

(19)



(11)

EP 3 765 345 B1

(12)

EUROPÄISCHE PATENTSCHRIFT

(45) Veröffentlichungstag und Bekanntmachung des Hinweises auf die Patenterteilung:

25.12.2024 Patentblatt 2024/52

(51) Internationale Patentklassifikation (IPC):

B61L 19/06^(2006.01) B61L 27/20^(2022.01)

(21) Anmeldenummer: **19720404.3**

(52) Gemeinsame Patentklassifikation (CPC):

B61L 19/06; B61L 27/20; B61L 2019/065

(22) Anmeldetag: **09.04.2019**

(86) Internationale Anmeldenummer:

PCT/EP2019/058932

(87) Internationale Veröffentlichungsnummer:

WO 2019/214888 (14.11.2019 Gazette 2019/46)

(54) **VORRICHTUNG ZUR GESTEUERTEN DURCHFÜHRUNG EINER SICHERHEITSRELEVANTEN HANDLUNG IM SCHIENENVERKEHR**

DEVICE FOR CONTROLLED IMPLEMENTATION OF A SECURITY-RELEVANT OPERATION IN RAIL TRAFFIC

DISPOSITIF POUR EFFECTUER DE MANIÈRE COMMANDÉE UNE ACTION LIÉE À LA SÉCURITÉ DANS LE TRAFIC FERROVIAIRE

(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**

(72) Erfinder:

- **BRABAND, Jens**
38106 Braunschweig (DE)
- **ROSAUER, Bernd**
81673 München (DE)
- **STURM, Monika**
1190 Wien (AT)

(30) Priorität: **09.05.2018 DE 102018207306**

(43) Veröffentlichungstag der Anmeldung:

20.01.2021 Patentblatt 2021/03

(74) Vertreter: **Siemens Patent Attorneys**

**Postfach 22 16 34
80506 München (DE)**

(73) Patentinhaber: **Siemens Mobility GmbH**

81739 München (DE)

(56) Entgegenhaltungen:

**DE-A1- 102005 014 050 DE-A1- 102007 005 638
DE-A1- 102011 081 479 GB-A- 2 540 976**

EP 3 765 345 B1

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

Beschreibung

Technisches Gebiet

[0001] Gemäß einiger Ausführungsformen wird eine Vorrichtung zur gesteuerten Durchführung einer sicherheitsrelevanten Handlung im Schienenverkehr offenbart. Gemäß weiterer Ausführungsformen wird eine zentrale Autorität zur Autorisierung einer Vorrichtung zur gesteuerten Durchführung einer sicherheitsrelevanten Handlung im Schienenverkehr offenbart. Gemäß weiterer Ausführungsformen wird ein Netzwerkknoten eines Datennetzwerks zum Empfangen von Datensignalen einer Vorrichtung zur gesteuerten Durchführung einer sicherheitsrelevanten Handlung im Schienenverkehr offenbart.

Hintergrund

[0002] Anders als im Luftverkehr basieren sicherheitsrelevante Handlungen im Schienenverkehr, beispielsweise das Schalten und/oder Passieren eines Haltezeichens oder das Stellens einer Weiche, gegenwärtig in vielen Fällen auf Individualentscheidungen, das heißt sie können von einer Einzelperson getroffen und/oder umgesetzt werden. Zwar begünstigt eine derartige Handhabung ein effizientes Entscheiden und Handeln, sodass Handlungsmaßnahmen zur Umsetzung möglichst frühzeitig eingeleitet werden können. Nachteilig hieran ist jedoch, dass Entscheidungen, welche durch die Einzelperson getroffen werden, unkontrolliert erfolgen können, wodurch sich Sicherheitsrisiken ergeben. Insbesondere berücksichtigt die gegenwärtige Herangehensweise keine Spezifika einer derartigen Entscheidung für die Beurteilung, ob ein allgemeines Interesse an dem Treffen der Entscheidung durch die Einzelperson besteht. Derartige Spezifika können sich beispielsweise auf den Schwierigkeitsgrad der Entscheidung, die Auswirkungen der jeweiligen Entscheidung sowie den Sachstand der betreffenden Einzelperson beziehen und sind unter Sicherheitsaspekten für eine spezifische Ermächtigungserteilung der Einzelperson von enormer Bedeutung.

[0003] D10 2005 014 050 A1 D1 offenbart ein Gerät, das Signale an technische Geräte sendet und Zugriffskontrolldaten speichert, die bestimmen, auf welche Funktionalität der Benutzer zugreifen darf.

[0004] GB 2540976 A1 offenbart eine Zugriffskontrollverfahren für eine eingeschränkte Ressource in einem vernetzten Computersystem, wobei eine Blockkette-Datenstruktur von Miner-Komponenten validierte Datensätze speichert.

Kurzzusammenfassung der Erfindung

[0005] Demzufolge besteht ein Bedarf ein effizientes Verfahren zur Steuerung von sicherheitsrelevanten Handlungen im Schienenverkehr bereitzustellen.

[0006] Gemäß einiger Ausführungsformen liegt daher

die Aufgabe zugrunde technische Mittel bereitzustellen, mittels welchen ein effizientes Anfragen betreffend die Zulässigkeit des Durchführens einer sicherheitsrelevanten Handlung im Schienenverkehr ermöglicht wird.

[0007] Gemäß einiger weiterer Ausführungsformen liegt daher die Aufgabe zugrunde technische Mittel bereitzustellen, mittels welchen ein effizientes Autorisieren betreffend spezifische sicherheitsrelevante Handlungen im Schienenverkehr ermöglicht wird.

[0008] Gemäß einiger Ausführungsformen liegt daher die Aufgabe zugrunde technische Mittel bereitzustellen, mittels welchen ein Zulassen des Durchführens einer sicherheitsrelevanten Handlung im Schienenverkehr bei Zulässigkeit der Handlung in effizienter Weise ermöglicht wird.

[0009] Diese Aufgaben werden gemäß entsprechender Ausführungsformen durch eine Vorrichtung zur gesteuerten Durchführung einer sicherheitsrelevanten Handlung im Schienenverkehr gemäß Anspruch 1, durch eine zentrale Autorität zur Autorisierung einer Vorrichtung zur gesteuerten Durchführung einer sicherheitsrelevanten Handlung im Schienenverkehr gemäß Anspruch 8 sowie durch einen Netzwerkknoten eines Datennetzwerks zum Empfangen von Datensignalen einer Vorrichtung zur gesteuerten Durchführung einer sicherheitsrelevanten Handlung im Schienenverkehr gemäß Anspruch 12 gelöst. Weitere diese Ausführungsformen betreffende Ausgestaltungen werden in den abhängigen Ansprüchen beansprucht.

[0010] Gemäß einer Ausführungsform wird eine Vorrichtung offenbart, welche zur gesteuerten Durchführung einer sicherheitsrelevanten Handlung im Schienenverkehr eingerichtet ist. Dabei kann die Vorrichtung in einem Datennetzwerk angeordnet werden. Die Vorrichtung weist dabei eine Aufnahmeeinrichtung auf, welche zum Aufnehmen einer Autorisierungsinformation von einer zentralen Autorität eingerichtet ist. Die Vorrichtung weist ferner eine Speichereinrichtung auf, welche zum Speichern der Autorisierungsinformation eingerichtet ist. Die Vorrichtung weist ferner eine Instruktionseinrichtung auf, welche zum wahlweisen Bereitstellen einer Instruktion zur Durchführung der sicherheitsrelevanten Handlung in Abhängigkeit von der Autorisierungsinformation eingerichtet ist. Die Vorrichtung weist ferner eine Ausgabereinrichtung auf, welche zur Ausgabe eines Datensignals eingerichtet ist, wobei das Datensignal indikativ für die bereitgestellte Instruktion zur Durchführung der sicherheitsrelevanten Handlung sowie für die gespeicherte Autorisierungsinformation ist. Die Vorrichtung weist ferner eine Identifikationseinrichtung auf, welche dazu eingerichtet ist, einen Identifikationsparameter (16) der Vorrichtung zu verschlüsseln und den verschlüsselten Identifikationsparameter an eine zentrale Autorität zu übertragen. Die durch die Aufnahmeeinrichtung aufgenommenen Autorisierungsinformation basiert auf dem übertragbaren verschlüsselten Identifikationsparameter.

