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

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
11. Oktober 2012 (11.10.2012)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2012/136525 A1

(51) Internationale Patentklassifikation:
B61L 15/00 (2006.01) *B61L 27/00* (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2012/055460

(22) Internationales Anmeldedatum:
28. März 2012 (28.03.2012)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2011 006 772.8 5. April 2011 (05.04.2011) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: **FALK, Rainer** [DE/DE]; Parkstraße 43, 85435 Erding (DE). **FRIES, Steffen** [DE/DE]; Eberweg 3, 85598 Baldham (DE).

(74) Gemeinsamer Vertreter: **SIEMENS AKTIENGESELLSCHAFT**; Postfach 22 16 34, 80506 München (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

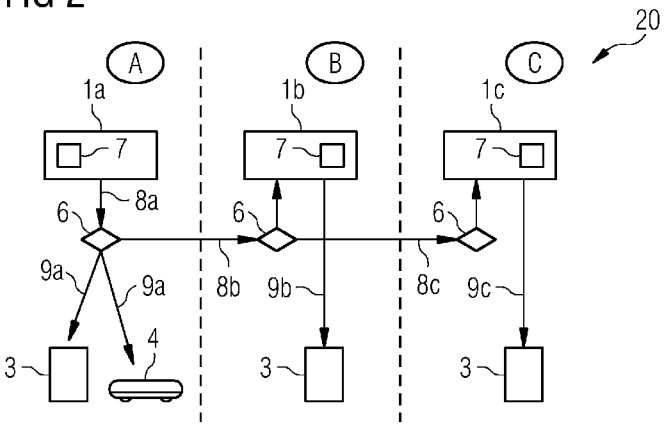
(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB,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

[Fortsetzung auf der nächsten Seite]

(54) Title: KEY MANAGEMENT SYSTEM AND METHOD FOR A TRAIN PROTECTION SYSTEM

(54) Bezeichnung : SYSTEM UND VERFAHREN FÜR EIN SCHLÜSSELMANAGEMENT EINES ZUGSICHERUNGSSYSTEMS

FIG 2



(57) Abstract: The invention relates to a method for distributing communication keys (6) for the encryption of traffic control messages of a rail vehicle protection system, having the steps of generating a communication key (6) at a first key allocation point (1a) of a first track operator as a function of a planned route of a rail vehicle (4), making available the communication key (6) to a second key allocation point (1b) of a second track operator, making available the communication key (6) to the rail vehicle (4) by means of the first key allocation point, and encrypting traffic control messages of the rail vehicle (4) with the communication key (6) in order to permit tamper-proof communication of the rail vehicle (4) with operation control centres (3) of the first track operator and with operational control centres (3) of the second track operator.

(57) Zusammenfassung:

[Fortsetzung auf der nächsten Seite]

WO 2012/136525 A1

Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

Die Erfindung betrifft ein Verfahren zum Verteilen von Kommunikationsschlüsseln (6) für die Verschlüsselung von Verkehrsleitnachrichten eines Schienenfahrzeugsicherungssystems, mit den Schritten des Erzeugens eines Kommunikationsschlüssels (6) in einer ersten Schlüsselvergabestelle (1a) eines ersten Streckenbetreibers in Abhängigkeit von einer geplanten Fahrtroute eines Schienenfahrzeugs (4), des Bereitstellens des Kommunikationsschlüssels (6) an eine zweite Schlüsselvergabestelle (1b) eines zweiten Streckenbetreibers, des Bereitstellens des Kommunikationsschlüssels (6) an das Schienenfahrzeug (4) durch die erste Schlüsselvergabestelle, und des Verschlüsselns von Verkehrsleitnachrichten des Schienenfahrzeugs (4) mit dem Kommunikationsschlüssel (6) zum manipulationssicheren Kommunizieren des Schienenfahrzeugs (4) mit Streckenzentralen (3) des ersten Streckenbetreibers und mit Streckenzentralen (3) des zweiten Streckenbetreibers.

