(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 2 452 316 B1**

(12) **EUROPÄISCHE PATENTSCHRIFT**

(45) Veröffentlichungstag und Bekanntmachung des Hinweises auf die Patenterteilung:
22.06.2016 Patentblatt 2016/25

(21) Anmeldenummer: **10726106.7**

(22) Anmeldetag: **25.06.2010**

(51) Int Cl.:
E05B 47/00 *(2006.01)* ***G07C 9/00*** *(2006.01)*
E05B 47/06 *(2006.01)*

(86) Internationale Anmeldenummer:
PCT/EP2010/059041

(87) Internationale Veröffentlichungsnummer:
WO 2011/003749 (13.01.2011 Gazette 2011/02)

(54) **VERFAHREN ZUM BETREIBEN EINES ZUTRITTSKONTROLLSYSTEMS**

Method for operating an access control system

Procédé de fonctionnement d'une système de contrôle d'accès

(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 SE SI SK SM TR

(30) Priorität: **06.07.2009 EP 09164689**

(43) Veröffentlichungstag der Anmeldung:
16.05.2012 Patentblatt 2012/20

(73) Patentinhaber: **Inventio AG**
6052 Hergiswil NW (CH)

(72) Erfinder:
- **FRIEDLI, Paul**
  5453 Remetschwil (CH)
- **SCHWARZENTRUBER, Josef**
  6403 Küssnacht a/Rigi (CH)

(74) Vertreter: **Blöchle, Hans et al**
Inventio AG,
Seestrasse 55
Postfach
6052 Hergiswil (CH)

(56) Entgegenhaltungen:
WO-A-2006/056085
DE-A1- 4 307 360
US-A- 6 064 316
US-A1- 2004 003 257
US-A1- 2004 243 812
US-A1- 2007 176 739

EP 2 452 316 B1

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zum Betreiben eines Zutrittskontrollsystems sowie ein Zutrittskontrollsystem gemäss dem Oberbegriff der unabhängigen Ansprüche 1 und 8.

[0002] WO2008/089207A1 offenbart ein Verfahren zum Betreiben eines Zutrittskontrollsystems für die Zutrittskontrolle zu einem gesicherten Bereich eines Gebäudes wie ein Stockwerk oder einen Abschnitt eines Stockwerks. Das Zutrittskontrollsystem umfasst eine Zentralrechnereinheit und einen Türöffner. Der Türöffner gewährt Zutritt zum gesicherten Bereich. Die Zentralrechnereinheit steht über netzwerkgestützte Zutrittspunkte in kommunikativer Verbindung mit dem Türöffner. Der Türöffner weist eine Lesevorrichtung auf, die einen Identifikationscode von einem mobilen Datenträger einliest. Der eingelesene Identifikationscode wird entweder von der Lesevorrichtung oder der Zentralrechnereinheit mit einem Identifikationscode einer Liste mit gültiger Identifikationscodes für den gesicherten Bereich überprüft. Bei erfolgreicher Überprüfung wird vom Türöffner Zutritt zum gesicherten Bereich gewährt.

[0003] WO 2006/056085 A1 zeigt ebenfalls ein zentral verwaltetes Zutrittskontrollsystem. **Aufgabe** der vorliegenden Erfindung ist es, dieses Verfahren, bzw. System weiterzuentwickeln.

[0004] Diese Aufgabe wird durch die kennzeichnenden Merkmale der unabgängigen Ansprüche 1 und 8 gelöst.

[0005] Im **erfindungsgemässen Verfahren** zum Betreiben eines Zutrittskontrollsystem weist das Zutrittskontrollsystems mindestens einen Türbeschlag zu einem gesicherten Bereich eines Gebäudes und mindestens einen Identifikationscode auf einem mobilen Datenträger auf; welcher Identifikationscode von einer Lesevorrichtung eines Türbeschlags eingelesen wird; wobei falls ein eingelesener Identifikationscode gültig ist, Zutritt zu dem vom Türbeschlag gesicherten Bereich gewährt wird; von einer Rechnereinheit wird über mindestens eine kommunikative Verbindung ein Berechtigungscode an eine Zentralrechnereinheit übermittelt; es wird überprüft, ob der Berechtigungscode mit einem gültigen Berechtigungscode für ein Bereichsprofil übereinstimmt; bei erfolgreicher Überprüfung des übermittelten Berechtigungscodes werden Schreib- und Leserechte für das Bereichsprofil an die den Berechtigungscode übermittelnde Rechnereinheit freigegeben; von der Rechnereinheit wird über eine kommunikative Verbindung das freigegebene Bereichsprofil verändert.

[0006] Dies hat den Vorteil, dass von einer beliebigen Rechnereinheit aus, ein Bereichsprofil mit einem gültigen Identifikationscode zu einem gesicherten Bereich des Gebäudes verändert werden kann, was den Betrieb des Zutrittskontrollsystems einfach und flexibel gestaltet. Die Rechnereinheit muss sich mit einem Berechtigungscode bei einer Zentralrechnereinheit als berechtigt für diese Veränderung des Bereichsprofils ausweisen. Die Gültigkeit dieses Berechtigungscode wird überprüft. Die Übermittlung des Berechtigungscodes und die Veränderung des freigegebenen Bereichsprofils erfolgt über eine kommunikative Verbindung. Auf diese Weise ist der Betrieb des Zutrittskontrollsystems sicher.

[0007] Vorteilhafte Weiterbildungen des Verfahrens sind in den abhängigen Ansprüchen beschrieben.

[0008] Vorteilhafterweise wird von der Rechnereinheit ein Identifikationscode eines mobilen Datenträgers als gültiger Identifikationscode in das freigegebene Bereichsprofil aufgenommen. Vorteilhafterweise wird von der Rechnereinheit ein Identifikationscode eines mobilen Datenträgers als gültiger Identifikationscode aus dem freigegebenen Bereichsprofil entfernt.

[0009] Dies hat den Vorteil, dass von der Rechnereinheit aus ein gültiger Identifikationscode eines mobilen Datenträgers in das Bereichsprofil aufgenommen und/oder entfernt werden kann. Weder die Rechnereinheit noch der mobilen Datenträger müssen physisch am Ort des Türbeschlags und/oder der Zentralrechnereinheit sein, was den Betrieb des Zutrittskontrollsystems einfach und flexibel gestaltet.

[0010] Vorteilhafterweise wird von der Rechnereinheit eine Gültigkeit eines Identifikationscodes des freigegebenen Bereichsprofils verändert. Vorteilhafterweise wird von der Rechnereinheit eine Entität in das freigegebene Bereichsprofil aufgenommen. Vorteilhafterweise wird von der Rechnereinheit eine Entität aus dem freigegebenen Bereichsprofil entfernt. Vorteilhafterweise wird von der Rechnereinheit ein Leserecht einer Entität des freigegebenen Bereichsprofils verändert. Vorteilhafterweise wird von der Rechnereinheit ein Schreibrecht einer Entität des freigegebenen Bereichsprofils verändert. Vorteilhafterweise von der Rechnereinheit eine Zeitzone einer Entität des freigegebenen Bereichsprofils verändert.

[0011] Dies hat den Vorteil, dass vielfältige Angaben des freigegebenen Bereichprofils von der die Rechnereinheit aus gewartet werden können, was den Betrieb des Zutrittskontrollsystems einfach und flexibel gestaltet.

[0012] Ferner wird von der Rechnereinheit ein Identifikationscode eines mobilen Datenträgers in einem freigegebenen Bereichsprofil als provisorischer Identifikationscode angelegt; und falls von der Lesevorrichtung des Türbeschlags, der Zutritt zu dem gesicherten Bereich des freigegebenen Bereichprofils gewährt, ein Identifikationscode eingelesen wird, der mit dem provisorischen Identifikationscode übereinstimmt, der eingelesene Identifikationscode in das freigegebene Bereichsprofil als gültiger Identifikationscode aufgenommen wird.

[0013] Dies hat den Vorteil, dass ein provisorischer Identifikationscode eines mobilen Datenträgers von der Recheneinheit zuerst im freigegebenen Bereichsprofil angelegt wird und erst bei tatsächlich erfolgtem Einlesen des provisorischen Identifikationscodes wird der eingelesene Identifikationscode in das freigegebene Bereichsprofil als gültiger Identifikationscode aufgenommen. Somit wird ein neuer Identifikationscodes erst dann in das

Bereichsprofil aufgenommen, wenn er tatsächlich von der Lesevorrichtung eingelesen wird, was den Betrieb des Zutrittskontrollsystems sicher gestaltet. Auch ist so für das Aufnehmen eines Identifikationscodes in ein Bereichsprofil keine Lesevorrichtung bei der Rechnereinheit nötig, was den Betrieb des Zutrittskontrollsystems einfach und kostengünstig gestaltet.

[0014] Vorteilhafterweise wird ein provisorischer Identifikationscode durch Angabe einer Ziffernfolge in einem freigegebenen Bereichsprofil angelegt; und falls von der Lesevorrichtung des Türbeschlags, der Zutritt zu dem gesicherten Bereich des freigegebenen Bereichprofils gewährt, eine Ziffernfolge eingelesen wird, die mit der Ziffernfolge des provisorischen Identifikationscodes übereinstimmt, ein mit der Ziffernfolge eingelesener Identifikationscode in das freigegebene Bereichsprofil als gültiger Identifikationscode aufgenommen wird.

[0015] Dies hat den Vorteil, dass von der Rechnereinrichtung nicht ein vollständiger Identifikationscode in das freigegebene Bereichsprofil aufgenommen werden muss, sondern dass es reicht Teile des Identifikationscodes, beispielsweise die ersten zwei oder drei Ziffern des Identifikationscodes in das freigegebene Bereichsprofil aufzunehmen. Auch kann es reichen, Angaben des Bereichsprofils, beispielsweise einen Namen oder einen Vornamen in das freigegebene Bereichsprofil aufzunehmen und beim Einlesen dieser Angaben den mit mit diesen Angaben eingelesenen Identifikationscode in das Bererichsprofil als gültigen Identifikationscode aufzunehmen. Dies gestaltet den Betrieb des Zutrittskontrollsystems einfach und flexibel.

[0016] Vorteilhafterweise wird ein provisorischer Identifikationscode durch Angabe einer Zeitdauer in einem freigegebenen Bereichsprofil angelegt; und falls innerhalb der Zeitdauer von der Lesevorrichtung des Türbeschlags, der Zutritt zu dem gesicherten Bereich des freigegebenen Bereichsprofils gewährt, ein Identifikationscode eingelesen wird, der mit dem provisorischen Identifikationscode übereinstimmt, der eingelesene Identifikationscode in das freigegebene Bereichsprofil als gültiger Identifikationscode aufgenommen wird.

[0017] Dies hat den Vorteil, dass von der Rechnereinrichtung gar kein Identifikationscode in das freigegebene Bereichsprofil aufgenommen werden muss, sondern dass beispielsweise der zeitlich nächste eingelesene Identifikationscode in das Bereichsprofil als gültiger Identifikationscode aufgenommen wird, was den Betrieb des Zutrittskontrollsystems einfach und flexibel gestaltet.

[0018] Vorteilhafterweise wird von der Zentralrechnereinheit zumindest ein Teil eines Bereichsprofil für den von einem Türbeschlag gesicherten Bereich über eine kommunikative Verbindung an den Türbeschlag übermittelt; von einem Prozessor eines Türbeschlags wird überprüft, ob ein von der Lesevorrichtung des Türbeschlags eingelesener Identifikationscode mit einem gültigen Identifikationscode des übermittelten Bereichsprofils für den von dem Türbeschlag gesicherten Bereich übereinstimmt. Vorteilhafterweise ist das Bereichsprofil zumindest teilweise in einem computerlesbaren Datenspeicher der Zentralrechnereinheit gespeichert. Vorteilhafterweise ist das Bereichsprofil zumindest teilweise in einem computerlesbaren Datenspeicher des Türbeschlags gespeichert. Vorteilhafterweise wird von der Zentralrechnereinheit zumindest ein Teil eines Bereichsprofil für den von einem Türbeschlag gesicherten Bereich über eine kommunikative Verbindung an den Türbeschlag übermittelt; von einem Prozessor eines Türbeschlags wird überprüft, ob ein von der Lesevorrichtung des Türbeschlags eingelesener Identifikationscode mit einem gültigen Identifikationscode des übermittelten Bereichsprofils für den von dem Türbeschlag gesicherten Bereich übereinstimmt; bei erfolgreicher Überprüfung des eingelesenen Identifikationscodes wird von dem Prozessor ein Zutrittssignal an einen Aktuator des Türbeschlags übermittelt; und vom Aktuator wird für das übermittelte Zutrittssignal Zutritt zu dem vom Türbeschlag gesicherten Bereich gewährt. Dies hat den Vorteil, dass ein Prozessor eines Türbeschlags vor Ort überprüft, ob ein von der Lesevorrichtung des Türbeschlags eingelesener Identifikationscode mit einem gültigen Identifikationscode des Bereichsprofils für den von dem Türbeschlag gesicherten Bereich übereinstimmt, was den Betrieb des Zutrittskontrollsystems rasch gestaltet, da keine zeitaufwändigen Anfragen des Türbeschlags bei der vom Türbeschlag entfernten Zentralrechnereinheit für die Zwecke der Überprüfung nötig sind. Die Kommunikation des Bereichsprofils für den vom Türbeschlag gesicherten Bereich an die Lesevorrichtung kann in regelmässigen und/oder unregelmässigen Zeitabständen, beispielsweise bei Bedarf einer Aktualisierung des im computerlesbaren Datenspeicher des Türbeschlags gespeicherten Bereichsprofils erfolgen. Auch muss nicht das gesamte Bereichsprofil übermittelt werden, sondern es reicht aus, einen Teil des Bereichsprofils zu übermitteln, was die Übertragungszeit reduziert. Beispielsweise wird nur ein geänderter Teil des Bereichsprofils übermittelt.

[0019] Vorteilhafterweise wird ein von einer Lesevorrichtung eingelesener Identifikationscode über eine kommunikative Verbindung an die Zentralrechnereinheit übermittelt. Vorteilhafterweise wird von der Zentralrechnereinheit überprüft, ob ein von einer Lesevorrichtung eines Türbeschlags eingelesener Identifikationscode mit einem gültigen Identifikationscode eines Bereichsprofils für den vom Türbeschlag der Lesevorrichtung gesicherten Bereich übereinstimmt. Vorteilhafterweise wird bei erfolgreicher Überprüfung des eingelesenen Identifikationscodes von der Zentralrechnereinheit ein Zutrittssignal über die kommunikative Verbindung an einen Aktuator des Türbeschlags übermittelt; und vom Aktuator wird für das übermittelte Zutrittssignal Zutritt zu dem vom Türbeschlag gesicherten Bereich gewährt.

[0020] Dies hat den Vorteil, dass die entfernte Zentralrechnereinheit überprüft, ob ein von der Lesevorrichtung eingelesener Identifikationscode mit einem gültigen Identifikationscode des Bereichsprofils für den vom Tür-

beschlag der Lesevorrichtung gesicherten Bereich übereinstimmt, was den Betrieb des Zutrittskontrollsystems sicher gestaltet.

[0021] Vorteilhafterweise wird von der Zentralrechnereinheit ein übermittelter Berechtigungscode über eine kommunikative Verbindung an eine Gebäuderechnereinheit übermittelt; von der Gebäuderechnereinheit wird überprüft, ob der übermittelte Berechtigungscode mit einem gültigen Berechtigungscode für ein Bereichsprofil übereinstimmt; und bei erfolgreicher Überprüfung des übermittelten Berechtigungscodes wird von der Gebäuderechnereinheit ein Berechtigungssignal über eine kommunikative Verbindung an die Zentralrechnereinheit übermittelt. Vorteilhafterweise werden von der Zentralrechnereinheit für ein übermitteltes Berechtigungssignal Schreib- und Leserechte für das Bereichsprofil an die den Berechtigungscode übermittelnde Rechnereinheit freigegeben.

[0022] Dies hat den Vorteil, dass eine Gebäuderechnereinheit als weitere Instanz die Überprüfung des übermittelten Berechtigungscodes durchführt. Die Kommunikation des übermittelten Berechtigungscodes von der Zentralrechnereinheit an die Gebäuderechnereinheit und die Übermittlung des Berechtigungssignal zurück an die Zentralrechnereinheit erfolgt über eine kommunikative Verbindung, was den Betrieb des Zutrittskontrollsystems sicher gestaltet.

