oder dergleichen enthalten.

[0014] Die elektronischen Schlüssel können in Form mobiler Endgeräte, beispielsweise Smartphones, Notebooks, Tablet-Computer und/oder dergleichen vorliegen. Es kann sich auch um Smartcards, Transponder und/oder dergleichen handeln.

[0015] Die datentechnische Kommunikationsverbindung kann durch Kurzstrecken-Funktechnik, beispielsweise Bluetooth, NFC, RFID und/oder dergleichen erfolgen. Es handelt sich insbesondere um eine drahtlose Kommunikationsverbindung.

[0016] Konfiguration meint, dass auf der Grundlage von Konfigurationsdaten innerhalb eines elektronischen Schlosses Parameter für den Betrieb des elektronischen Schlosses eingestellt werden.

[0017] Die Konfigurationsdaten können automatisiert auf den elektronischen Schlüssel übertragen werden. Ergänzend oder alternativ können die Kommunikationsdaten automatisch vom elektronischen Schlüssel ausgelesen werden. Dies bedeutet, dass der Benutzer von der Durchführung eines erfindungsgemäßen Verfahrens überhaupt nichts mitbekommt. Er muss in keiner Weise aktiv werden, um eine erfindungsgemäße Verfahrensdurchführung zu gewährleisten. Er beziehungsweise sein Schlüssel wird lediglich unbemerkt als Informationsträger benutzt.

[0018] Die Konfigurationsdaten werden vorzugsweise auf dem elektronischen Schlüssel gespeichert. Hierbei kann es sich um einen dauerhaften Speicher handeln, so dass beispielsweise auch ein Benutzer, der längere Zeit abwesend war, beispielsweise aus Urlaubsgründen, immer noch die Konfigurationsdaten auf seinem elektronischen Schlüssel trägt, welche im Falle einer Kommunikationsverbindung mit einem noch nicht neu konfigurierten Schloss auch nach einer längeren Zeitdauer auf das noch nicht konfigurierte Schloss übertragen werden können.

[0019] Vorzugsweise nehmen mehrere Benutzer mit jeweils einem zugeordneten elektronischen Schlüssel am Verfahren teil. Im Falle einer datentechnischen Kommunikationsverbindung zwischen einem bereits konfigurierten Schloss und einem weiteren elektronischen Schlüssel können die neuen Konfigurationsdaten in dem weiteren elektronischen Schlüssel empfangen und gespeichert werden, wobei die neuen Konfigurationsdaten im Falle einer datentechnischen Kommunikationsverbindung zwischen einem weiteren noch nicht konfigurierten Schloss und dem weiteren elektronischen Schlüssel zum Zwecke der Konfiguration auf das weitere noch nicht konfigurierte Schloss übertragen werden.

[0020] Nach und nach verteilen sich somit die Konfigurationsdaten auf viele elektronische Schlüssel der Benutzer eines Schließsystems und somit auch nach und nach auf alle elektronischen Schlösser des Schließsystems. Nach den Gesetzen der Wahrscheinlichkeitstheorie kann zumindest annähernd sichergestellt werden, dass bei einer entsprechenden Anzahl Schlösser und Nutzer und einem bekannten Verhaltensmuster nach einer vorbestimmten Zeitdauer alle elektronischen Schlösser die neuen Konfigurationsdaten erhalten haben.

[0021] Ein Anwendungsbeispiel für das erfindungsgemäße Verfahren betrifft die Konfiguration von elektronischen Türschlössern in Hotels. Derartige Türschlösser können üblicherweise nicht zentral beispielsweise durch die Rezeption, konfiguriert werden. Es werden vielmehr Smartcards an die Hotelgäste ausgegeben, welche nach dem Aufenthalt im Hotel wieder abgegeben werden müssen. Darüber hinaus sind jedoch bereits Verfahren zum Zugang zu elektronischen Türschlössern mittels beispielsweise Smartphones bekannt geworden. Hierbei stellt sich das Problem, dass beispielsweise im Falle eines vom Benutzer vorzeitig abgebrochenen Hotelaufenthalts das Türschloss neu programmiert werden muss, da der Benutzer sonst mit den ursprünglichen Zugangsdaten auf seinen Smartphone nach wie vor Zutritt zum Schloss hätte. Hier kann das erfindungsgemäße Verfahren verwendet werden, um durch sich innerhalb des Hotels bewegend Personen mit mobilen Endgeräten eine "stille" Konfiguration des jeweiligen Schlosses durchzuführen. Man spricht in diesem Zusammenhang auch von silent-update.