Beschreibung

System und Verfahren für ein Schlüsselmanagement eines Zugsicherungssystems

Die vorliegende Erfindung bezieht sich auf ein System und ein Verfahren für ein Schlüsselmanagement eines Zugsicherungssystems.

Stand der Technik

Ein im Schienenverkehr zur Zugsicherung eingesetztes Sicherungssystem ist das sogenannte europäische Zugsteuersystem "ETCS", European Train Control System). Dieses Verkehrsleitsystem nutzt üblicherweise Funkdatenübertragung, beispielsweise über GSM-R, um Leitnachrichten und Sicherungsnachrichten zwischen Schienentriebfahrzeugen bzw. deren Zugsicherungsrechnern, wie zum Beispiel dem European Vital Computer (EVC) und stationären Streckenzentralen, den Funkblockzentralen ("RBC", Radio Block Centres), auszutauschen. Um die Daten bei der Übertragung vor unbemerkten Manipulationen und Übertragungsfehlern zu schützen, sind sie mit einer kryptographischen Prüfsumme geschützt, zu deren Berechnung und/oder Überprüfung ein kryptographischer Schlüssel notwendig ist.

Üblicherweise werden symmetrische Kryptographieverfahren eingesetzt, so dass sowohl das Schienentriebfahrzeug als auch die Streckenzentrale zumindest einen Schlüssel besitzen muss. Da sich das Schienenfahrzeug auf seiner vorbestimmten Route durch Zuständigkeitsbereiche verschiedener stationärer Streckenzentralen entlang der Route bewegt, ist es notwendig, dass jeder der temporär zuständigen Streckenzentralen ein passender Schlüssel zur Kommunikation mit dem Schienenfahrzeug mitgeteilt wird. Die Schlüsselverteilung an die Streckenzentralen ist daher ein grundlegendes Problem eines effektiven Zugsicherungssystems, um die Kommunikation des Schienenfahrzeugs mit allen Streckenzentralen, gegebenenfalls

auch mit Streckenzentralen anderer Streckenbetreiber, in manipulationssicherer Form zu gewährleisten.

Fig. 1 zeigt den prinzipiellen Aufbau eines Schienenfahrzeugleitsystems 10 in einer schematischen Darstellung. Ein Schienenfahrzeug 4, beispielsweise ein Zug mit einem steuerbaren Triebfahrzeug, welches einen EVC an Bord hat, bewegt sich entlang einer Route 5 durch verschiedene Domänen A, B und C, welche unter der Kontrolle verschiedener Streckenbetreiber stehen, und welche durch die gepunkteten Linien optisch voneinander abgegrenzt sind. Die Domänen A, B und C können beispielsweise Länder wie Deutschland, Österreich und Italien mit jeweils eigenen Schienennetzen sein, und der Zug 4 kann beispielsweise eine geplante Route 5 von München nach Venedig haben, die ihn durch alle drei Länder Deutschland, Österreich und Italien führt.

Jeder Streckenbetreiber besitzt eine Schlüsselmanagementzentrale oder Schlüsselvergabestelle 1a, 1b bzw. 1c, auch KMC ("Key Management Centre") genannt. Das heißt, in der Domäne A ist die KMC 1a für das Schlüsselmanagement verantwortlich, in der Domäne B die KMC 1b und in der Domäne C die KMC 1c. Unter der Ägide der KMCs 1a, 1b und 1c stehen jeweils Streckenzentralen 3, sogenannte RBCs, die Schlüsselnachrichtencodes, sogenannte KMACs ("Key Message Authentication Codes") von den KMCs erhalten können. Die KMACs können dabei Kommunikationsschlüssel umfassen, welche zur sicheren Kommunikation der RBCs 3 mit dem Zug 4 dienen können.