[0023] Vorteilhafterweise werden bei erfolgreicher Überprüfung des übermittelten Berechtigungscodes von der Zentralrechnereinheit Schreib- und Leserechte für das Bereichsprofil an die den Berechtigungscode übermittelnden Rechnereinheit freigegeben.

[0024] Dies hat den Vorteil, dass die entfernte Zentralrechnereinheit bei erfolgreicher Überprüfung des übermittelten Berechtigungscodes Schreib- und Leserechte für das Bereichsprofil an die den Berechtigungscode übermittelnden Rechnereinheit freigibt, was den Betrieb des Zutrittskontrollsystems sicher gestaltet.

[0025] Vorteilhafterweise umfasst das Zutrittskontrollsystem zur Durchführung des Verfahrens die Rechnereinheit. Vorteilhafterweise umfasst das Zutrittskontrollsystem die Zentralrechnereinheit. Vorteilhafterweise umfasst das Zutrittskontrollsystem eine Gebäuderechnereinheit. Vorteilhafterweise umfasst das Zutrittskontrollsystem eine netzwerkgestützte kommunikative Verbindung zwischen der Rechnereinheit und der Zentralrechnereinheit. Vorteilhafterweise umfasst das Zutrittskontrollsystem eine netzwerkgestützte kommunikative Verbindung zwischen der Zentralrechnereinheit und dem Türbeschlag. Vorteilhafterweise umfasst das Zutrittskontrollsystem ein Einlesen des Identifikationscode des mobilen Datenträgers über eine Datenübermittlung durch die Lesevorrichtung. Vorteilhafterweise umfasst das Zutrittskontrollsystem eine netzwerkgestützte kommunikative Verbindung zwischen der Zentralrechnereinheit und einer Gebäuderechnereinheit.

[0026] Dies hat den Vorteil, dass eine einfache und sichere kommunikative Verbindung zwischen der Rechnereinheit und der Zentralrechnereinheit, eine einfache und sichere kommunikative Verbindung zwischen der Zentralrechnereinheit und dem Türbeschlag, eine einfache und sichere Datenübermittlung vom mobilen Datenträger zum Türbeschlag, sowie eine einfache und sichere kommunikative Verbindung zwischen der Zentralrechnereinheit und der Gebäuderechnereinheit erfolgt.

[0027] Vorteilhafterweise ist der Türbeschlag auf einem Türblatt einer Tür zum vom Türbeschlag gesicherten Bereich angeordnet. Vorteilhafterweise ist die Lesevorrichtung in einer Türgarnitur des Türbeschlags angeordnet. Vorteilhafterweise ist ein Prozessor in einer Türgarnitur des Türbeschlags angeordnet. Vorteilhafterweise ist ein computerlesbarer Datenspeicher in einer Türgarnitur des Türbeschlags angeordnet. Vorteilhafterweise ist eine Sende- und Empfangseinheit für eine netzwerkgestützte kommunikative Verbindung zwischen der Zentralrechnereinheit und dem Türbeschlag in einer Türgarnitur des Türbeschlags angeordnet. Vorteilhafterweise ist eine elektrische Stromversorgung in einer Türgarnitur des Türbeschlags angeordnet.

[0028] Dies hat den Vorteil, dass das Türbeschlag sowie seine Bestandteile kompakt und vandalensicher angeordnet sind. Vorteilhafterweise ist die Rechnereinheit im vom Türbeschlag gesicherten Bereich angeordnet.

[0029] Dies hat den Vorteil, dass von einem gesicherten Bereich des Gebäudes aus, ein Identifikationscode eines mobilen Datenträgers in das Bereichsprofil für einen gesicherten Bereich des Gebäudes aufgenommen und/oder entfernt werden kann, was den Betrieb des Zutrittskontrollsystems einfach, flexibel und sicher gestaltet.

[0030] Vorteilhafterweise umfasst ein Computerprogrammprodukt mindestens ein Computerprogramm-Mittel, das geeignet ist, das Verfahren zum Betreiben eines Zutrittskontrollsystems dadurch zu realisieren, dass mindestens ein Verfahrensschritt ausgeführt wird, wenn das Computerprogramm-Mittel in mindestens einen Prozessor des Türbeschlags und/oder in mindestens einen Prozessor der Rechnereinheit und/oder in mindestens einen Prozessor der Zentralrechnereinheit und/oder in mindestens einen Prozessor der Gebäuderechnereinheit geladen wird. Vorteilhafterweise umfasst ein computerlesbarer Datenspeicher ein solches Computerprogrammprodukt.

[0031] Anhand der **Figuren** werden Ausführungsbeispiele der Erfindung im Detail erläutert.

Fig. 1 zeigt eine schematische Darstellung des Verfahrens zum Betreiben eines Zutrittskontrollsystems;

Fig. 2 zeigt eine schematische Ansicht eines Teils eines Türbeschlags eines Zutrittskontrollsystems gemäss Fig. 1;

Fig. 3 zeigt ein Flussdiagramm mit Schritten eines erstes Ausführungsbeispiels des Verfahrens

gemäss Fig. 1; und

Fig. 4 zeigt ein Flussdiagramm mit Schritten eines zweiten Ausführungsbeispiels des Verfahrens gemäss Fig. 1;

Fig. 5 zeigt ein Flussdiagramm mit Schritten eines dritten Ausführungsbeispiels des Verfahrens gemäss Fig. 1;

Fig. 6 zeigt ein Flussdiagramm mit Schritten eines vierten Ausführungsbeispiels des Verfahrens gemäss Fig. 1;

Fig. 7 zeigt ein Flussdiagramm mit Schritten eines fünften Ausführungsbeispiels des Verfahrens gemäss Fig. 1; und

Fig. 8 zeigt ein Flussdiagramm mit Schritten eines sechsten Ausführungsbeispiels des Verfahrens gemäss Fig. 1.

[0032] Fig. 1 zeigt eine schematische Darstellung des Verfahrens zum Betreiben eines Zutrittskontrollsystems in einem **Gebäude.** Im Sinne der vorliegenden Erfindung ist der Begriff Gebäude weit auszulegen. Ein Gebäude weist mindestens einen gesicherten Bereich auf. Die Tür 5 ermöglicht Zutritt zu diesem gesicherten Bereich des Gebäudes. Der gesicherte Bereich kann ein Raum, ein Gang, ein Treppenhaus, ein Aufzug, ein Trakt, eine Halle, eine Garage, ein Lichthof, ein Garten, eine Wohnung, ein Büro, eine Praxis, ein Hotelzimmer, ein Labor, eine Zelle, usw. des Gebäudes sein.

[0033] Die **Tür 5** weist gemäss Fig. 1 mindestens ein Türblatt 51, mindestens einen Türbeschlag 1, mindestens einen Türrahmen 52 und mindestens eine Türschwelle 53 auf. Der Türrahmen 52 ist fest und stabil im Mauerwerk des Gebäudes verankert. Die Tür 5 kann geöffnet und geschlossen werden. Zutritt zum gesicherten Bereich des Gebäudes erfolgt bei geöffneter Tür 5 durch Überschreiten der Türschwelle 52. Bei geschlossener Tür 5 erfolgt kein Zutritt zum gesicherten Bereich des Gebäudes.

[0034] Der **Türbeschlag 1** weist gemäss Fig. 2 mindestens eine Türgarnitur 11 mit mindestens einem Riegel 16 und mindestens einer Klinke 17 auf. Die Türgarnitur 11 weist einen Innenbeschlag und einen Aussenbeschlag auf. Zwischen dem Innenbeschlag und dem Aussenbeschlag bildet die Türgarnitur einen Hohlraum. Der Innenbeschlag ist auf der Seite der Tür 5 zum Inneren des Gebäudes bzw. zum Inneren des gesicherten Bereichs des Gebäudes angeordnet. Sowohl am Innenbeschlag als auch beim Aussenbeschlag kann eine Klinke 17 angeordnet sein. Der Aussenbeschlag ist auf der Seite der Tür 5 zum Äusseren des Gebäudes bzw. zum Äusseren des gesicherten Bereichs des Gebäudes angeordnet. Die Türgarnitur 11 ist zum Schutz gegen Sabotage zumindest bereichsweise widerstandsfest und aus gehärtetem Edelstahl, Federstahl, usw. gefertigt. Bei geschlossener Tür 5 ist der Riegel 16 in mindestens ein Schliessblech 54 des Türrahmens 52 eingerastet. Bei geöffneter Tür 5 ist der Riegel 16 nicht im Schliessblech 54 des Türrahmens 52 eingerastet. Der Riegel 16 kann durch Drücken der Klinke 17 betätigt werden. Riegel 16 und Klinke 17 sind über eine Kupplung 15 kraftschlüssig miteinander gekoppelt. Die Kupplung 15 ist durch Bewegung mindestens eines Kupplungshebels aktivierbar bzw. deaktivierbar. Bei aktivierter Kupplung 15 wird ein Betätigen der Klinke 17 auf den Riegel 16 übertragen. Bei deaktivierter Kupplung 15 wird kein Betätigen der Klinke 17 auf den Riegel 16 übertragen. In diesem Fall sind Klinke 17 und Riegel 16 entkoppelt und die geschlossene Tür 5 ist durch Betätigen der Klinke 17 nicht zu öffnen. Mindestens ein Aktuator 18 kann den Kupplungshebel bewegen und die Kupplung 15 aktiveren bzw. deaktivieren. Der Aktuator 18 ist beispielsweise ein Elektromotor, der von mindestens einer elektrischen Stromversorgung 19 mit elektrischem Strom versorgt wird und den Kupplungshebel bewegt. Der Aktuator 18 wird durch mindestens ein Zutrittssignal angesteuert. Bei Nichtvorliegen eines Zutrittssignals ist die Kupplung 15 deaktiviert, bei Vorliegen eines Zutrittssignals ist die Kupplung 15 aktiviert. Die Aktivierung der Kupplung 15 ist vorteilhafterweise zeitlich auf einige Sekunden, beispielsweise fünf Sekunden, usw. begrenzt, derart, dass der Aktuator 18 die Kupplung 15 nach Ablauf dieser Zeitdauer automatisch deaktiviert. Eine solche kurze Zeitdauer ist aber nicht zwingend. Der Fachmann kann bei Kenntnis der vorliegenden Erfindung die Kupplung 15 auch für beliebige längere Zeitdauern aktiviert lassen. Die elektrischen Stromversorgung 19 ist ebenfalls im Hohlraum der Türgarnitur 15 angeordnet und besteht aus einer Batterie bzw. einem Akkumulator bzw. einer Brennstoffzelle bzw. einer Solarzelle mit einer energetischen Autonomie von einem Jahr, vorzugsweise zwei Jahren. Auf dem Türbeschlag 1 kann auch mindestens eine Leuchte wie eine Light Emitting Diode (LED), eine Organic Light Emitting Diode (OLED), usw. angeordnet sein. Beispielsweise ist eine bunte LED angeordnet, die in verschiedenen Farben wie grün, rot, gelb, blau, usw. leuchten kann. Beispielsweise sind mehrere LED angeordnet, die in verschiedenen Farben wie grün, rot, gelb, blau, usw. leuchten können. Auf dem Türbeschlag 1 kann auch mindestens ein Lautprecher angeordnet sein, der mindestens einen Ton ausgeben kann. Das Leuchten der Leuchte und/oder der Ton des Lautsprechers ist/sind von einer Person im Bereich der Tür wahrnehmbar und kann/können mindestens eine Statusinformation wiedergeben. Beispielsweise wird bei Vorliegen eines Zutrittssignals die Leuchte zu einem grünen Blinken aktiviert; beispielsweise wird bei Vorliegen eines Störrsignals die Leuchte zu einem roten Blinken. Beispielsweise wird bei Vorliegen eines Zutrittssignals der Lautsprecher zu einem 500Hz Ton aktiviert; Beispielsweise wird bei Vorliegen eines Störrsignals der Lautsprecher zu einem 1000Hz Ton aktiviert.

[0035] Mindestens eine **Lesevorrichtung 10** ist in der

Türgarnitur 11 angeordnet und wird von der elektrischen Stromversorgung 17 mit elektrischem Strom versorgt. Die Lesevorrichtung 10 weist mindestens eine Antenne für Radiofrequenzen, einen magnetischen Durchzugleser, einen elektronischen Durchzugleser, einen biometrischer Sensor, usw. für eine Datenübermittlung 21 von mindestens einem **mobilen Datenträger 2** auf. Im Folgenden werden Ausführungsbeispiele des mobilen Datenträgers 2 erläutert:

- Die Datenübermittlung 21 basiert beispielsweise auf einer kontaktlosen Datenübermittlung 21 wie Radio Frequency Identification Device (**RFID** gemäss ISO11785). Die Radiofrequenzen liegen beispielsweise in Bändern bei 125kHz, 13.6MHz, usw.. Der mobile Datenträger 2 ist ein RFID mit mindestens einer elektrischen Spule und mindestens einem computerlesbaren Datenspeicher, in dem mindestens ein Identifikationscode gespeichert ist. Das RFID weist keine eigene elektrische Stromversorgung auf. Das RFID hat beispielsweise die Form einer Kreditkarte oder ist in einem Schlüsselanhänger integriert. Die Antenne der Lesevorrichtung 10 sendet Radiofrequenzen aus. Die Reichweite der Antenne beträgt einige Zentimeter. Sobald das RFID in der Reichweite der Radiofrequenzverbindung 21 gelangt, wird das RFID über die elektrische Spule durch die Radiofrequenzen energetisch aktiviert und der im computerlesbaren Datenspeicher gespeicherte Identifikationscode des RFID über die elektrische Spule des RFID an die Antenne der Lesevorrichtung 10 gesendet.

- Die Datenübermittlung 21 basiert beispielsweise auf einer kontaktlosen Datenübermittlung 21 wie **Bluetooth** (IEEE802.15.1), **ZigBee** (IEEE802.15.4), **WiFi** (IEEE802.11), usw.. Die Radiofrequenzen liegen beispielsweise in Bändern bei 800 bis 900MHz, 1800 bis 1900MHz, 1.7 bis 2.7GHz, usw.. Die Reichweite der Antenne variiert von einigen Metern bei Bluetooth und ZigBee, bis zu einigen hundert Metern bei WiFi. Der mobile Datenträger 2 ist ein mobiles Gerät wie ein Mobiltelefon, Personal Digital Assistant (PDA), usw. mit mindestens einer Antenne, mindestens einem Prozessor, mindestens einem computerlesbaren Datenspeicher und einer eigenen elektrischen Stromversorgung. Die Antenne der Lesevorrichtung 10 sendet Radiofrequenzen mit Anfragesignalen aus. Sobald das mobile Gerät in der Reichweite der Radiofrequenzverbindung 21 gelangt und ein Anfragesignal der Lesevorrichtung 10 empfängt, sendet die Antenne des mobilen Geräts ein Antwortsignal an die Antenne der Lesevorrichtung 10. Der im computerlesbaren Datenspeicher des mobilen Geräts gespeicherte Identifikationscode wird über die Antenne des mobilen Geräts an die Antenne der Lesevorrichtung 10 gesendet.

- Die Datenübermittlung 21 kann aber auch auf einem kontaktbehafteten Einlesen eines **Magnetstreifens** und/oder eines **elektronischen Datenspeichers** basieren. In diesem Fall ist der mobile Datenträger 2 eine Karte mit einem Magnetstreifen und/oder einem elektronischen Datenspeicher. Der Magnetstreifen und/oder der elektronische Datenspeicher wird von einem magnetischen Durchzugleser oder einem elektronischen Durchzugleser der Lesevorrichtung 10 gelesen.

- Auch kann die Datenübermittlung 21 auf dem Lesen eines **biometrischen Signals** durch einen biometrischen Sensor basieren. In diesem Fall ist der mobile Datenträger 2 eine Fingerkuppe einer Person, eine Hand einer Person, ein Gesicht einer Person, eine Iris einer Person, ein Körper einer Person, ein Geruch einer Person, usw., der von einem biometrischen Sensor der Lesevorrichtung 10 als Fingerabdruck, Handgeometrie, Gesichtsprofil, Irisprofil, Netzhautscan, Thermogramm, Geruch, Gewicht, Stimme, Unterschrift, usw. gelesen wird.