[0011] Basierend auf einem derartigen Ansatz wird es ermöglicht, Autorisierungsinformationen betreffend spe-

zifische Ermächtigungen zur Durchführung sicherheitsrelevanter Handlungen im Schienenverkehr zu erlangen und hieraus situativ erwünschte spezifische Ermächtigungen auszuwählen. Aus den ausgewählten Ermächtigungen können Instruktionen ermittelt werden, welchen ergänzend gespeicherte Autorisierungsinformationen zugefügt werden, wobei letztere Zusatzinformationen betreffend das Erlöschen dieser Autorisierungsinformationen aufweisen können. Durch das kombinierte Ausgeben dieser Informationen als gemeinsames Datensignal werden Anfrageinformationen betreffend ein Durchführen einer sicherheitsrelevanten Handlung im Schienenverkehr auf effiziente Weise bereitgestellt, wobei die erwünschte Handlungskontrolle sicherheitsrelevanter Entscheidungen im Schienenverkehr verbessert gewährleistet werden kann.

[0012] Gemäß einer weiteren Ausführungsform wird eine zentrale Autorität zur Autorisierung einer Vorrichtung zur gesteuerten Durchführung einer sicherheitsrelevanten Handlung im Schienenverkehr offenbart. Dabei weist die zentrale Autorität eine erste Empfangseinrichtung auf, welche dazu eingerichtet ist, einen verschlüsselten Identifikationsparameter einer Vorrichtung zu empfangen. Die zentrale Autorität weist dabei ferner eine Entschlüsselungseinrichtung zur Entschlüsselung des verschlüsselten Identifikationsparameters der Vorrichtung auf. Die zentrale Autorität weist ferner eine Allokationseinrichtung auf, welche zum Zuordnen einer Autorisierungsinformation zu dem entschlüsselten Identifikationsparameter der Vorrichtung eingerichtet ist. Die zentrale Autorität weist ferner eine Übertragungseinrichtung auf, welche zum Übertragen der dem Identifikationsparameter zugeordneten Autorisierungsinformation an die zugehörige Vorrichtung eingerichtet ist.

[0013] Basierend auf einem derartigen Ansatz wird es ermöglicht, der Vorrichtung zur gesteuerten Durchführung einer sicherheitsrelevanten Handlung im Schienenverkehr eine individualisierte Autorisierungsinformation auf der Basis eines einzigartigen Identifikationsparameters zu ermitteln, sodass der Vorrichtung eine möglichst passgenaue Berechtigungsinformation zugeführt werden kann. Durch die Einrichtung zur Entschlüsselung unmittelbar vor Zuweisung einer passgenauen Autorisierungsinformation wird ferner die Manipulationssicherheit der Identifikationsdaten der betreffenden Vorrichtung verbessert.

[0014] Gemäß einer weiteren Ausführungsform wird ein Netzwerkknoten eines Datennetzwerks offenbart, welcher zum Empfangen von Datensignalen einer Vorrichtung zur gesteuerten Durchführung einer sicherheitsrelevanten Handlung im Schienenverkehr eingerichtet ist. Der Netzwerkknoten weist dabei eine zweite Empfangseinrichtung auf, welche zum Empfangen des Datensignals der Vorrichtung, welches eine bereitgestellte Instruktion zur Durchführung der sicherheitsrelevanten Handlung sowie Daten einer gespeicherten Autorisierungsinformation aufweist, eingerichtet ist. Der Netzwerkknoten weist ferner eine Prüfeinrichtung auf, welche

dazu eingerichtet ist basierend auf dem Datensignal zu prüfen, ob die bereitgestellte Instruktion zur Durchführung der sicherheitsrelevanten Handlung zulässig ist. Der Netzwerkknoten weist ferner eine zweite Hinterlegungseinrichtung auf, welche abhängig von dem Prüfen der Prüfeinrichtung das empfangene Datensignal in einer verteilten Datenbank hinterlegen kann.

[0015] Basierend auf einem derartigen Ansatz wird ein Verfielfältigen von zulässigen Datensignalen mittels einer verteilten Datenbank, wodurch eine sicherheitsrelevante Handlung im Schienenverkehr ermöglicht werden kann, abhängig von der Datensignalprüfung der Prüfeinrichtung ermöglicht. Somit wird das Zuführen der Daten zu der verteilten Datenbank zuverlässig und mit möglichst einfachen technischen Mitteln bewerkstelligt.

[0016] Unter einer sicherheitsrelevanten Handlung im Sinne der Erfindung ist eine Maßnahme zu verstehen, welche die Sicherheit eines Ablaufes im Schienenverkehr beeinträchtigen kann. Dabei kann vorgesehen sein, dass die Handlung von einer am Schienenverkehr beteiligten Person vollzogen werden kann. Basierend auf der sicherheitsrelevanten Handlung kann ferner vorgesehen sein, dass die Fortbewegung eines Schienenverkehrsteilnehmers beeinträchtigt werden kann. Auch kann vorgesehen sein, dass durch die sicherheitsrelevante Handlung der Zeitpunkt des Fortbewegens des Schienenverkehrsteilnehmers und/oder die Richtung des Fortbewegens des Schienenverkehrsteilnehmers kontrolliert wird. Beispielsweise kann sich eine derartige sicherheitsrelevante Handlung auf eine Weichenstellung oder ein Haltezeichen im Schienenverkehr beziehen.

[0017] Unter einer Autorisierungsinformation im Sinne der Erfindung sind elektronische Daten zu verstehen, welche Informationen betreffend eine Berechtigung des Durchführens der sicherheitsrelevanten Handlung umfassen. Es kann dabei vorgesehen sein, dass derartige Autorisierungsinformationen von einer zentralen Autorität ausgegeben werden.

[0018] Unter einer zentralen Autorität im Sinne der Erfindung ist ein Netzwerkknoten eines elektronischen Datennetzes zu verstehen, welcher für eine Vielzahl weiterer Netzwerkknoten Informationen betreffend deren Berechtigung zum Durchführen der sicherheitsrelevanten Handlung ausgeben kann. Eine entsprechende zentrale Autorität kann durch ein elektronisches Stellwerk im Schienenverkehr ausgebildet werden.

[0019] Unter einer Instruktion im Sinne der Erfindung ist eine Anweisung zur Ausübung einer sicherheitsrelevanten Handlung im Schienenverkehr zu verstehen, deren Zulässigkeit auf Basis bestehender Berechtigungen überprüft werden kann.

[0020] Unter einem Identifikationsparameter im Sinne der Erfindung sind Daten zu verstehen, welche für ein elektronisches Gerät kennzeichnend sind. Derartige Identifikationsparameter können zum Übertragen innerhalb eines Datennetzwerkes vorgesehen sein und auf den Entsender des Identifikationsparameters hinweisen.

Derartige Identifikationsparameter können zum Übertragen an eine zentrale Autorität vorgesehen sein und eine Anfrage für eine Autorisierung für sicherheitsrelevante Handlungen konstituieren. Dabei kann vorgesehen sein, dass jedes elektronische Gerät einen unterschiedlichen Identifikationsparameter an die zentrale Autorität übertragen kann. Derartige Identifikationsparameter können in verschlüsselter und entschlüsselter Form vorliegen. Durch eine Entschlüsselungsvorrichtung kann vorgesehen sein, dass ein verschlüsselter Identifikationsparameter in einen entschlüsselten Identifikationsparameter transformiert wird.