Die Streckenzentralen oder RBCs 3 sind lokal stationär für bestimmte Blockabschnitte des Schienennetzwerks verantwortlich. Ein RBC 3 kann dabei jeweils einer Schlüsselgruppe 2a, 2b, 2c zugeordnet sein, welche von dem jeweils übergeordneten KMC 1a, 1b, 1c in der jeweiligen Domäne A, B oder C mit Kommunikationsschlüsseln versorgt wird. Es kann dabei vorgesehen sein, dass mehrere RBCs 3 der gleichen Schlüsselgruppe zugeordnet sind. Beispielhaft sind in der Domäne A und in der Do-

mäne C je zwei RBCs 3 einer Schlüsselgruppe 2a bzw. 2c zugeordnet. Es kann alternativ auch sein, dass ein RBC 3 gleichzeitig auch seine eigene Schlüsselgruppe bildet, wie beispielhaft in der Domäne B mit der Schlüsselgruppe 2b dargestellt. Jede Schlüsselgruppe 2a, 2b, 2c erhält von dem übergeordneten KMC 1a, 1b, 1c einen gruppenspezifischen Kommunikationsschlüssel zugeteilt.

Das Schienenfahrzeug 4 kommuniziert dabei über Kommunikationsverbindungen 5a mit RBCs 3 in der ersten Domäne A, über Kommunikationsverbindungen 5b mit dem RBC 3 in der zweiten Domäne B und über Kommunikationsverbindungen 5c mit RBCs 3 in der dritten Domäne A. Dabei werden die Kommunikationsverbindungen 5a, 5b und 5c jeweils über die von den KMCs 1a, 1b, 1c zur Verfügung gestellten Kommunikationsschlüsseln abgesichert.

Eine Möglichkeit zur Schlüsselverteilung von Kommunikationsschlüsseln an die verschiedenen Streckenzentralen 3 besteht in einer manuellen Verteilung der Kommunikationsschlüssel durch einen Mitarbeiter des Zugbetreibers oder des jeweiligen Streckenbetreibers. In diesem Fall kann es sein, dass der Mitarbeiter vor Fahrtantritt domänenspezifische Kommunikationsschlüssel von jedem der KMCs 1a, 1b, 1c anfordert und diese domänenspezifischen Kommunikationsschlüssel auf dem Steuerrechner, der sogenannten OBU ("On-Board Unit") des Zugs 4 installiert. Die Installation kann beispielsweise durch manuelle Eingabe über eine Eingabeschnittstelle, zum Beispiel eine Tastatur oder ein berührungsempfindlicher Bildschirm, über eine lokale Netzwerkverbindung, ein lokal eingesetztes Speichermedium, zum Beispiel eine Diskette oder ein USB-Stick, oder eine gesicherte drahtlose Fernwartungsverbindung erfolgen.

Eine derartige Schlüsselverteilung ist aufwändig, fehleranfällig und ineffizient. Insbesondere ist hierzu eine ständige Verbindung zwischen KMCs verschiedener Domänen notwendig, um

den ständigen Austausch von Kommunikationsschlüsseln zwischen den KMCs zu gewährleisten.

Es besteht daher ein Bedarf nach einfacheren Lösungen für eine Schlüsselverteilung für Kommunikationsschlüssel in domänenübergreifenden Sicherungssystemen für Schienenfahrzeuge.

Zusammenfassung der Erfindung

Eine Idee der vorliegenden Erfindung ist es, einen Schlüsselverteilungsplan anhand einer geplanten Zugroute auszuarbeiten und für die Befahrung dieser Route notwendige Kommunikationsschlüssel automatisch zu konfigurieren. Hierzu können Kommunikationsschlüssel durch eine zentrale verantwortliche Schlüsselvergabestelle erzeugt werden, die auf die geplante Route abgestimmt sind. Diese Kommunikationsschlüssel können den beteiligten Schlüsselvergabestellen anderer Domänen bzw. Streckenbetreiber zur Verfügung gestellt werden, so dass die zentral und automatisch erstellten Kommunikationsschlüssel gezielt an die Züge und die Streckenzentralen verteilt werden können.