[0036] Mindestens eine **Sende- und Empfangseinheit 12,** mindestens ein **Prozessor 13** und mindestens ein **computerlesbarer Datenspeicher 14** sind in der Türgarnitur 11 angeordnet und werden von der elektrischen Stromversorgung 17 mit elektrischem Strom versorgt. Die Sende- und Empfangseinheit 12 realisiert mindestens eine netzwerkgestützte kommunikative Verbindung 41 zwischen dem Türbeschlag 1 und mindestens einer Zentralrechnereinheit 4. Die Sende- und Empfangseinheit 12, der Prozessor 13 und der computerlesbare Datenspeicher 14 sind auf mindestens einer Platine angeordnet und über mindestens eine Signalleitung miteinander verbunden. Aus dem computerlesbaren Datenspeicher 14 wird mindestens ein Computerprogramm-Mittel in den Prozessor 13 geladen und ausgeführt. Das Computerprogramm-Mittel steuert die Kommunikation zwischen der Sende- und Empfangseinheit 12, dem Prozessor 13 und dem computerlesbare Datenspeicher 14. Das Computerprogramm-Mittel steuert auch die kommunikative Verbindung 41.

[0037] Mindestens eine **Zentralrechnereinheit 4** weist mindestens eine **Sende- und Empfangseinheit 42,** mindestens einen **Prozessor 43** und mindestens einen **computerlesbaren Datenspeicher 44** auf. Die Sende- und Empfangseinheit 42 realisiert mindestens eine netzwerkgestützte kommunikative Verbindung 41 zwischen der Zentralrechnereinheit 4 und mindestens einem Türbeschlag 1 und/oder mindestens eine netzwerkgestützte kommunikative Verbindung 31, 31' zwischen der Zentralrechnereinheit 4 und mindestens einer Rechnereinheit 3. Aus dem computerlesbaren Datenspeicher 44 wird mindestens ein Computerprogramm-Mittel in den Prozessor 43 geladen und ausgeführt. Das Computerprogramm-Mittel steuert die Kommunikation zwischen der Sende- und Empfangseinheit 42, dem Prozessor 43

und dem computerlesbare Datenspeicher 44. Das Computerprogramm-Mittel steuert auch die kommunikative Verbindung 31, 31', 41, 41'. Die Zentralrechnereinheit 4 kann ein Mikrocomputer wie eine Workstation, Personal Computer (PC), usw. sein. Die Zentralrechnereinheit 4 kann aus einem hierarchischen Verbund mehrerer Mikrocomputer bestehen. Die Zentralrechnereinheit 4 kann im Gebäude und/oder entfernt vom Gebäude angeordnet sein. In einer Ausführungsform können der Prozessor 43 und ein erster computerlesbarer Datenspeicher 44 in einer Zentrale zur Wartung des Zutrittkontrollsystems angeordnet sein, während ein weiterer computerlesbarer Datenspeicher 44 im Gebäude des Zutrittkontrollsystems angeordnet ist.

[0038] Mindestens eine **Rechnereinheit 3** weist mindestens eine Sende- und Empfangseinheit 32, mindestens einen Prozessor 33 und mindestens einen computerlesbaren Datenspeicher 34 auf. Die Sende- und Empfangseinheit 32 realisiert mindestens eine netzwerkgestützte kommunikative Verbindung 41, 41' zwischen der Rechnereinheit 3 und mindestens einer Zentralrechnereinheit 4. Aus dem computerlesbaren Datenspeicher 34 wird mindestens ein Computerprogramm-Mittel in den Prozessor 33 geladen und ausgeführt. Das Computerprogramm-Mittel steuert die Kommunikation zwischen der Sende- und Empfangseinheit 32, dem Prozessor 33 und dem computerlesbare Datenspeicher 34. Die Rechnereinheit 3 kann ein mobiler Mikrocomputer wie ein PC, Notebook, Netbook, Mobiltelefon, PDA, usw. sein. Das Computerprogramm-Mittel steuert auch die kommunikative Verbindung 41. Von der Rechnereinheit 3 aus kann somit über ein Computerprogramm-Mittel eine netzwerkgestützte kommunikative Verbindung 41, 41' zwischen der Rechnereinheit 3 und der Zentralrechnereinheit 4 aufgebaut, aufrechterhalten und wieder beendet werden. Das Computerprogramm-Mittel kann ein Computerprogramm zum Betrachten von computergestützten Seiten des World Wide Web sein. Solche Webbrowser sind unter den Namen Internet Explorer, Firefox, Opera, usw. bekannt. Die Rechnereinheit 3 kann im Gebäude und/oder entfernt vom Gebäude angeordnet sein.

[0039] Mindestens eine **Gebäuderechnereinheit 6** weist mindestens eine **Sende- und Empfangseinheit 62,** mindestens einen **Prozessor 63** und mindestens einen **computerlesbaren Datenspeicher 64** auf. Die Sende- und Empfangseinheit 62 realisiert mindestens eine netzwerkgestützte kommunikative Verbindung 61, 61' zwischen der Gebäuderechnereinheit 6 und der Zentralrechnereinheit 4. Aus dem computerlesbaren Datenspeicher 64 wird mindestens ein Computerprogramm-Mittel in den Prozessor 63 geladen und ausgeführt. Das Computerprogramm-Mittel steuert die Kommunikation zwischen der Sende- und Empfangseinheit 62, dem Prozessor 63 und dem computerlesbare Datenspeicher 64. Das Computerprogramm-Mittel steuert auch die kommunikative Verbindung 61, 61'. Die Gebäuderechnereinheit 6 kann ein Mikrocomputer wie eine Workstation, Personal Computer (PC), usw. sein. Die Gebäuderechnereinheit 6 kann aus einem hierarchischen Verbund mehrerer Mikrocomputer bestehen. Die Gebäuderechnereinheit 6 kann im Gebäude und/oder entfernt vom Gebäude angeordnet sein.

[0040] Im Folgenden werden Ausführungsbeispiele der kommunikativen Verbindung 31, 31', 41, 41', 61, 61' erläutert:

- Die kommunikativen Verbindung 31, 31', 41, 41', 61, 61' kann ein **Netzwerk** wie Ethernet, ARCNET, usw. mit mindestens einer elektrischen- bzw. optischen Signalleitung sein. Das Netzwerk erlaubt eine bidirektionale Kommunikation gemäss bekannten und bewährten Netzwerk-Protokollen wie das Transmission Control Protocol / Internet-Protocol (TCP/IP), Hypertext Transfer Protocol (HTML), Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP), Internet Packet Exchange (IPX), usw.. Die Teilnehmer im Netzwerk sind über Netzwerkadressen eindeutig adressierbar. Zur Erhöhung der Sicherheit bei der kommunikative Verbindung 31, 31', 41, 41', 61, 61' erfolgt die Übermittlung von sicherheitsrelevanten Daten in verschlüsselter Form über eine verschlüsselte kommunikative Verbindung 31', 41', 61'. Bekannte Verschlüsselungsprotokolle sind das Secure Sockets Layer (SSL), Secure Multipurpose Internet Mail Extensions (S/MIME), usw.. Das Verschlüsselungsprotokoll ist im Open Systems Interconnection (OSI) Referenzmodell oberhalb der TCP Transportschicht und unterhalb von Anwendungsprogrammen wie HTML oder SMTP platziert. Mit 31, 41, 61 wird eine unverschlüsselte kommunikative Verbindung bezeichnet.

- Die kommunikative Verbindung 31, 41, 61 kann ein **Telefon-Funknetz** wie Global Systems for Mobile Communications (GSM), General Radio Packet Services (GPRS), Enhanced Data Rate for GSM Evolution (EDGE), Universal Mobile Telecommunications System (UMTS), High Speed Download Packet Access (HSDPA), usw. sein. Die vom Telefon-Funknetz verwendeten Frequenzen liegen bei GSM und GPRS in Bändern bei 800 bis 900MHz und 1800 bis 1900MHz, sowie bei UMTS und HSDPA bei 700 bis 900MHz und 1.7 bis 2.7GHz.

- Die kommunikative Verbindung 31, 41, 61 kann ein **Telefon-Festnetz** wie Public Switched Telecommunication Network (PSTN) sein. Das Telefon-Festnetz kann analog und/oder digital ausgestaltet sein. Bei einem analogen Telefon-Festnetz werden analoge Tonsignale übermittelt. Die Bandbreite ist dabei auf den Frequenzbereich von 300 bis 3400Hz begrenzt. Neben einem Sprachsignal werden weitere Signale wie ein Wählsignal, ein Rufsignal, usw. übermittelt. Ein digitales Telefon-Festnetz ist als Integrated Services Digital Network (ISDN), Asymetric Digital Subscriber Line (ADSL), Very High Data Rate Digital

Subscriber Line (VDSL), usw. bekannt. Beim ADSL wird ein wesentlich grösserer Frequenzbereich von 200Hz bis 1.1MHz ausgenutzt.

[0041] Bei Kenntnis der vorliegenden Erfindung kann der Fachmann auch die kommunikative Verbindung 31, 41, 61 über ein Telefon-Funknetz und/oder ein Telefon-Festnetz in verschlüsselter Form realisieren.

[0042] Das Zutrittskontrollsystem betreibt den Zutritt zu einem gesicherten Bereich des Gebäudes über mindestens ein **Bereichsprofil.** Das Bereichsprofil ist beispielsweise eine computerlesbare Datei und kann zumindest teilweise in einem computerlesbaren Datenspeicher 14 des Türbeschlags 1 und/oder in einem computerlesbaren Datenspeicher 44 der Zentralrechnereinheit 4 gespeichert sein. Ein Bereichsprofil bezieht sich auf einen gesicherten Bereich des Gebäudes und umfasst mindestens eine Entität und für diese Entität umfasst das Bereichsprofil verschiedene Angaben wie Name, Vorname, Identifikationscode, Leserecht, Schreibrecht, Historie, Zeitzone, Gültigkeit, usw..

- Mit Entität wird mindestens eine Person und/oder sachlicher Gegenstand bezeichnet, welche Entität für diesen Identifikationscode Zutritt zu diesem gesicherten Bereich des Gebäudes hat. Die Person kann ein Mensch oder ein Tier sein. Der sachliche Gegenstand kann ein Fahrzeug, eine Pallette, ein Container, ein Roboter, usw. sein.

- Mit Name und Vorname werden der Name und Vorname der Entität bezeichnet. Bei einer Person werden der Name und der Vorname der Person angegeben, wie sie in offiziellen Dokumenten wie einem Personalausweis, Reiseausweis, usw. dieser Person angegeben sind.

- Der Identifikationscode besteht beispielsweise aus mindestens einer Ziffernfolge, die verschlüsselt oder unverschlüsselt sein kann, mit der sich die Entität identifizieren muss, um Zutritt zu diesem gesicherten Bereich des Gebäudes zu erhalten. Die Ziffernfolge kann numerisch, alphanumerisch, usw. sein. Der Identifikationscode kann auch mindestens eine eigenständige Datei sein, die verschlüsselt oder unverschlüsselt sein kann. Der Identifikationscode kann auch mindestens ein biometrisches Signal der Entität sein, das als eigenständige Datei verschlüsselt oder unverschlüsselt sein kann.

- Mit Leserecht wird eine Berechtigung der Entität verstanden, den Inhalt des Bereichsprofils zu lesen. Mit Schreibrecht wird eine Berechtigung der Entität verstanden, den Inhalt des Bereichsprofils zu lesen und zu verändern.

- Mit Historie werden gespeicherte Zutritte und/oder Austritte der Entität zu diesem gesicherten Bereich des Gebäudes bezeichnet. Beispielsweise umfasst die Historie das Datum und die Uhrzeit eines jeden Zutritts zu diesem gesicherten Bereich des Gebäudes sowie das Datum und die Uhrzeit eines jeden Austritts aus diesem gesicherten Bereich des Gebäudes.

- Mit Zeitzone wird eine zeitliche Begrenzung des Zutritts der Entität zu diesem gesicherten Bereich des Gebäudes bezeichnet. Die Zeitzone kann nur bestimmte Stunden einer Woche umfassen, beispielsweise für eine Entität die diesen gesicherten Bereich des Gebäudes Wochentags zwischen 20Uhr und 21Uhr reinigen soll. Die Zeitzone kann aber auch unbegrenzt sein, beispielsweise für eine Person, die in diesen gesicherten Bereich des Gebäudes permanent wohnt. Eine Zeitzone kann sich beliebig oft wiederholen, sie kann aber auch nur einmal dauern. Beispielsweise übernachtet eine Person eine einzige Nacht in einem Hotelzimmer als gesicherten Bereich des Gebäudes. Für diese Person beginnt die Zeitzone dann um zwölf Uhr mittags des ersten Tags und dauert ganze Nacht durch bis elf Uhr mittags des darauffolgenden Tages.

- Mit Gültigkeit wird angegeben, ob der Identifikationscode zu diesem gesicherten Bereich des Gebäudes zum jetzigen Zeitpunkt gültig ist. Falls ein Identifikationscode zu einem früheren Zeitpunkt gültig gewesen ist und zum jetzigen Zeitpunkt ungültig ist, kann diese frühere Gültigkeit mit einem Datum und einer Uhrzeit dieser Veränderung versehen sein.

[0043] Im Betrieb des Zutrittskontrollsystem werden die Angaben des **Bereichsprofils gewartet.** Im Folgenden werden dazu Ausführungsbeispiele erläutert:

- Der gesicherte Bereich des Gebäudes besteht beispielsweise aus mehreren Büros einer Firma, in denen wochentags mehrere Personen arbeiten. Für die Büros dieser Firma existieren mehrere Bereichsprofile, mit einem Bereichsprofil für jedes Büro. Wenn nun eine dieser Personen die Tätigkeit wechselt und nicht mehr im alten Büro, sondern in einem neuen Büro der Firma arbeitet, so müssen die Bereichsprofile für dieses alte Büro und für dieses neue Büro verändert werden. Im Bereichsprofil für das alte Büro werden entweder die Angaben zur Entität, zum Namen, zum Vornamen dieser Person entfernt oder im Bereichsprofil für das alte Büro wird die Angabe Gültigkeit für diese Person auf ungültig gesetzt oder im Bereichsprofil für das alte Büro wird die Angabe Zeitzone auf Null gesetzt, d.h. Zutritt wird zu keiner Zeit gewährt. Im Bereichsprofil für das neue Büro werden die Angaben zur Entität, zum Namen, zum Vornamen, zum Identifikationscode und zur Zeitzone für diese Person aufgenommen. Die Person hat weder ein Leserecht noch ein Schreibrecht am Be-

reichsprofil für das neue Büro.

- Der gesicherte Bereich des Gebäudes besteht beispielsweise aus einer Wohnung, in der eine Familie mit mehreren Personen permanent wohnt. Das Bereichsprofil für diese Wohnung umfasst nur Angaben zu den Personen der Familie. Wenn nun die Familie in die Ferien geht und die Wohnung für zwei Wochen verlässt, und der Nachbar in diesen zwei Wochen die Blumen in der Wohnung giessen soll, so muss das Bereichsprofil für diese Wohnung verändert werden. Im Bereichsprofil für diese Wohnung wird eine neue Entität für den Nachbarn aufgenommen, mit Angaben zum Namen, zum Vornamen, zum Identifikationscode und zur Zeitzone. Der Nachbar hat weder ein Leserecht noch ein Schreibrecht. Die Zeitzone beträgt zwei Wochen, solange wie die Ferien dauern.

[0044] Zur Wartung eines Bereichsprofils wird von der Rechnereinheit 3 aus mindestens ein **Berechtigungscode** an die Zentralrechnereinheit 4 übermittelt. Der Berechtigungscode besteht ähnlich wie der Identifikationscode aus mindestens einer Ziffernfolge, die verschlüsselt oder unverschlüsselt sein kann. Die Ziffernfolge kann numerisch, alphanumerisch, usw. sein. Auch kann der Berechtigungscode mindestens eine eigenständige Datei sein, die verschlüsselt oder unverschlüsselt ist. Der Berechtigungscode kann auch mindestens ein biometrisches Signal der Entität sein, das als eigenständige Datei verschlüsselt oder unverschlüsselt sein kann. Der Berechtigungscode kann mit dem Identifikationscode identisch sein. Der Berechtigungscode kann eine Adresse, beispielsweise eine Postadresse (E-Mail-Adresse) für eine Kommunikation gemäss SMTP, IMAP, usw. sein.