[0021] Unter einer verteilten Datenbank im Sinne der Erfindung ist eine Sicherungseinheit für Daten zu verstehen, wobei die Sicherung der Daten an unterschiedlichen Lokalisationen erfolgt. Beispielsweise kann eine derartig verteilte Datenbank als Blockchain basierte Datenbank ausgebildet sein.

[0022] Unter einem Smart Contract im Sinne der Erfindung ist ein Computerprotokoll zu verstehen, welches in einer elektronischen Autorisierungsinformation implementiert ist und zur Prüfung der Zulässigkeit einer sicherheitsrelevanten Handlung im Schienenverkehr eingerichtet ist. Dabei kann vorgesehen sein, dass der Smart Contract die durch die Ausgabeeinrichtung ausgegebenen Datensignale prüft.

[0023] Gemäß einer Ausführungsform der Vorrichtung ist die Speichereinrichtung zum Anpassen der gespeicherten Autorisierungsinformation in Abhängigkeit von der Ausgabe des Datensignals eingerichtet.

[0024] Auf diese Weise können bereits angefragte und/oder durchgeführte sicherheitsrelevante Handlungen im Schienenverkehr bei der Zulässigkeit neuer Anfragen berücksichtigt werden. Hierdurch kann die Entscheidung betreffend die Zulässigkeit einer angefragten sicherheitsrelevanten Handlung zielgenauer auf Basis vergangener Vorkommnisse erfolgen.

[0025] Gemäß einer Ausführungsform der Vorrichtung weist die Autorisierungsinformation räumliche und/oder zweckgebundene Berechtigungsinformationen zur Durchführung der sicherheitsrelevanten Handlung auf, und die Instruktionseinrichtung ist dazu eingerichtet, um die Instruktion in Übereinstimmung mit der räumlichen und/oder zweckgebundenen Berechtigungsinformation bereitzustellen.

[0026] Auf diese Weise können Berechtigungen, welche kriterienspezifisch eine hohe Ähnlichkeit aufweisen, als gemeinsame Autorisierungsinformationen ausgegeben werden, wodurch sich Effizienzvorteile ergeben.

[0027] Gemäß einer Ausführungsform der Vorrichtung umfasst die Autorisierungsinformation Einheiten einer Kryptowährung.

[0028] Auf diese Weise kann eine Berechtigungsinformation betreffend sicherheitsrelevanter Maßnahmen mittels digitaler Einheiten auf eine endliche, klar definierte Menge limitiert werden.

[0029] Gemäß einer Ausführungsform der Vorrichtung umfasst das auszugebende Datensignal mindestens eine

Einheit der Kryptowährung. Gemäß einer Ausführungsform der Vorrichtung ist die Ausgabeeinrichtung dazu eingerichtet, bei der Ausgabe der Daten der gespeicherten Autorisierungsinformation mindestens eine Einheit der Kryptowährung aus der Speichereinrichtung zu entfernen.

[0030] Nach Verbrauch derartigen Anfragen kann es somit möglich sein, dass eine darüber hinausgehende Anfrage zum Durchführen der sicherheitsrelevanten Handlung mangels Zulässigkeit abgelehnt wird, da die Vorrichtung dazu eingerichtet ist vergangene ausgegebene Datensignale festzuhalten.

[0031] Gemäß einer Ausführungsform der Vorrichtung sind die Einheiten der Kryptowährung unterscheidbar.

[0032] Basierend auf der Unterscheidbarkeit der Kryptowährungseinheiten können Spezifika der jeweiligen Berechtigungsinformation unmittelbar der jeweiligen Währungseinheit entnommen werden, sodass ein Auslesen der Berechtigungsinformationen von den Einheiten der Kryptowährung mit einfachen technischen Mitteln durchführbar ist.

[0033] Gemäß einer Ausführungsform der Vorrichtung umfasst die Autorisierungsinformation ausführbare Smart Contracts.

[0034] Auf diese Weise können weitere zulässigkeitsrelevante Aspekte, welche die sicherheitsrelevante Handlung im Schienenverkehr betreffen, in einem effizient bearbeitbaren Protokoll implementiert werden.

[0035] Gemäß einer Ausführungsform der Vorrichtung ist die Ausgabeeinrichtung zur Ausgabe des Datensignals an ein Steuergerät eines elektronischen Stellwerks des Schienenverkehrs eingerichtet.

[0036] Hierdurch wird es ermöglicht, Informationen betreffend die Zulässigkeit einer sicherheitsrelevanten Handlung im Schienenverkehr an einem Ort bereitzustellen, welcher zum Treffen artgerechter Folgemaßnahmen eingerichtet ist, sodass sich hierdurch Effizienzvorteile beim Erwirken entsprechender sicherheitsrelevanter Handlungen ergeben.

[0037] Gemäß der Erfindung, weist die Vorrichtung ferner eine Identifikationseinrichtung auf, welche dazu eingerichtet ist, einen Identifikationsparameter der Vorrichtung zu verschlüsseln und den verschlüsselten Identifikationsparameter an die zentrale Autorität zu übertragen. Gemäß der Erfindung basiert die durch die Aufnahmeeinrichtung aufnehmbare Autorisierungsinformation auf dem übertragbaren verschlüsselten Identifikationsparameter.

[0038] Auf diese Weise kann die zentrale Autorität vorrichtungsspezifisch und individuell Autorisierungsdaten an die betreffende Vorrichtung ausgeben. Dabei können Aspekte der Vorrichtung, beispielsweise ihres Aufenthaltsortes, sowie der Bedienperson der Vorrichtung, beispielsweise dessen Fachkenntnisse und Erfahrung, berücksichtigt werden.

[0039] Gemäß einer Ausführungsform der Vorrichtung weist diese ferner eine erste Hinterlegungseinrichtung auf, welche zur Hinterlegung einer Aufwendung bei der

zentralen Autorität abhängig von der aufgenommenen Autorisierungsinformation eingerichtet ist.

[0040] Auf diese Weise werden Anreize geschaffen, welche es der zentralen Autorität ermöglichen oder zumindest erleichtern, die erteilte Autorisierung zu einem späteren Zeitpunkt zu widerrufen. Somit kann die zentrale Autorität eine erteilte Autorisierung bei Veränderung der äußeren Umstände oder auf Basis eines jeweiligen Benutzerverhaltens der Vorrichtung nachträglich anpassen.

[0041] Gemäß einer Ausführungsform der zentralen Autorität weist diese ferner eine Publikationseinrichtung auf, mittels welcher ein Identifikationsschlüssel der zentralen Autorität öffentlich zugänglich gemacht werden kann.

[0042] Auf diese Weise wird ein Vertrauensanker der zentralen Autorität öffentlich zur Verfügung gestellt und somit die Sicherheit einer Vorrichtung, die die Autorisierung durch die zentrale Autorität erfragt, gewährleistet.

[0043] Gemäß einer Ausführungsform der zentralen Autorität ist diese dazu eingerichtet den entschlüsselten Identifikationsparameter in einer verteilten Datenbank zu hinterlegen.

[0044] Auf diese Weise kann ein Dritter, welcher an dem Datennetz beteiligt ist, die Autorisierungen der Vorrichtung zur gesteuerten Durchführung der sicherheitsrelevanten Handlung im Schienenverkehr verbessert einsehen und kann somit weitere, von dem Netzwerkknoten dieser Vorrichtung ausgehende Anfragen verbessert beurteilen.

[0045] Gemäß einer Ausführungsform der zentralen Autorität ist diese dazu eingerichtet das Hinterlegen des entschlüsselten Identifikationsparameters in der verteilten Datenbank zu widerrufen.

[0046] Auf diese Weise kann die zentrale Autorität eine Berechtigungsänderung der Vorrichtung der Öffentlichkeit möglichst zeitnah publik machen.