Einer der Vorteile dieser Vorgehensweise ist es, dass die Definition eines Schlüsselverteilungsplans erheblich vereinfacht wird. Außerdem kann die Gültigkeit der Kommunikationsschlüssel hinsichtlich Fahrstrecke und Fahrtzeit des Zugs in einfacher Weise örtlich und zeitlich begrenzt werden, so dass der erfindungsgemäße Schlüsselverteilungsplan weniger fehleranfällig ist als herkömmliche Schlüsselverteilungspläne.

Ein weiterer Vorteil ist die Automatisierbarkeit des Schlüsselverteilungsplans durch die Möglichkeit, den Plan automatisch aus extern bereitgestellten Fahrtroutenplänen zu generieren und zu verifizieren.

Eine Ausführungsform der vorliegenden Erfindung besteht daher in einem Verfahren zum Verteilen von Kommunikationsschlüsseln

für die Verschlüsselung von Verkehrsleitnachrichten eines Schienenfahrzeugsicherungssystems, mit den Schritten des Erzeugens eines Kommunikationsschlüssels in einer ersten Schlüsselvergabestelle eines ersten Streckenbetreibers in Abhängigkeit von einer geplanten Fahrtroute eines Schienenfahrzeugs, des Bereitstellens des Kommunikationsschlüssels an eine zweite Schlüsselvergabestelle eines zweiten Streckenbetreibers, des Bereitstellens des Kommunikationsschlüssels an das Schienenfahrzeug durch die erste Schlüsselvergabestelle, und des Verschlüsselns von Verkehrsleitnachrichten des Schienenfahrzeugs mit dem Kommunikationsschlüssel zum manipulationssicheren Kommunizieren des Schienenfahrzeugs mit Streckenzentralen des ersten Streckenbetreibers und mit Streckenzentralen des zweiten Streckenbetreibers.

Vorteilhafterweise erfolgt ein Bereitstellen des Kommunikationsschlüssels an erste Streckenzentralen durch den ersten Streckenbetreiber und ein Bereitstellen des Kommunikationsschlüssels an zweite Streckenzentralen durch den zweiten Streckenbetreiber.

Gemäß einer bevorzugten Ausführungsform umfasst der Kommunikationsschlüssel eine Vielzahl von streckenzentralenspezifischen Kommunikationsschlüsseln, wobei das Bereitstellen des Kommunikationsschlüssels an die zweite Schlüsselvergabestelle das Bereitstellen einer Gruppe von streckenzentralenspezifischen Kommunikationsschlüsseln, welche den zweiten Streckenzentralen des zweiten Streckenbetreibers zugeordnet sind, an die zweite Schlüsselvergabestelle umfasst. Dies hat den Vorteil, dass von unterschiedlichen Streckenzentralen unterschiedliche Kommunikationsschlüssel verwendet werden, so dass bei versehentlicher Offenlegung oder bei Manipulation eines der Kommunikationsschlüssel die Kompromittierung des Gesamtsystems auf lediglich eine Streckenzentrale begrenzt bleibt.

Gemäß einer Ausführungsform erfolgt das Erzeugen des Kommunikationsschlüssels in einer ersten Schlüsselvergabestelle das

Ableiten der streckenzentralenspezifischen Kommunikationsschlüssel von einem Hauptkommunikationsschlüssel durch ein Schlüsselableitungsverfahren. Dies bietet den Vorteil, dass das Ableiten der streckenzentralenspezifischen Kommunikationsschlüssel von einem Steuerrechner des Schienenfahrzeugs selbst durchgeführt werden kann.