[0022] Weitere Vorteile und Merkmale der Erfindung ergeben sich anhand der nachfolgenden Figurenbeschreibung. Die einzige Figur zeigt schematisch eine Ausführungsform eines erfindungsgemäßen Verfahrens.

[0023] Fig. 1 zeigt eine Ausführungsform eines erfindungsgemäßen Verfahrens. Beispielhaft sind vier elektronische Schlösser 1, 2, 3, 4 dargestellt. Diese können innerhalb eines Gebäudes an unterschiedlichen Türen angeordnet sein. Jedes elektronische Schloss 1, 2, 3, 4 verfügt über eine Kommunikationsschnittstelle 12. Über die Kommunikationsschnittstelle 12 kann es mit einer Programmiereinrichtung 8 eines Administrators 5 und/oder elektronischen Schlüssel 10 von Benutzern 6, 7 kommunizieren.

[0024] Die Programmiereinrichtung des Administrators 5 verfügt ebenfalls über eine Kommunikationsschnittstelle 9. Dadurch kann zwischen der Programmiereinrichtung 8 und einem elektrischen Schloss 1 eine Kommunikationsverbin-

dung 14 ausgebildet werden.

[0025] Die Benutzer 6, 7 tragen die Schlüssel 10 bei sich. Die Schlüssel 10 verfügen ebenfalls über Kommunikationsschnittstellen 11, durch welche entsprechende Kommunikationsverbindungen mit den elektronischen Schlössern 1, 2, 3, 4 aufgebaut werden können. Die Schlüssel 10 verfügen zudem über einen Speicher 13. In dem Speicher 13 können Konfigurationsdaten gespeichert werden.

[0026] Die Ausführungsform des erfindungsgemäßen Verfahrens gemäß Fig. 1 geht wie folgt von statten. Die elektronischen Schlösser 1, 2, 3, 4 sollen mit neuen Konfigurationsdaten versehen werden. Hierbei kann es sich beispielsweise um Zugriffsrechte für einzelne elektronische Schlüssel handeln. Der Administrator 5 programmiert nun ein erstes elektronisches Schloss 1. Hierzu verwendet er seine Programmiereinrichtung 8. Hierbei kann es sich beispielsweise um ein Notebook handeln. Zwischen der Kommunikationsschnittstelle 9 der Programmiereinrichtung und der Kommunikationsschnittstelle 12 des elektronischen Schlosses 1 wird eine Kommunikationsverbindung 14 aufgebaut. Hierbei kann es sich um eine drahtlose oder drahtgebundene Kommunikationsverbindung handeln. Die Verbindung kann beispielsweise per LAN oder Bluetooth ausgebildet werden. Über die Kommunikationsverbindung 14 werden neue Konfigurationsdaten auf das elektronische Schloss 1 übertragen. Die elektronischen Schlösser können einen Speicher, einen Mikroprozessor und/oder dergleichen aufweisen.

[0027] Das elektronische Schloss 1 ist anschließend mit neuen Konfigurationsdaten konfiguriert. Bei den hier in Rede stehenden autarken elektronischen Schlössern müsste es nunmehr nach dem Stand der Technik vorgesehen sein, dass der Administrator 5 jedes einzelne dieser elektronischen Schlösser getrennt voneinander konfiguriert. Die hier vorgestellte Ausführungsform des erfindungsgemäßen Verfahrens schafft jedoch Abhilfe.

[0028] Sofern ein erster Benutzer 6 das erste elektronische Schloss 1 passiert, wird automatisiert eine Kommunikationsverbindung 15 zwischen der Kommunikationsschnittstelle 11 des Schlüssels 10 und der Kommunikationsschnittstelle 12 des elektronischen Schlosses 1 hergestellt. Dies kann unabhängig davon erfolgen, ob der Benutzer 6 tatsächlich das elektronische Schloss 1 betätigen möchte oder nur in dessen Nähe, das heißt Reichweite der Kommunikationsschnittstellen 11, 12 gelangt.