[0045] Es wird überprüft, ob der übermittelte Berechtigungscode mit einem gültigen Berechtigungscode für ein Bereichsprofil übereinstimmt. Jedes Bereichsprofil ist mit einem gültigen Berechtigungscode verknüpft. Der gültige Berechtigungscodes kann in der Zentralrechnereinheit 4 oder in der Gebäuderechnereinheit 6 gespeichert sein. Die Überprüfung kann durch die Zentralrechnereinheit 4 und/oder die Gebäuderechnereinheit 6 erfolgen. In einer vorteilhaften Ausgestaltung des Verfahrens wird der übermittelte Berechtigungscode von der Zentralrechnereinheit 4 über eine kommunikative Verbindung 61, 61' an die Gebäuderechnereinheit 6 übermittelt, welche Gebäuderechnereinheit 6 den übermittelte Berechtigungscode überprüft und bei erfolgreicher Überprüfung ein Berechtigungssignal über eine kommunikative Verbindung 61, 61' an die Zentralrechnereinheit 4 übermittelt.

[0046] Bei erfolgreicher Überprüfung des übermittelten Berechtigungscodes gibt die Zentralrechnereinheit 4 Schreib- und Leserechte für das Bereichsprofil, das mit dem übermittelten Berechtigungscode verknüpft ist, an die den Berechtigungscode übermittelnden Rechnereinheit 3 frei. Falls die Überprüfung des übermittelten Berechtigungscodes durch die Gebäuderechnereinheit 6 erfolgt ist, gibt die Zentralrechnereinheit 4 Schreib- und Leserechte für ein Bereichsprofil erst nach Übermittlung eines entsprechenden Berechtigungssignals frei. Für ein freigegebenes Bereichsprofil wird von der Zentralrechnereinheit 4 über die kommunikative Verbindung 31, 31' ein Freigabesignal an die Rechnereinheit 3 übermittelt. Von der Rechnereinheit 3 aus wird über die kommunikative Verbindung 31, 31' das freigegebene Bereichsprofil verändert. Dazu wird von der Rechnereinheit 3 mindestens ein Veränderungssignal über die kommunikative Verbindung 31, 31' an die Zentralrechnereinheit 4 übermittelt, welche Zentralrechnereinheit 4 für ein empfangenes Veränderungssignal eine Veränderung des Bereichsprofils umsetzt. Die Veränderung des Bereichsprofils kann ein Löschen, Hinzufügen, Abändern einer Angabe des Bereichsprofils wie Name, Vorname, Identifikationscode, Leserecht, Schreibrecht, Historie, Zeitzone, Gültigkeit, usw. umfassen.

[0047] Die Fig. 3 bis 8 zeigen **Flussdiagramme** von Schritten von Ausführungsbesipielen des Verfahrens zum Betreiben eines Zutrittkontrollsystems. Im Folgenden werden die einzelnen Schritte beschrieben:

- In einem **Schritt S1** wird gemäss Fig. 3 ein Bereichsprofil T1 mit einem gültigen Identifikationscode T2' in der Zentralrechnereinheit 4 gespeichert und liegt dort vor.

- In einem **Schritt S1** wird gemäss Fig. 4 und 5 ein Bereichsprofil T1 mit einem gültigen Identifikationscode T2' von der Zentralrechnereinheit 4 über eine kommunikative Verbindung 41, 41' an eine Netzwerkadresse des Türbeschlags 1 übermittelt, der Zutritt zu dem gesicherten Bereich gewährt, auf den sich das Bereichsprofil 1 bezieht. Der Schritt S1 kann bei Bedarf erfolgen, beispielsweise in regelmässigen Zeitabständen wie wöchenbtlich, monatlich, usw. und/oder bei erfolgter Veränderung des Bereichsprofils 1 des durch den Türbeschlag 1 gesicherten Bereichs. Die kommunikative Verbindung 41, 41' kann permanent aufrecht erhalten werden oder sie kann nur für die Belange der Übermittlung des Bereichsprofils T1 aufgebaut werden.

- In einem **Schritt S2** wird gemäss Fig. 3 bis 5 ein **Identifikationscode T2** eines mobilen Datenträgers 2 von einer Lesevorrichtung 10 des Türbeschlags 1 per Datenübermittlung 21 eingelesen.

- In einem **Schritt S3** wird gemäss Fig. 3 ein eingelesener Identifikationscode T2 vom Türbeschlag 1 über eine kommunikative Verbindung 41, 41' an die Netzwerkadresse der Zentralrechnereinheit 4 übermittelt.

- Gemäss Fig. 3 wird der eingelesene Identifikationscode T2 von der Zentralrechnereinheit 4 über die

kommunikative Verbindung 41, 41' empfangen. Gemäss Fig. 4 und 5 liegt der eingelesene Identifikationscode T2 im Türbeschlag 1 vor. In einem **Schritt S4** wird gemäss Fig. 3 von der Zentralrechnereinheit 4 überprüft, ob der eingelesene Identifikationscode T2 mit einem gültigen Identifikationscode T2' für den durch den Türbeschlag 1 gesicherten Bereich übereinstimmt, welcher gültige Identifikationscode im Bereichsprofil T1 gespeichert ist. Wenn der eingelesene Identifikationscode T2 mit dem gültigen Identifikationscode T2' übereinstimmt, wird von der Zentralrechnereinheit 4 ein **Zutrittssignal T4** erzeugt und über eine kommunikative Verbindung 41, 41' an die Netzwerkadresse des Türbeschlags 1 übermittelt, der den Identifikationscode T2 eingelesen und an die Zentralrechnereinheit 4 übermittelt hat. Wenn der eingelesene Identifikationscode T2 mit dem gültigen Identifikationscode T2' nicht übereinstimmt, wird von der Zentralrechnereinheit 4 ein **Sperrsignal T4'** erzeugt und über eine kommunikative Verbindung 41, 41' an die Netzwerkadresse des Türbeschlags 1 übermittelt, der den Identifikationscode T2 eingelesen und an die Zentralrechnereinheit 4 übermittelt hat.

- In einem **Schritt S4** wird gemäss Fig. 4 und 5 vom Türbeschlag 1 überprüft, ob der eingelesene Identifikationscode T2 mit einem gültigen Identifikationscode T2' für den durch den Türbeschlag 1 gesicherten Bereich übereinstimmt, welcher gültige Identifikationscode T2' im Bereichsprofil T1 gespeichert ist. Wenn der eingelesene Identifikationscode T2 mit dem gültigen Identifikationscode T2' übereinstimmt, wird vom Türbeschlag 1 ein **Zutrittssignal T4** erzeugt. Wenn der eingelesene Identifikationscode T2 mit dem gültigen Identifikationscode T2' nicht übereinstimmt, wird vom Türbeschlag 1 ein **Sperrsignal T4'** erzeugt. Gemäss Fig. 5 wird ein eingelesener Identifikationscode T2 und das für diesen ein eingelesenen Identifikationscode T2 erzeugte Sperrsignal T4' vom Türbeschlag 1 über eine kommunikative Verbindung 41, 41' an die Netzwerkadresse der Zentralrechnereinheit 4 übermittelt.

- Gemäss Fig. 5 werden ein eingelesener Identifikationscode T2 und ein für diesen Identifikationscode T2 erzeugtes Sperrsignal T4' von der Zentralrechnereinheit 4 über die kommunikative Verbindung 41, 41' empfangen. In einem **Schritt S4'** wird gemäss Fig. 5 von der Zentralrechnereinheit 4 überprüft, ob der eingelesene Identifikationscode T2 mit einem gültigen Identifikationscode T2' für den durch den Türbeschlag 1 gesicherten Bereich übereinstimmt, welcher gültige Identifikationscode T2' im Bereichsprofil T1 gespeichert ist. Wenn der eingelesene Identifikationscode T2 mit dem gültigen Identifikationscode T2' übereinstimmt, wird von der Zentralrechnereinheit 4 ein **Zutrittssignal T4"** erzeugt. Gemäss Fig. 5 werden ein eingelesener Identifikationscode T2 und das für diesen eingelesenen Identifikationscode T2 erzeugte Zutrittssignal T4'' von der Zentralrechnereinheit 4 über eine kommunikative Verbindung 41, 41' an die Netzwerkadresse des Türbeschlags 1 übermittelt, der den Identifikationscode T2 eingelesen und an die Zentralrechnereinheit 4 übermittelt hat. Wenn der eingelesene Identifikationscode T2 mit dem gültigen Identifikationscode T2' nicht übereinstimmt, wird von der Zentralrechnereinheit 4 ein **Sperrsignal T4"'** erzeugt. Gemäss Fig. 5 werden ein eingelesener Identifikationscode T2 und das für diesen eingelesenen Identifikationscode T2 erzeugte Sperrsignal T4''' von der Zentralrechnereinheit 4 über eine kommunikative Verbindung 41, 41' an die Netzwerkadresse des Türbeschlags 1 übermittelt, der den Identifikationscode T2 eingelesen und an die Zentralrechnereinheit 4 übermittelt hat.

- Gemäss Fig. 3 wird ein Zutrittssignal T4 vom Türbeschlag 1 über die kommunikative Verbindung 41, 41' empfangen. Gemäss Fig. 4 liegt ein Zutrittssignal T4 im Türbeschlag 1 vor. Gemäss Fig. 5 werden ein eingelesener Identifikationscode T2 und ein für diesen eingelesenen Identifikationscode T2 erzeugtes Zutrittssignal T4'' vom Türbeschlag 1 über die kommunikative Verbindung 41, 41' empfangen. In einem **Schritt S5** wird gemäss Fig. 3 bis 5 vom Türbeschlag 1 für ein vorliegendes Zutrittssignal T4 Zutritt zu dem vom Türbeschlag 1 gesicherten Bereich gewährt und/oder eine Zutrittsinformation beispielsweise in Form einer aktivierten Leuchte und/oder eines aktivierten Lautsprechers des Türbeschlags 1 ausgegeben.

- Gemäss Fig. 3 wird ein Sperrsignal T4' vom Türbeschlag 1 über die kommunikative Verbindung 41, 41' empfangen. Gemäss Fig. 4 liegt ein Sperrsignal T4' im Türbeschlag 1 vor. Gemäss Fig. 5 werden ein eingelesener Identifikationscode T2 und ein für diesen eingelesenen Identifikationscode T2 erzeugtes Sperrsignal T4"' vom Türbeschlag 1 über die kommunikative Verbindung 41, 41' empfangen. In einem **Schritt S5'** wird gemäss Fig. 3 bis 5 vom Türbeschlag 1 für ein vorliegendes Sperrsignal T4', T4"' kein Zutritt zu dem vom Türbeschlag 1 gesicherten Bereich gewährt und/oder eine Sperrinformation beispielsweise in Form einer aktivierten Leuchte und/oder eines aktivierten Lautsprechers des Türbeschlags 1 ausgegeben.

- In einem **Schritt S11** wird gemäss Fig. 6 und 7 eine Wartung eines Bereichsprofils initiiert, in dem von der Rechnereinheit 3 über eine kommunikative Verbindung 31 eine Wartungsanfrage eines **Bereichsprofils T1** an die Netzwerkadresse der Zentralrechnereinheit 4 übermittelt wird.

- Gemäss Fig. 6 und 7 werden die Wartungsanfrage, das Bereichsprofil T1 und die Netzwerkadresse der Rechnereinheit 3 von der Zentralrechnereinheit 4 über die kommunikative Verbindung 31 empfangen. In einem **Schritt S12** überprüft gemäss Fig. 6 und 7 die Zentralrechnereinheit 4, ob das Bereichsprofil T1 im Zutrittskontrollsystem existiert. Wenn das Bereichsprofil T1 im Zutrittskontrollsystem existiert, wird von der Zentralrechnereinheit 4 über die kommunikative Verbindung 31 eine **Postadresse-Anfrage T12** an die Netzwerkadresse der Rechnereinheit 3 übermittelt. Wenn das Bereichsprofil T1 im Zutrittskontrollsystem nicht existiert, wird von der Zentralrechnereinheit 4 über die kommunikative Verbindung 31 eine Anfragewiederholungs-Anfrage T12' an die Netzwerkadresse der Rechnereinheit 3 übermittelt.

- Gemäss Fig. 6 und 7 wird die Postadresse-Anfrage T12 von der Rechnereinheit 3 über die kommunikative Verbindung 31 empfangen. In einem **Schritt S13** wird gemäss Fig. 6 und 7 von der Rechnereinheit 3 über eine kommunikative Verbindung 31' eine **Postadresse T13 der Rechnereinheit 3** an die Netzwerkadresse der Zentralrechnereinheit 4 übermittelt. Die Übermittlung der Postadresse T3 erfolgt über eine verschlüsselte kommunikative Verbindung 31', die über einen elektronischen Verweis (Hyperlink) von der Rechnereinheit 3 aus der empfangenen Postadresse-Anfrage T12 heraus aufgebaut wird.

- Gemäss Fig. 6 und 7 wird die Postadresse T13 von der Zentralrechnereinheit 4 über die verschlüsselte kommunikative Verbindung 31' empfangen. In einem **Schritt S14** gemäss Fig. 6 und 7 übermittelt die Zentralrechnereinheit 4 über eine verschlüsselte kommunikative Verbindung 31' eine **Berechtigungscode-Anfrage T14** an die Netzwerkadresse der Rechnereinheit 3. Zusätzlich zur Berechtigungscode-Anfrage T14 kann von der Zentralrechnereinheit 4 eine Forderung nach Bestätigung der Postadresse T13 der Rechnereinheit 3 an die Netzwerkadresse der Rechnereinheit 3 übermittelt werden.

- Gemäss Fig. 6 und 7 wird/werden die Berechtigungscode-Anfrage T14 und gegebenenfalls die Forderung nach Bestätigung der Postadresse T13 von der Rechnereinheit 3 über die kommunikative Verbindung 31' empfangen. In einem **Schritt S15** gemäss Fig. 6 und 7 übermittelt die Rechnereinheit 3 über eine verschlüsselte kommunikative Verbindung 31' einen **Berechtigungscode T15** und gegebenenfalls eine Bestätigung der Postadresse T3 an die Netzwerkadresse der Zentralrechnereinheit 4.

- Gemäss Fig. 6 und 7 wird/werden der Berechtigungscode T15 und gegebenenfalls die Bestätigung der Postadresse T13 von der Zentralrechnereinheit 4 über die verschlüsselte kommunikative Verbindung 31' empfangen. In einem **Schritt S16** wird gemäss Fig. 6 von der Zentralrechnereinheit 4 über eine kommunikative Verbindung 61 eine **Berechtigungscodeüberprüfungs-Anfrage** T16 mit dem Berechtigungscode T15 und dem Bereichsprofil T1 an eine Postadresse der Gebäuderechnereinheit 6 übermittelt.

- Gemäss Fig. 6 werden die Berechtigungscodeüberprüfungs-Anfrage T16, der Berechtigungscode T15 und das Bereichsprofil T1 von der Gebäuderechnereinheit 6 über die kommunikative Verbindung 61 empfangen. In einem **Schritt S17** wird gemäss Fig. 6 von der Gebäuderechnereinheit 6 überprüft, ob der Berechtigungscode T15 für das Bereichsprofil T1 gültig ist. Wenn der Berechtigungscode T15 für das Bereichsprofil T1 gültig ist, wird gemäss Fig. 6 von der Gebäuderechnereinheit 6 ein **Berechtigungssignal T17** erzeugt und über eine verschlüsselte kommunikative Verbindung 61' an die Netzwerkadresse der Zentralrechnereinheit 4 übermittelt. Wenn der Berechtigungscode T15 für das Bereichsprofil T1 ungültig ist, wird gemäss Fig. 6 von der Gebäuderechnereinheit 6 ein **Nichtberechtigungssignal T17'** erzeugt und über die verschlüsselte kommunikative Verbindung 61' an die Netzwerkadresse der Zentralrechnereinheit 4 übermittelt. Die Übermittlung des Berechtigungsignals T17 oder des Nichtberechtigungssignals T17' erfolgt über eine verschlüsselte kommunikative Verbindung 61', die über einen elektronischen Verweis (Hyperlink) von der Gebäuderechnereinheit 6 aus der empfangenen Berechtigungscodeüberprüfungs-Anfrage T16 heraus aufgebaut wird.

- Gemäss Fig. 7 liegen die Berechtigungscodeüberprüfungs-Anfrage T16, der Berechtigungscode T15 und das Bereichsprofil T1 in der Zentralrechnereinheit 4 vor. In einem **Schritt S17** wird gemäss Fig. 7 von der Zentralrechnereinheit 4 überprüft, ob der Berechtigungscode T15 für das Bereichsprofil T1 gültig ist. Wenn der Berechtigungscode T15 für das Bereichsprofil T1 gültig ist, wird gemäss Fig. 7 von der Zentralrechnereinheit 4 ein **Berechtigungssignal T17** erzeugt. Wenn der Berechtigungscode T15 für das Bereichsprofil T1 ungültig ist, wird gemäss Fig. 7 von der Zentralrechnereinheit 4 ein **Nichtberechtigungssignal T17'** erzeugt.