Gemäß einer bevorzugten Ausführungsform erfolgt das Ableiten der streckenzentralenspezifischen Kommunikationsschlüssel durch die erste Schlüsselvergabestelle nur für die ersten Streckenzentralen und das Ableiten der streckenzentralenspezifischen Kommunikationsschlüssel durch die zweite Schlüsselvergabestelle nur für die zweiten Streckenzentralen. Dadurch kann vorteilhafterweise bei einem hohen Fahrzeugaufkommen die Schlüsselverwaltung in einer Schlüsselvergabestelle nur auf diejenigen abgeleiteten Kommunikationsschlüssel begrenzt werden, die in dieser Schlüsselvergabestelle tatsächlich benötigt werden. Vorteilhafterweise begrenzt sich dadurch das Datenaufkommen bei einem Bereitstellen der Kommunikationsschlüssel durch die erste Schlüsselvergabestelle an weitere Schlüsselvergabestellen.

Gemäß einer vorteilhaften Ausführungsform umfasst der Kommunikationsschlüssel eine Vielzahl von schienenfahrzeugspezifischen Kommunikationsschlüsseln, wobei das Bereitstellen des Kommunikationsschlüssels an das Schienenfahrzeug das Bereitstellen eines für das Schienenfahrzeug spezifischen Kommunikationsschlüssels aus der Vielzahl von schienenfahrzeugspezifischen Kommunikationsschlüsseln umfasst. Dies bietet den Vorteil, dass beispielsweise bei einem Zusammenkoppeln von zwei Schienenfahrzeugen unterschiedlicher Schienenfahrzeugbetreiber eine sichere Schienenfahrzeugkommunikation der gekoppelten Schienenfahrzeuge untereinander möglich ist, wenn die betreffenden Schienenfahrzeuge untereinander ihre fahrzeugspezifischen Kommunikationsschlüssel abgleichen.

Vorteilhafterweise kann die geplante Fahrtroute des Schienenfahrzeugs von einem Leitsystem zur Fahrdienststeuerung bereitgestellt werden, so dass die erste Schlüsselvergabestelle das Erzeugen und das Bereitstellen des Kommunikationsschlüssels automatisiert durchführt. Damit wird die Erzeugung und Verteilung von Kommunikationsschlüssels zum Einen erheblich beschleunigt, zum Anderen kann automatisch überprüft werden, ob entlang der geplanten Fahrtroute alle notwendigen Kommunikationsschlüssel erzeugt und verteilt worden sind. So können frühzeitig und verlässlich Abweichungen und Fehleingaben erkannt werden.

Gemäß einer weiteren Ausführungsform schafft die Erfindung eine Steuereinrichtung in einer ersten Schlüsselvergabestelle eines ersten Schienennetzstreckenbetreibers zum Verteilen von Kommunikationsschlüsseln für die Verschlüsselung von Verkehrsleitnachrichten eines Schienenfahrzeugsicherungssystems, mit einer Erzeugungseinrichtung, welche dazu ausgelegt ist, einen Kommunikationsschlüssel in Abhängigkeit von einer geplanten Fahrtroute eines Schienenfahrzeugs zu erzeugen, und einer Bereitstellungseinrichtung, welche dazu ausgelegt ist, den erzeugten Kommunikationsschlüssel an eine zweite Schlüsselvergabestelle eines zweiten Streckenbetreibers und an das Schienenfahrzeug bereitzustellen, wobei der Kommunikationsschlüssel zum Verschlüsseln von Verkehrsleitnachrichten des Schienenfahrzeugs zum manipulationssicheren Kommunizieren des Schienenfahrzeugs mit Streckenzentralen des ersten Streckenbetreibers und mit Streckenzentralen des zweiten Streckenbetreibers ausgelegt ist.

Gemäß einer weiteren Ausführungsform schafft die Erfindung ein Schienenfahrzeugsicherungssystem mit einer erfindungsgemäßen Steuereinrichtung, einer ersten Schlüsselvergabestelle, in der die Steuereinrichtung angeordnet ist, einer Vielzahl von ersten Streckenzentralen, welche dazu ausgelegt sind, von der ersten Schlüsselvergabestelle mit einem von der Steuereinrichtung erzeugten Kommunikationsschlüssel für die Ver-

schlüsselung von Verkehrsleitnachrichten eines Schienenfahrzeugs versorgt zu werden, einer zweiten Schlüsselvergabestelle, und einer Vielzahl von zweiten Streckenzentralen, welche dazu ausgelegt sind, von der zweiten Schlüsselvergabestelle mit einem von der Steuereinrichtung erzeugten Kommunikationsschlüssel für die Verschlüsselung von Verkehrsleitnachrichten eines Schienenfahrzeugs versorgt zu werden.