[0047] Gemäß einer Ausführungsform des Netzwerkknotens wird dieser durch ein Steuergerät eines elektronischen Stellwerks implementiert.

[0048] Hierdurch wird es ermöglicht, Informationen betreffend die Zulässigkeit einer sicherheitsrelevanten Handlung im Schienenverkehr an einem Ort zu erlangen, welcher zum Treffen artgerechter Folgemaßnahmen eingerichtet ist, sodass sich hierdurch Effizienzvorteile beim Erwirken entsprechender sicherheitsrelevanter Handlungen ergeben.

[0049] Gemäß einer Ausführungsform der zentralen Autorität oder des Netzwerkknotens ist die verteilte Datenbank eine Blockchain basierte Datenbank.

[0050] Auf diese Weise wird es ermöglicht, dass Informationen, welche einmal in die verteilte Datenbank aufgenommen wurden, aufgrund eines speziellen, die Blockchain betreffenden Verschlüsselungsverfahrens in der verteilten Datenbank verbleiben und somit jederzeit für alle Netzwerkteilnehmer einsehbar sind. Dadurch wird es Dritten erleichtert, Situationen betreffend Zulässigkeitsanfragen zur Durchführung einer sicherheitsre-

levanten Handlung in möglichst sachgerechter Weise und basierend auf möglichst vollständigen diesbezüglichen Kenntnissen zu beurteilen.

[0051] Die im Vorstehenden beschriebenen, die jeweilige Ausführungsform betreffenden Aspekte und die dazugehörigen, zur Weiterbildung der Vorrichtung, der zentralen Autorität sowie des Netzwerkknoten offenbarten Vorteile gelten gleichsam auf für zugehörige Verfahren, welche basierend auf den beanspruchten Gegenständen durchführbar sind.

[0052] Unter einer Berechtigungsinformation im Sinne der Erfindung sind Informationen betreffend eine Autorisierung zur Durchführung einer sicherheitsrelevanten Handlung zu verstehen, durch welche die Charakteristika betreffend diese Autorisierung definiert werden können. Derartige Berechtigungsinformationen können beispielsweise die Art und/oder das Ausmaß einer derartigen Autorisierung spezifizieren. Eine derartige Spezifikation kann beispielsweise von sachlicher und/oder räumlicher und/oder zeitlicher Natur sein.

[0053] Unter einer Kryptowährung im Sinne der Erfindung ist ein auf kryptographischen Methoden basierendes digitales Zahlungsmittel zu verstehen, dessen Einheiten zwischen verschiedenen Teilnehmern eines Datennetzwerkes austauschbar sind. Dabei kann vorgesehen sein, dass die Einheiten der Kryptowährung eindeutig identifizierbar sind.

[0054] Obige sowie weitere Vorteile, Merkmale und Anwendungsmöglichkeiten einer Ausführungsform ergeben sich aus der nachfolgenden Beschreibung von bevorzugten Ausführungsbeispielen anhand von wenigsten teilweise schematischen Figuren.

KURZE BESCHREIBUNG DER FIGUREN

[0055]

In Figur 1 ist eine Vorrichtung zur gesteuerten Durchführung einer sicherheitsrelevanten Handlung im Schienenverkehr gemäß einer Ausführungsform schematisch dargestellt.

In Figur 2 ist eine zentrale Autorität zur Autorisierung einer Vorrichtung zur gesteuerten Durchführung einer sicherheitsrelevanten Handlung im Schienenverkehr gemäß einer Ausführungsform schematisch dargestellt.

In Figur 3 ist ein Netzwerkknoten eines Datennetzwerks zum Empfangen von Datensignalen einer Vorrichtung zur gesteuerten Durchführung einer sicherheitsrelevanten Handlung im Schienenverkehr gemäß einer Ausführungsform schematisch dargestellt.

DETAILLIERTE BESCHREIBUNG VON AUSFÜHRUNGSFORMEN

[0056] In Figur 1 ist eine Vorrichtung 1 zur gesteuerten Durchführung einer sicherheitsrelevanten Handlung 2 im Schienenverkehr 3 gemäß einer Ausführungsform schematisch dargestellt. Die Vorrichtung 1 kann dabei in einem Datennetzwerk 4 angeordnet sein. Das gesteuerte Durchführen der sicherheitsrelevanten Handlung 2 im Schienenverkehr 3 kann sich auf ein Schienenverkehrssteuerelement 31 beziehen. Ein derartiges Schienenverkehrssteuerelement 31 kann sicherheitsrelevant auf den Schienenverkehr 3 einwirken. So kann durch ein derartiges Schienenverkehrssteuerelement 31 die Fortbewegung von Fahrzeugen im Schienenverkehr 3 beeinträchtigt werden. Beispielsweise kann sich das Schienenverkehrssteuerelement 31 auf ein Haltezeichen, eine Signallampe oder eine Weichenstellung beziehen.

[0057] Die Vorrichtung 1 kann dabei in Datenkommunikation mit einer zentralen Autorität 7 und/oder mit einem Steuergerät 13 eines elektronischen Stellwerks 14 stehen. Die Vorrichtung 1 kann dabei eine Aufnahmeeinrichtung 5 aufweisen, welche zum Aufnehmen einer Autorisierungsinformation 6 von der zentralen Autorität 7 eingerichtet ist. Dabei kann die Autorisierungsinformation 6 räumliche und/oder zweckgebundene Berechtigungsinformationen zur Durchführung sicherheitsrelevanter Handlungen 2 aufweisen. Ferner kann die Autorisierungsinformation 6 Einheiten einer Kryptowährung umfassen, wobei vorgesehen sein kann, dass die Einheiten dieser Kryptowährung unterscheidbar sind. Die Autorisierungsinformation 6 kann ferner ausführbare Smart-Contracts umfassen.

[0058] Die Vorrichtung 1 kann ferner eine Speichereinrichtung 8 aufweisen, welche zum Speichern der Autorisierungsinformation 6 eingerichtet ist.

[0059] Die Vorrichtung 1 kann ferner eine Instruktionseinrichtung 9 aufweisen, die zum wahlweisen Bereitstellen einer Instruktion 10 zur Durchführung der sicherheitsrelevanten Handlung 2 in Abhängigkeit von der Autorisierungsinformation 6 eingerichtet ist. Beispielsweise kann die Instruktionseinrichtung 9 eine oder mehrere Berechtigungsinformationen der Autorisierungsinformation 6 auswählen und die ausgewählten Berechtigungsinformationen als Instruktion 10 bereitstellen. Dabei kann die Instruktionseinrichtung 9 dazu eingerichtet sein, die Instruktion 10 in Übereinstimmung mit einer räumlichen und/oder zweckgebundenen Berechtigungsinformation bereitzustellen.

[0060] Die Vorrichtung 1 kann ferner eine Ausgabeeinrichtung 11 aufweisen, welche zur Ausgabe eines Datensignals 12, welches indikativ für die bereitgestellte Instruktion 10 zur Durchführung der sicherheitsrelevanten Handlung 2 sowie für die gespeicherte Autorisierungsinformation 6' ist, eingerichtet ist. Dabei kann gemäß einer Ausführungsform vorgesehen sein, dass das Datensignal 12 die bereitgestellte Instruktion 10 und die gespeicherte Autorisierungsinformation 6' ausgibt. Da-

bei kann das ausgebbare Datensignal 12 mindestens eine Einheit einer Kryptowährung umfassen. Ferner kann die Ausgabeeinrichtung dazu eingerichtet sein, bei der Ausgabe der Daten der gespeicherten Autorisierungsinformation 6' mindestens eine Einheit der Kryptowährung aus der Speichereinrichtung 8 zu entfernen. Entsprechend kann die Speichereinrichtung 8 zum Anpassen der gespeicherten Autorisierungsinformation 6' in Abhängigkeit von der Ausgabe des Datensignals 12 eingerichtet sein. Eine entsprechende Anpassung kann beispielsweise durch ein von dem Steuergerät 13 des elektronischen Stellwerks 14 ausgehenden Anpassungssignal 32 ermöglicht werden, wobei die Ausgabeeinrichtung 11 zur Ausgabe des Datensignals 12 an das Steuergerät 13 des elektronischen Stellwerks 14 des Schienenverkehrs 3 eingerichtet ist.

