



(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:  
**15.11.2023 Patentblatt 2023/46**

(51) Internationale Patentklassifikation (IPC):  
**B66B 5/00 (2006.01)**

(21) Anmeldenummer: **22172517.9**

(52) Gemeinsame Patentklassifikation (CPC):  
**B66B 5/0087**

(22) Anmeldetag: **10.05.2022**

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

(71) Anmelder: **INVENTIO AG**  
**6052 Hergiswil (CH)**

(72) Erfinder: **Colombano, Claudio**  
**6375 Beckenried (CH)**

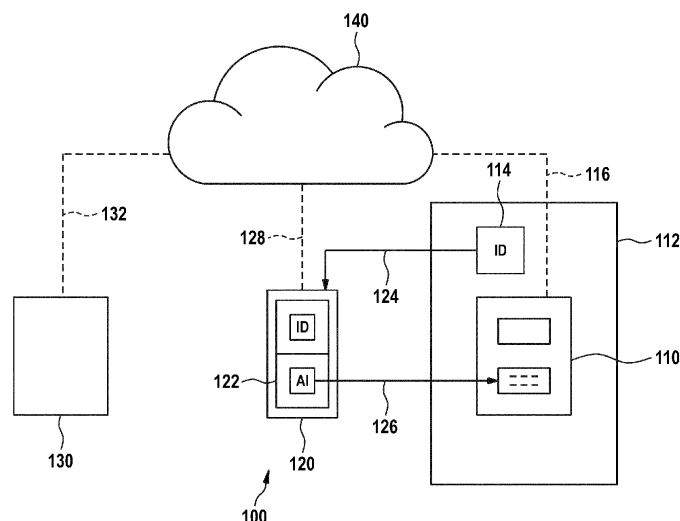
(74) Vertreter: **Inventio AG**  
**Seestrasse 55**  
**6052 Hergiswil (CH)**

(54) **METHODE UND AUTHENTIFIZIERUNGSSYSTEM ZUR ZUGRIFFSKONTROLLE EINER SCHNITTSTELLE ZUR WARTUNG EINER PERSONENBEFÖRDERUNGSEINRICHTUNG**

(57) Methode zur Zugriffskontrolle einer Schnittstelle zur Wartung einer Personenbeförderungseinrichtung in Form eines Fahrstuhls, Fahrsteigs oder einer Fahrtreppe, wobei ein mit der der Schnittstelle assoziierter Identifizierungs-Indikator zur Identifizierung der Schnittstelle vorgesehen ist; umfassend: Übermitteln einer Anfrage an eine Authentifizierungs-Infrastruktur mit einem Kommunikationsgerät, wobei die Anfrage ein Identifizierungs-Token beinhaltet, und wobei das Identifizierungs-Token auf Basis des Identifizierungs-Indikators erstellt ist; Verarbeiten der Anfrage mit der Authentifizierungs-Infrastruktur; Übermitteln eines Authentifizierungstokens an das Kommunikationsgerät durch die Authentifizierungs-Infrastruktur; Übermitteln eines Berechtigungs-Tokens an die Schnittstelle durch die Au-

thentifizierungs-Infrastruktur, wobei das Berechtigungs-Token das Authentifizierungstoken umfasst; Wiedergabe eines Authentifizierungs-Indikators mit dem Kommunikationsgerät, wobei der Authentifizierungs-Indikator auf Basis des Authentifizierungstokens erstellt ist; Eingabe des Authentifizierungs-Indikators an einer Eingabeeinrichtung der Schnittstelle; Überprüfen des Authentifizierungs-Indikators mit der Schnittstelle, umfassend: einen Abgleich des Authentifizierungs-Indikators mit dem Berechtigungs-Token, und eine Auswahl einer Berechtigungsstufe auf Basis des Berechtigungs-Tokens; und Wechsel der Schnittstelle in einen Wartungsmodus auf Basis des Abgleichs und der Berechtigungsstufe.

**Fig. 1**



## Beschreibung

**[0001]** Die Erfindung liegt auf dem Gebiet der Personenbeförderungseinrichtungen in Form eines Fahrstuhls, Fahrsteigs oder einer Fahrtreppe und der Zugriffskontrolle einer Schnittstelle zur Wartung der Personenbeförderungseinrichtung. Die Erfindung betrifft insbesondere die Verbesserung der Sicherheit der Zugriffskontrolle, sowie die Verwendung von Berechtigungsstufen.

**[0002]** Bekannte Personenbeförderungseinrichtungen wie Fahrstühle, Fahrteige und Fahrtreppen müssen hohen Sicherheitsstandards genügen. Personenbeförderungseinrichtungen umfassen dazu Komponenten zur Steuerung und/oder Überwachung, die beispielsweise in Steuerschränken vorgesehen sind. Moderne Einrichtungen umfassen dazu häufig mikroprozessor- oder speicherprogrammierbare Steuerkomponenten. Zur Wartung solcher Steuerkomponenten ist in der Regel eine der Steuerkomponente zugeordnete Schnittstelle vorgesehen, über die Wartungspersonal vor Ort beispielsweise Betriebszustände ablesen oder Eingaben tätigen kann, beispielsweise um Betriebsparameter zu überprüfen oder zu ändern.

**[0003]** Die Zugriffskontrolle derartiger Schnittstellen und/oder Komponenten ist in manchen Fällen unzureichend. Beispielsweise ist häufig die Eingabe eines Passworts an der Schnittstelle vorgesehen, um Zugriff auf die Steuerkomponente zu erhalten. Werden jedoch einfache Passwörter oder Standardpasswörter vergeben oder werksseitig vergebene Passwörter nicht geändert, kann es in nachteiliger Weise dazu kommen, dass unberechtigte Personengruppen Zugang zu sensiblen Wartungsfunktionen erhalten. Gleichermäßen kann es unvorteilhaft sein, für wenig sensible Wartungsfunktionen, wie beispielsweise die Anzeige von Betriebsparametern, durch die Eingabe des Passworts gleichzeitig Zugriff auf sicherheitsrelevante Funktionen, beispielsweise die Änderung von sicherheitsrelevanten Parametern, zu erhalten.

**[0004]** Die Erfindung ergibt sich aus den unabhängigen Ansprüchen und löst die genannten Probleme zumindest teilweise. Besonders vorteilhafte Weiterbildungen ergeben sich aus den abhängigen Ansprüchen und den im Folgenden beschriebenen Ausführungsformen.

**[0005]** Gemäß einem Aspekt ist eine Methode zur Zugriffskontrolle einer Schnittstelle zur Wartung einer Personenbeförderungseinrichtung in Form eines Fahrstuhls, Fahrsteigs oder einer Fahrtreppe beschrieben. Es ist ein mit der der Schnittstelle assoziierter Identifizierungs-Indikator zur Identifizierung der Schnittstelle vorgesehen. Die Methode umfasst das Übermitteln einer Anfrage an eine Authentifizierungs-Infrastruktur mit einem Kommunikationsgerät. Die Anfrage beinhaltet ein Identifizierungs-Token. Das Identifizierungs-Token ist auf Basis des Identifizierungs-Indikators erstellt. Die Methode umfasst weiterhin das Verarbeiten der Anfrage mit der Authentifizierungs-Infrastruktur, das Übermitteln ei-

nes Authentifizierungs-Tokens an das Kommunikationsgerät durch die Authentifizierungs-Infrastruktur, und das Übermitteln eines Berechtigungs-Tokens an die Schnittstelle durch die Authentifizierungs-Infrastruktur. Das Berechtigungs-Token beinhaltet das Authentifizierungs-Token. Die Methode umfasst die Wiedergabe eines Authentifizierungs-Indikators mit dem Kommunikationsgerät. Der Authentifizierungs-Indikator ist auf Basis des Authentifizierungs-Tokens erstellt. Die Methode umfasst die Eingabe des Authentifizierungs-Indikators an einer Eingabeeinrichtung der Schnittstelle und das Überprüfen des Authentifizierungs-Indikators mit der Schnittstelle. Das Überprüfen des Authentifizierungs-Indikators umfasst einen Abgleich des Authentifizierungs-Indikators mit dem Berechtigungs-Token, und eine Auswahl einer Berechtigungsstufe auf Basis des Berechtigungs-Tokens. Die Methode umfasst den Wechsel der Schnittstelle in einen Wartungsmodus auf Basis des Abgleichs und der Berechtigungsstufe.

**[0006]** Gemäß einem Aspekt ist ein Authentifizierungssystem zur Zugriffskontrolle einer Schnittstelle zur Wartung einer Personenbeförderungseinrichtung in Form eines Fahrstuhls, Fahrsteigs oder einer Fahrtreppe beschrieben. Das Authentifizierungssystem umfasst ein Kommunikationsgerät, die Schnittstelle und eine Authentifizierungs-Infrastruktur. Die Schnittstelle umfasst einen mit der der Schnittstelle assoziierten Identifizierungs-Indikator zur Identifizierung der Schnittstelle, sowie eine Eingabeeinrichtung zur Eingabe eines Authentifizierungs-Indikators an einer Eingabeeinrichtung der Schnittstelle. Die Schnittstelle ist dazu eingerichtet, ein Berechtigungs-Token von der Authentifizierungs-Infrastruktur zu empfangen, den Authentifizierungs-Indikator zu überprüfen, wobei die Überprüfung einen Abgleich des Authentifizierungs-Indikators mit dem Berechtigungs-Token und eine Auswahl einer Berechtigungsstufe auf Basis des Berechtigungs-Tokens umfasst, und auf Basis des Abgleichs und der Berechtigungsstufe in einen Wartungsmodus zu wechseln. Das Kommunikationsgerät ist dazu eingerichtet ist, den Identifizierungs-Indikator einzulesen, und eine Anfrage zu generieren. Die Anfrage beinhaltet ein Identifizierungs-Token. Das Identifizierungs-Token ist auf Basis des Identifizierungs-Indikators erstellt. Das Kommunikationsgerät ist dazu eingerichtet, die Anfrage an die Authentifizierungs-Infrastruktur zu übermitteln, ein Authentifizierungs-Token von der Authentifizierungs-Infrastruktur zu empfangen, einen Authentifizierungs-Indikator auf Basis des Authentifizierungs-Tokens zu generieren, und den Authentifizierungs-Indikator wiederzugeben. Die Authentifizierungs-Infrastruktur ist dazu eingerichtet, die Anfrage von dem Kommunikationssystem zu empfangen, das Authentifizierungs-Token auf Basis des Identifizierungs-Tokens zu generieren und das Authentifizierungs-Token an das Kommunikationsgerät zu übermitteln, das Berechtigungs-Token zu generieren, wobei das Berechtigungs-Token das Authentifizierungs-Token umfasst, und das Berechtigungs-Token an die Schnittstelle zu übermitteln.

**[0007]** Gemäß einem Aspekt ist ein Computerprogrammprodukt zur Ausführung auf einer Schnittstelle zur Wartung einer Personenbeförderungseinrichtung in Form eines Fahrstuhls, Fahrsteigs oder einer Fahrtreppe, beschrieben. Das Computerprogrammprodukt umfasst Befehle, die bei der Ausführung des Programms durch die Schnittstelle diese veranlassen, die folgenden Schritte auszuführen: Empfangen eines Berechtigungs-Tokens von einer Authentifizierungs-Infrastruktur, Überprüfen eines eingegebenen Authentifizierung-Indikators, wobei die Überprüfung einen Abgleich des Authentifizierung-Indikators mit dem Berechtigungs-Token und eine Auswahl einer Berechtigungsstufe auf Basis des Berechtigungs-Tokens umfasst, und Wechsel in einen Wartungsmodus auf Basis des Abgleichs und der Berechtigungsstufe.