[0029] Durch die Kommunikationsverbindung 15 werden automatisiert die neuen Konfigurationsdaten in den Speicher 13 des Schlüssels 10 geladen. Sofern der Benutzer 6 anschließend ein weiteres elektronisches Schloss des Systems passiert, wird ebenfalls automatisiert eine Kommunikationsverbindung 16, 17 mit dem jeweiligen elektronischen Schloss 2, 3 ausgebildet. Sofern eine Kommunikationsverbindung 16, 17 ausgebildet wird, werden die Konfigurationsdaten automatisiert, das heißt ohne aktives Tun des Benutzers 6 vom Speicher 13 des Schlüssels 10 ausgelesen und in das elektronische Schloss 2, 3 geladen. Das elektronische Schloss 2, 3 ist derart eingerichtet, dass es sich beim Vorliegen neuer Konfigurationsdaten automatisiert neu konfiguriert.

[0030] Ein zweiter Benutzer 7, der ebenfalls einen Schlüssel 10 bei sich trägt, passiert anschließend beispielsweise das elektronische Schloss 2. Da dieses bereits über die neuen Konfigurationsdaten verfügt, werden diese ebenso automatisiert über eine weitere Kommunikationsverbindung 18 in den Speicher 13 des Schlüssels 10 des zweiten Benutzers 7 geladen. Sofern der zweite Benutzer 7 nun ein weiteres, noch nicht neu konfiguriertes elektronisches Schloss 4 passiert, werden wiederum die jetzt auch auf seinem Schlüssel 10 vorhandenen Konfigurationsdaten auf dieses elektronische Schloss 4 übertragen. Hierzu dient eine weitere Kommunikationsverbindung 19.

[0031] Sofern nur vier elektronische Schlösser vorgesehen sind, wären diese nunmehr allesamt mit den neuen Konfigurationsdaten versorgt. Da die Benutzer 6, 7 im Alltag die elektronischen Schlösser ohnehin passieren, ist insgesamt keinerlei zusätzlicher Aufwand zur Konfiguration der elektronischen Schlösser nötig, als lediglich die Programmierung eines ersten elektronischen Schlosses 1 durch den Administrator 5. Alternativ zu dieser Programmierung könnte der Administrator 5 aber auch einen der Schlüssel 10 der Benutzer 6, 7 mit den neuen Konfigurationsdaten versehen. Der Administrator 5 müsste dann kein einziges der elektronischen Schlösser 1, 2, 3, 4 konfigurieren, wobei trotzdem sichergestellt wäre, dass die Benutzer 6, 7 im Laufe der Zeit die elektronischen Schlösser passieren und somit die Konfigurationsdaten übertragen werden.

Bezugszeichenliste

1	elektronisches Schloss	17	Kommunikationsverbindung
2	elektronisches Schloss	18	Kommunikationsverbindung
3	elektronisches Schloss	19	Kommunikationsverbindung
4	elektronisches Schloss		
5	Administrator		
6	Benutzer		
7	Benutzer		
8	Programmiereinrichtung		
9	Kommunikationsschnittstelle		

(fortgesetzt)

5	10	Schlüssel
	11	Kommunikationsschnittstelle
	12	Kommunikationsschnittstelle
	13	Speicher
	14	Kommunikationsverbindung
	15	Kommunikationsverbindung
10	16	Kommunikationsverbindung