[0061] Die Vorrichtung 1 kann ferner eine Identifikationseinrichtung 15 aufweisen, welche dazu eingerichtet ist, einen Identifikationsparameter 16 der Vorrichtung 1 zu verschlüsseln und den verschlüsselten Identifikationsparameter 16' an die zentrale Autorität 7 zu übertragen. Dabei kann die durch die Aufnahmeeinrichtung 5 aufnehmbare Autorisierungsinformation 6 auf dem übertragbaren verschlüsselten Identifikationsparameter 16' basieren.

[0062] Die Vorrichtung 1 kann ferner eine erste Hinterlegungseinrichtung 17 aufweisen, welche zur Hinterlegung einer Aufwendung 18 bei der zentralen Autorität 7 abhängig von der aufgenommenen Autorisierungsinformation 6 eingerichtet ist.

[0063] In Figur 2 ist eine zentrale Autorität 7 zur Autorisierung einer Vorrichtung 1 zur gesteuerten Durchführung einer sicherheitsrelevanten Handlung 2 im Schienenverkehr 3 gemäß einer Ausführungsform schematisch dargestellt. Dabei kann die zentrale Autorität 7 mit der Vorrichtung 1 in einem Datenaustausch stehen. Hierbei kann beispielsweise eine Aufwendung 18 von der Vorrichtung 1 zu der zentralen Autorität 7 übertragen werden.

[0064] Die zentrale Autorität 7 kann eine erste Empfangseinrichtung 19 aufweisen, welche dazu eingerichtet ist, einen verschlüsselten Identifikationsparameter 16' der Vorrichtung 1 zu empfangen. Die zentrale Autorität 7 kann ferner eine Entschlüsselungseinrichtung 20 zur Entschlüsselung des verschlüsselten Identifikationsparameter 16' der Vorrichtung 1 aufweisen. Ferner kann die zentrale Autorität 7 eine Allokationseinrichtung 21 aufweisen, welcher der entschlüsselte Identifikationsparameter 16 zugeführt werden kann. Hierauf basierend kann die Allokationseinrichtung 21 zum Zuordnen einer Autorisierungsinformation 6 zu dem entschlüsselten Identifikationsparameter 16 der Vorrichtung 1 eingerichtet sein. Es kann ferner vorgesehen sein, dass diese Autorisierungsinformation 6 einer Übertragungseinrichtung 22 zugeführt wird, welche zum Übertragen der dem Identifikationsparameter 16 zugeordneten Autorisierungsinformation 6 an die zugehörige Vorrichtung 1 eingerichtet ist.

[0065] Die zentrale Autorität 7 kann ferner eine Publikationseinrichtung 23 aufweisen, mittels welcher ein Identifikationsschlüssel 24 der zentralen Autorität 7 öffentlich zugänglich gemacht werden kann. Zur öffentlichen Zugänglichmachung kann beispielsweise ein Öffentlichkeitsbereich 33 vorgesehen sein.

[0066] Es kann ferner vorgesehen sein, dass die zentrale Autorität 7 in einem Datenaustausch mit einer verteilten Datenbank 25 steht. Dabei kann vorgesehen sein, dass die zentrale Autorität 7 dazu eingerichtet ist, den entschlüsselten Identifikationsparameter 16 in der verteilten Datenbank 25 zu hinterlegen. Eine derartige Hinterlegung kann vorübergehend vorgesehen sein, da die zentrale Autorität 7 dazu eingerichtet sein kann, das Hinterlegen des entschlüsselten Identifikationsparameters 16 in der verteilten Datenbank 15 mittels eines Widerrufssignals 34 zu widerrufen. Es sei darauf hingewiesen, dass die verteilte Datenbank 25 als Blockchain basierte Datenbank 30, auch Digital Ledger genannt, eingerichtet sein kann.

[0067] In Figur 3 ist ein Netzwerkknoten 26 eines Datennetzwerks zum Empfangen von Datensignalen 12 einer Vorrichtung 1 zur gesteuerten Durchführung einer sicherheitsrelevanten Handlung 2 im Schienenverkehr 3 gemäß einer Ausführungsform schematisch dargestellt. Der Netzwerkknoten 26 kann dabei durch ein Steuergerät 13 eines elektronischen Stellwerks 14 implementiert werden. Dabei kann das Steuergerät 13 in Datenaustausch mit der Vorrichtung 1 stehen.

[0068] Der Netzwerkknoten 26, gemäß der Ausführungsform aus Figur 3 durch das Steuergerät 13 ausgebildet, kann eine zweite Empfangseinrichtung 27 aufweisen, welche zum Empfangen des Datensignals 12 der Vorrichtung 1 eingerichtet ist, wobei das Datensignal 12 eine bereitgestellte Instruktion 10 zur Durchführung einer sicherheitsrelevanten Handlung 2 sowie Daten einer gespeicherten Autorisierungsinformation 6' aufweist. Ferner kann das Steuergerät 13 gemäß der Ausführungsform aus Figur 3 eine Prüfeinrichtung 28 aufweisen, welche dazu eingerichtet ist, basierend auf dem Datensignal 12 zu prüfen, ob die bereitgestellte Instruktion 10 zur Durchführung der sicherheitsrelevanten Handlung 2 zulässig ist. Das Steuergerät 13 gemäß der Ausführungsform aus Figur 3 kann ferner eine zweite Hinterlegungseinrichtung 29 aufweisen, welche das Datensignal 12 und ein Prüfsignal 35, welches aus der Prüfung der Prüfeinrichtung 28 resultieren kann, zugeführt werden kann. Dabei kann die zweite Hinterlegungseinrichtung 29 dazu eingerichtet sein, abhängig von dem Prüfen der Prüfeinrichtung 28 das empfangene Datensignal 12 in einer verteilten Datenbank 25 zu hinterlegen. Hierbei kann vorgesehen sein, dass die verteilte Datenbank 25 eine Blockchain basierte Datenbank 30, auch Digital Ledger genannt, ist.

Bezugszeichenliste

[0069]

1	Vorrichtung
2	Sicherheitsrelevante Handlung
3	Schienenverkehr
4	Datennetzwerk
5	5 Aufnahmeeinrichtung
6	6 Autorisierungsinformation
6'	6' Gespeicherte Autorisierungsinformation
7	7 Zentrale Autorität
8	8 Speichereinrichtung
10	9 Instruktionseinrichtung
10	10 Instruktion
11	11 Ausgabereinrichtung
12	12 Datensignal
13	13 Steuergerät
15	14 Elektronisches Stellwerk
15	15 Identifikationseinrichtung
16	16 Identifikationsparameter
16'	16' Verschlüsselter Identifikationsparameter
17	17 Hinterlegungseinrichtung
20	18 Aufwendung
19	19 Erste Empfangseinrichtung
20	20 Entschlüsselungseinrichtung
21	21 Allokationseinrichtung
22	22 Übertragungseinrichtung
25	23 Publikationseinrichtung
24	24 Identifikationsschlüssel
25	25 Verteilte Datenbank
26	26 Netzwerkknoten
27	27 Zweite Empfangseinrichtung
30	28 Prüfeinrichtung
29	29 Zweite Hinterlegungseinrichtung
30	30 Blockchain basierte Datenbank
31	31 Schienenverkehrssteuerelement
32	32 Anpassungssignal
35	33 Öffentlichkeitsbereich
34	34 Widerrufssignal
35	35 Prüfsignal