**[0008]** Gemäß einem Aspekt ist eine Schnittstelle beschrieben. Die Schnittstelle kann eine Schnittstelle einer Überwachungs- und/oder Steuerkomponente ("Komponente") einer Personenbeförderungseinrichtung sein, beispielsweise eines Controllers oder eines Sicherheitsmoduls. Die Schnittstelle kann von der Komponente getrennt oder trennbar sein. Die Schnittstelle kann in die Komponente integriert sein. Die Komponente kann die Schnittstelle umfassen, beispielsweise kann die Schnittstelle in einem gemeinsamen Gehäuse oder auf einer gemeinsamen Platine der Komponente vorgesehen sein. Bei der Komponente und der Schnittstelle kann es sich um ein eingebettetes System handeln. Funktionen der Schnittstelle, insbesondere die hierin beschriebenen Funktionen, können zumindest teilweise in der Komponente implementiert sein bzw. von dieser ausgeführt werden.

**[0009]** Gemäß einem Aspekt umfasst die Schnittstelle eine Eingabeeinrichtung, beispielsweise einen oder mehrere Tasten, ein Keypad, eine Tastatur, einen Touchscreen, ein Jog Dial oder dergleichen. Die Eingabeeinrichtung ist zur Eingabe eines Authentifizierung-Indikators geeignet, beispielsweise in Form eines Passworts in Form einer Zeichenfolge, Ziffernfolge, Symbolfolge, oder einer sonstigen Ausgestaltungsform einer eindeutig identifizierbaren Abfolge von Eingaben, beispielsweise eine Abfolge von Drehrichtungen und Klicks des Jog Dials.

**[0010]** Gemäß einem Aspekt kann die Schnittstelle eine Ausgabeeinrichtung, insbesondere eine Anzeigeeinrichtung umfassen, beispielsweise ein Display, ein oder mehrere Indikatorlichter, und/oder akustische Signalgeber. Durch die Ausgabeeinrichtung können beispielsweise das Resultat der Zugriffskontrolle, z.B. «Zugang erteilt» oder «Zugang nicht erteilt» ausgegeben werden, sowie beispielsweise Menüsteuerung, Ausgaben oder Wartungsfunktionen der Komponente für den Nutzer zur Verfügung gestellt werden.

**[0011]** Gemäß einem Aspekt ist ein Kommunikationsgerät beschrieben. Bei dem Kommunikationsgerät kann es sich um ein tragbares Gerät handeln, das einem Nutzer zumindest zeitweise eindeutig zuordenbar ist, bei-

spielsweise durch Besitz oder alleinige Zugriffsmöglichkeit des Nutzers. Durch die eindeutige Zuordenbarkeit kann für jeden Nutzer die vorgesehene Berechtigungsstufe des Nutzers durch Einrichten des Kommunikationsgerätes möglich sein. Geeignete Kommunikationsgeräte umfassen Passwort-Generatoren mit Kommunikationsfunktion, tragbare Computer wie beispielsweise Laptops, Tablets und/oder Smartwatches. Bei dem Kommunikationsgerät kann es sich insbesondere um ein Smartphone handeln. Das Kommunikationsgerät kann beispielsweise durch die Ausführung eines Programms oder einer Software ("App") dazu geeignet sein, die hierin beschriebenen Funktionen auszuführen. Das Kommunikationsgerät ist dazu geeignet, einen Authentifizierung-Indikator wiederzugeben. Vorteilhafterweise umfasst das Kommunikationsgerät zur Wiedergabe ein Display das zur Anzeige des Authentifizierung-Indikators geeignet ist, und/oder eine sonstige Ausgabeeinrichtung, beispielsweise akustische Signalgeber. Das Kommunikationsgerät ist dazu geeignet, einen Identifizierungs-Indikator einzulesen. Einlesen des Identifizierungs-Indikators kann vorteilhafterweise das Einlesen beispielsweise eines optischen Codes mit einem optischen Sensor des Kommunikationsgerätes umfassen, jedoch kann ein Identifizierungs-indikator in Ausführungsformen auch händisch eingegeben werden, beispielsweise über eine Eingabeeinrichtung des Kommunikationsgerätes, wie z.B. ein Keypad oder ein Touchscreen.

**[0012]** Gemäß einem Aspekt ist eine Authentifizierungs-Infrastruktur beschrieben. Die Authentifizierungs-Infrastruktur kann zumindest eine Datenverarbeitungsanlage, beispielsweise einen oder mehrere Computer umfassen. Die Authentifizierungs-Infrastruktur kann durch ein auf der Datenverarbeitungsanlage ausgeführtes Programm oder eine Software dazu eingerichtet sein, die hierin beschriebenen Funktionen des Authentifizierung-Systems auszuführen. Die Authentifizierungs-Infrastruktur kann beispielsweise in Form eines serverbasierten Dienstes, insbesondere eines Cloud-Dienstes, implementiert sein. Die Authentifizierungs-Infrastruktur kann von der Personenbeförderungseinrichtung und/oder der Schnittstelle ortsunabhängig sein.

**[0013]** Gemäß einem Aspekt sind das Kommunikationsgerät, die Authentifizierungs-Infrastruktur und die Schnittstelle zur Kommunikation eingerichtet bzw. umfassen eine Kommunikationsfunktion, sind also kommunikativ verbunden, insbesondere zum Austausch von Daten oder Datenpaketen, wobei die Daten insbesondere die hierin beschriebenen Token (Identifizierungs-Token, Authentifizierungs-Token, Berechtigungs-Token) enthalten können. Insbesondere können das Kommunikationsgerät und die Authentifizierungs-Infrastruktur untereinander Daten senden und empfangen. Insbesondere können die Schnittstelle und die Authentifizierungs-Infrastruktur kommunikativ so verbunden sein, dass Daten von der Authentifizierungs-Infrastruktur an die Schnittstelle übermittelbar und die Daten von der Schnittstelle empfangbar sind. Die Eingabe des Authentifizie-

rung-Indikators an einer Eingabeeinrichtung der Schnittstelle wird in diesem Zusammenhang nicht als kommunikative Verbindung zum Austausch von Daten verstanden. Der Austausch von Daten kann einer *Internet-of-Things*-Kommunikation (IoT) entsprechen, insbesondere kann, beispielsweise durch Verschlüsselung der Daten, beispielsweise durch Endezu-Ende Verschlüsselung und/oder Zertifikat-basierte Authentifizierung, eine sichere Kommunikation vorgesehen sein. Mögliche Sicherheitsstandards umfassen *Standard Trusted Network Connect* und *Mutual Authentication*.

**[0014]** In Ausführungsformen umfassen das Kommunikationsgerät, die Authentifizierungs-Infrastruktur und die Schnittstelle jeweils zumindest ein Netzwerkmodul zum Austausch der Daten. Die Netzwerkmodule können beispielsweise Netzwerkadapter umfassen und zur Anbindung an ein Datennetzwerk und/oder Kommunikationsnetzwerk vorgesehen sein. Das Datennetzwerk kann dazu eingerichtet sein, eine Kommunikation des Kommunikationsgeräts, der Schnittstelle und der Authentifizierungs-Infrastruktur untereinander zu ermöglichen. Die Netzwerkmodule können zur drahtlosen oder drahtgebundenen Kommunikation bestimmt sein. Die Netzwerkmodule können eine kommunikative Verbindung mit einem paketbasierten Datennetzwerk ermöglichen, beispielsweise einem lokalen Netzwerk und/oder dem Internet. Die Authentifizierungs-Infrastruktur kann vorteilhafterweise über ein Netzwerkmodul mit dem Internet verbunden sein. Die Schnittstelle kann vorteilhafterweise über ein Netzwerkmodul mit einem lokalen Datennetzwerk, beispielsweise einem für die Personenbeförderungseinrichtung vorgesehenen Datennetzwerk verbunden werden, wobei die Personenbeförderungseinrichtung eine *edge device*, beispielsweise einen Gateway zur Anbindung des lokalen Datennetzwerks an das Internet umfassen kann, über die eine Datenübertragung zwischen der Schnittstelle und dem Internet möglich ist. Die Schnittstelle und/oder das Kommunikationsgerät können, insbesondere zur Verbindung mit dem Internet, ein Netzwerkmodul zur Kommunikation mit einem drahtlosen Netzwerk umfassen, beispielsweise ein W-LAN Interface, ein Mobilfunk-Interface wie etwa ein 2G, 3G, 4G, LTE und/oder 5G-Interface, zur Kommunikation mit einem drahtlosen Netzwerk oder Mobilfunknetzwerk. Über das drahtlose Netzwerk und/oder das Mobilfunknetzwerk kann eine Verbindung mit dem Internet möglich sein.

**[0015]** Gemäß einem Aspekt ist ein Identifizierungs-Indikator beschrieben. Der Identifizierungs-Indikator umfasst Information zur Identifizierung der Schnittstelle. Der Identifizierungs-Indikator kann beispielsweise Information enthalten, die eine eindeutige Identifizierung der Schnittstelle ermöglicht, beispielsweise eine Seriennummer der Personenbeförderungseinrichtung und/oder der Schnittstelle, ein zuvor vergebener Zufallswert, eine MAC-Adresse der Schnittstelle oder ein für die Schnittstelle eingestellter Wert. Der Identifizierungs-Indikator kann sichtbar sein, insbesondere für Wartungspersonal, das sich in Nähe der Schnittstelle zur Wartung der Per-

sonenbeförderungseinrichtung befindet. Der Identifizierungs-Indikator kann ohne Berechtigung, oder sogar ohne Zugriff auf die Schnittstelle einlesbar sein, beispielsweise ohne die Schnittstelle in einen Wartungsmodus zu wechseln. In Ausführungsformen kann der Identifizierungs-Indikator beispielsweise auf einem Display der Schnittstelle angezeigt werden. In weiteren Ausführungsformen kann der Identifizierungs-Indikator in räumlicher Nähe der Schnittstelle, beispielsweise an einem Gehäuseteil der Schnittstelle, und/oder beispielsweise in oder an einem Steuerschrank, in dem sich die Schnittstelle befindet, vorgesehen sein, beispielsweise durch Anbringen eines Labels, beispielsweise eines Druckerzeugnisses, beispielsweise eines Aufklebers. In Ausführungsformen kann der Identifizierungs-Indikator eine Zeichenfolge umfassen, beispielsweise eine menschenlesbare Zeichenfolge, die beispielsweise von einem Wartungsmechaniker lesbar und in das Kommunikationsgerät eingebbar ist. In bevorzugten Ausführungsformen kann der Identifizierungs-Indikator, alternativ dazu oder zusätzlich, in maschinenlesbarer Form vorgesehen sein. Beispielsweise kann der Identifizierungs-Indikator in optisch erfassbarer Form vorgesehen sein, beispielsweise in Form eines Strichcodes oder Matrix-Codes. Vorteilhafterweise kann der Identifizierungs-Indikator eine sichtbare Kennzeichnung in Form eines QR-Codes umfassen. Weitere sichtbare Kennzeichnungen bzw. Codes umfassen DataMatrix, MaxiCode, Aztec-Code, JAB-Code, Han-Xin-Code, Dotcode und sonstige optoelektronisch lesbare Schriften.

**[0016]** Gemäß einem Aspekt ist das Kommunikationsgerät dazu eingerichtet, den Identifizierungs-Indikator einzulesen. Das Einlesen des Identifizierungs-Indikators kann eine menschliche Eingabe umfassen. Vorteilhafterweise kann das Einlesen die optische Erfassung einer sichtbaren Kennzeichnung des Identifizierungs-Indikators umfassen. Dazu kann das Kommunikationsgerät einen optischen Sensor, beispielsweise eine Kamera oder einen Kamerascanner, zur Erfassung der sichtbaren Kennzeichnung umfassen und für die Decodierung der sichtbaren Kennzeichnung eingerichtet sein, um aus der sichtbaren Kennzeichnung den Identifizierungs-Indikator abzuleiten. Insbesondere kann zur Decodierung eine App vorgesehen sein.