Weitere Modifikationen und Variationen ergeben sich aus den Merkmalen der abhängigen Ansprüche.

Kurze Beschreibung der Figuren

Verschiedene Ausführungsformen und Ausgestaltungen der vorliegenden Erfindung werden nun in Bezug auf die beiliegenden Zeichnungen genauer beschrieben, in denen

Fig. 1 eine schematische Darstellung eines Aufbaus eines Schienenfahrzeugleitsystems;

Fig. 2 eine schematische Darstellung eines Schienenfahrzeugsicherungssystems gemäß einer Ausführungsform der Erfindung;

Fig. 3 eine schematische Darstellung eines Schienenfahrzeugsicherungssystems gemäß einer weiteren Ausführungsform der Erfindung;

Fig. 4 eine schematische Darstellung eines Schienenfahrzeugsicherungssystems gemäß einer weiteren Ausführungsform der Erfindung;

Fig. 5 eine schematische Darstellung eines Schienenfahrzeugsicherungssystems gemäß einer weiteren Ausführungsform der Erfindung; und

Fig. 6 eine schematische Darstellung eines Verfahrens zum Verteilen von Kommunikationsschlüsseln für die Verschlüsselung von Verkehrsleitnachrichten eines Schienenfahrzeugsicherungssystems gemäß einer weiteren Ausführungsform der Erfindung zeigt.

Die beschriebenen Ausgestaltungen und Weiterbildungen lassen sich, sofern sinnvoll, beliebig miteinander kombinieren. Weitere mögliche Ausgestaltungen, Weiterbildungen und Implementierungen der Erfindung umfassen auch nicht explizit genannte Kombinationen von zuvor oder im Folgenden bezüglich der Ausführungsbeispiele beschriebenen Merkmale der Erfindung.

Die beiliegenden Zeichnungen sollen ein weiteres Verständnis der Ausführungsformen der Erfindung vermitteln. Sie veranschaulichen Ausführungsformen und dienen im Zusammenhang mit der Beschreibung der Erklärung von Prinzipien und Konzepten der Erfindung. Andere Ausführungsformen und viele der genannten Vorteile ergeben sich im Hinblick auf die Zeichnungen. Die Elemente der Zeichnungen sind nicht notwendigerweise maßstabsgetreu zueinander gezeigt. Gleiche Bezugszeichen bezeichnen dabei gleiche oder ähnlich wirkende Komponenten.

Ausführliche Beschreibung der Erfindung

Kommunikationsschlüssel im Sinne der folgenden Beschreibung umfassen alle kryptographischen Informationen und Dateneinheiten, welche dazu geeignet sind, Daten im Klarformat zu verschlüsseln und daraus abhör- und/oder auslesesichere Daten im Geheimformat zu erzeugen, bzw. die dazu geeignet sind, die Integrität von Daten im Klarformat zu schützen und eine kryptographische Prüfsumme zu errechnen, und welche weiterhin dazu geeignet sind, in Kenntnis der kryptographischen Informationen aus den Daten im Geheimformat die Daten im Klarformat zurückzugewinnen bzw. zu prüfen, dass die Daten während des Transports nicht manipuliert wurden. Kommunikationsschlüssel im Sinne der Erfindung können beispielsweise symmetrische

Schlüsselpaare, asymmetrische Schlüsselpaare oder ähnliche kryptographische Verfahren beinhalten. Kommunikationsschlüssel können dabei beispielsweise mit Verfahren wie AES, DES, KDF, IPsec, SSL/TLS, MACsec, L2TP, PPTP, PGP, S/MIME oder eine ähnliche Technik mit einem dazugehörigen Schlüsselmanagement, wie zum Beispiels IKE, EAP oder anderer Verfahren eingesetzt werden.