- Gemäss Fig. 6 wird das Berechtigungssignal T17 oder das Nichtberechtigungssignal T17' von der Zentralrechnereinheit 4 über die verschlüsselte kommunikative Verbindung 61' empfangen. Gemäss Fig. 7 liegt ein Berechtigungssignal T17 oder ein Nichtberechtigungssignal T17' in der Zentralrechnereinheit 4 vor. In einem **Schritt S18** gemäss Fig. 6 und 7 gibt die Zentralrechnereinheit 4 für ein

vorliegendes Berechtigungssignal T17 Schreib- und Leserechte für das Bereichsprofil T1 frei. Sie erzeugt ein **Freigabesignal T18** und übermittelt das Freigabesignal T18 über eine kommunikative Verbindung 31 an die Postadresse der Rechnereinheit 3.

- Gemäss Fig. 6 und 7 wird das Freigabesignal T18 von der Rechnereinheit 3 über die kommunikative Verbindung 31 empfangen.

[0048] In einem **Schritt S19** wird gemäss Fig. 6 bis 8 von der Rechnereinheit 3 ein **Veränderungssignal T19** erzeugt und über eine kommunikative Verbindung 31' an die Netzwerkadresse der Zentralrechnereinheit 4 übermittelt. Die Übermittlung des Veränderungssignals T19 erfolgt über eine verschlüsselte kommunikative Verbindung 31', die über einen elektronischen Verweis (Hyperlink) von der Rechnereinheit 3 aus dem empfangenen Freigabesignal T18 heraus aufgebaut wird.

- Gemäss Fig. 6 bis 8 wird das Veränderungssignal T19 von der Zentralrechnereinheit 4 über die verschlüsselte kommunikative Verbindung 31' empfangen. In einem **Schritt S20** gemäss Fig. 6 und 7 setzt die Zentralrechnereinheit 4 für ein empfangenes Veränderungssignal T19 Änderungen im Bereichsprofil T1 um und übermittelt über eine verschlüsselte kommunikative Verbindung 31' ein **Veränderungsbestätigungssignal T20** an die Netzwerkadresse der Rechnereinheit 3.

[0049] Bei Kenntnis der vorliegenden Erfindung kann der Fachmann die vorgängig beschriebene verschlüsselte kommunikative Verbindung 31', 61' auch durch eine unverschlüsselte kommunikative Verbindung 31, 61 realisieren.

- In einem **Schritt S20** wird gemäss Fig. 8 von der Zentralrechnereinheit 4 ein Veränderungssignal T19 derart in einer Änderung eines freigegebenen Bereichsprofils T1 umgesetzt, dass darin ein ein provisorischer Identifikationscode T2* angelegt wird.

- In einem **Schritt S21** wird gemäss Fig. 8 ein eingelesener Identifikationscode T2 mit dem angelegten provisorischen Identifikationscode T2* verglichen. Falls der eingelesene Identifikationscode T2 an dem Türbeschlag 1 eingelesen wirden ist, der Zutritt zu dem gesicherten Bereich des freigegebenen Bereichprofils T1 mit dem angelegten provisorischen Identifikationscode T2* gewährt, und der eingelesene Identifikationscode T2 mit diesem provisorischen Identifikationscode T2* übereinstimmt, wird der eingelesene Identifikationscode T2 in das freigegebene Bereichsprofil als gültiger Identifikationscode T2' aufgenommen. Falls dem nicht so ist und der eingelesene Identifikationscode T2 vom angelegten provisorischen Identifikationscode T2" abweicht, wird von der Zentralrechnereinheit 4 ein Fehlersignal T21 erzeugt.

[0050] In einem **Schritt S22** wird gemäss Fig. 8 von der Zentralrechnereinheit 4 für den im Bereichsprofil T1 gültig aufgenommenen Identifikationscode T2' über eine kommunikative Verbindung 31, 31' ein **Veränderungsbestätigungssignal T20** an die Netzwerkadresse der Rechnereinheit 3 übermittelt.

Patentansprüche

1. Verfahren zum Betreiben eines Zutrittskontrollsystems mit mindestens einem Türbeschlag (1) zu einem gesicherten Bereich eines Gebäudes und mindestens einem Identifikationscode (T2) auf einem mobilen Datenträger (2); welcher Identifikationscode (T2) von einer Lesevorrichtung (10) des Türbeschlags (1) eingelesen wird; wobei falls ein eingelesener Identifikationscode (T2) gültig ist, Zutritt zu dem vom Türbeschlag (1) gesicherten Bereich gewährt wird;
   dass von einer Rechnereinheit (3) über mindestens eine kommunikative Verbindung (31, 31') ein Berechtigungscode (T15) an eine Zentralrechnereinheit (4) übermittelt wird;
   dass von einer Gebäuderechnereinheit (6) überprüft wird, ob der übermittelte Berechtigungscode (T15) mit einem gültigen Berechtigungscode für ein Bereichs-profil (T1) übereinstimmt;
   dass bei erfolgreicher Überprüfung des übermittelten Berechtigungscodes (T15) von der Zentralrechnereinheit (4) Schreib- und Leserechte für das Bereichsprofil (T1) an die den Berechtigungscode (T15) übermittelnde Rechnereinheit (3) freigegeben werden;
   dass von der Rechnereinheit (3) über eine kommunikative Verbindung (31, 31') das freigegebene Bereichsprofil (T1) verändert wird;
   dass von der Rechnereinheit (3) der Identifikationscode des mobilen Datenträgers (2) in dem freigegebenen Bereichs-profil (T1) als provisorischer Identifikationscode (T2*) angelegt wird; und
   dass falls von der Lesevorrichtung (10) des Türbeschlags (1), der Zutritt zu dem gesicherten Bereich des freigegebenen Bereichprofils (T1) gewährt, ein Identifikationscode (T2) eingelesen wird, der mit dem provisorischen Identifikationscode (T2*) übereinstimmt, der eingelesene Identifikationscode (T2) in das freigegebene Bereichsprofil (T1) als gültiger Identifikationscode (T2') aufgenommen wird.

2. Verfahren gemäss Anspruch 1, **dadurch gekennzeichnet, dass** von der Rechnereinheit (3) ein Identifikationscode (T2) eines mobilen Datenträgers (2) als gültiger Identifikationscode (T2') aus dem freigegebenen Bereichsprofil (T1) entfernt wird und/oder

dass von der Rechnereinheit (3) eine Gültigkeit eines Identifikationscodes des freigegebenen Bereichsprofils (T1) verändert wird
und/oder dass von der Rechnereinheit (3) eine Entität in das freigegebene Bereichsprofil (T1) aufgenommen wird und/oder dass von der Rechnereinheit (3) eine Entität aus dem freigegebenen Bereichsprofil (T1) entfernt wird und/oder dass von der Rechnereinheit (3) ein Leserecht einer Entität des freigegebenen Bereichsprofils (T1) verändert wird und/oder dass von der Rechnereinheit (3) ein Schreibrecht einer Entität des freigegebenen Bereichsprofils (T1) verändert wird
und/oder dass von der Rechnereinheit (3) eine Zeitzone einer Entität des freigegebenen Bereichsprofils (T1) verändert wird.

3. Verfahren gemäss Anspruch 1, **dadurch gekennzeichnet, dass** der provisorische Identifikationscode (T2*) durch Angabe einer Ziffernfolge in dem freigegebenen Bereichsprofil (T1) angelegt wird; und dass falls von der Lesevorrichtung (10) des Türbeschlags (1), der Zutritt zu dem gesicherten Bereich des freigegebenen Bereichprofils (T1) gewährt, eine Ziffernfolge eingelesen wird, die mit der Ziffernfolge des provisorischen Identifikationscodes (T2*) übereinstimmt, ein mit der Ziffernfolge eingelesener Identifikationscode (T2) in das freigegebene Bereichsprofil (T1) als der gültige Identifikationscode (T2') aufgenommen wird
und/oder der provisorische Identifikationscode (T2*) durch Angabe einer Zeitdauer in dem freigegebenen Bereichsprofil (T1) angelegt wird; und dass falls innerhalb der Zeitdauer von der Lesevorrichtung (10) des Türbeschlags (1), der Zutritt zu dem gesicherten Bereich des freigegebenen Bereichsprofils (T1) gewährt, ein Identifikationscode (T2) eingelesen wird, der mit dem provisorischen Identifikationscode (T2*) übereinstimmt, der eingelesene Identifikationscode (T2) in das freigegebene Bereichsprofil (T1) als der gültige Identifikationscode (T2') aufgenommen wird.

4. Verfahren gemäss einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet, dass** von einem Prozessor (13) eines Türbeschlags (1) überprüft wird, ob ein von der Lesevorrichtung (10) des Türbeschlags (1) eingelesener Identifikationscode (T2) mit einem gültige Identifikationscode (T2') eines Bereichsprofils (T1) für den von dem Türbeschlag (1) gesicherten Bereich übereinstimmt und/oder dass von der Zentralrechnereinheit (4) zumindest ein Teil eines Bereichsprofils (T1) für den von einem Türbeschlag (1) gesicherten Bereich über eine kommunikative Verbindung (41, 41') an den Türbeschlag (1) übermittelt wird; und dass von einem Prozessor (13) des Türbeschlags (1) überprüft wird, ob ein von der Lesevorrichtung (10) des Türbeschlags (1) eingelesener Identifikationscode (T2) mit einem gültigen Identifikationscode (T2') des übermittelten Bereichsprofils (T1) übereinstimmt
und/oder dass von der Zentralrechnereinheit (4) zumindest ein Teil eines Bereichsprofils (T1) für den von einem Türbeschlag (1) gesicherten Bereich über eine kommunikative Verbindung (41, 41') an den Türbeschlag (1) übermittelt wird; dass von einem Prozessor (13) des Türbeschlags (1) überprüft wird, ob ein von der Lesevorrichtung (10) des Türbeschlags (1) eingelesener Identifikationscode (T2) mit einem gültigen Identifikationscode (T2') des übermittelten Bereichsprofils (T1) übereinstimmt; dass bei erfolgreicher Überprüfung des eingelesenen Identifikationscodes (T2) von dem Prozessor (13) ein Zutrittssignal (T4) an einen Aktuator (18) des Türbeschlags (1) übermittelt wird; und dass vom Aktuator (18) für das übermittelte Zutrittssignal (T4) Zutritt zu dem vom Türbeschlag (1) gesicherten Bereich gewährt wird.

5. Verfahren gemäss einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet, dass** von der Zentralrechnereinheit (4) überprüft wird, ob ein von einer Lesevorrichtung (10) eines Türbeschlags (1) eingelesener Identifikationscode (T2) mit einem gültigen Identifikationscode (T2') eines Bereichsprofils (T1) für den vom Türbeschlag (1) der Lesevorrichtung (10) gesicherten Bereich übereinstimmt
und/oder dass ein von einer Lesevorrichtung (10) eingelesener Identifikationscode (T2) über eine kommunikative Verbindung (41, 41') an die Zentralrechnereinheit (4) übermittelt wird; und dass von der Zentralrechnereinheit (4) überprüft wird, ob der eingelesene Identifikationscode (T2) mit einem gültigen Identifikationscode (T2') eines Bereichsprofils (T1) für den vom Türbeschlag (1) der Lesevorrichtung (10) übereinstimmt und/oder dass ein von einer Lesevorrichtung (10) eingelesener Identifikationscode (T2) über eine kommunikative Verbindung (41, 41') an die Zentralrechnereinheit (4) übermittelt wird; und dass von der Zentralrechnereinheit (4) überprüft wird, ob der eingelesene Identifikationscode (T2) mit einem gültigen Identifikationscode (T2') eines Bereichsprofils (T1) für den vom Türbeschlag (1) der Lesevorrichtung (10) übereinstimmt; dass bei erfolgreicher Überprüfung des eingelesenen Identifikationscodes (T2) von der Zentralrechnereinheit (4) ein Zutrittssignal (T4) über die kommunikative Verbindung (41, 41') an einen Aktuator (18) des Türbeschlags (1) übermittelt wird; und dass vom Aktuator (18) für das übermittelte Zutrittssignal (T4) Zutritt zu dem vom Türbeschlag (1) gesicherten Bereich gewährt wird.

6. Verfahren gemäss einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet, dass** von der Zentralrechnereinheit (4) ein übermittelter Berechtigungscode (T15) über eine kommunikative Verbindung (61, 61')

an eine Gebäuderechnereinheit (6) übermittelt wird; dass von der Gebäuderechnereinheit (6) überprüft wird, ob der übermittelte Berechtigungscode (T15) mit einem gültigen Berechtigungscode für ein Bereichsprofil (T1) übereinstimmt; und dass bei erfolgreicher Überprüfung des übermittelten Berechtigungscodes (T15) von der Gebäuderechnereinheit (6) ein Berechtigungssignal (T17) über eine kommunikative Verbindung (61, 61') an die Zentralrechnereinheit (4) übermittelt wird und/oder dass von der Zentralrechnereinheit (4) ein übermittelter Berechtigungscode (T15) über eine kommunikative Verbindung (61, 61') an eine Gebäuderechnereinheit (6) übermittelt wird; dass von der Gebäuderechnereinheit (6) überprüft wird, ob der übermittelte Berechtigungscode (T15) mit einem gültigen Berechtigungscode für ein Bereichsprofil (T1) übereinstimmt; dass bei erfolgreicher Überprüfung des übermittelten Berechtigungscodes (T15) von der Gebäuderechnereinheit (6) ein Berechtigungssignal (T17) über eine kommunikative Verbindung (61, 61') an die Zentralrechnereinheit (4) übermittelt wird; und dass von der Zentralrechnereinheit (4) für ein übermitteltes Berechtigungssignal (T17) Schreib- und Leserechte für das Bereichsprofil (T1) an die den Berechtigungscode (T15) übermittelnde Rechnereinheit (3) freigegeben werden.

7. Verfahren gemäss einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet, dass** bei erfolgreicher Überprüfung des übermittelten Berechtigungscodes (T15) von der Zentralrechnereinheit (4) Schreib- und Leserechte für das Bereichsprofil (T1) an die den Berechtigungscode (T15) übermittelnden Rechnereinheit (3) freigegeben werden.

8. Zutrittskontrollsystem zur Durchführung des Verfahrens gemäss einem der Ansprüche 1 bis 7 wobei das Zutrittskontrollsystem eine Rechnereinheit (3), eine Zentralrechnereinheit (4), eine Gebäuderechnereinheit (6), einen mobilen Datenträger (2), der einen Identifikationscode (T2) speichert, und einen Türbeschlag (1) mit einer Lesevorrichtung (10) umfasst,
dass das Zutrittskontrollsystem eine netzwerkgestützte kommunikative Verbindung (31, 31') zwischen der Rechnereinheit (3) und der Zentralrechnereinheit (4) zur Übermittlung eines Berechtigungscodes (T15) an die Zentralrechnereinheit (4), eine netzwerkgestützte kommunikative Verbindung (61, 61') zwischen der Zentralrechnereinheit (4) und der Gebäuderechnereinheit (6) und
eine netzwerkgestützte kommunikative Verbindung (41, 41') zwischen der Zentralrechnereinheit (4) und dem Türbeschlag (1) umfasst,
dass die Lesevorrichtung (10) den Identifikationscode (T2) des mobilen Datenträgers (2) über eine Datenübermittlung (21) einliest,
dass die Zentralrechnereinheit (4) bei erfolgreicher Überprüfung des übermittelten Berechtigungscodes (T15) Schreib- und Leserechte für das Bereichsprofil (T1) an die den Berechtigungscode (T15) übermittelnde Rechnereinheit (3) freigibt;
dass die Rechnereinheit (3) über die kommunikative Verbindung (31, 31') zwischen der Rechnereinheit (3) und der Zentralrechnereinheit (4) das freigegebene Bereichsprofil (T1) verändert;
dass die Rechnereinheit (3) den Identifikationscode des mobilen Datenträgers (2) in einem freigegebenen Bereichsprofil (T1) als provisorischen Identifikationscode (T2*) anlegt,
dass falls die Lesevorrichtung (10) einen Identifikationscode (T2), der mit dem provisorischen Identifikationscode (T2*) übereinstimmt, einliest, die Rechnereinheit (3) den Identifikationscode (T2) als gültigen Identifikationscode (T2') in das freigegebene Bereichsprofil (T1) aufnimmt.