**[0017]** Gemäß einem Aspekt ist das Kommunikationsgerät dazu eingerichtet, eine Anfrage zu generieren und die Anfrage an eine Authentifizierungs-Infrastruktur zu übermitteln. Gemäß einem Aspekt umfasst die hierin beschriebene Methode das Übermitteln der Anfrage an die Authentifizierungs-Infrastruktur. Die Übermittlung kann über die hierin beschriebenen kommunikativen Verbindungen erfolgen. Insbesondere kann die Übermittlung über das Internet erfolgen. Die Anfrage umfasst ein Identifizierungs-Token. Das Identifizierungs-Token ist auf Basis des Identifizierungs-Indikators erstellt. Beispielsweise kann das Identifizierungs-Token den Identifizierungs-Indikator umfassen, sodass die Schnittstelle auf Basis des Identifizierungs-Indikators für die Authentifizierungs-

Infrastruktur eindeutig identifizierbar ist.

**[0018]** Gemäß einem Aspekt ist eine Authentifizierungs-Infrastruktur beschrieben. Die Authentifizierungs-Infrastruktur ist dazu eingerichtet, die Anfrage von dem Kommunikationssystem zu empfangen. Gemäß einem Aspekt umfasst die hierin beschriebene Methode die Verarbeitung der Anfrage. Die Authentifizierungs-Infrastruktur ist, insbesondere zur Verarbeitung der Anfrage, dazu eingerichtet, ein Authentifizierungs-Token auf Basis des Identifizierungs-Tokens zu generieren und ein Berechtigungs-Token zu generieren. Das Berechtigungs-Token umfasst das Authentifizierungs-Token. In Ausführungsformen ist das Berechtigungs-Token identisch zum Authentifizierungs-Token. In weiteren Ausführungsformen umfasst das Berechtigungs-Token zusätzliche Informationen, insbesondere Informationen, auf deren Basis eine Berechtigungsstufe ausgewählt werden kann, wie beispielsweise den im Folgenden beschriebenen Berechtigungs-Indikator oder eine Information, die aus dem Berechtigungs-Indikator abgeleitet ist.

**[0019]** Gemäß einem Aspekt ist die Authentifizierungs-Infrastruktur dazu eingerichtet, in Folge der Verarbeitung der Anfrage das Authentifizierungs-Token an das Kommunikations-Gerät zu übermitteln und das Berechtigungs-Token an die Schnittstelle zu übermitteln. Die Übermittlung kann über die hierin beschriebenen kommunikativen Verbindungen erfolgen. Insbesondere kann die Übermittlung über das Internet erfolgen.

**[0020]** Gemäß einem Aspekt ist der Wechsel der Schnittstelle in einen Wartungsmodus beschrieben. Der Wechsel findet auf Basis eines Abgleichs des Authentifizierungs-Indikators mit dem Berechtigungs-Token, sowie einer Auswahl einer Berechtigungs-Stufe auf Basis des Berechtigungs-Tokens und/oder des Abgleichs statt. Gemäß einem Aspekt kann ein Authentifizierungs-Indikator, für das der Abgleich mit dem Berechtigungs-Token keine Übereinstimmung ergibt, eine Berechtigungsstufe ohne Berechtigung bedeuten. Gemäß einem Aspekt kann ein Authentifizierungs-Indikator, für das der Abgleich mit dem Berechtigungs-Token eine Übereinstimmung ergibt, eine Berechtigungsstufe aus einer Vielzahl von Berechtigungsstufen bedeuten. In einem ersten Ausführungsbeispiel kann ein erfolgreicher Abgleich des Authentifizierungs-Indikators mit dem Berechtigungs-Token direkt die Vergabe einer Berechtigungsstufe, beispielsweise Vollzugriff, bedeuten. Insbesondere kann der Berechtigungs-Indikator Information zur vorgesehenen Berechtigungsstufe umfassen, sodass die Schnittstelle in die durch das Berechtigungs-Token vorgegebene Wartungsstufe wechselt. Mögliche Berechtigungsstufen, die aus dem Berechtigungstoken abgeleitet werden können, umfassen beispielsweise keine Berechtigung, etwa wenn für das Kommunikationsgerät keine Berechtigung vorgesehen ist. In diesem Fall kann die Wartungsstufe etwa dem Zustand entsprechen, den die Schnittstelle aufweist, wenn keine Berechtigung vorliegt. Gleichermäßen können Wartungsstufen mit Teilberechtigungen, wie beispielsweise beschränkte Zugriffsrechte, wie etwa

ausschließliche Leseberechtigung, oder volle Zugriffsrechte, wie beispielsweise Schreib-/Leseberechtigung vorgesehen sein. In Ausführungsformen können für Teilfunktionen, oder sogar für jede einzelne Funktion, die dem Wartungspersonal für die jeweilige Schnittstelle zur Verfügung stehen, getrennte Berechtigungen vergeben werden.

**[0021]** Gemäß einem Aspekt umfasst die hierin beschriebene Methode das Einrichten des Kommunikationsgeräts. Das Einrichten umfasst die Speicherung eines Berechtigungs-Indikators in einem Speicher des Kommunikationsgeräts. Der Berechtigungs-Indikator ist indikativ für die Berechtigungsstufe eines Nutzers. Das Identifizierungs-Token kann auf Basis des Berechtigungs-Indikators erstellt sein. Beispielsweise kann das Einrichten des Geräts die Installation einer App umfassen, sowie die Vergabe von Berechtigungsstufen, beispielsweise in einer App des Kommunikationsgeräts oder eines weiteren Kommunikationsgeräts, oder sogar in einem Administrationssystem, beispielsweise durch einen Administrator, der zur Vergabe der Berechtigungsstufen berechtigt ist. Vorteilhafterweise kann ein mit der Wartung von einer oder mehreren Personenbeförderungseinrichtungen beauftragter Administrator so für jede Person des Wartungspersonals ("Nutzer") gezielt Berechtigungen, beispielsweise in Abhängigkeit der Befähigung der Person des Wartungspersonals, vergeben. Beispielsweise kann ein Auszubildender für das ihm zugewiesene Kommunikationsgerät Leseberechtigung für ein oder mehrere Schnittstellen erhalten, während ein vollbefähigter Wartungsmechaniker Schreib-/Leseberechtigungen für ein oder mehrere Schnittstellen erhalten kann.

**[0022]** Das Identifizierungs-Token kann den Berechtigungs-Indikator umfassen, sodass dieser zusammen mit der Anfrage an die Authentifizierungs-Infrastruktur übermittelt wird und die Berechtigungsstufe für die Authentifizierungs-Infrastruktur somit direkt ermittelbar ist. Gleichermäßen kann der Berechtigungs-Indikator einen Identifikator des Kommunikationsgeräts umfassen, und die Authentifizierungs-Infrastruktur eine Datenbank umfassen, in der für eine Vielzahl von Identifikatoren von Kommunikationsgeräten Berechtigungen, vorzugsweise für die jeweilige Schnittstelle, hinterlegt sind, sodass auf Basis des Berechtigungs-Indikators durch die Authentifizierungs-Infrastruktur, beispielsweise während der Verarbeitung der Anfrage, die jeweilige Berechtigungsstufe durch Zugriff auf die Datenbank ermittelbar ist. Einträge der Datenbank können beispielsweise durch einen Administrator, z.B. dezentral, oder bei Einrichtung des Kommunikationsgeräts statt oder zusätzlich zur Speicherung des Berechtigungs-Indikators in dem Speicher des Kommunikationsgeräts in der Datenbank gespeichert werden.

**[0023]** Gemäß einem Aspekt umfasst die hierin beschriebene Verarbeitung der Anfrage die Generierung eines Zufallswerts. Der Zufallswert kann insbesondere durch die Authentifizierungs-Infrastruktur generiert wer-

den, beispielsweise durch einen Zufallsgenerator. Die Generierung des Authentifizierungs-Tokens und des Berechtigungs-Tokens kann auf Basis des Identifizierungs-Tokens und des Zufallswerts erfolgen. Beispielsweise kann der Zufallswert den Authentifizierung-Indikator umfassen oder der Authentifizierung-Indikator sein. Gleichmaßen kann der Zufallswert ein Wert sein, aus dem sich, insbesondere durch das Kommunikationsgerät und die Schnittstelle, ein Authentifizierung-Indikator ableiten lässt, und/oder durch das in der Schnittstelle ein Abgleich des Authentifizierung-Indikators mit dem Berechtigungs-Token möglich ist. Vorteilhafterweise kann für jede Anfrage ein neuer Zufallswert erzeugt werden, beispielsweise bei der Verarbeitung der Anfrage. So kann für jede Anfrage ein neuer Authentifizierung-Indikator erstellt werden. Dadurch kann beispielsweise der Authentifizierung-Indikator ein Einmalpasswort, eine Einmal-Kennzahl oder dergleichen sein und insbesondere potentielle Sicherheitslücken durch unberechtigte Weitergabe oder mehrmalige Verwendbarkeit vermieden werden.

**[0024]** Gemäß einem Aspekt erfolgt die Wiedergabe des Authentifizierung-Indikators in menschenlesbarer Form, beispielsweise über ein Display des Kommunikationsgeräts. Dies ermöglicht dem Wartungspersonal die Eingabe des Authentifizierung-Indikators an einer Eingabeeinrichtung der Schnittstelle, beispielsweise in Form eines Passworts in Form einer Zeichenfolge, Ziffernfolge, Symbolfolge, oder einer sonstigen Ausgestaltungsform einer eindeutig identifizierbaren Abfolge von Eingaben, beispielsweise eine Abfolge von Drehrichtungen und Klicks des Jog Dials. Das Kommunikationsgerät kann dazu eingerichtet sein, verschiedene Typen von Authentifizierung-Indikatoren anzuzeigen, insbesondere so, dass ein für die jeweilige Schnittstelle auf besonders günstig eingebbare Weise Authentifizierung-Indikator angezeigt werden. Beispielsweise kann der Authentifizierung-Indikator auf den Zeichensatz der Eingabeeinrichtung der Schnittstelle beschränkt sein. In einem Beispiel kann für eine Schnittstelle mit einer Eingabeeinrichtung, die ausschließlich Zahlen umfasst, ein Authentifizierung-Indikator bestehend ausschließlich aus Zahlen vorgesehen sein. Der zu wählende Zeichensatz kann in dem Identifizierungs-Indikator enthalten sein, von dem Wartungspersonal beispielsweise per Befehl gewählt werden, in einer Datenbank des Authentifizierungs-Systems hinterlegt sein oder durch Kommunikation zwischen der Schnittstelle und dem Authentifizierungs-System an das Authentifizierungs-System übermittelbar sein. Gleichmaßen können von dem Kommunikations-system aus dem Authentifizierungs-Token mehrere mögliche Authentifizierung-Indikatoren mit selbem oder ähnlichem Informationsgehalt wiedergegeben werden, die unterschiedlichen Zeichensätzen entsprechen und von dem Wartungspersonal für die jeweilige Schnittstelle ausgewählt werden können.

**[0025]** Gemäß einem Aspekt umfasst das Überprüfen des Authentifizierung-Indikators die Überprüfung, ob die Eingabe des Authentifizierung-Indikators innerhalb einer

vorbestimmten Zeitspanne erfolgt ist. Die vorbestimmte Zeitspanne kann einer Gültigkeitsdauer eines Passworts ab Erzeugung entsprechen. Beispielsweise kann die Zeitspanne etwa 30 Sekunden, eine Minute, zwei Minuten oder fünf Minuten betragen. Dadurch können die zuvor beschriebenen Vorteile eines Einmal-Passworts zusätzlich verstärkt werden, insbesondere indem dadurch keine Passwörter auf Vorrat erzeugt werden können.