Patentansprüche

1. Verfahren zur Konfiguration elektronischer Schlösser (1, 2, 3, 4), mit einer Vielzahl elektronischer Schlösser (1, 2, 3, 4), welche insbesondere durch einen Administrator (5) konfigurierbar und durch einen Benutzer (6, 7) unter Verwendung eines elektronischen Schlüssels (10) betätigbar sind, **dadurch gekennzeichnet, dass** neue Konfigurationsdaten für zumindest einen Teil der elektronischen Schlösser (1, 2, 3, 4) auf zumindest einen elektronischen Schlüssel (10) übertragen werden, wobei diese Konfigurationsdaten im Falle einer datentechnischen Kommunikationsverbindung (15, 16, 17, 28, 19) zwischen einem noch nicht neu konfigurierten Schloss (1, 2, 3, 4) und dem elektronischen Schlüssel (10) zum Zwecke der Konfiguration auf das insbesondere neu zu konfigurierende Schloss (1, 2, 3, 4) übertragen werden.
2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** die neuen Konfigurationsdaten vom Administrator (5) auf den elektronischen Schlüssel (10) übertragen werden.
3. Verfahren nach Anspruch 2, **dadurch gekennzeichnet, dass** die neuen Konfigurationsdaten per Wide-Area-Network, GSM, WLAN, LAN und/oder Kurzstrecken-Funktechnik übertragen werden.
4. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** der Administrator (5) nur einen Teil, insbesondere nur eines, der Schlösser (1, 2, 3, 4) konfiguriert, wobei im Falle einer datentechnischen Kommunikationsverbindung zwischen einem bereits konfigurierten Schloss und dem elektronischen Schlüssel (10) die neuen Konfigurationsdaten auf den elektronischen Schlüssel (10) übertragen werden.
5. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, dass** die Konfigurationsdaten automatisiert auf den elektronischen Schlüssel (10) übertragen werden.
6. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, dass** die Konfigurationsdaten auf dem elektronischen Schlüssel (10) gespeichert werden.
7. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, dass** die Konfigurationsdaten vom Benutzer (6, 7) unbemerkt übertragen werden.
8. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, dass** im Falle einer datentechnischen Kommunikationsverbindung zwischen einem bereits konfigurierten Schloss (1, 2, 3, 4) und einem weiteren elektronischen Schlüssel (10) die neuen Konfigurationsdaten in dem weiteren elektronischen Schlüssel (10) empfangen und gespeichert werden, wobei die neuen Konfigurationsdaten im Falle einer datentechnischen Kommunikationsverbindung zwischen einem weiteren noch nicht konfigurierten Schloss (1, 2, 3, 4) und dem weiteren elektronischen Schlüssel (10) zum Zwecke der Konfiguration auf das weitere noch nicht konfigurierte Schloss (1, 2, 3, 4) übertragen werden.
9. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, dass** Konfigurationsdaten zwischen einem elektronischen Schloss (1, 2, 3, 4) und einem elektronischen Schlüssel per Kurzstrecken-Funktechnik übertragen werden.
10. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, dass** ein elektronisches Schloss (1, 2, 3, 4) im Falle einer datentechnischen Kommunikationsverbindung mit einem elektronischen Schlüssel (10) einen Speicher (13) des elektronischen Schlüssels für Konfigurationsdaten ausliest.