9. Zutrittskontrollsystem gemäss Anspruch 8, **dadurch gekennzeichnet, dass** das Bereichsprofil (T1) zumindest teilweise in einem computerlesbaren Datenspeicher (43) der Zentralrechnereinheit (4) gespeichert ist
und/oder dass das Bereichsprofil (T1) zumindest teilweise in einem computerlesbaren Datenspeicher (14) des Türbeschlags (1) gespeichert ist.

10. Zutrittskontrollsystem gemäss einem der Ansprüche 8 oder 9, **dadurch gekennzeichnet, dass** der Türbeschlag (1) auf einem Türblatt einer Tür zum von dem Türbeschlag (1) gesicherten Bereich angeordnet ist.

11. Zutrittskontrollsystem gemäss einem der Ansprüche 8 bis 10, **dadurch gekennzeichnet, dass** die Lesevorrichtung (10) in einer Türgarnitur (11) des Türbeschlags (1) angeordnet ist und/oder dass ein Prozessor (13) in einer Türgarnitur (11) des Türbeschlags (1) angeordnet ist
und/oder ein computerlesbarer Datenspeicher (14) in einer Türgarnitur (11) des Türbeschlags (1) angeordnet ist und/oder eine Sende- und Empfangseinheit (12) für eine netzwerkgestützte kommunikative Verbindung (41) zwischen der Zentralrechnereinheit (4) und dem Türbeschlag (1) in einer Türgarnitur (11) des Türbeschlags (1) angeordnet ist und/oder eine elektrische Stromversorgung (19) in einer Türgarnitur (11) des Türbeschlags (1) angeordnet ist.

12. Zutrittskontrollsystem gemäss einem der Ansprüche 8 bis 11, **dadurch gekennzeichnet, dass** die Rechnereinheit (3) im vom Türbeschlag (1) gesicherten Bereich angeordnet ist.

Claims

1. A method for operating an access control system with at least one door fitting (1) to a secured area of a building and at least one identification code (T2) of the mobile data carrier (2); which identification code (T2) is read in by a reader (10) of the door fitting (1); wherein if a read-in identification code (T2) is valid, access to the area secured by the door fitting (1) is granted;
in that a computer unit (3) communicates an authorization code (T15) to a central computer unit (4) via at least one communicative connection (31,31'); in that a check is made by a building computer unit (6) to determine whether the communicated authorization code (T15) corresponds to a valid authorization code for an area profile (T1);
in that, upon successful checking of the communicated authorization code (T15), write and read rights for the area profile (T1) are released by the central computer unit (4) to the computer unit (3) communicating the authorization code (T15);
in that the released area profile (T1) is changed by the computer unit (3) via a communicative connection (31, 31');
in that the computer unit (3) creates the identification code of the mobile data carrier (2) in a released area profile (T1) as provisional identification code (T2*);
and in that if the reader (10) of the door fitting (1) that grants access to the secured area of the released area profile (T1) reads in an identification code (T2) corresponding to the provisional identification code (T2*), the read-in identification code (T2) is included in the released area profile (T1) as valid identification code (T2').

2. The method as claimed in claim 1, **characterized in that** the computer unit (3) removes an identification code (T2) of a mobile data carrier (2) as valid identification code (T2') from the released area profile (T1) and/or **in that** the computer unit (3) changes a validity of an identification code of the released area profile (T1)
and/or **in that** the computer unit (3) includes an entity in the released area profile (T1)
and/or **in that** the computer unit (3) removes an entity from the released area profile (T1)
and/or **in that** the computer unit (3) changes a read right of an entity of the released area profile (T1)
and/or **in that** the computer unit (3) changes a write right of an entity of the released area profile (T1)
and/or **in that** the computer unit (3) changes a time zone of an entity of the released area profile (T1).

3. The method as claimed in claim 1, **characterized in that** the provisional identification code (T2*) is created by the specification of a digit sequence in the released area profile (T1); and **in that** if the reader (10) of the door fitting (1) that grants access to the secured area of the released area profile (T1) reads in a digit sequence corresponding to the digit sequence of the provisional identification code (T2*), an identification code (T2) read in with the digit sequence is included in the released area profile (T1) as the valid identification code (T2')
and/or the provisional identification code (T2*) is created by the specification of a time duration in the released area profile (T1); and **in that** if, within the time duration, the reader (10) of the door fitting (1) that grants access to the secured area of the released area profile (T1) reads in an identification code (T2) corresponding to the provisional identification code (T2*), the read-in identification code (T2) is included in the released area profile (T1) as the valid identification code (T2').

4. The method as claimed in any of claims 1 to 3, **characterized in that** a processor (13) of a door fitting (1) checks whether an identification code (T2) read in by the reader (10) of the door fitting (1) corresponds to a valid identification code (T2') of an area profile (T1) for the area secured by the door fitting (1) and/or **in that** the central computer unit (4) communicates at least one part of an area profile (T1) for the area secured by a door fitting (1) via a communicative connection (41, 41') to the door fitting (1); and **in that** a processor (13) of the door fitting (1) checks whether an identification code (T2) read in by the reader (10) of the door fitting (1) corresponds to a valid identification code (T2') of the communicated area profile (T1)
and/or **in that** the central computer unit (4) communicates at least one part of an area profile (T1) for the area secured by a door fitting (1) via a communicative connection (41, 41') to the door fitting (1); **in that** a processor (13) of the door fitting (1) checks whether an identification code (T2) read in by the reader (10) of the door fitting (1) corresponds to a valid identification code (T2') of the communicated area profile (T1); **in that**, upon successful checking of the read-in identification code (T2), the processor (13) communicates an access signal (T4) to an actuator (18) of the door fitting (1); and **in that** access to the area secured by the door fitting (1) is granted by the actuator (18) for the communicated access signal (T4).

5. The method as claimed in any of claims 1 to 3, **characterized in that** the central computer unit (4) checks whether an identification code (T2) read in by a reader (10) of a door fitting (1) corresponds to a valid identification code (T2') of an area profile (T1) for the area secured by the door fitting (1) of the reader (10)
and/or **in that** an identification code (T2) read in by a reader (10) is communicated to the central com-

puter unit (4) via a communicative connection (41, 41'); and **in that** the central computer unit (4) checks whether the read-in identification code (T2) corresponds to a valid identification code (T2') of an area profile (T1) for the by the door fitting (1) of the reader (10) and/or **in that** an identification code (T2) read in by a reader (10) is communicated to the central computer unit (4) via a communicative connection (41, 41'); and **in that** the central computer unit (4) checks whether the read-in identification code (T2) corresponds to a valid identification code (T2') of an area profile (T1) for the by the door fitting (1) of the reader (10);
in that, upon successful checking of the read-in identification code (T2), the central computer unit (4) communicates an access signal (T4) via the communicative connection (41, 41') to an actuator (18) of the door fitting (1); and **in that** access to the area secured by the door fitting (1) is granted by the actuator (18) for the communicated access signal (T4).

6. The method as claimed in any of claims 1 to 5, **characterized in that** the central computer unit (4) communicates a communicated authorization code (T15) via a communicative connection (61, 61') to a building computer unit (6); **in that** the building computer unit (6) checks whether the communicated authorization code (T15) corresponds to a valid authorization code for an area profile (T1); and **in that**, upon successful checking of the communicated authorization code (T15), the building computer unit (6) communicates an authorization signal (T17) via a communicative connection (61, 61') to the central computer unit (4)
and/or **in that** the central computer unit (4) communicates a communicated authorization code (T15) via a communicative connection (61, 61') to a building computer unit (6); **in that** the building computer unit (6) checks whether the communicated authorization code (T15) corresponds to a valid authorization code for an area profile (T1); and **in that**, upon successful checking of the communicated authorization code (T15), the building computer unit (6) communicates an authorization signal (T17) via a communicative connection (61, 61') to the central computer unit (4) and **in that** the central computer unit (4), for a communicated authorization signal (T17), releases write and read rights for the area profile (T1) to the computer unit (3) communicating the authorization code (T15).

7. The method as claimed in any of claims 1 to 6, **characterized in that**, upon successful checking of the communicated authorization code (T15), the central computer unit (4) releases write and read rights for the area profile (T1) to the computer unit (3) communicating the authorization code (T15).

8. An access control system for carrying out the method as claimed in any of claims 1 to 7, wherein the access control system comprises a computer unit (3), a central computer unit (4), a building computer unit (6), a mobile data carrier (2), which stores an identification code (T2), and a door fitting (1) with a reader (10), in that the access control system comprises a network-supported communicative connection (31, 31') between the computer unit (3) and the central computer unit (4) for communicating an authorization code (T15) to the central computer unit (4), a network-supported communicative connection (61, 61') between the central computer unit (4) and the building computer unit (6), and
a network-supported communicative connection (41, 41') between the central computer unit (4) and the door fitting (1),
in that the reader (10) reads in the identification code (T2) of the mobile data carrier (2) via a data communication (21),
in that, upon successful checking of the communicated authorization code (T15), the central computer unit (4) releases write and read rights for the area profile (T1) to the computer unit (3) communicating the authorization code (T15);
in that the computer unit (3) changes the released area profile (T1) via the communicative connection (31, 31') between the computer unit (3) and the central computer unit (4);
in that the computer unit (3) creates the identification code of the mobile data carrier (2) in a released area profile (T1) as provisional identification code (T2*),
in that if the reader (10) reads in an identification code (T2) corresponding to the provisional identification code (T2*), the computer unit (3) includes the identification code (T2) as valid identification code (T2') in the released area profile (T1).

9. The access control system as claimed in claim 8, **characterized in that** the area profile (T1) is stored at least partly in a computer-readable data memory (43) of the central computer unit (4)
and/or **in that** the area profile (T1) is stored at least partly in a computer-readable data memory (14) of the door fitting (1).

10. The access control system as claimed in either of claims 8 and 9, **characterized in that** the door fitting (1) is arranged on a door leaf of a door to the area secured by the door fitting (1).

11. The access control system as claimed in any of claims 8 to 10, **characterized in that** the reader (10) is arranged in a door mounting (11) of the door fitting (1) and/or **in that** a processor (13) is arranged in a door mounting (11) of the door fitting (1)
and/or a computer-readable data memory (14) is arranged in a door mounting (11) of the door fitting (1)

and/or a transmitting and receiving unit (12) for a network-supported communicative connection (41) between the central computer unit (4) and the door fitting (1) is arranged in a door mounting (11) of the door fitting (1) and/or an electrical power supply (19) is arranged in a door mounting (11) of the door fitting (1).

12. The access control system as claimed in any of claims 8 to 11, **characterized in that** the computer unit (3) is arranged in the area secured by the door fitting (1).

Revendications

1. Procédé pour faire fonctionner un système de contrôle d'accès avec au moins une ferrure de porte (1) pour une zone protégée d'un bâtiment, et au moins un code d'identification (T2) sur un support de données mobile (2) ; lequel code d'identification (T2) est lu par un lecteur (10) de la ferrure de porte (1), étant précisé que dans le cas où un code d'identification (T2) lu est valable, l'accès à la zone protégée par la ferrure de porte (1) est validé ;
qu'un code d'autorisation (T15) est transmis par une unité informatique (3), par l'intermédiaire d'au moins une liaison de communication (31, 31'), à une unité informatique centrale (4) ;
qu'une unité informatique de bâtiment (6) vérifie si le code d'autorisation (T15) transmis correspond à un code d'autorisation valable pour un profil de zone (T1) ;
que si la vérification du code d'autorisation (T15) transmis est réussie, des droits d'écriture et de lecture pour le profil de zone (T1) sont validés par l'unité informatique centrale (4), pour l'unité informatique (3) qui transmet le code d'autorisation (T15) ;
que le profil de zone (T1) validé est modifié par l'unité informatique (3) par l'intermédiaire d'une liaison de communication (31,31');
que le code d'identification du support de données mobile (2) est créé par l'unité informatique (3) comme code d'identification provisoire (T2*) dans le profil de zone (T1) validé ; et
que dans le cas où le lecteur (10) de la ferrure de porte (1) autorise l'accès à la zone protégée du profil de zone (T1) validé, un code d'identifcation (T2) qui correspond au code d'identification provisoire (T2*) est lu, le code d'identification (T2) lu est enregistré comme code d'identification valable (T2') dans le profil de zone (T1) validé.

2. Procédé selon la revendication 1, **caractérisé en ce qu'**un code d'identification (T2) d'un support de données mobile (2) est supprimé du profil de zone (T1) valide, comme code d'identification valable (T2'), par l'unité informatique (3),
et/ou **en ce qu'**une validité d'un code d'identification du profil de zone (T1) validé est modifiée par l'unité informatique (3),
et/ou **en ce qu'**une entité est enregistrée par l'unité informatique (3) dans le profil de zone (T1) validé,
et/ou **en ce qu'**une entité est supprimée par l'unité informatique du profil de zone (T1) validé,
et/ou **en ce qu'**un droit de lecture d'une entité du profil de zone (T1) validé est modifié par l'unité informatique (3),
et/ou **en ce qu'**une zone de temps d'une entité du profil de zone (T1) validé est modifiée par l'unité informatique (3).

3. Procédé selon la revendication 1, **caractérisé en ce que** le code d'identification provisoire (T2*) est créé sous la forme d'une suite de chiffres dans le profil de zone (T1) validé ; et **en ce que** dans le cas où le lecteur (10) de la ferrure de porte (1) autorise l'accès à la zone protégée du profil de zone (T1) validé, une suite de chiffres est lue, qui correspond à la suite de chiffres du code d'identification provisoire (T2*), un code d'identification (T2) lu avec la suite de chiffres est enregistré comme code d'identification valable (T2') dans le profil de zone validé (T1),
et/ou le code d'identifcation provisoire (T2*) est créé grâce à l'indication d'une durée dans le profil de zone (T1) validé, et **en ce que** dans le cas où à l'intérieur de cette durée l'accès à la zone protégée du profil de zone (T1) validé est autorisé par le lecteur (10) de la ferrure de porte (1), un code d'identification (T2) est lu qui correspond au code d'identifcation provisoire (T2*), le code d'identification (T2) lu est enregistré comme code d'identification valable (T2') dans le profil de zone (T1) validé.

4. Procédé selon l'une des revendications 1 à 3, **caractérisé en ce qu'**un processeur (13) d'une ferrure de porte (1) vérifie si un code d'identification (T2) lu par le lecteur (10) de la ferrure de porte (1) correspond à un code d'identification valable (T2') d'un profil de zone (T1) pour la zone protégée par la ferrure de porte (1)
et/ou **en ce qu'**une partie au moins du profil de zone (T1) pour la zone protégée par une ferrure de porte (1) est transmise par l'unité informatique centrale (4) à la ferrure de porte (1) par l'intermédiaire d'une liaison de communication (41, 41') ; et **en ce qu'**un processeur (13) de la ferrure de porte (1) vérifie si un code d'identifcation (T2) lu par le lecteur (10) de la ferrure de porte (1) correspond à un code d'identification valable (T2') du profil de zone (T1) transmis
et/ou **en ce qu'**une partie au moins du profil de zone (T1) pour la zone protégée par une ferrure de porte (1) est transmise par l'unité informatique centrale (4) à la ferrure de porte (1) par l'intermédiaire d'une liaison de communication (41, 41'); **en ce qu'**un processeur (13) de la ferrure de porte (1) vérifie si un

code d'identifcation (T2) lu par le lecteur (10) de la ferrure de porte (1) correspond à un code d'identification valable (T2') du profil de zone (T1) transmis ; **en ce que** si la vérification du code d'identification (T2) lu est réussie, un signal d'accès (T4) est transmis par le processeur (13) à un actionneur (18) de la ferrure de porte (1) ; et **en ce que** pour le signal d'accès (T4) transmis, l'accès à la zone protégée par la ferrure de porte (1) est autorisé par l'actionneur (18).