Patentansprüche

1. Vorrichtung (1), eingerichtet zur gesteuerten Durchführung einer sicherheitsrelevanten Handlung (2) im Schienenverkehr (3), wobei die Vorrichtung (1) in einem Datennetzwerk (4) angeordnet werden kann, aufweisend:
 - eine Aufnahmeeinrichtung (5), eingerichtet zum Aufnehmen einer Autorisierungsinformation (6) von einer zentralen Autorität (7),
 - eine Speichereinrichtung (8), eingerichtet zum Speichern der Autorisierungsinformation (6),
 - eine Instruktionseinrichtung (9), eingerichtet zum wahlweisen Bereitstellen einer Instruktion (10) zur Durchführung der sicherheitsrelevanten Handlung (2) in Abhängigkeit von der Autorisierungsinformation (6), und
 - eine Ausgabereinrichtung (11), eingerichtet zur Ausgabe eines Datensignals (12), welches in-

- dikativ für die bereitgestellte Instruktion (10) zur Durchführung der sicherheitsrelevanten Handlung (2) sowie für die gespeicherte Autorisierungsinformation (6') ist, und
- eine Identifikationseinrichtung (15), welche dazu eingerichtet ist, einen Identifikationsparameter (16) der Vorrichtung (1) zu verschlüsseln und den verschlüsselten Identifikationsparameter (16') an die zentrale Autorität (7) zu übertragen, wobei die durch die Aufnahmeeinrichtung (5) aufnehmbare Autorisierungsinformation (6) auf dem übertragbaren verschlüsselten Identifikationsparameter (16') basiert.
2. Vorrichtung (1) nach Anspruch 1, wobei die Speichereinrichtung (8) zum Anpassen der gespeicherten Autorisierungsinformation (6') in Abhängigkeit von der Ausgabe des Datensignals (12) eingerichtet ist.
 3. Vorrichtung (1) nach einem der Ansprüche 1 und 2, wobei die Autorisierungsinformation (6) räumliche und/oder zweckgebundene Berechtigungsinformationen zur Durchführung der sicherheitsrelevanten Handlung (2) aufweist, wobei die Instruktionseinrichtung (9) eingerichtet ist, um die Instruktion (10) in Übereinstimmung mit der räumlichen und/oder zweckgebundenen Berechtigungsinformation bereitzustellen.
 4. Vorrichtung (1) nach einem der Ansprüche 2 bis 3, wobei die Ausgabereinrichtung (11) dazu eingerichtet ist, bei der Ausgabe der Daten der gespeicherten Autorisierungsinformation (6') mindestens eine Einheit einer Kryptowährung aus der Speichereinrichtung (8) zu entfernen.
 5. Vorrichtung (1) nach einem der vorhergehenden Ansprüche, wobei die Autorisierungsinformation (6) ausführbare Smart Contracts umfasst.
 6. Vorrichtung (1) nach einem der vorhergehenden Ansprüche, wobei die Ausgabereinrichtung (11) zur Ausgabe des Datensignals (12) an ein Steuergerät (13) eines elektronischen Stellwerks (14) des Schienenverkehrs (3) eingerichtet ist.
 7. Vorrichtung (1) nach einem der vorhergehenden Ansprüche, ferner aufweisend eine erste Hinterlegungseinrichtung (17), welche zur Hinterlegung einer Aufwendung (18) bei der zentralen Autorität (7) abhängig von der aufgenommenen Autorisierungsinformation (6) eingerichtet ist.
 8. Zentrale Autorität (7) zur Autorisierung einer Vorrichtung (1) zur gesteuerten Durchführung einer sicherheitsrelevanten Handlung (2) im Schienenverkehr (3), wobei die zentrale Autorität (7) aufweist:
 - eine erste Empfangseinrichtung (19), welche dazu eingerichtet ist, einen verschlüsselten Identifikationsparameter (16') einer Vorrichtung (1) zu empfangen,
 - eine Entschlüsselungseinrichtung (20) zur Entschlüsselung des verschlüsselten Identifikationsparameters (16') der Vorrichtung (1),
 - eine Allokationseinrichtung (21), eingerichtet zum Zuordnen einer Autorisierungsinformation (6) zu dem entschlüsselten Identifikationsparameter (16) der Vorrichtung (1), und
 - eine Übertragungseinrichtung (22), eingerichtet zum Übertragen der dem Identifikationsparameter (16) zugeordneten Autorisierungsinformation (6) an die zugehörige Vorrichtung (1).
 9. Zentrale Autorität (7) nach Anspruch 8, ferner aufweisend eine Publikationseinrichtung (23), mittels welcher ein Identifikationsschlüssel (24) der zentralen Autorität (7) öffentlich zugänglich gemacht werden kann.
 10. Zentrale Autorität (7) nach einem der Ansprüche 8 und 9, welche dazu eingerichtet ist den entschlüsselten Identifikationsparameter (16) in einer verteilten Datenbank (25) zu hinterlegen.
 11. Zentrale Autorität (7) nach Anspruch 10, welche dazu eingerichtet ist das Hinterlegen des entschlüsselten Identifikationsparameters (16) in der verteilten Datenbank (25) zu widerrufen.
 12. Netzwerkknoten (26) eines Datennetzwerks (4), welcher zum Empfangen von Datensignalen (12) einer Vorrichtung (1) zur gesteuerten Durchführung einer sicherheitsrelevanten Handlung (2) im Schienenverkehr (3) nach einem der Ansprüche 1 bis 7 eingerichtet ist, aufweisend:
 - eine zweite Empfangseinrichtung (27), welche zum Empfangen des Datensignals (12) der Vorrichtung (1), welches eine bereitgestellte Instruktion (10) zur Durchführung der sicherheitsrelevanten Handlung (2) sowie Daten einer gespeicherten Autorisierungsinformation (6') aufweist, eingerichtet ist,
 - eine Prüfeinrichtung (28), welches dazu eingerichtet ist, basierend auf dem Datensignal (12) zu prüfen, ob die bereitgestellte Instruktion (10) zur Durchführung der sicherheitsrelevanten Handlung (2) zulässig ist, und
 - eine zweite Hinterlegungseinrichtung (29), welche abhängig von dem Prüfen der Prüfeinrichtung (28) das empfangene Datensignal (12) in einer verteilten Datenbank (25) hinterlegen kann.
 13. Netzwerkknoten (26) nach Anspruch 12, welcher

durch ein Steuergerät (13) eines elektronischen Stellwerks (14) implementiert wird.

Claims

1. Device (1) designed for controlled implementation of a security-relevant operation (2) in rail traffic (3), wherein the device (1) can be arranged in a data network (4), having:

- a recording facility (5), designed to record authorisation information (6) from a central authority (7),
- a storage facility (8), designed to store the authorisation information (6),
- an instruction facility (9), designed to optionally provide an instruction (10) to implement the security-relevant operation (2) as a function of the authorisation information (6), and
- an output facility (11), designed to output a data signal (12), which is indicative of the provided instruction (10) to implement the security-relevant operation (2) and of the stored authorisation information (6'), and

an identification facility (15), which is designed to encrypt an identification parameter (16) of the device (1) and to transmit the encrypted identification parameter (16') to the central authority (7), wherein the authorisation information (6) which can be recorded by the recording facility (5) is based on the transmittable encrypted identification parameter (16').

2. Device (1) according to claim 1, wherein the storage facility (8) is designed to adjust the stored authorisation information (6') as a function of the output of the data signal (12).

3. Device (1) according to one of claims 1 and 2, wherein the authorisation information (6) has spatial and/or designated authorisation information for implementation of the security-relevant operation (2) wherein the instruction facility (9) is designed to provide the instruction (10) in agreement with the spatial and/or designated authorisation information.