**[0026]** Gemäß einem Aspekt umfasst das Überprüfen des Authentifizierung-Indikators die Überprüfung, ob die Eingabe des Authentifizierung-Indikators, insbesondere desselben Authentifizierung-Indikators, öfter als eine vorbestimmte Anzahl von Eingaben erfolgt ist. Beispielsweise kann, nach einer mehrmaligen Eingabe desselben Passworts, oder bereits nach einer zweimaligen Eingabe desselben oder eines falschen Passworts, ein Wechsel in einen Wartungsmodus mit mehr als keiner Berechtigung verhindert werden. Dadurch können die mehrmalige Verwendung desselben Passworts, sowie insbesondere *bruteforce*-Angriffe vermieden werden.

**[0027]** Gemäß einem Aspekt kann das Kommunikationsgerät eine Nutzeroberfläche umfassen. Die Nutzeroberfläche kann eine graphische Nutzeroberfläche sein. Die Nutzeroberfläche kann eine Nutzeroberfläche sein, die auf einem Display des Kommunikationsgeräts angezeigt wird. Die Nutzeroberfläche kann durch eine Software oder ein Programm, beispielsweise die hierin beschriebene App, generierbar sein. Die Nutzeroberfläche kann einem Nutzer, etwa einer Person des Wartungspersonals, die Beantragung von Zugangsrechten ermöglichen. Beispielsweise kann die Nutzeroberfläche hierzu eine Auswahlmöglichkeit, beispielsweise eine auswählbare Schaltfläche umfassen. Das Kommunikationsgerät kann dazu eingerichtet sein, in Folge einer Eingabe durch den Nutzer, durch die die Beantragung von Zugriffsrechten beantragt wird, den Nutzer zur Erfassung des Identifizierungs-Indikators aufzufordern, beispielsweise durch eine Anzeige über die Nutzeroberfläche. Die Erfassung des Identifizierungs-Indikators kann beispielsweise die hierin beschriebene optische Erfassung, beispielsweise die Erfassung eines QR-Codes mit einer Kamera eines Kommunikationsgerätes in Form eines Smartphones, umfassen. Das Kommunikationsgerät kann dazu eingerichtet sein, eine erfolgreiche Erfassung zu bestätigen, beispielsweise durch eine Anzeige über die Nutzeroberfläche und/oder die Ausgabe eines akustischen Signals. Das Kommunikationsgerät kann dazu eingerichtet sein, in Folge der Erfassung des Identifizierungs-Indikators die Anfrage an die Authentifizierungs-Infrastruktur zu übermitteln, beispielsweise wie hierin im Zusammenhang mit Aspekten und Ausführungsformen beschrieben. Das Kommunikationsgerät kann dazu eingerichtet sein, in Folge des Empfangens des Authentifizierungs-Tokens von der Authentifizierungs-Infrastruktur den Authentifizierung-Indikator über die Nutzeroberfläche anzuzeigen, beispielsweise wie hierin im Zusammenhang mit Aspekten und Ausführungsformen beschrieben. Insbesondere kann die Anzeige des Authen-

tifizierung-Indikators über die Schnittstelle in menschenlesbarer Form erfolgen, insbesondere sodass der Nutzer den Authentifizierung-Indikator an einer Eingabeeinrichtung der Schnittstelle eingeben kann.

**[0028]** Gemäß einem Aspekt wird die Verwendung des hierin beschriebenen Authentifizierungs-Systems zur Ausführung einer hierin beschriebenen Methode zur Zugriffskontrolle beschrieben. Die Personenbeförderungseinrichtung ist ein Fahrstuhl, eine Fahrtreppe oder ein Fahrsteig. Die Verwendung umfasst die Wartung der Personenbeförderungseinrichtung. Als Wartung ist eine Einflussnahme von Wartungspersonal auf die Funktion der Personenbeförderungseinrichtung, und/oder die Überprüfung der Personenbeförderungseinrichtung zu verstehen. Insbesondere kann die Wartung eine Interaktion mit der Schnittstelle, insbesondere zur Einflussnahme oder Überprüfung der der Schnittstelle zugeordneten Komponente umfassen. Die Verwendung kann das räumliche Aufsuchen der Schnittstelle und des Identifizierungs-Indikators durch einen Nutzer umfassen, beispielsweise das Betreten eines Betriebsraums oder das Öffnen eines Schaltschranks.

**[0029]** Gemäß einem Aspekt ist ein Computerprogrammprodukt beschrieben. Das Computerprogrammprodukt kann dazu eingerichtet sein, bei der Ausführung des Programms die Schnittstelle zu veranlassen, Funktionen gemäß den hierin beschriebenen Aspekten und Ausführungsformen auszuführen. Das Computerprogrammprodukt kann auf einem Datenträger vorgesehen sein. Das Computerprogrammprodukt kann in einem Speicher der Schnittstelle oder einer mit der Schnittstelle assoziierten Komponente der Personenbeförderungseinrichtung gespeichert sein. Das Computerprogrammprodukt kann übermittelbar sein und beispielsweise dazu eingerichtet sein, bei einem Update, beispielsweise einem Firmware-Update, installiert zu werden. Die Übermittlung kann beispielsweise über ein hierin beschriebenes Kommunikationsmodul der Schnittstelle für die Schnittstelle empfangbar sein.

**[0030]** Gemäß einem Aspekt umfasst die Schnittstelle einen Prozessor, beispielsweise einen Mikroprozessor oder eine CPU. Die Schnittstelle kann weiterhin einen Speicher umfassen. In dem Speicher kann das hierin beschriebene Computerprogramm gespeichert sein. Das Computerprogramm kann, bei Ausführung auf dem Prozessor, die Schnittstelle dazu veranlassen, die hierin beschriebenen Funktionen der Schnittstelle auszuführen oder durchzuführen. Alternativ oder zusätzlich dazu können Prozessor und Speicher in der der Schnittstelle zugeordneten Komponente, beispielsweise einem Controller, vorgesehen sein.

**[0031]** Gemäß einem Aspekt umfasst das Kommunikationsgerät einen Prozessor, beispielsweise einen Mikroprozessor oder eine CPU. Das Kommunikationsgerät kann weiterhin einen Speicher umfassen. In dem Speicher kann die hierin beschriebene App gespeichert sein, sowie weitere Programme, beispielsweise zur Steuerung der hierin nicht im Zusammenhang mit der App beschrie-

benen Funktionen, wie z.B. die Steuerung einer Kamera des Kommunikationsgeräts. Die App kann, bei Ausführung auf dem Prozessor, das Kommunikationsgerät dazu veranlassen, die hierin beschriebenen Funktionen des Kommunikationsgeräts auszuführen oder durchzuführen.

**[0032]** Gemäß einem Aspekt umfasst die Authentifizierungs-Infrastruktur einen Prozessor, beispielsweise einen oder mehrere CPUs. Die Authentifizierungs-Infrastruktur kann weiterhin einen Speicher umfassen. In dem Speicher kann eine Software zur Steuerung der Authentifizierungs-Infrastruktur gespeichert sein. Die Software kann, bei Ausführung auf dem Prozessor, die Authentifizierungs-Infrastruktur dazu veranlassen, die hierin beschriebenen Funktionen der Authentifizierungs-Infrastruktur auszuführen oder durchzuführen. Der Speicher kann zusätzlich dazu eine Datenbank speichern, in der die hierin im Zusammenhang mit der Datenbank beschriebenen Daten gespeichert sind. Die Datenbank kann Daten über Nutzer, Berechtigungsstufen der Nutzer, insbesondere für eine jeweilige Schnittstelle, Kommunikationsgeräte, insbesondere dem jeweiligen Nutzer zugeordnete Kommunikationsgeräte, Schnittstellen, insbesondere den der jeweiligen Schnittstelle zugeordnete Identifizierungs-Indikator, sowie weitere Daten, beispielsweise Ortsdaten der Schnittstelle, und/oder Adressen, beispielsweise IP-Adressen oder URLs, der Schnittstelle und/oder des Kommunikationsgeräts in dem Datennetzwerk beinhalten. Die Datenbank kann optional sein, insbesondere in Ausführungsformen, in denen die genannten Daten beispielsweise zusammen mit der Anfrage, beispielsweise zusammen mit dem Identifizierungstoken, an die Authentifizierungs-Infrastruktur übermittelt werden.

**[0033]** Im Folgenden wird die Erfindung anhand von Ausführungsformen beschrieben, wobei ein oder mehrere Beispiele in den Figuren gezeigt sind. In den folgenden Zeichnungen beziehen sich gleiche Bezugszeichen auf gleiche oder ähnliche Komponenten. Im Allgemeinen werden nur die Unterschiede zwischen den einzelnen Ausführungsformen beschrieben. Die Beispiele dienen der Beschreibung und sollen nicht als Einschränkung verstanden werden. Merkmale, die in Bezugnahme auf eine Ausführungsform beschrieben wurden, können mit weiteren Ausführungsformen kombiniert werden und somit weitere Ausführungsformen ergeben. Die Beschreibung umfasst derartige Modifikationen und Variationen. Es zeigen

Fig. 1 ein Authentifizierungs-System gemäß einer Ausführungsform;

Fig. 2 Identifizierungs-Indikator, Identifizierungstoken, Authentifizierungstoken, und Berechtigungstoken gemäß Ausführungsformen; und

Fig. 3 eine Methode zur Zugriffskontrolle einer Schnittstelle gemäß einer Ausführungsform.

**[0034]** Fig. 1 zeigt ein Authentifizierungs-System 100

gemäß einer beispielhaften Ausführungsform. In der gezeigten Ausführungsform umfasst das Authentifizierungssystem 100 einen Steuerschrank 112 einer Personenbeförderungseinrichtung, in dem sich eine Steuerkomponente mit einer Schnittstelle 110 befindet. Die Schnittstelle 110 umfasst ein Keypad, das als Eingabeeinrichtung dient, und ein Display, das als Ausgabeeinrichtung dient. Die Schnittstelle 110 ist über eine Netzwerkverbindung 116 mit dem Internet 140 verbunden. Im Steuerschrank 112 ist ein Identifizierungs-Indikator 114 an einer sichtbaren Stelle befestigt. In der Ausführungsform ist der Identifizierungs-Indikator 114 als QR-Code codiert. Der Identifizierungs-Indikator 114 kann beispielsweise bei der Installation der Schnittstelle 110 angebracht worden sein, oder bei einem Update der Schnittstelle mit dem hierin beschriebenen Computerprogrammprodukt.

**[0035]** Das in Fig. 1 gezeigte Authentifizierungssystem 100 umfasst ein Kommunikationsgerät 120. Bei dem Kommunikationsgerät 120 handelt es sich in der gezeigten Ausführungsform um ein Smartphone, das mittels einer darauf installierten App dazu eingerichtet ist, die hierin beschriebenen Funktionen auszuführen. Das Kommunikationsgerät 120 ist einem Nutzer eindeutig zugeordnet, z.B. kann das Kommunikationsgerät 120 ein Smartphone sein, das sich, zumindest zeitweise, ausschließlich im Besitz des Nutzers befindet und/oder auf das nur der Nutzer Zugriff hat. Das Kommunikationsgerät 120 ist eingerichtet, i.e. in einem Speicher des Kommunikationsgeräts 120 ist ein Berechtigungs-Indikator gespeichert, der die Berechtigungsstufe des Nutzers umfasst.

**[0036]** In Ausführungsformen, wie etwa der in Fig. 1 gezeigten Ausführungsform, ist das Kommunikationsgerät 120 nicht ausschließlich für die Authentifizierung an einer einzelnen Personenbeförderungseinrichtung vorgesehen. Das Kommunikationsgerät 120 kann beispielsweise bei dem Nutzer verbleiben und wird beispielsweise nur dann benötigt, wenn die hierin beschriebenen Schritte zur Ausführung einer Methode zur Zugriffskontrolle an der Schnittstelle 110 der jeweiligen Personenbeförderungseinrichtung ausgeführt werden.