Fig. 2 zeigt eine schematische Darstellung eines Schienenfahrzeugsicherungssystems 20. Das Schienenfahrzeugsicherungssystem 20 unterscheidet sich von dem in Fig. 1 gezeigten Schienefahrzeugleitsystem 10 dadurch, dass in jeder der Schlüsselvergabestellen 1a, 1b, 1c (KMCs) eine Steuereinrichtung 7 angeordnet ist, welche für das Erzeugen und Verteilen von Kommunikationsschlüsseln für die Verschlüsselung von Verkehrsleitnachrichten ausgelegt ist. Die Steuereinrichtung 7 kann dabei beispielsweise ein Softwaremodul sein, welches auf den KMCs aufgespielt ist und ausgeführt wird.

Die Steuereinrichtung 7 umfasst eine Erzeugungseinrichtung zum Erzeugen von Kommunikationsschlüsseln 6 zum kryptographischen Schützen von Verkehrsleitnachrichten eines Schienenfahrzeugs 4. In den folgenden Beispielen wird angenommen, dass das Schienenfahrzeug 4 der Domäne A zugeordnet ist, so dass das KMC 1a das sogenannte "Heim-KMC" des Schienenfahrzeugs 4 ist, das heißt, dass das Erzeugen und Verteilen von Kommunikationsschlüsseln unter der Kontrolle des KMC 1a vorgenommen wird. Die übrigen KMCs 1b und 1c sind in diesem Fall von der Steuerung durch das KMC 1a abhängig. Es ist selbstverständlich ebenso möglich, dass die anderen KMC 1b und 1c in anderen Fällen, beispielsweise für andere Schienenfahrzeuge die Rolle des Heim-KMC übernehmen. Die Steuereinrichtungen 7 der KMC 1b und 1c sind dabei genauso wie die Steuereinrichtung 7 des KMC 1a aufgebaut. Es ist überdies selbstverständlich, dass die Anzahl der KMCs 1a, 1b und 1c nicht auf die gezeigte Anzahl von drei beschränkt ist. Jede andere Anzahl von KMCs ist ebenso möglich. Die KMCs 1a, 1b, 1c können dabei

insbesondere von verschiedenen Streckenbetreibern betrieben werden.

Die Erzeugungseinrichtung kann dazu ausgelegt sein, in einem Schritt 8a einen Kommunikationsschlüssel 6 in Abhängigkeit von einer geplanten Fahrtroute des Schienenfahrzeugs 4 zu erzeugen. Dabei kann die Erzeugungseinrichtung dazu ausgelegt sein, die geplante Fahrtroute von einem (nicht gezeigten) Fahrdienststeuersystem oder einem Fahrplanauskunftssystem automatisch zur Verfügung gestellt zu bekommen.

Der Kommunikationsschlüssel 6 kann durch das erste KMC 1a dann in einem Schritt 8b einem zweiten KMC 1b zur Verfügung gestellt werden und in einem Schritt 8c einem dritten KMC 1c zur Verfügung gestellt werden. Die KMC 1b, 1c, denen der Kommunikationsschlüssel 6 zur Verfügung gestellt wird, richtet sich dabei nach der geplanten Fahrtroute des Schienenfahrzeugs 4. Beispielsweise können die KMC 1b, 1c für Streckenzentralen 3 verantwortlich sein, durch deren Leitbereich die geplante Fahrtroute des Schienenfahrzeugs 4 führt. Die Bereitstellung von Kommunikationsschlüsseln kann dabei über eine Bereitstellungseinrichtung der Steuereinrichtung 7 erfolgen.