11. Verfahren nach Anspruch 10, **dadurch gekennzeichnet, dass** der Speicher (13) automatisiert ausgelesen wird.

5

10

15

20

25

30

35

40

45

50

55

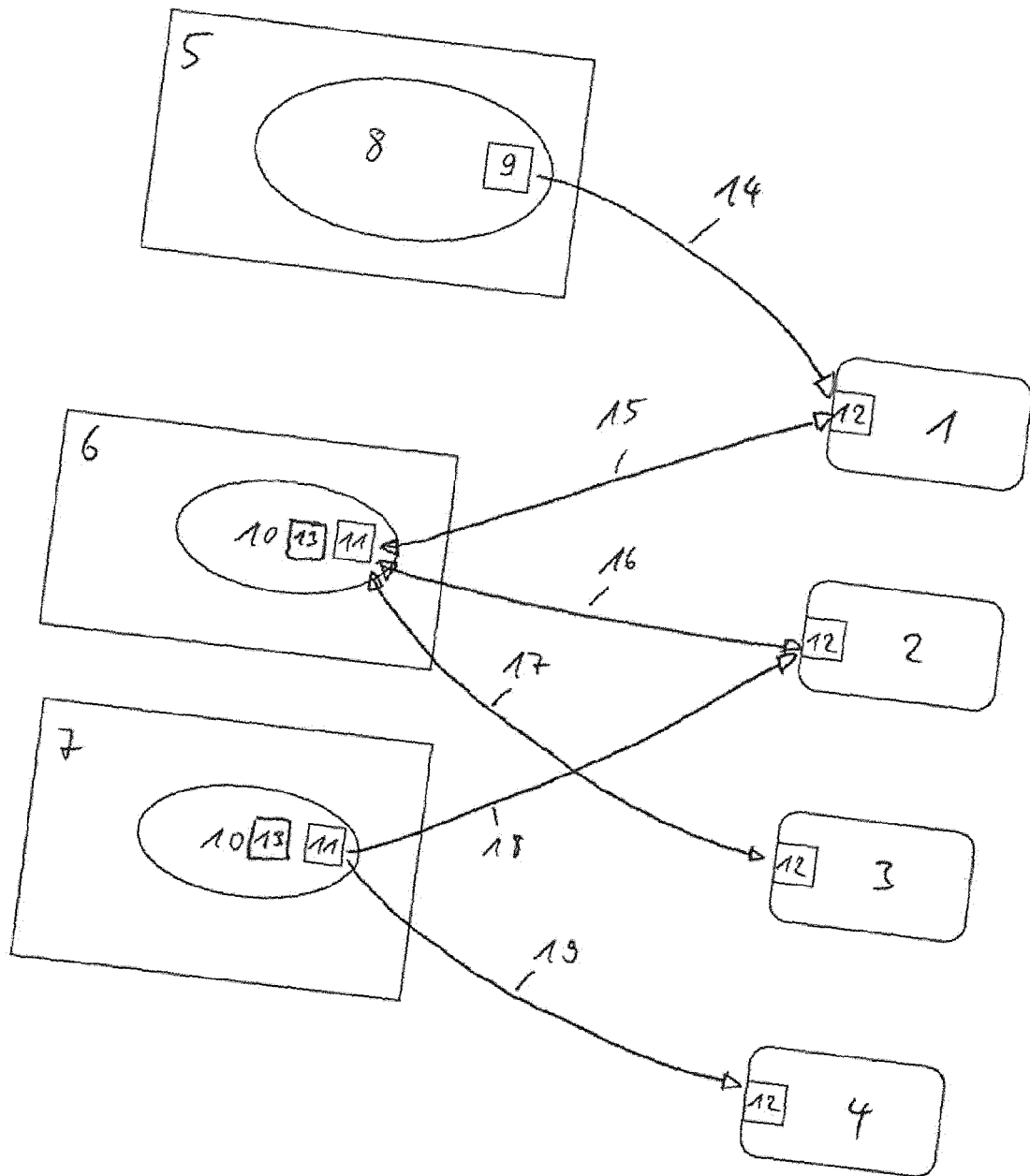


Figure 1



EUROPÄISCHER RECHERCHENBERICHT

 Nummer der Anmeldung
EP 14 17 3032

EINSCHLÄGIGE DOKUMENTE			
Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
X	EP 1 562 153 A2 (SALTO SYSTEMS SL [ES]) 10. August 2005 (2005-08-10)	1-7,9-11	INV. G07C9/00
Y	* Zusammenfassung; Abbildungen 1,2 * * Absätze [0010] - [0042] *	8	
X	DE 10 2011 122461 A1 (AIRBUS OPERATIONS GMBH [DE]; UNIV HAMBURG HARBURG TECH [DE]) 27. Juni 2013 (2013-06-27)	1-7,9-11	
A	* Zusammenfassung; Abbildungen 2b,2c,3b,3c,4 * * Absätze [0019] - [0026] * * Absätze [0041] - [0054] *	8	
X	US 2010/077474 A1 (YACOUB KHALIL W [US] ET AL) 25. März 2010 (2010-03-25)	1-7,9-11	
A	* Zusammenfassung; Abbildungen 3,4,8A-C * * Absätze [0044] - [0058] * * Absätze [0063] - [0092] *	8	
Y	WO 2006/021047 A1 (HONEYWELL LTD [AU]; GOEL PAREEN KUMAR [AU]) 2. März 2006 (2006-03-02)	8	RECHERCHIERTE SACHGEBIETE (IPC) G07C
A	* Zusammenfassung; Abbildungen 1,6-10 * * Seite 22, Zeile 4 - Seite 42, Zeile 33 *	1-7,9-11	
A	US 2014/052777 A1 (EBERWINE TODD [US] ET AL) 20. Februar 2014 (2014-02-20)	1-11	
	* Zusammenfassung; Abbildungen 1,3 * * Absätze [0009] - [0017] * * Absätze [0023] - [0038] *		
A	EP 1 699 019 A2 (EVVA SICHERHEITSSYSTEME GMBH [AT]) 6. September 2006 (2006-09-06)	1-11	
	* Zusammenfassung; Abbildungen 1,2 * * Absätze [0009] - [0027] *		
-/--			
Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt			
Recherchenort Den Haag		Abschlußdatum der Recherche 28. Oktober 2015	Prüfer Pfyffer, Gregor
KATEGORIE DER GENANNTEN DOKUMENTE X : von besonderer Bedeutung allein betrachtet Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie A : technologischer Hintergrund O : nichtschriftliche Offenbarung P : Zwischenliteratur		T : der Erfindung zugrunde liegende Theorien oder Grundsätze E : älteres Patentedokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist D : in der Anmeldung angeführtes Dokument L : aus anderen Gründen angeführtes Dokument & : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument	