**[0037]** Das in Fig. 1 gezeigte Kommunikationsgerät 120 umfasst eine Kamera. Die Kamera ist dazu eingerichtet, den als QR-Code codierten Identifizierungs-Indikator 114 einzulesen, insbesondere so, dass der QR-Code dekodiert werden kann und der decodierte Identifizierungs-Indikator von dem Kommunikationsgerät 120 weiterverarbeitet werden kann. Das Einlesen des als QR-Code codierten Identifizierungs-Indikators ist in Fig. mit Pfeil 124 dargestellt.

**[0038]** Das in Fig. 1 gezeigte Kommunikationsgerät 120 umfasst ein Display 122. In dem gezeigten Ausführungsbeispiel wird auf dem Display 122 eine Rohausgabe der von der Kamera des Kommunikationsgerätes 120 erfassten Bilddaten, hier eine Wiedergabe des als QR-Code codierte Identifizierungs-Indikators 114 angezeigt ("ID"). In dem gezeigten Ausführungsbeispiel wird auf

dem Display 122 weiterhin ein Authentifizierung-Indikator ("AI") angezeigt, der von dem Kommunikationsgerät 120 aus einem zuvor empfangenen Authentifizierung-Tokens abgeleitet wurde. Die Anzeige des Authentifizierung-Indikators erlaubt es dem Nutzer, den Authentifizierung-Indikator an der Eingabeeinrichtung der Schnittstelle 110 einzugeben. Die Eingabe des Authentifizierung-Indikators ist in Fig. 1 mit dem Pfeil 126 dargestellt.

**[0039]** Das in Fig. 1 gezeigte Kommunikationsgerät 120 ist über eine drahtlose Netzwerkverbindung 128 mit dem Internet 140 verbunden, beispielsweise über ein Mobilfunknetz oder ein lokales drahtloses Netzwerk.

**[0040]** Das in Fig. 1 gezeigte Authentifizierungssystem 100 umfasst eine Authentifizierungs-Infrastruktur 130. Im gezeigten Beispiel ist die Authentifizierungs-Infrastruktur 130 ein Server-basierter Cloud-Dienst, der dazu eingerichtet ist, die hierin beschriebenen Funktionen der Authentifizierungs-Infrastruktur auszuführen. Die Funktionen umfassen zumindest eine Anfrage von dem Kommunikationssystem zu empfangen, ein Authentifizierung-Token auf Basis des Identifizierung-Tokens zu generieren und das Authentifizierung-Token an das Kommunikationsgerät zu übermitteln, ein Berechtigung-Token zu generieren, und das Berechtigung-Token an die Schnittstelle zu übermitteln. Die hierin beschriebenen Indikatoren und Token sind in Fig. 2 genauer beschrieben. Die Authentifizierungs-Infrastruktur ist über die Verbindung 132 mit dem Internet 140 verbunden.

**[0041]** In Ausführungsformen sind die in Fig. 1 gezeigten Komponenten, insbesondere die Schnittstelle 110, das Kommunikationsgerät 120 und die Authentifizierungs-Infrastruktur 130 dazu eingerichtet, die hierin für die jeweilige Komponente beschriebenen Funktionen auszuführen, insbesondere um eine Methode zur Zugriffskontrolle der Schnittstelle 110 auszuführen. Eine Ausführungsform einer solchen Methode ist in Fig. 3 genauer beschrieben.

**[0042]** Wie in Fig. 1 gezeigt sind die Schnittstelle 110, das Kommunikationsgerät 120 und die Authentifizierungs-Infrastruktur 130, beispielsweise über die hierin beschriebenen Netzwerkmodule, direkt oder indirekt mit dem Internet verbunden. Dadurch können Daten, beispielsweise Datenpakete umfassend die hierin beschriebenen Token, zwischen der Schnittstelle 110 und der Authentifizierungs-Infrastruktur 130 und zwischen dem Kommunikationsgerät 120 und der Authentifizierungs-Infrastruktur 130 ausgetauscht werden. Eine direkte Übertragung von Datenpaketen über das Internet 140 zwischen dem Kommunikationsgerät 120 und der Schnittstelle 110 ist nicht erforderlich. Dies kann vorteilhafterweise die Sicherheit der Zugriffskontrolle erhöhen.

**[0043]** Fig. 2 zeigt beispielhafte Ausführungsformen der hierin beschriebenen Indikatoren und Token.

**[0044]** Der Identifizierungs-Indikator 210 dient der eindeutigen Zuordenbarkeit der Schnittstelle und kann entsprechend der hierin beschriebenen Aspekte oder Ausführungsformen gestaltet sein. Der Identifizierungs-Indi-



kator kann beispielsweise in Form des in Fig. 1 gezeigten QR-Code codierten Identifizierungs-Indikators im Steuerschrank 112 vorgesehen sein. Nach dem Einlesen des Identifizierungs-Indikators 210 kann der Identifizierungs-Indikator 210 als ein Computer-verarbeitbares Element, etwa eine Ziffern- oder Zeichenfolge vorliegen.

**[0045]** Das Identifizierungs-Token 220 wird durch ein Kommunikationsgerät, beispielsweise das in Fig. 1 gezeigte Kommunikationsgerät 120, nach dem Einlesen des Identifizierungs-Indikators 210 generiert. In Ausführungsformen umfasst das Identifizierungs-Token den Identifizierungs-Indikator 210. Der Identifizierungs-Indikator 210 kann direkt in das Token integriert sein. Der Identifizierungs-Indikator 210 des Identifizierungs-Tokens 220 kann verarbeitet sein, beispielsweise komprimiert, umcodiert oder verschlüsselt sein.

**[0046]** In Ausführungsformen umfasst das Identifizierungs-Token, wie in Fig. 2 gezeigt, weitere Informationen. Die weiteren Informationen können optional sein. Beispielsweise kann das Identifizierungs-Token einen Identifikator des Kommunikationsgeräts 222 umfassen. Der Identifikator des Kommunikationsgeräts 222 kann dazu bestimmt sein, das Kommunikations-Gerät gegenüber einer Authentifizierungs-Infrastruktur, wie etwa die in Fig. 1 gezeigte Authentifizierungs-Infrastruktur 130, zu identifizieren. Dadurch kann beispielsweise der dem Kommunikationsgerät zugewiesene Nutzer identifiziert und/oder gegenüber der Authentifizierungs-Infrastruktur authentifiziert werden, und beispielsweise eine in einer Datenbank der Authentifizierungs-Infrastruktur gespeicherte Berechtigungsstufe des Nutzers ermittelbar sein. Auf einen Identifikator des Kommunikationsgeräts 222 kann in Ausführungsformen verzichtet werden, wenn stattdessen alternative Identifizierungs-Methoden angewendet werden, beispielsweise ein Session-Login des Kommunikationsgeräts an der Authentifizierungs-Infrastruktur.

**[0047]** In Ausführungsformen umfasst das Identifizierungs-Token 220 einen Berechtigungs-Indikator 224. Der Berechtigungs-Indikator 224 kann Informationen umfassen, aus denen sich die Berechtigungs-Stufe des Nutzers ergibt. Der Berechtigungs-Indikator 224 des Identifizierungs-Tokens 220 ist von dem Kommunikationsgerät erstellt. Demzufolge kann es sich bei dem Berechtigungs-Indikator 224 um einen Berechtigungs-Indikator handeln, der bei der Einrichtung des Kommunikationsgeräts gemäß hierin beschriebener Aspekte und Ausführungs-Formen in einem Speicher des Kommunikationsgerätes gespeichert wurde. Der Berechtigungs-Indikator 224 des Identifizierungs-Tokens 220 kann es sich in Ausführungsformen um den Berechtigungs-Indikator des Berechtigungs-Tokens 240 handeln, insbesondere in Ausführungsformen, in denen die Verarbeitung der Anfrage durch die Authentifizierungs-Infrastruktur keine Modifizierung des Berechtigungs-Indikators 224 oder erstmalige Erstellung des Berechtigungs-Indikators 242 vorsieht. Auf den Berechtigungs-Indikator 224 des Identifizierungs-Tokens 220 kann in Ausführungsformen

verzichtet werden, beispielsweise in Ausführungsformen, in denen die Berechtigungs-Stufe des Nutzers in einer Datenbank der Authentifizierungs-Infrastruktur hinterlegt ist, oder in denen die Berechtigungs-Stufe des Nutzers von der Authentifizierungs-Infrastruktur ermittelt wird.

**[0048]** Die weiteren Informationen, z.B. der Identifikator des Kommunikationsgeräts 222 und/oder der Berechtigungs-Indikator 224 des Identifizierungs-Tokens 220 können verarbeitet sein, beispielsweise komprimiert, umcodiert oder verschlüsselt sein.

**[0049]** Alternativ oder zusätzlich zu einer Verschlüsselung der einzelnen im Identifizierungs-Token 220 enthaltenen Informationen kann das gesamte Identifizierungs-Token 220 verschlüsselt sein. Eine Verschlüsselung, sowohl des Identifizierungs-Tokens 220 als auch der im Identifizierungs-Token 220 enthaltenen Informationen kann dazu geeignet sein, von der hierin beschriebenen Authentifizierungs-Infrastruktur entschlüsselt zu werden.

**[0050]** Das Authentifizierungs-Token 230 wird von einer Authentifizierungs-Infrastruktur generiert, beispielsweise der in Fig. 1 gezeigte Authentifizierungs-Infrastruktur 130, nach Empfangen der Anfrage durch das Kommunikationsgerät umfassend das Identifizierungs-Token 220. Das Authentifizierungs-Token 230 ist von der Authentifizierungs-Infrastruktur an das Kommunikationsgerät übermittelbar. Das Authentifizierungs-Token umfasst zumindest einen Authentifizierungs-Indikator 232. Der Authentifizierungs-Indikator 232 kann ein Authentifizierungs-Indikator gemäß hierin beschriebenen Aspekten oder Ausführungsformen sein. Insbesondere kann der Authentifizierungs-Indikator auf Basis eines Zufallswerts erstellt sein.

**[0051]** Das Authentifizierungs-Token 230 kann weitere optionale Informationen 234 umfassen. Die optionalen Informationen 234 können Informationen sein, die vorteilhafterweise dem Nutzer zur Verfügung gestellt werden sollen, beispielsweise durch Ausgabe durch das Kommunikationsgerät. Die optionalen Informationen 234 können beispielsweise Informationen umfassen, die in gleicher oder ähnlicher Weise im Berechtigungs-Token 240 enthalten sind, beispielsweise eine Gültigkeitsdauer des Authentifizierungs-Indikators 232, eine Berechtigungsstufe des Nutzers, eine Modellbezeichnung und/oder Versionsnummer der Schnittstelle oder dergleichen.

**[0052]** Das Berechtigungs-Token 240 wird von einer Authentifizierungs-Infrastruktur generiert, beispielsweise der in Fig. 1 gezeigte Authentifizierungs-Infrastruktur 130, nach Empfangen der Anfrage durch das Kommunikationsgerät umfassend das Identifizierungs-Token 220. Das Authentifizierungs-Token 230 ist von der Authentifizierungs-Infrastruktur an eine Schnittstelle übermittelbar. Das Berechtigungs-Token 240 umfasst das Authentifizierungs-Token 230. In Ausführungsformen umfasst das Berechtigungs-Token 240 somit zumindest den Authentifizierungs-Indikator 232. In weiteren Ausführungs-

formen kann das Berechtigungs-Token 240 die für das Authentifizierungs-Token 232 beschriebenen optionalen Informationen 234 umfassen.

**[0053]** Das Berechtigungs-Token 240 umfasst den Berechtigungs-Indikator 242. Der Berechtigungs-Indikator 242 kann optional sein, beispielsweise in Ausführungsformen, für die nur zwei Berechtigungs-Stufen vorgesehen sind, beispielsweise "vollständige Berechtigung" und "keine Berechtigung". In diesen Ausführungsformen kann die Berechtigung beispielsweise durch das Vorhandensein eines gültigen Authentifizierungs-Indikators 230 oder bereits durch das Empfangen eines Berechtigungs-Tokens 240 durch die Schnittstelle gegeben sein. In weiteren Ausführungsformen kann der Berechtigungs-Indikator 242 dazu geeignet sein, auf Basis des Berechtigungs-Indikators 242 eine Berechtigungsstufe auszuwählen und die Schnittstelle in einen Wartungsmodus auf Basis der Berechtigungsstufe zu wechseln.