4. Device (1) according to one of claims 2 to 3, wherein the output facility (11) is designed to remove at least one unit of a cryptocurrency from the storage facility (8) when data from the stored authorisation information (6') is output.

5. Device (1) according to one of the preceding claims, wherein the authorisation information (6) comprises executable smart contracts.

6. Device (1) according to one of the preceding claims, wherein the output facility (11) is designed to output the data signal (12) to a control device (13) of an electronic signal box (14) of the rail traffic (3).

7. Device (1) according to one of the preceding claims, further having a first storage facility (17), which is designed to store an outlay (18) with the central authority (7) as a function of the recorded authorisation information (6).

8. Central authority (7) for authorisation of a device (1) for controlled implementation of a security-relevant operation (2) in rail traffic (3), wherein the central authority (7) has:

- a first receive facility (19), which is designed to receive an encrypted identification parameter (16') of a device (1),
- a decryption facility (20) for decrypting the encrypted identification parameter (16') of the device (1),
- an allocation facility (21), which is designed to assign authorisation information (6) to the decrypted identification parameter (16) of the device (1), and
- a transmission facility (22), which is designed to transmit the authorisation information (6) assigned to the identification parameter (16) to the associated device (1).

9. Central authority (7) according to claim 8, further having a publication facility (23), by means of which an identification key (24) of the central authority (7) can be made publicly accessible.

10. Central authority (7) according to one of claims 8 and 9, which is designed to store the decrypted identification parameter (16) in a distributed database (25).

11. Central authority (7) according to claim 10, which is designed to revoke the storage of the decrypted identification parameter (16) in the distributed database (25).

12. Network node (26) of a data network (4), which is designed to receive data signals (12) of a device (1) for the controlled implementation of a security-relevant operation (2) in rail traffic (3) according to one of claims 1 to 7, having:

- a second receive facility (27), which is designed to receive the data signal (12) of the device (1), which has a provided instruction (10) to implement the security-relevant operation (2) and data of stored authorisation information (6'),
- a test facility (28), which is designed, on the basis of the data signal (12), to test whether the

provided instruction (10) to implement the security-relevant operation (2) is permissible, and
 - a second storage facility (29), which can store the received data signal (12) in a distributed database (25) as a function of the test of the test facility (28).

13. Network node (26) according to claim 12, which is implemented by a control device (13) of an electronic signal box (14).

Revendications

1. Installation (1), agencée pour effectuer de manière commandée, une opération (2) pertinente du point de vue de la sécurité dans le trafic (3) ferroviaire, dans laquelle l'installation (1) peut être mise dans un réseau (4) de données, comportant :

- un dispositif (5) de réception, agencé pour recevoir une information (6) d'autorisation d'une autorité (7) centrale,
- un dispositif (8) de mémoire, agencé pour mettre l'information (6) d'autorisation en mémoire,
- un dispositif (9) d'instruction, agencé pour disposer au choix d'une instruction (10) pour effectuer l'opération (2) pertinente du point de vue de la sécurité en fonction de l'information (6) d'autorisation, et
- un dispositif (11) d'émission, agencé pour émettre un signal (12) de données, qui est indicateur de l'instruction (10) mise à disposition pour effectuer l'opération (2) pertinente du point de vue de la sécurité ainsi que l'information (6') d'autorisation mise en mémoire, et

un dispositif (15) d'identification, qui est agencé pour chiffrer un paramètre (16) d'identification de l'installation (1) et transmettre le paramètre (16') d'identification chiffré à l'autorité (7) centrale, dans laquelle l'information (6) d'autorisation pouvant être reçue par le dispositif (5) de réception repose sur le paramètre (16') d'identification chiffré, qui peut être transmis.

2. Installation (1) suivant la revendication 1, dans laquelle le dispositif (8) de mémoire est agencé pour adapter l'information (6') d'autorisation mise en mémoire en fonction de l'émission du signal (12) de données.
3. Installation (1) suivant l'une des revendications 1 et 2, dans laquelle l'information (6) d'autorisation comporte une information de justification spatiale et/ou affectée pour effectuer l'opération (2) pertinente du point de vue de la sécurité,

dans laquelle le dispositif (9) d'instruction est agencé pour mettre l'instruction (10) en accord avec l'information de justification spatiale et/ou affectée.

4. Installation (1) suivant l'une des revendications 2 à 3, dans laquelle le dispositif (11) d'émission est agencé pour retirer au moins une unité d'une cryptomonnaie du dispositif (8) de mémoire lors de l'émission des données de l'information (6') d'autorisation mise en mémoire.

5. Installation (1) suivant l'une des revendications précédentes, dans laquelle l'information (6) d'autorisation comprend des smart contracts pouvant être exécutés.

6. Installation (1) suivant l'une des revendications précédentes, dans laquelle le dispositif (11) d'émission est agencé pour l'envoi du signal (12) de donnée à un appareil (13) de commande d'un poste (14) électronique d'aiguillage du trafic (3) ferroviaire.

7. Installation (1) suivant l'une des revendications précédentes, comportant en outre un premier dispositif (17) de consignation, qui est agencé pour la consignation d'un coût (18) auprès de l'autorité (7) centrale en fonction de l'information (6) d'autorisation reçue.

8. Autorité (7) centrale pour autoriser une installation (1) à effectuer de manière commandée une opération (2) pertinente du point de vue de la sécurité dans le trafic (3) ferroviaire, dans laquelle l'autorité (7) centrale comporte :

- un premier dispositif (19) de réception, qui est agencé pour recevoir un paramètre (16') d'identification chiffré d'une installation (1),
- un dispositif (20) de déchiffrement pour le déchiffrement du paramètre (16') d'identification chiffré de l'installation (1),
- un dispositif (21) d'allocation, agencé pour affecter une information (6) d'autorisation au paramètre (16) d'identification déchiffré de l'installation (1), et
- un dispositif (22) de transmission, agencé pour transmettre à l'installation (1), qui lui appartient, l'information (6) d'autorisation associée au paramètre (16) d'identification.

9. Autorité (7) centrale suivant la revendication 8, comportant en outre un dispositif (23) de publication, au moyen duquel une clé (24) d'identification de l'autorité (7) centrale peut être rendue accessible publiquement.

10. Autorité (7) centrale suivant l'une des revendications 8 et 9, qui est agencée pour mettre, dans une base

(25) de données répartie, le paramètre (16) d'identification déchiffré.

11. Autorité (7) centrale suivant la revendication 10, qui est agencée pour révoquer la mise du paramètre (16) d'identification déchiffré dans la base (25) de données répartie. 5
12. Noeud (26) d'un réseau (4) de données, qui est agencé pour la réception de signaux (12) de données d'une installation (1) pour effectuer de manière commandée une opération (2) pertinente du point de vue de la sécurité dans le trafic (3) ferroviaire suivant l'une des revendications 1 à 7, comportant : 10
15
 - un deuxième dispositif (27) de réception, qui est agencé pour la réception du signal (12) de données de l'installation (1), lequel comporte une instruction (10) mise à disposition pour effectuer l'opération (2) pertinente du point de vue de la sécurité ainsi que des données d'une information (6') d'autorisation mise en mémoire, 20
 - un dispositif (28) de contrôle, qui est agencé pour contrôler, en se fondant sur le signal (12) de données, si l'instruction (10) mise à disposition pour effectuer l'opération (2) pertinente du point de vue de la sécurité est admissible, et 25
 - un deuxième dispositif (29) de mise en mémoire, qui, en fonction du contrôle du dispositif (28) de contrôle, met le signal (12) de données reçu dans une base (25) de données répartie. 30
13. Noeud (26) de réseau suivant la revendication 12, qui est mis en oeuvre par un appareil (13) de commande d'un poste (14) électronique d'aiguillage. 35