EPO FORM 1503 03.82 (P04C03)



EUROPÄISCHER RECHERCHENBERICHT

 Nummer der Anmeldung
 EP 14 17 3032

EINSCHLÄGIGE DOKUMENTE			
Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
A	US 2014/118107 A1 (ALMOMANI NEDAL AKRAM [US]) 1. Mai 2014 (2014-05-01) * Zusammenfassung; Abbildungen 4-7 * * Absätze [0024] - [0042] * -----	1-11	
			RECHERCHIERTE SACHGEBIETE (IPC)
Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt			
Recherchenort		Abschlußdatum der Recherche	
Den Haag		28. Oktober 2015	
		Prüfer	
		Pfyffer, Gregor	
KATEGORIE DER GENANNTEN DOKUMENTE			
X : von besonderer Bedeutung allein betrachtet Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie A : technologischer Hintergrund O : mündliche Offenbarung P : Zwischenliteratur		T : der Erfindung zugrunde liegende Theorien oder Grundsätze E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist D : in der Anmeldung angeführtes Dokument L : aus anderen Gründen angeführtes Dokument & : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument	

EPO FORM 1503 03 82 (P04C03)

**ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT
 ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR.**

EP 14 17 3032

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentedokumente angegeben.

Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
 Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

28-10-2015

Im Recherchenbericht angeführtes Patentedokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 1562153 A2	10-08-2005	EP 1562153 A2	10-08-2005
		ES 2253971 A1	01-06-2006
		US 2005174214 A1	11-08-2005
DE 102011122461 A1	27-06-2013	DE 102011122461 A1	27-06-2013
		EP 2795585 A1	29-10-2014
		WO 2013093070 A1	27-06-2013
US 2010077474 A1	25-03-2010	EP 2350982 A1	03-08-2011
		US 2010077474 A1	25-03-2010
		WO 2010036471 A1	01-04-2010
WO 2006021047 A1	02-03-2006	CN 101052970 A	10-10-2007
		EP 1807788 A1	18-07-2007
		HK 1113213 A1	18-05-2012
		WO 2006021047 A1	02-03-2006
US 2014052777 A1	20-02-2014	AU 2013302381 A1	02-04-2015
		CA 2886378 A1	20-02-2014
		CN 104798111 A	22-07-2015
		EP 2885168 A1	24-06-2015
		US 2014049370 A1	20-02-2014
		US 2014052777 A1	20-02-2014
		WO 2014028900 A1	20-02-2014
EP 1699019 A2	06-09-2006	AT 502458 A1	15-03-2007
		EP 1699019 A2	06-09-2006
US 2014118107 A1	01-05-2014	AU 2013334157 A1	28-05-2015
		CA 2888971 A1	01-05-2014
		CN 104885127 A	02-09-2015
		EP 2912638 A1	02-09-2015
		KR 20150077434 A	07-07-2015
		PH 12015500910 A1	13-07-2015
		US 2014118107 A1	01-05-2014
		WO 2014066763 A1	01-05-2014

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82