**[0054]** Das Berechtigungs-Token 240 kann weitere optionale Informationen 244 umfassen, beispielsweise zusätzlich oder anstelle der optionalen Informationen 234, die in dem im Berechtigungs-Token 240 enthaltenen Authentifizierungs-Token 230 vorhanden sind. Die optionalen Informationen 244 können Informationen sein, die vorteilhafterweise der Schnittstelle zur Verfügung gestellt werden sollen, beispielsweise um die Schnittstelle auf Basis der optionalen Informationen 244 zu betreiben oder einzustellen. Beispielsweise können die optionalen Informationen eine Gültigkeitsdauer des Authentifizierungs-Indikators 232, und/oder eine maximale Anzahl von Eingabeversuchen des Authentifizierungs-Indikators umfassen.

**[0055]** Das Authentifizierungs-Token 230 und das Berechtigungs-Token 240 können, analog zu dem Identifizierungs-Token 220 verschlüsselt sein. Alternativ oder zusätzlich zu einer Verschlüsselung der einzelnen im Authentifizierungs-Token 230 oder der einzelnen im Berechtigungs-Token 240 enthaltenen Informationen kann das gesamte Authentifizierungs-Token 230 und/oder das gesamte Berechtigungs-Token 240 verschlüsselt sein. Eine Verschlüsselung, sowohl des Authentifizierungs-Tokens 230, des Berechtigungs-Tokens 240 als auch der im Authentifizierungs-Token 230 und/oder Berechtigungs-Token 240 enthaltenen Informationen kann dazu geeignet sein, von dem Kommunikationsgerät (Authentifizierungs-Token 230) und der Schnittstelle (Berechtigungs-Token 240) entschlüsselt zu werden.

**[0056]** Fig. 3 zeigt eine Methode 300 zur Zugriffskontrolle einer Schnittstelle zur Wartung einer Personenbeförderungseinrichtung gemäß einer beispielhaften Ausführungsform. Die Methode kann durch das in Fig. 1 gezeigte Authentifizierungs-System 100 ausgeführt werden. Fig. 3 zeigt dazu, welche Operationen in den jeweiligen Komponenten Schnittstelle 110, Kommunikationsgerät 120 und Authentifizierungs-Infrastruktur 130 durchgeführt werden können. Die als Pfeile gezeigten Operationen 316, 328 und 332 zeigen dabei eine Kommunikation, insbesondere einen Austausch von Da-

ten, die zwischen den jeweiligen Komponenten stattfindet und beispielsweise gemäß den hierin beschriebenen Aspekten und Ausführungsformen, beispielsweise über das Internet erfolgen kann. Die als Pfeile gezeigten Operationen 324 und 326 umfassen einen Informationsaustausch, der direkt an der Schnittstelle stattfindet, also ohne einen Datenaustausch über beispielsweise das Internet, sondern durch Einlesen 324 des Identifikations-Indikators und Eingeben 326 des Authentifizierungs-Indikators.

**[0057]** Die Methode umfasst in Operation 310 das Bereitstellen eines Identifizierungs-Indikators, beispielsweise des in Fig. 1 gezeigten Identifizierungs-Indikators 114. Das Bereitstellen kann beispielsweise durch Anzeige auf einem Display der Schnittstelle, oder durch Anbringen eines sichtbaren Labels in räumlicher Nähe der Schnittstelle erfolgen.

**[0058]** Die Methode umfasst in Operation 324 das Einlesen des Identifizierungs-Indikators mit dem Kommunikationsgerät 120. Das Einlesen kann ein optisches Erfassen umfassen. In Operation 320 wird der Identifizierungs-Indikator verarbeitet, beispielsweise kann ein QR-Code codierter Identifizierungs-Indikator in Form von Bild-Daten in dem Kommunikationsgerät 120 vorliegen, und das Kommunikationsgerät 120 kann die Bilddaten decodieren, um den Identifizierungs-Indikator in Form einer verarbeitbaren Datenstruktur, beispielsweise einer Zeichenfolge wie z.B. einem String, weiterverarbeiten zu können.

**[0059]** In Operation 322 wird ein Identifizierungs-Token auf Basis des Identifizierungs-Indikators gemäß den hierin beschriebenen Aspekten und Ausführungsformen erstellt. In Operation 323 wird eine Anfrage gemäß den hierin beschriebenen Aspekten und Ausführungsformen erstellt. Die Anfrage umfasst das Identifizierungs-Token. Das Erstellen der Anfrage in Operation 323 kann das Herstellen einer kommunikativen Verbindung mit der Authentifizierungs-Infrastruktur umfassen, beispielsweise das Herstellen einer gesicherten Verbindung, die Übermittlung und Überprüfung von Zertifikaten, und/oder die Authentifizierung des Kommunikationsgeräts gegenüber der Authentifizierungs-Infrastruktur.

**[0060]** In Operation 328 wird die Anfrage an die Authentifizierungs-Infrastruktur 130 gemäß den hierin beschriebenen Aspekten und Ausführungsformen übermittelt. In Operation 330 wird die Anfrage durch die Authentifizierungs-Infrastruktur 130 gemäß den hierin beschriebenen Aspekten und Ausführungsformen verarbeitet. Das Verarbeiten der Anfrage in Operation 330 kann beispielsweise eine Plausibilitätsprüfung der Anfrage umfassen.

**[0061]** Das Verarbeiten der Anfrage in Operation 330 kann, sofern erforderlich, den Zugriff auf eine Datenbank durch die Authentifizierungs-Infrastruktur umfassen, beispielsweise um das Kommunikationsgerät zu identifizieren, und/oder eine Berechtigungsstufe des dem Kommunikationsgerät zugeordneten Nutzers für die dem Identifizierungs-Indikator zugeordnete Schnittstelle abzufragen.

gen.

**[0062]** In Operation 331 werden ein Berechtigungs-Token und ein Authentifizierungs-Token gemäß den hierin beschriebenen Aspekten und Ausführungsformen erstellt. In Operation 332 wird das Authentifizierungs-Token an das Kommunikationsgerät 120 übermittelt. In Operation 316 wird das Berechtigungs-Token an die Schnittstelle 110 übermittelt.

**[0063]** In Operation 340 wird durch das Kommunikationsgerät 120 ein Authentifizierung-Indikator gemäß den hierin beschriebenen Aspekten und Ausführungsformen aus dem Authentifizierungs-Token generiert. Beispielsweise kann, sofern erforderlich, das Authentifizierungs-Token entschlüsselt werden. Beispielsweise kann ein in dem Authentifizierungs-Token enthaltener Authentifizierung-Indikator extrahiert werden, oder ein Authentifizierung-Indikator auf Basis von in dem Authentifizierungs-Token enthaltener Information erstellt werden. In Operation 342 wird der Authentifizierung-Indikator durch das Kommunikationsgerät wiedergegeben.

**[0064]** In Operation 326 wird der Authentifizierung-Indikator gemäß den hierin beschriebenen Aspekten und Ausführungsformen an einer Eingabeeinrichtung der Schnittstelle eingegeben.

**[0065]** In Operation 350 wird der eingegebene Authentifizierung-Indikator überprüft und mit dem Berechtigungs-Token abgeglichen. Der Abgleich kann für das Berechtigungs-Token dieselben Schritte umfassen, die in Operation 340 für das Authentifizierungs-Token und die Generation des Authentifizierung-Indikators aus dem Authentifizierungs-Token beschrieben wurden, d.h. die Schnittstelle kann ihrerseits einen Authentifizierung-Indikator aus dem in dem Berechtigungs-Token enthaltenen Authentifizierungs-Token generieren. Der Abgleich kann den Vergleich umfassen, ob der eingegebene Authentifizierung-Indikator mit dem in der Schnittstelle generierten Authentifizierung-Indikator übereinstimmt. Gleichmaßen kann der Abgleich beispielsweise über entsprechende mathematische oder kryptographische Funktionen erfolgen. Beispielsweise kann der Authentifizierung-Indikator aus dem Authentifizierungs-Token über eine kryptographische Funktion abgeleitet sein, und der Abgleich in Operation 350 kann die Anwendung derselben oder einer komplementären kryptographischen Funktion umfassen.

**[0066]** In Operation 352 erfolgt der Wechsel der Schnittstelle in einen Wartungsmodus gemäß den hierin beschriebenen Aspekten und Ausführungsformen. Operation 352 kann das Auslesen einer im Berechtigungs-Token enthaltenen Berechtigungsstufe umfassen, sowie die Auswahl einer Berechtigungsstufe auf Basis des Berechtigungs-Tokens. Auf Basis der ausgewählten Berechtigungsstufe kann die Operation 352 den Wechsel der Schnittstelle in einen Wartungsmodus umfassen, der der jeweiligen ausgewählten Berechtigungsstufe entspricht.

**[0067]** Die hierin beschriebenen Ausführungsformen ermöglichen eine sichere und einfache Zugriffskontrolle.

Anstelle eines statischen Passworts wird ein Authentifizierung-Indikator verwendet, der für jeden Nutzer und bei jeder Wartungsaktivität erstellt wird. Dadurch erhöht sich die Sicherheit in besonders vorteilhafter Weise. Aufwändige Berechtigungsverfahren, wie etwa das Erfragen des voreingestellten Passworts für die jeweilige Schnittstelle bei einer zentralen Autorität durch das Wartungspersonal sind nicht nötig. Für den Nutzer der vorgeschlagenen Lösung ist, im Vergleich zur bekannten Eingabe eines voreingestellten Passworts, vorteilhafterweise nur ein zusätzlicher Schritt, nämlich das Einlesen des Identifizierungs-Indikators nötig. Zusätzlich dazu kann für jeden Nutzer und sogar für jede Schnittstelle ein Wartungsmodus mit einer voreingestellten Berechtigungsstufe erlaubt werden, sodass ein böswilliger oder versehentlicher Eingriff in sicherheitsrelevante Funktionen in vielen Fällen ausgeschlossen werden kann. Die vorgeschlagenen Lösungen erlauben das schnelle und einfache Vergeben von Berechtigungen für temporäre Wartungsteams und es kann am Ende der Wartung auf einfache Weise sichergestellt werden, dass keine Zugriffsrechte bei den Mitgliedern des temporären Wartungsteams verbleiben, ohne dazu beispielsweise ein Passwort an jeder Schnittstelle ändern zu müssen. Die vorgeschlagene Lösung kann in vielen Fällen vorteilhafterweise durch ein Software-Update der Schnittstelle mit dem hierin vorgeschlagenen Computerprogrammprodukt implementiert werden, sodass eine Hardware-Nachrüstung der Schnittstelle oder der der Schnittstelle zugeordneten Komponente vorteilhafterweise nicht nötig ist.