40

45

50

55

FIG 1

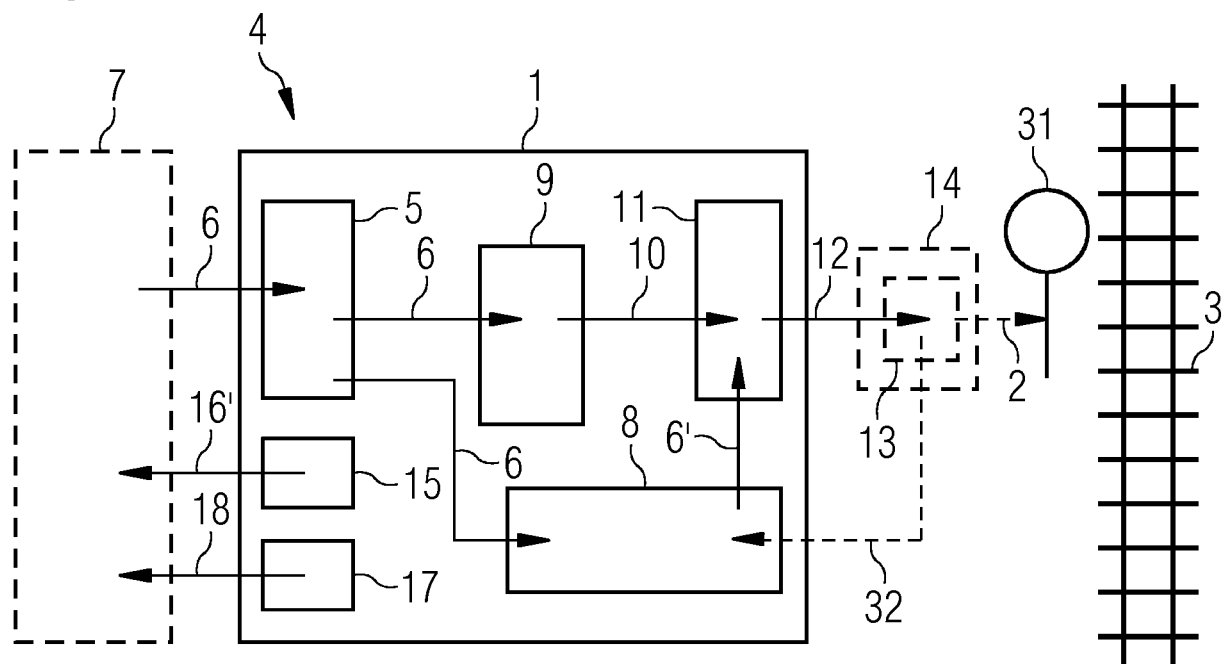


FIG 2

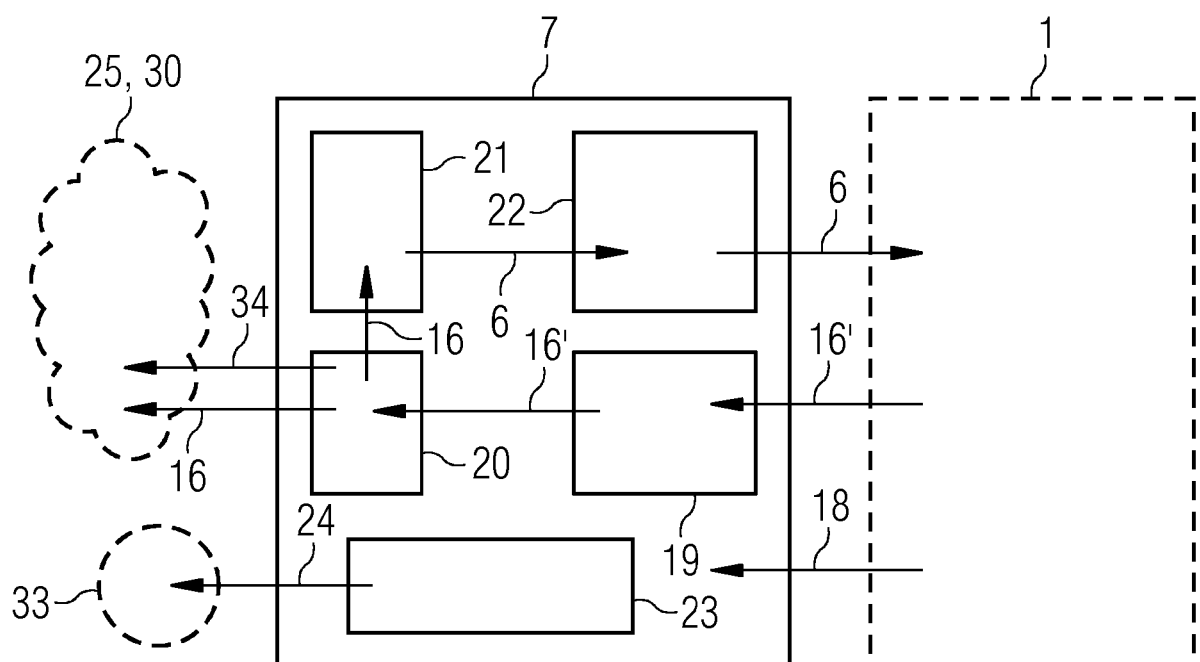
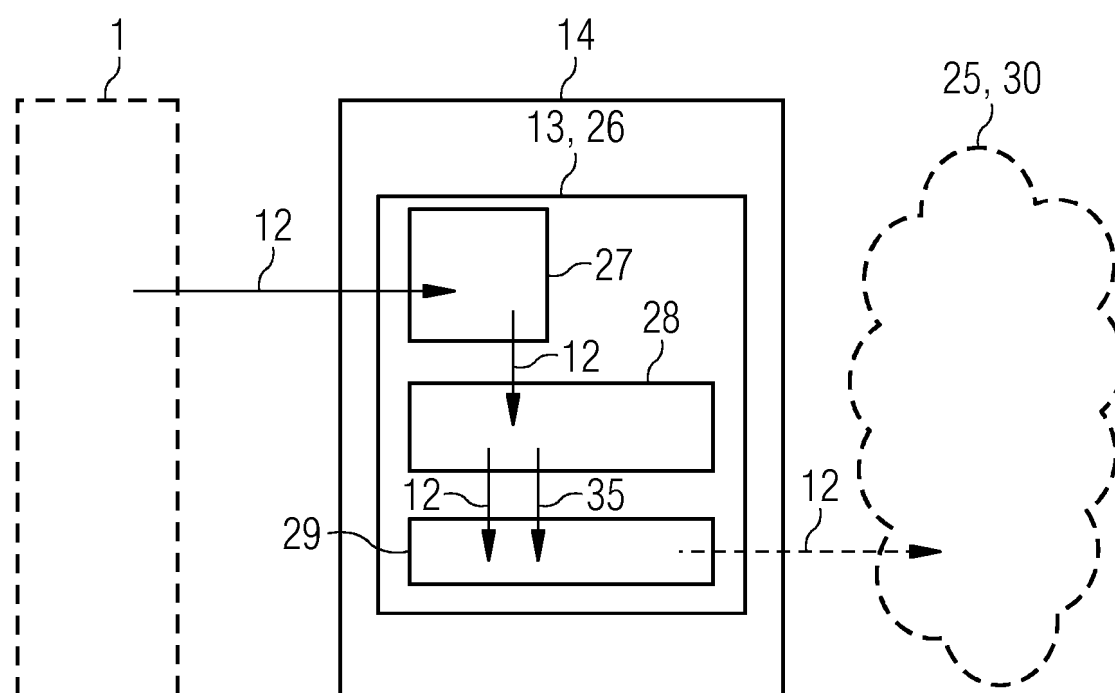


FIG 3



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 D102005014050 A1 **[0003]**
- GB 2540976 A1 **[0004]**