5. Procédé selon l'une des revendications 1 à 3, **caractérisé en ce que** l'unité informatique centrale (4) vérifie si un code d'identification (T2) lu par un lecteur (10) d'une ferrure de porte (1) correspond à un code d'identification valable (T2') d'un profil de zone (T1) pour la zone protégée par la ferrure de porte (1),
et/ou **en ce qu'**un code d'identification (T2) lu par un lecteur (10) est transmis à l'unité informatique centrale (4) par l'intermédiaire d'une liaison de communication (41, 41') ;
et **en ce que** l'unité informatique centrale (4) vérifie si le code d'identification (T2) lu correspond à un code d'identification valable (T2') d'un profil de zone (T1) pour la zone protégée par la ferrure de porte (1) du lecteur (10)
et/ou **en ce qu'**un code d'identification (T2) lu par un lecteur (10) est transmis à l'unité informatique centrale (4) par l'intermédiaire d'une liaison de communication (41, 41') ;
et **en ce que** l'unité informatique centrale (4) vérifie si le code d'identification (T2) lu correspond à un code d'identification valable (T2') d'un profil de zone (T1) pour la zone protégée par la ferrure de porte (1) du lecteur (10) ;
en ce que si la vérification du code d'identification (T2) lu est réussie, un signal d'accès (T4) est transmis par l'unité informatique centrale (4) à un actionneur (18) de la ferrure de porte (1) par l'intermédiaire d'une liaison de communication (41, 41') ; et **en ce que** pour le signal d'accès (T4) transmis, l'accès à la zone protégée par la ferrure de porte (1) est autorisé par l'actionneur (18).

6. Procédé selon l'une des revendications 1 à 5, **caractérisé en ce qu'**un code d'autorisation (T15) est transmis par l'unité informatique centrale (4), par l'intermédiaire d'une liaison de communication (61, 61'), à une unité informatique de bâtiment (6); **en ce que** l'unité informatique de bâtiment (6) vérifie si le code d'autorisation (T15) transmis correspond à un code d'autorisation valable pour un profil de zone (T1) ; et **en ce que** si la vérification du code d'autorisation (T15) transmis est réussie, l'unité informatique de bâtiment (6) transmet un signal d'autorisation (T17) à l'unité informatique centrale (4) par l'intermédiaire d'une liaison de communication (61, 61')
et/ou **en ce que** l'unité informatique centrale (4) transmet à une unité informatique de bâtiment (6), par l'intermédiaire d'une liaison de communication (61, 61'), un code d'autorisation (T15) transmis ; **en ce que** l'unité informatique de bâtiment (6) vérifie si le code d'autorisation (T15) transmis correspond à un code d'autorisation valable pour un profil de zone (T1) ; **en ce que** si la vérification du code d'autorisation (T15) transmis est réussie, l'unité informatique de bâtiment (6) transmet un signal d'autorisation (T17) à l'unité informatique centrale (4) par l'intermédiaire d'une liaison de communication (61, 61'); et **en ce que** pour un signal d'autorisation (T17) transmis, des droits d'écriture et de lecture pour le profil de zone (T1) sont validés par l'unité informatique centrale (4), pour l'unité informatique (3) qui transmet le code d'autorisation (T15).

7. Procédé selon l'une des revendications 1 à 6, **caractérisé en ce que** si la vérification du code d'autorisation (T15) transmis est réussie, des droits d'écriture et de lecture pour le profil de zone (T1) sont validés par l'unité informatique centrale (4), pour l'unité informatique (3) qui transmet le code d'autorisation (T15).

8. Système de contrôle d'accès pour la mise en oeuvre du procédé selon l'une des revendications 1 à 7, étant précisé que le système de contrôle d'accès comprend une unité informatique (3), une unité informatique centrale (4), une unité informatique de bâtiment (6), un support de données mobile (2) qui stocke un code d'identification (T2), et une ferrure de porte (1) avec un lecteur (10),
que le système de contrôle d'accès comprend une liaison de communication par réseau (31, 31') entre l'unité informatique (3) et l'unité informatique centrale (4), pour transmettre un code d'autorisation (T15) à l'unité informatique centrale (4), une liaison de communication par réseau (61, 61') entre l'unité informatique centrale (4) et l'unité informatique de bâtiment (6), et
une liaison de communication par réseau (41, 41') entre l'unité informatique centrale (4) et la ferrure de porte (1),
que le lecteur (10) lit le code d'identification (T2) du support de données mobile (2) par l'intermédiaire d'une transmission de données (21),
que l'unité informatique centrale (4), si la vérification du code d'autorisation (T15) transmis est réussie, valide, pour l'unité informatique (3) qui transmet ledit code d'autorisation (T15), des droits d'écriture et de lecture pour le profil de zone (T1) ;
que l'unité informatique (3) modifie par l'intermédiaire de la liaison de communication (31, 31') entre l'unité informatique (3) et l'unité informatique centrale (4) le profil de zone (T1) validé ;
que l'unité informatique (3) crée le code d'identification du support de données mobile (2) comme code

d'identification provisoire (T2*) dans un profil de zone (T1) validé ; et
que dans le cas où le lecteur (10) lit un code d'identification (T2) qui correspond au code d'identifcation provisoire (T2*), l'unité informatique (3) enregistre dans le profil de zone (T1) validé le code d'identification (T2) comme code d'identification valable (T2').

9. Système de contrôle d'accès selon la revendication 8, **caractérisé en ce que** le profil de zone (T1) est stocké au moins en partie dans une mémoire de données lisible par ordinateur (43) de l'unité informatique centrale (4)
et/ou **en ce que** le profil de zone (T1) est stocké au moins en partie dans une mémoire de données lisible par ordinateur (14) de la ferrure de porte (1).

10. Système de contrôle d'accès selon l'une des revendications 8 ou 9, **caractérisé en ce que** la ferrure de porte (1) est disposée sur un battant d'une porte menant à la zone protégée par ladite ferrure de porte (1).

11. Système de contrôle d'accès selon l'une des revendications 8 à 10, **caractérisé en ce que** le lecteur (10) est disposé dans une garniture de porte (11) de la ferrure de porte (1)
et/ou **en ce qu'**un processeur (13) est disposé dans une garniture de porte (11) de la ferrure de porte (1)
et/ou une mémoire de données lisible par ordinateur (14) est disposée dans une garniture de porte (11) de la garniture de porte (1)
et/ou une unité d'émission et de réception (12) pour une liaison de communication par réseau (41) entre l'unité informatique centrale (4) et la ferrure de porte (1) est disposée dans une garniture de porte (11) de la ferrure de porte (1)
et/ou une alimentation en courant électrique (19) est disposée dans une garniture de porte (11) de la ferrure de porte (1).

12. Système de contrôle d'accès selon l'une des revendications 8 à 11, **caractérisé en ce que** l'unité informatique (3) est disposée dans la zone protégée par la ferrure de porte (1).

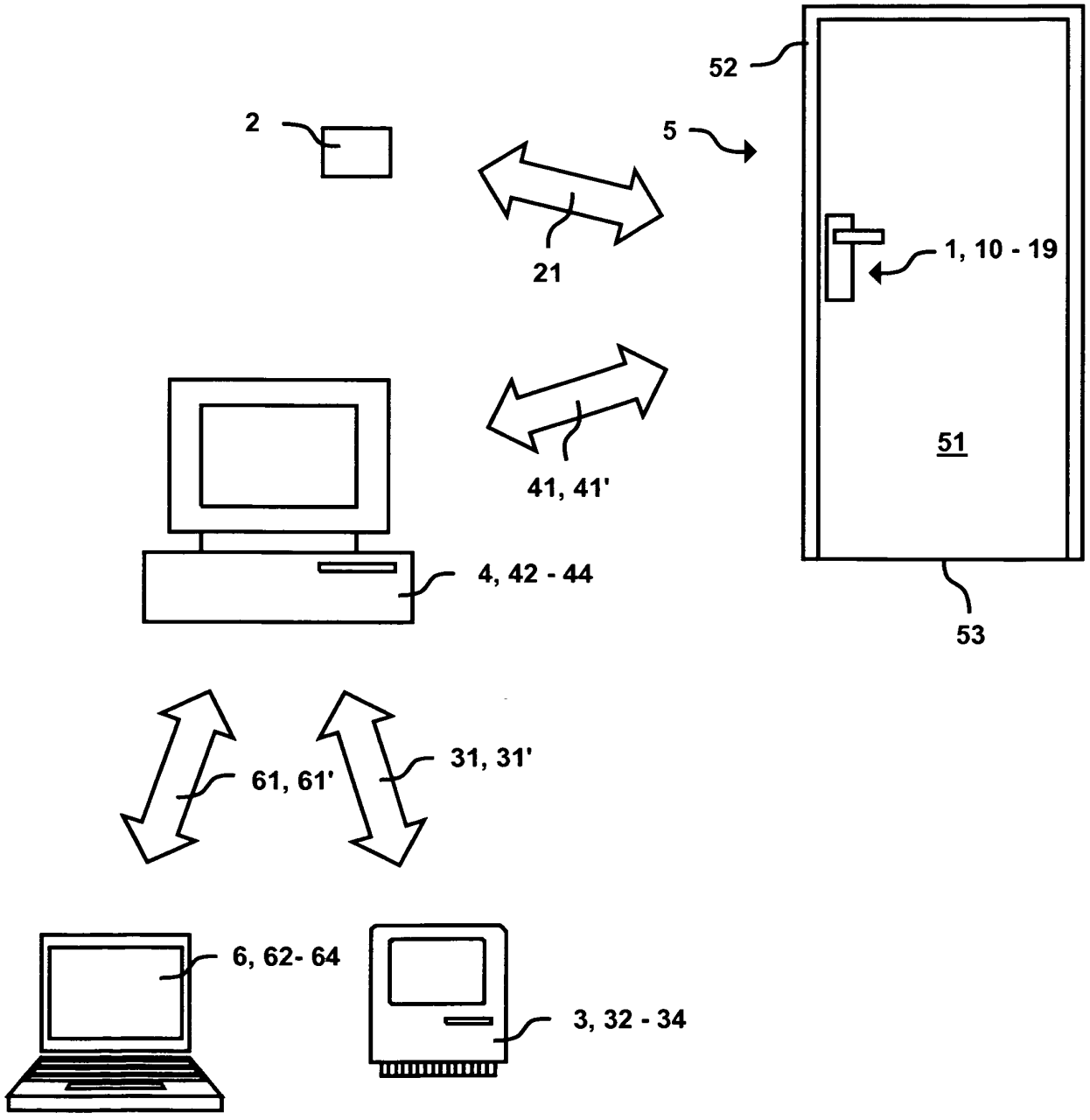

Fig. 1

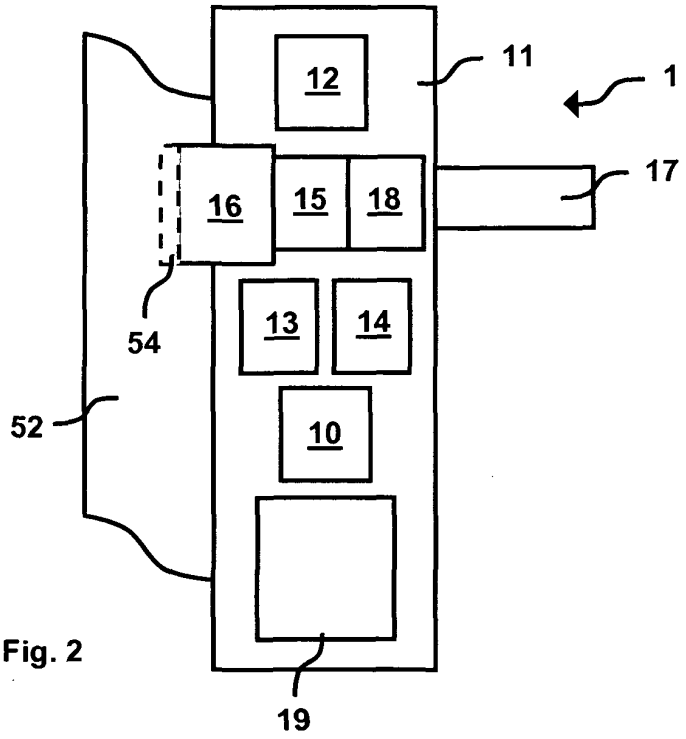
12
11
1
16
15
18
17
54
13
14
52
10
19

Fig. 2

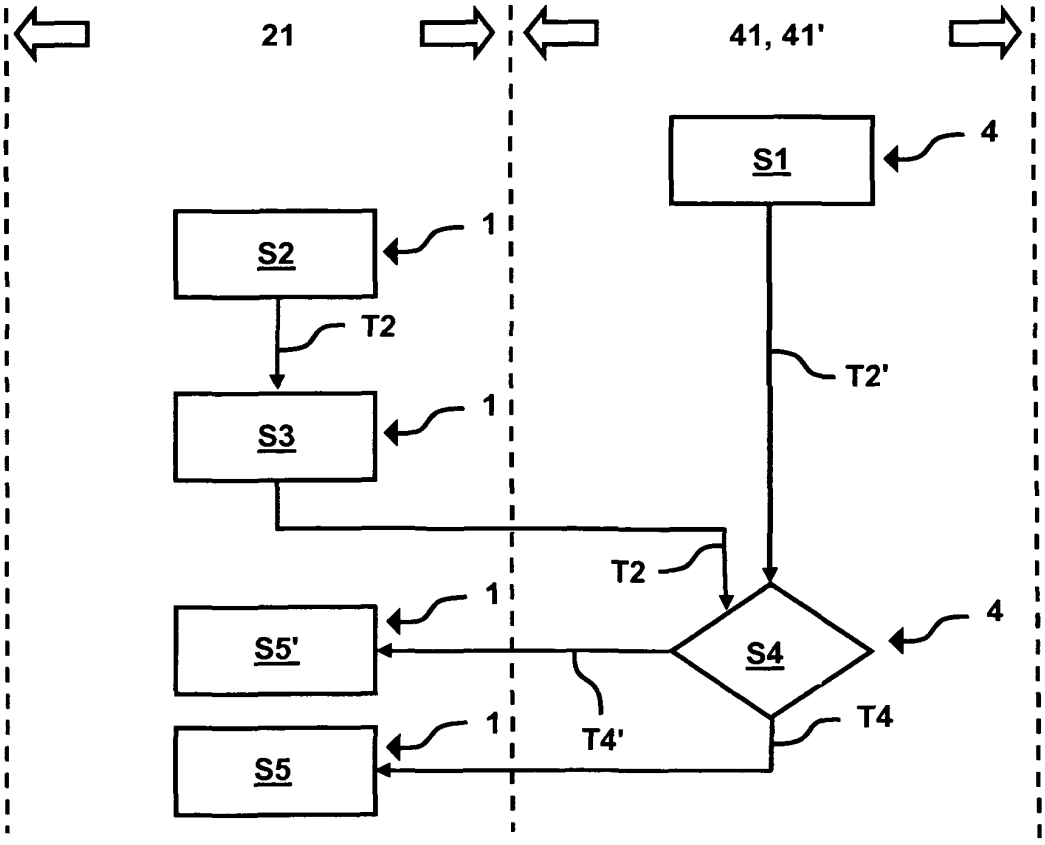
21
41, 41'
S1
4
S2
1
T2
T2'
S3
1
T2
1
S5'
S4
4
T4'
T4
1
S5