## Patentansprüche

1. Methode zur Zugriffskontrolle einer Schnittstelle zur Wartung einer Personenbeförderungseinrichtung in Form eines Fahrstuhls, Fahrsteigs oder einer Fahrtreppe, wobei ein mit der der Schnittstelle assoziierter Identifizierungs-Indikator zur Identifizierung der Schnittstelle vorgesehen ist; umfassend:

Übermitteln einer Anfrage an eine Authentifizierungs-Infrastruktur mit einem Kommunikationsgerät, wobei

- die Anfrage ein Identifizierungs-Token beinhaltet, und wobei
- das Identifizierungs-Token auf Basis des Identifizierungs-Indikators erstellt ist;

Verarbeiten der Anfrage mit der Authentifizierungs-Infrastruktur;

Übermitteln eines Authentifizierungs-Tokens an das Kommunikationsgerät durch die Authentifizierungs-Infrastruktur;

Übermitteln eines Berechtigungs-Tokens an die

- Schnittstelle durch die Authentifizierungs-Infrastruktur, wobei das Berechtigungs-Token das Authentifizierungs-Token umfasst;  
Wiedergabe eines Authentifizierung-Indikators mit dem Kommunikationsgerät, wobei der Authentifizierung-Indikator auf Basis des Authentifizierungs-Tokens erstellt ist;  
Eingabe des Authentifizierung-Indikators an einer Eingabeeinrichtung der Schnittstelle;  
Überprüfen des Authentifizierung-Indikators mit der Schnittstelle, umfassend: einen Abgleich des Authentifizierung-Indikators mit dem Berechtigungs-Token, und eine Auswahl einer Berechtigungsstufe auf Basis des Berechtigungs-Tokens; und  
Wechsel der Schnittstelle in einen Wartungsmodus auf Basis des Abgleichs und der Berechtigungsstufe.
2. Die Methode nach Anspruch 1, wobei die Auswahl einer Berechtigungsstufe die Auswahl einer Berechtigungsstufe einer Vielzahl von Berechtigungsstufen umfasst, und wobei die Vielzahl von Berechtigungsstufen zumindest keine Berechtigung, Leseberechtigung und Schreib-/Leseberechtigung umfasst.
3. Die Methode nach Anspruch 1 oder 2, weiterhin umfassend:
- Einrichten des Kommunikationsgeräts, umfassend die Speicherung eines Berechtigungs-Indikators in einem Speicher des Kommunikationsgeräts, wobei der Berechtigungs-Indikator indikativ für die Berechtigungsstufe eines Nutzers ist, und wobei das Identifizierungs-Token auf Basis des Berechtigungs-Indikators erstellt ist.
4. Die Methode nach einem der vorhergehenden Ansprüche, wobei die Verarbeitung der Anfrage umfasst:
- Generierung eines Zufallswerts,  
Generierung des Authentifizierung-Tokens und des Berechtigungs-Tokens mit der Authentifizierungs-Infrastruktur auf Basis des Identifizierungs-Tokens und des Zufallswerts.
5. Die Methode nach einem der vorhergehenden Ansprüche, weiterhin umfassend:
- Einlesen des Identifizierungs-Indikators mit dem Kommunikationsgerät.
6. Die Methode nach einem der vorhergehenden Ansprüche, wobei der Authentifizierung-Indikator ein Passwort und/oder eine Kennzahl ist.
7. Die Methode nach einem der vorhergehenden Ansprüche, wobei
- die Wiedergabe des Authentifizierung-Indikators in menschenlesbarer Form erfolgt.
8. Die Methode nach einem der vorhergehenden Ansprüche, wobei das Überprüfen des Authentifizierung-Indikators weiterhin umfasst:
- Überprüfen, ob die Eingabe des Authentifizierung-Indikators innerhalb einer vorbestimmten Zeitspanne erfolgt ist, und/oder
  - Überprüfen, ob die Eingabe des Authentifizierung-Indikators öfter als eine vorbestimmte Anzahl von Eingaben erfolgt ist.
9. Authentifizierungs-System zur Zugriffskontrolle einer Schnittstelle zur Wartung einer Personenbeförderungseinrichtung in Form eines Fahrstuhls, Fahrsteigs oder einer Fahrtreppe, umfassend:
- ein Kommunikationsgerät, die Schnittstelle und eine Authentifizierungs-Infrastruktur, wobei die Schnittstelle einen mit der der Schnittstelle assoziierten Identifizierungs-Indikator zur Identifizierung der Schnittstelle, sowie eine Eingabeeinrichtung zur Eingabe eines Authentifizierung-Indikators an einer Eingabeeinrichtung der Schnittstelle umfasst, wobei die Schnittstelle dazu eingerichtet ist:
- ein Berechtigungs-Token von der Authentifizierungs-Infrastruktur zu empfangen;
  - den Authentifizierung-Indikator zu überprüfen, wobei die Überprüfung einen Abgleich des Authentifizierung-Indikators mit dem Berechtigungs-Token und eine Auswahl einer Berechtigungsstufe auf Basis des Berechtigungs-Tokens umfasst; und
  - auf Basis des Abgleichs und der Berechtigungsstufe in einen Wartungsmodus zu wechseln; wobei das Kommunikationsgerät dazu eingerichtet ist:
  - den Identifizierungs-Indikator einzulesen;
  - eine Anfrage zu generieren, wobei die Anfrage ein Identifizierungs-Token beinhaltet, und wobei das Identifizierungs-Token auf Basis des Identifizierungs-Indikators erstellt ist;
  - die Anfrage an die Authentifizierungs-Infrastruktur zu übermitteln;
  - ein Authentifizierungs-Token von der Authentifizierungs-Infrastruktur zu empfangen;
  - einen Authentifizierung-Indikator auf Basis des Authentifizierungs-Tokens zu generieren; und
  - den Authentifizierung-Indikator wiederzugeben; wobei die Authentifizierungs-Infrastruktur

dazu eingerichtet ist:

- die Anfrage von dem Kommunikationssystem zu empfangen;
- das Authentifizierungs-Token auf Basis des Identifizierungs-Tokens zu generieren und das Authentifizierungs-Token an das Kommunikationsgerät zu übermitteln; 5
- das Berechtigungs-Token zu generieren, wobei das Berechtigungs-Token das Authentifizierungs-Token umfasst; und 10
- das Berechtigungs-Token an die Schnittstelle zu übermitteln.

10. Das Authentifizierungs-System nach Anspruch 9, wobei 15

der Identifizierungs-Indikator eine sichtbare Kennzeichnung, insbesondere einen QR-Code umfasst, und wobei das Kommunikationsgerät dazu eingerichtet ist, die sichtbare Kennzeichnung optisch zu erfassen. 20

11. Das Authentifizierungs-System nach Anspruch 9 oder 10, wobei das Kommunikationsgerät, die Schnittstelle und die Authentifizierungs-Infrastruktur jeweils ein Netzwerkmodul beinhalten, und jeweils dazu eingerichtet sind, über das Netzwerkmodul in einem Datennetzwerk untereinander zu kommunizieren. 25 30

12. Das Authentifizierungs-System nach einem der Ansprüche 9 bis 11, wobei das Kommunikationsgerät dazu eingerichtet ist: 35

- einem Nutzer über eine Nutzeroberfläche die Beantragung von Zugriffsrechten zu ermöglichen;
- in Folge einer Eingabe durch den Nutzer, durch die die Beantragung von Zugriffsrechten beantragt wird, den Nutzer zur Erfassung des Identifizierungs-Indikators aufzufordern; 40
- in Folge der Erfassung des Identifizierungs-Indikators die Anfrage an die Authentifizierungs-Infrastruktur zu übermitteln; und 45
- in Folge des Empfangens des Authentifizierungs-Tokens von der Authentifizierungs-Infrastruktur den Authentifizierungs-Indikator über die Nutzeroberfläche anzuzeigen. 50

13. Verwendung des Authentifizierungs-Systems nach einem der Ansprüche 9 bis 12 zur Ausführung der Methode zur Zugriffskontrolle nach einem der Ansprüche 1 bis 8 zur Wartung einer Personenbeförderungseinrichtung in Form eines Fahrstuhls, Fahrsteigs oder einer Fahrtreppe. 55

14. Computerprogrammprodukt zur Ausführung auf ei-

ner Schnittstelle zur Wartung einer Personenbeförderungseinrichtung in Form eines Fahrstuhls, Fahrsteigs oder einer Fahrtreppe, umfassend Befehle, die bei der Ausführung des Programms durch die Schnittstelle diese veranlassen, die folgenden Schritte auszuführen:

- Empfangen eines Berechtigungs-Tokens einer Authentifizierungs-Infrastruktur;
- Überprüfen eines eingegebenen Authentifizierungs-Indikators, wobei die Überprüfung einen Abgleich des Authentifizierungs-Indikators mit dem Berechtigungs-Token und eine Auswahl einer Berechtigungsstufe auf Basis des Berechtigungs-Tokens umfasst; und
- Wechsel in einen Wartungsmodus auf Basis des Abgleichs und der Berechtigungsstufe.