Fig. 3

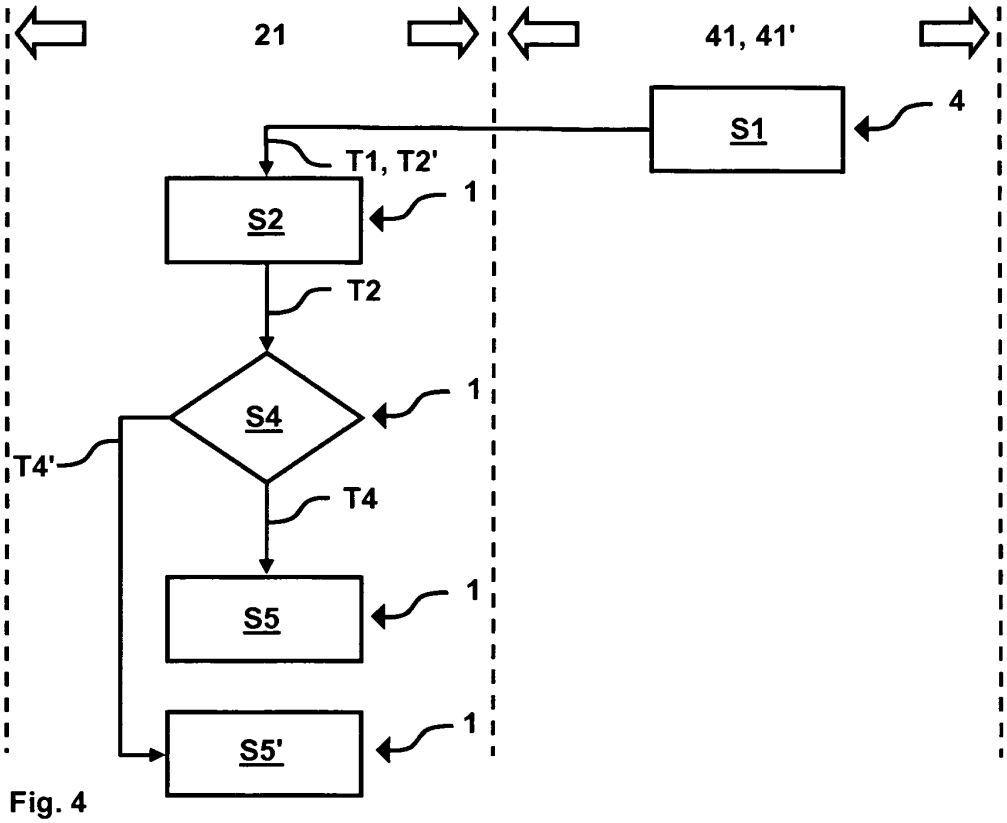
21
41, 41'
S1
4
T1, T2'
S2
1
T2
S4
1
T4'
T4
S5
1
S5'
1

Fig. 4

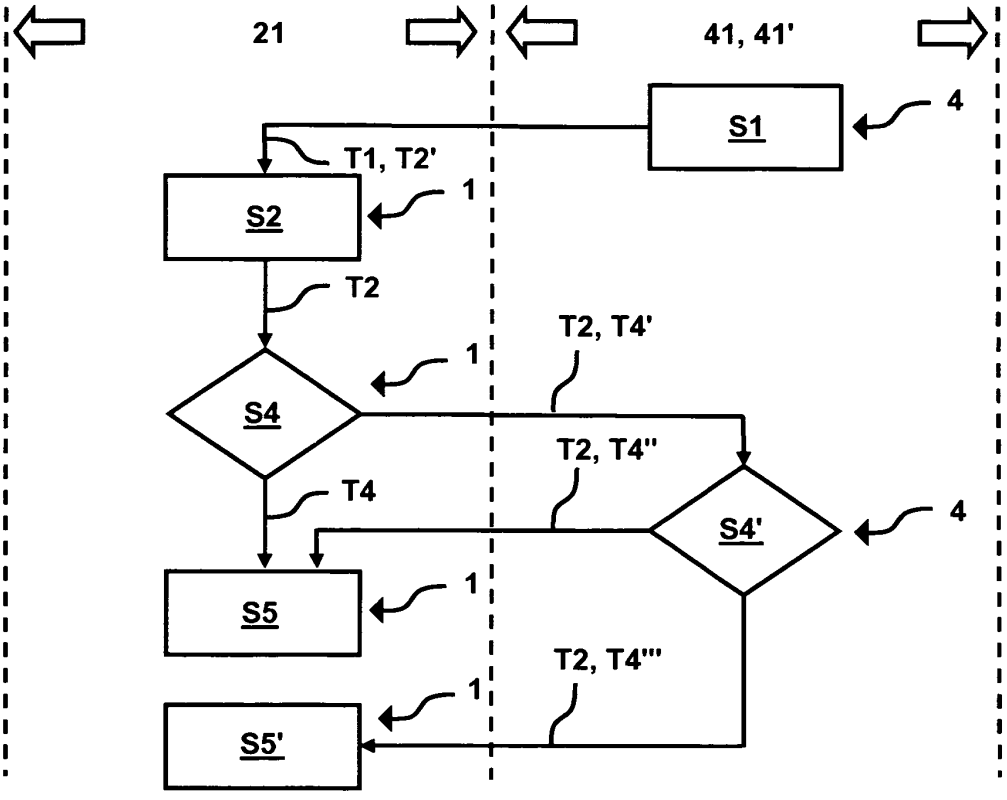
21
41, 41'
S1
4
T1, T2'
S2
1
T2
T2, T4'
S4
1
T2, T4''
T4
S4'
4
S5
1
T2, T4'''
S5'
1

Fig. 5

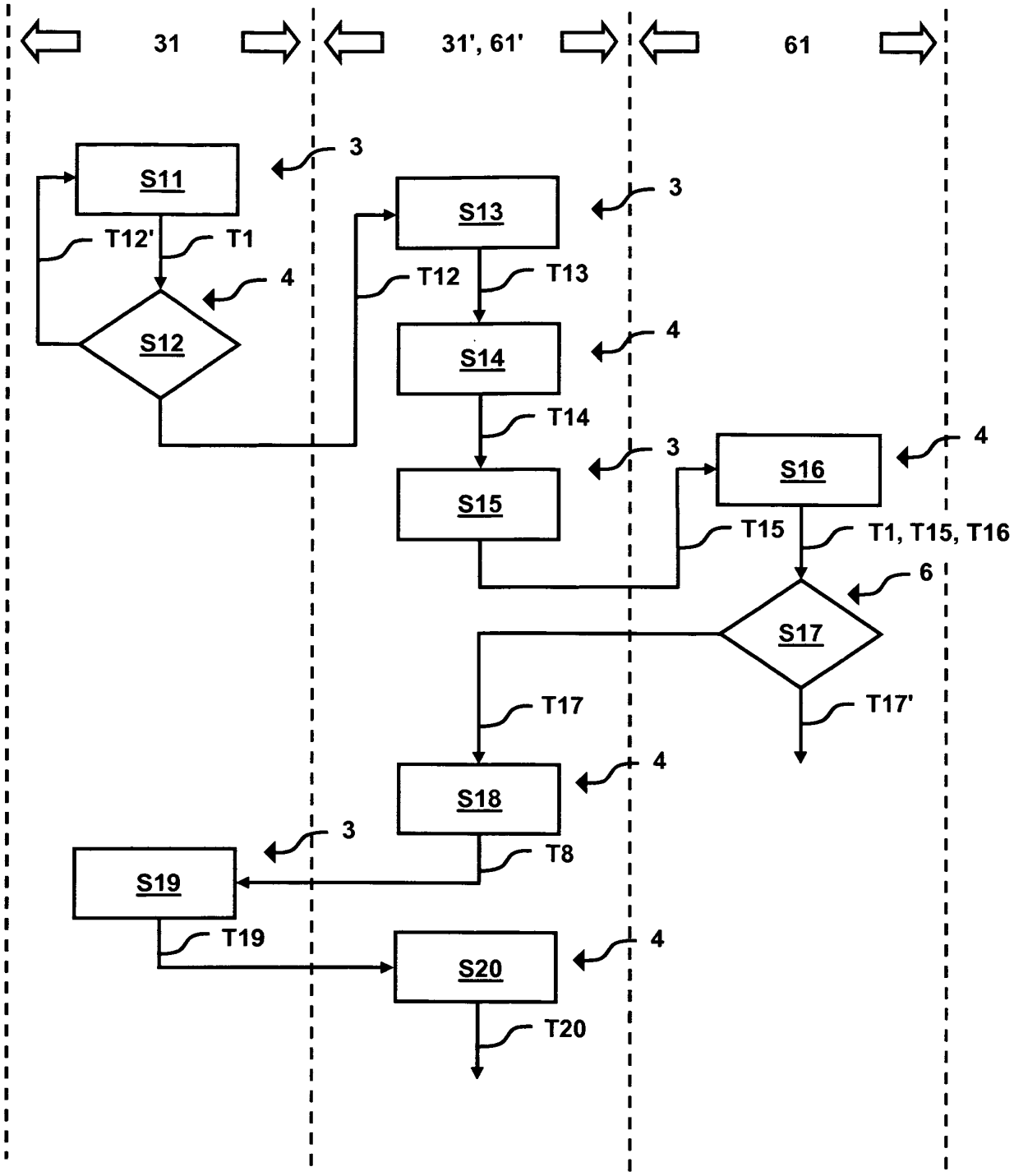
31
31', 61'
61
S11
S12
S13
S14
S15
S16
S17
S18
S19
S20
3
4
6
T12'
T1
T12
T13
T14
T15
T1, T15, T16
T17
T17'
T8
T19
T20

Fig. 6

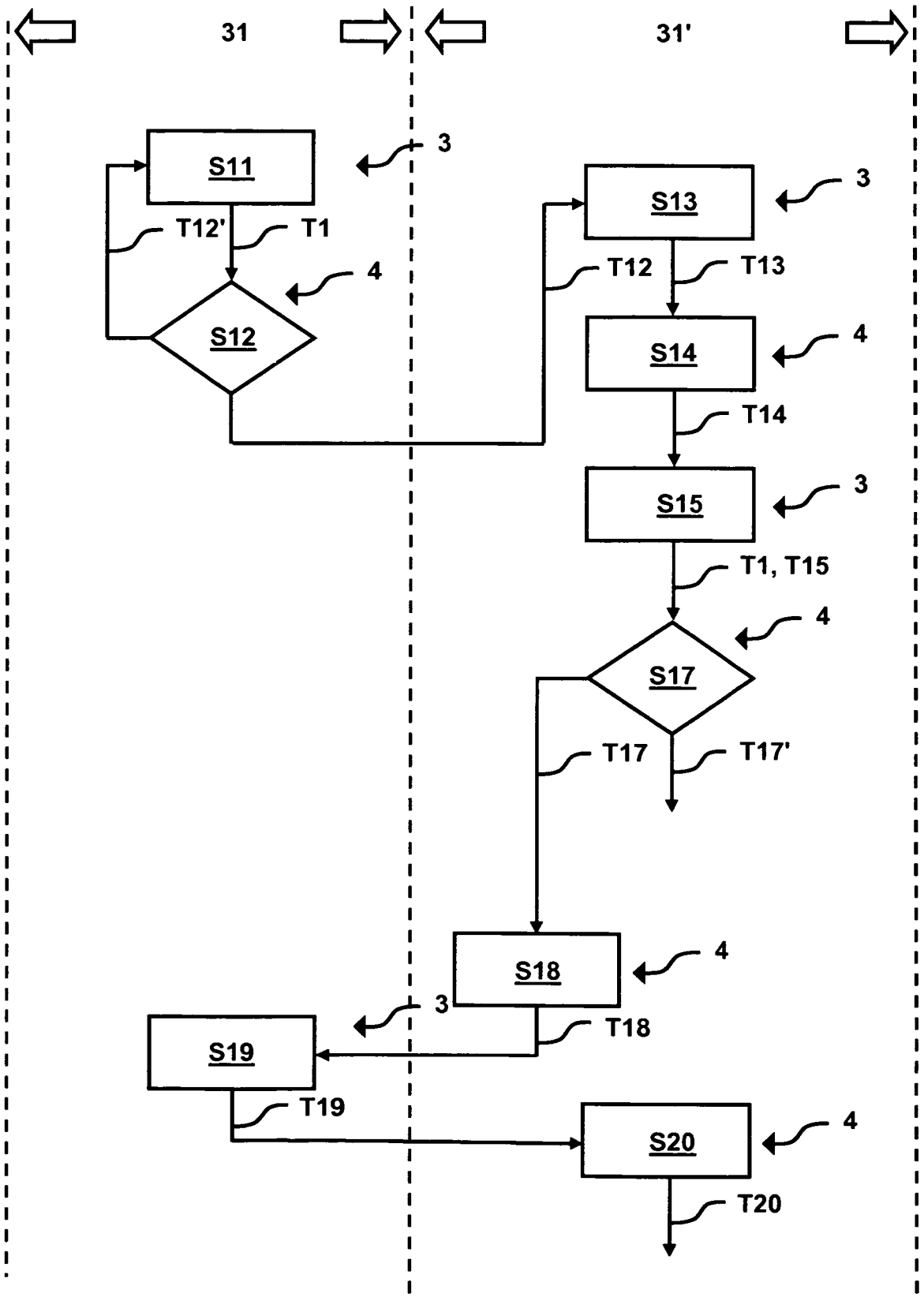
31
31'
S11
3
T12'
T1
4
S12
S13
3
T12
T13
S14
4
T14
S15
3
T1, T15
4
S17
T17
T17'
S18
4
3
T18
S19
T19
S20
4
T20

Fig. 7

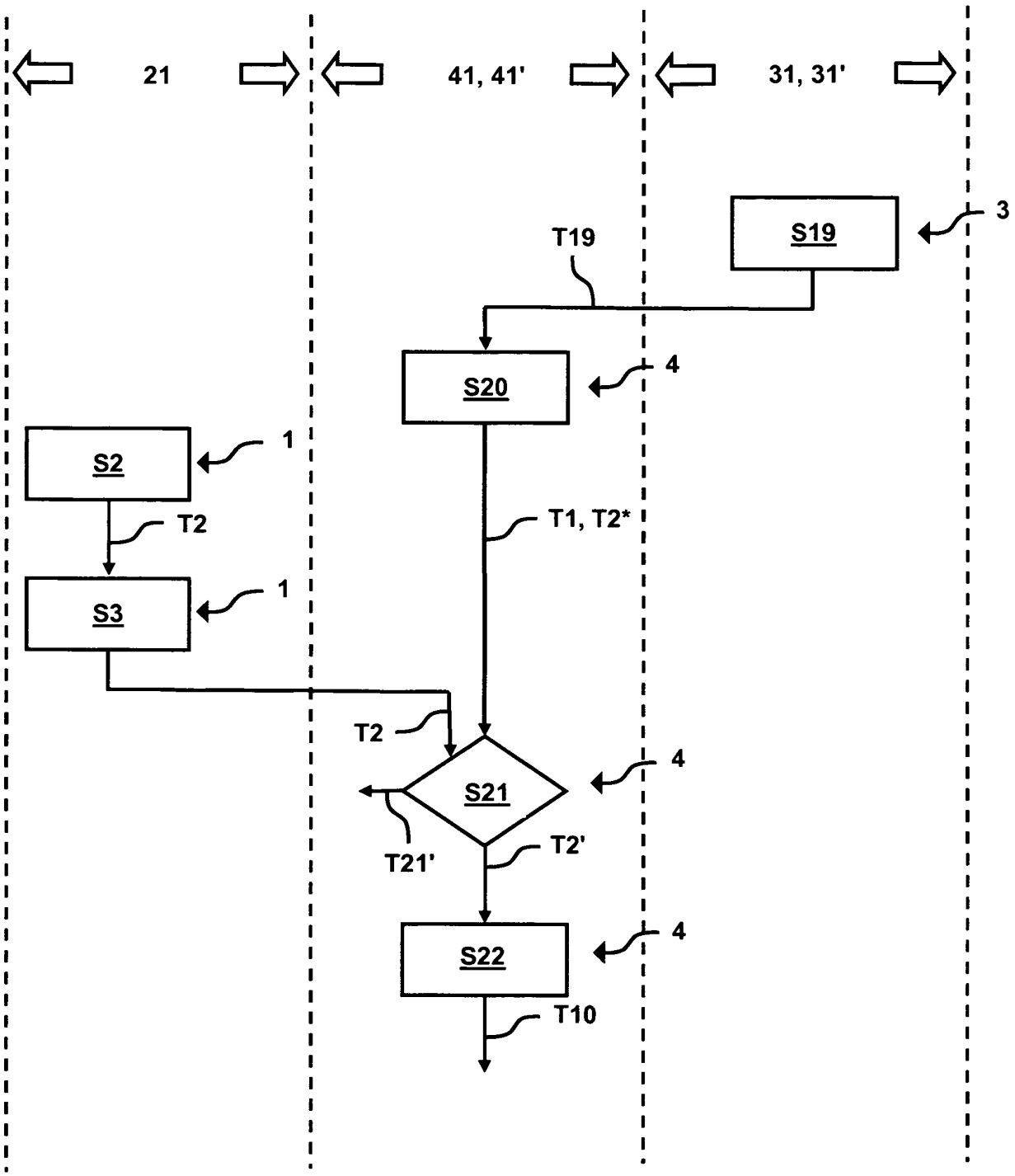
21
41, 41'
31, 31'
S19
3
T19
S20
4
S2
1
T1, T2*
T2
S3
1
T2
S21
4
T21'
T2'
S22
4
T10

Fig. 8

IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

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

In der Beschreibung aufgeführte Patentdokumente

- WO 2008089207 A1 **[0002]**
- WO 2006056085 A1 **[0003]**