Fig. 1

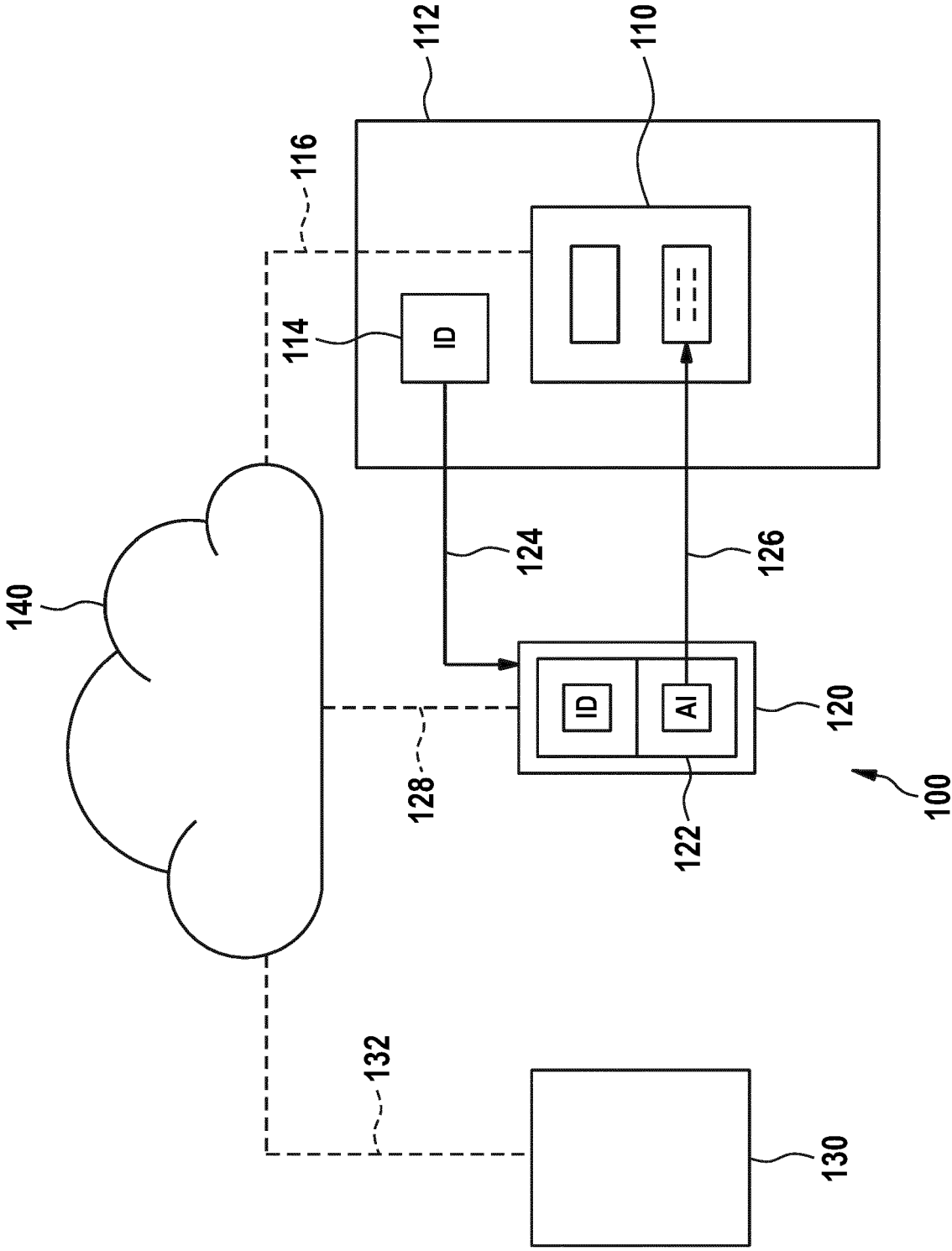


Fig. 2

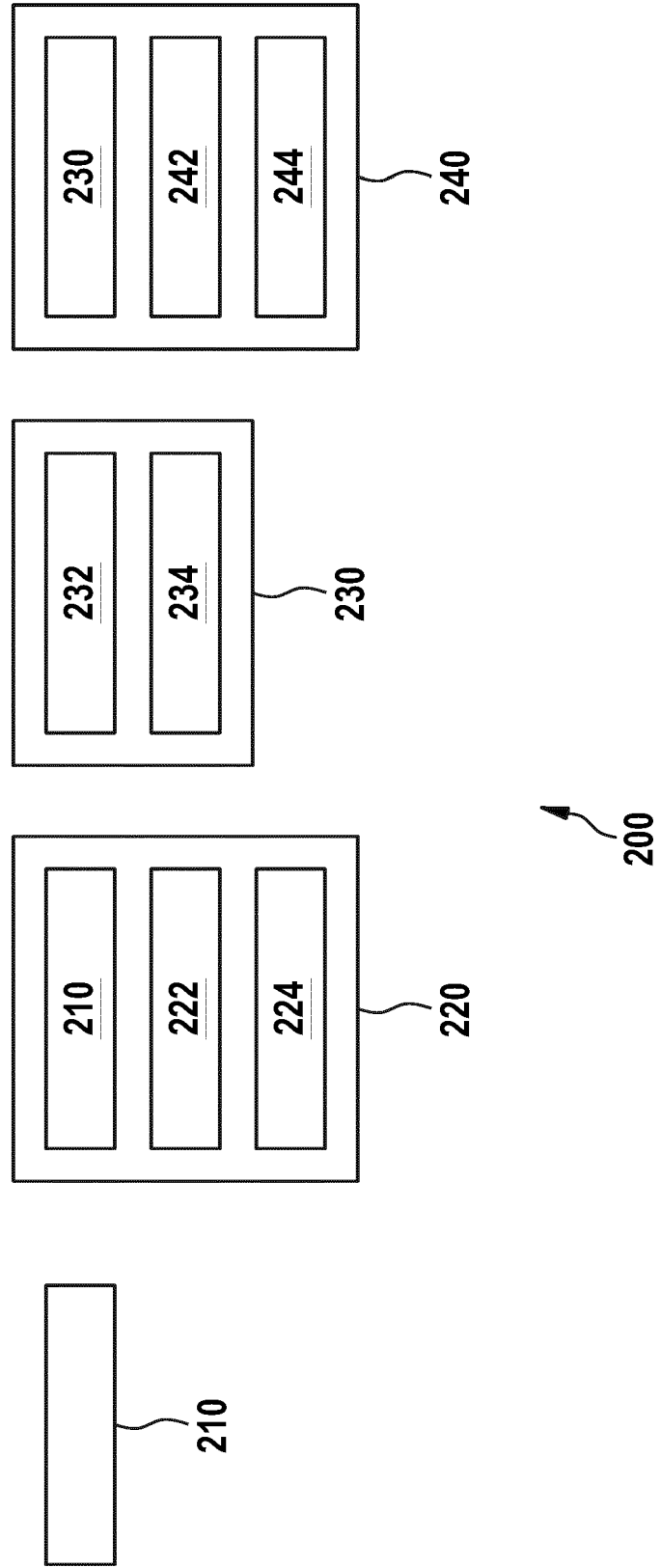
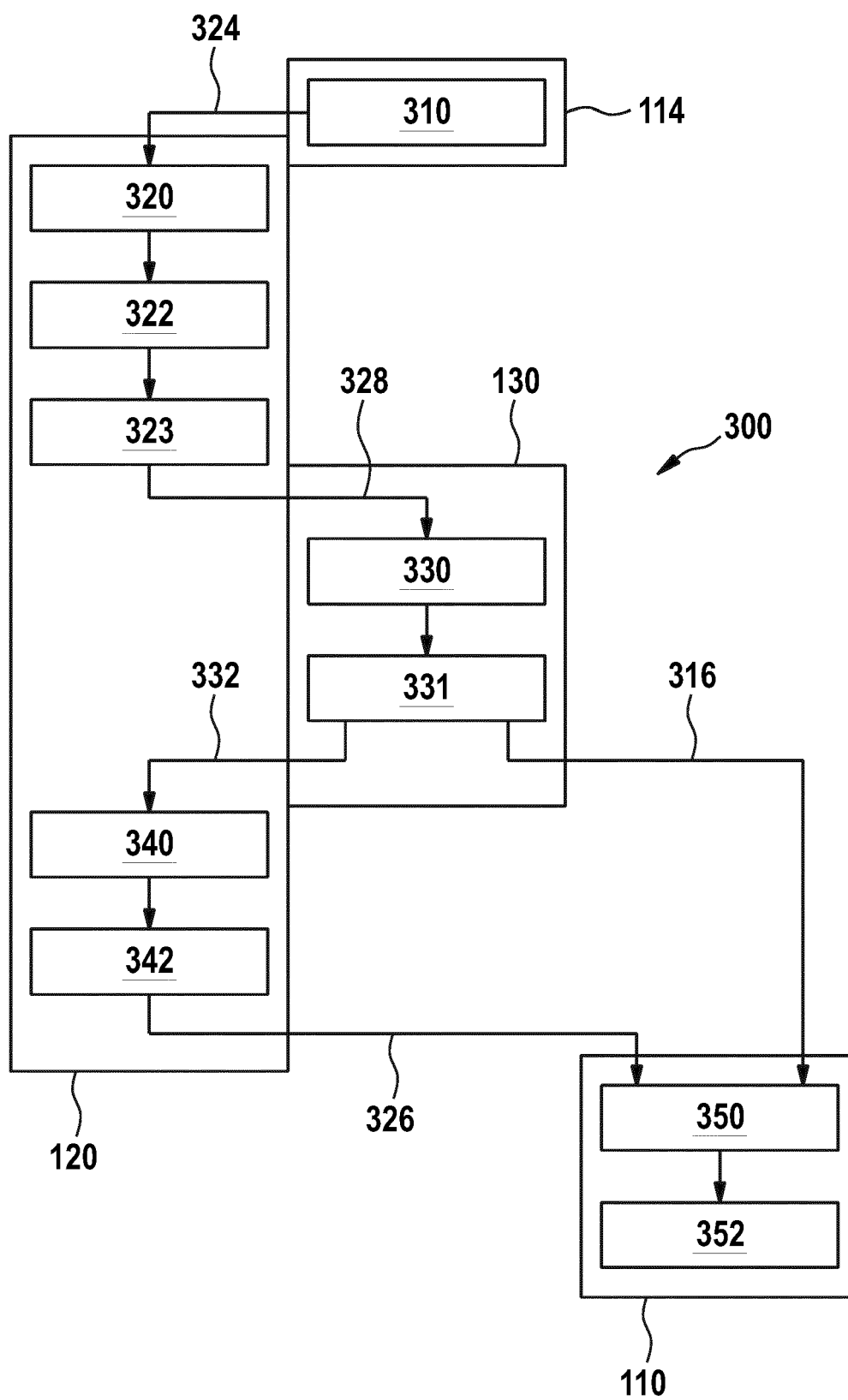


Fig. 3







## EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung

EP 22 17 2517

5

10

15

20

25

30

35

40

45

50

55

1

EPO FORM 1503 03.82 (P04C03)

EINSCHLÄGIGE DOKUMENTE			
Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
X	WO 2018/099793 A1 (INVENTIO AG [CH]) 7. Juni 2018 (2018-06-07)	1-3, 8, 9, 11-14	INV. B66B5/00
Y	* Seite 3, Zeile 4 - Seite 8, Zeile 33 * * Abbildungen 1, 2 *	5, 10	
	-----		
X	WO 2010/069347 A1 (OTIS ELEVATOR CO [US]; WILKE MICHAEL [DE] ET AL.) 24. Juni 2010 (2010-06-24)	1-4, 6, 7, 9, 11, 13, 14	
	* Seite 1, Zeile 24 - Seite 2, Zeile 15 * * Seite 2, Zeile 35 - Seite 3, Zeile 27 * * Seite 5, Zeile 9 - Seite 16, Zeile 27 * * Abbildungen 1-4 *		
	-----		
X	WO 2006/050626 A1 (INVENTIO AG [CH]; DEPLAZES ROMEO [CH]; BODMER CHRISTIAN [CH]) 18. Mai 2006 (2006-05-18)	1-3, 9, 13, 14	
	* Seite 6, Zeile 12 - Seite 10, Zeile 17 * * Seite 10, Zeile 19 - Seite 11, Zeile 20 * * Seite 18, Zeile 19 - Seite 20, Zeile 20 * * Abbildungen 1, 2 *		
	-----		
Y	EP 3 832 608 A1 (KONE CORP [FI]) 9. Juni 2021 (2021-06-09)	5, 10	
	* Absätze [0035], [0036] * * Abbildung 1 *		
	-----		
Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt			
Recherchenort <b>Den Haag</b>		Abschlußdatum der Recherche <b>26. Oktober 2022</b>	Prüfer <b>Baytekin, Hüseyin</b>
KATEGORIE DER GENANNTEN DOKUMENTE X : von besonderer Bedeutung allein betrachtet Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie A : technologischer Hintergrund O : nichtschriftliche Offenbarung P : Zwischenliteratur		T : der Erfindung zugrunde liegende Theorien oder Grundsätze E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist D : in der Anmeldung angeführtes Dokument L : aus anderen Gründen angeführtes Dokument ..... & : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument	

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

EP 22 17 2517

5 In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.  
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am  
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

26-10-2022

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
<b>WO 2018099793 A1</b>	<b>07-06-2018</b>	<b>AU 2017369390 A1</b>	<b>30-05-2019</b>
		<b>CN 110023223 A</b>	<b>16-07-2019</b>
		<b>EP 3548411 A1</b>	<b>09-10-2019</b>
		<b>US 2019276272 A1</b>	<b>12-09-2019</b>
		<b>WO 2018099793 A1</b>	<b>07-06-2018</b>
<b>WO 2010069347 A1</b>	<b>24-06-2010</b>	<b>BR PI0823337 A2</b>	<b>23-06-2015</b>
		<b>CN 102257536 A</b>	<b>23-11-2011</b>
		<b>EP 2368229 A1</b>	<b>28-09-2011</b>
		<b>KR 20110084552 A</b>	<b>25-07-2011</b>
		<b>RU 2011124771 A</b>	<b>27-01-2013</b>
		<b>US 2011247901 A1</b>	<b>13-10-2011</b>
		<b>WO 2010069347 A1</b>	<b>24-06-2010</b>
<b>WO 2006050626 A1</b>	<b>18-05-2006</b>	<b>AU 2005304247 A1</b>	<b>18-05-2006</b>
		<b>BR PI0518023 A</b>	<b>28-10-2008</b>
		<b>CA 2583131 A1</b>	<b>18-05-2006</b>
		<b>CN 101048330 A</b>	<b>03-10-2007</b>
		<b>EP 1814813 A1</b>	<b>08-08-2007</b>
		<b>ES 2432370 T3</b>	<b>03-12-2013</b>
		<b>HK 1110294 A1</b>	<b>11-07-2008</b>
		<b>JP 2008518863 A</b>	<b>05-06-2008</b>
		<b>NO 338661 B1</b>	<b>26-09-2016</b>
		<b>US 2008283342 A1</b>	<b>20-11-2008</b>
		<b>WO 2006050626 A1</b>	<b>18-05-2006</b>
<b>EP 3832608 A1</b>	<b>09-06-2021</b>	<b>CN 112989367 A</b>	<b>18-06-2021</b>
		<b>EP 3832608 A1</b>	<b>09-06-2021</b>
		<b>US 2021165542 A1</b>	<b>03-06-2021</b>

EPO FORM P0461

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