In einem Schritt 9a kann dann der erzeugte Kommunikationsschlüssel 6 an erste Streckenzentralen 3 (RBCs) in der ersten Domäne A verteilt werden. Weiterhin kann in dem Schritt 9a der Kommunikationsschlüssel 6 auf einem Steuerrechner (EVC) des Schienenfahrzeugs 4 installiert werden. Der Kommunikationsschlüssel 6 kann in Schritten 9b und 9c durch die KMCs 1b und 1c den RBCs 3 in der Domäne B bzw. der Domäne C bereitgestellt werden.

Das KMC 1a kann nach erfolgter Verteilung der Kommunikationsschlüssel 6 eine Bestätigung ausstellen, dass das Schienenfahrzeug 4 betriebsbereit ist und die Domänen A, B und C befahren kann. Wenn beispielsweise wegen einer Streckensperrung

oder einer sonstigen Umleitung des Schienenfahrzeugs 4 eine weitere (nicht gezeigte) Domäne D befahren werden soll, für die der Kommunikationsschlüssel 6 nicht den jeweiligen Streckenzentralen 3 zur Verfügung gestellt worden ist. Kann ein modifizierter Schlüsselverteilungsplan erstellt werden, wobei nach einer entsprechenden Autorisierung durch einen Bediener die Steuereinrichtung 7 den Kommunikationsschlüssel 6 auch an ein KMC der Domäne D weitergibt, welches dann seinerseits den Kommunikationsschlüssel an die RBCs 3 in seiner Domäne D weiterverteilt. Alternativ kann dem Bediener angezeigt werden, dass das Schienenfahrzeug 4 lediglich für die Domänen A, B und C, aber nicht für andere Domänen durchfahrberechtigt ist.

Fig. 3 zeigt eine schematische Darstellung eines Schienenfahrzeugsicherungssystems 30. Das Schienenfahrzeugsicherungssystem 30 unterscheidet sich von dem Schienenfahrzeugsicherungssystem 20 in Fig. 2 dadurch, dass der Kommunikationsschlüssel 6 eine Vielzahl von Kommunikationsschlüsseln 6a, 6b, 6c umfasst, welche domänenspezifisch bzw. streckenzentralenspezifisch erzeugt worden sind. Jeder der Kommunikationsschlüssel 6a, 6b, 6c kann dabei für ein RBC 3 gebietsspezifisch erzeugt werden. Die Kommunikationsschlüssel 6a, 6b, 6c können dabei zufällig oder pseudozufällig oder mittels einer Schlüsselableitungsfunktion aus einem Basisschlüssel und/oder einem RBC-abhängigen Ableitungsparameter erzeugt werden. Die Kommunikationsschlüssel 6a, 6b, 6c werden dann gemeinsam auf dem Steuerrechner des Schienenfahrzeugs 4 installiert.

Aus den Kommunikationsschlüsseln 6a, 6b, 6c werden dann Gruppen von Kommunikationsschlüsseln ausgewählt, welche den jeweiligen RBCs 3 der jeweiligen Domänen B und C zugeordnet werden können. In den Schritten 8b, 8c werden dann nur diejenigen Kommunikationsschlüssel 6b und 6c übermittelt, welche die KMCs 1b, 1c zur Bereitstellung an ihre RBCs benötigen.

Das Schienenfahrzeug 4 kann bei einem Durchfahren der Domänen A, B und C in Abhängigkeit von der aktuellen Position jeweils

einer der Kommunikationsschlüssel 6a, 6b, 6c auswählen, um mit den momentan aktuellen RBC 3 der jeweiligen Domäne zu kommunizieren. Die aktuelle Position kann beispielsweise über ein Satellitennavigationssystem wie zum Beispiel GPS oder GALILEO, durch Peilung von Funkbasisstationen, zum Beispiel über GSM-R oder WLAN, anhand von Adressen oder Identifikationscodes von Streckenrechnern des Schienennetzes oder durch Eurobalisen, wie beispielsweise Festdaten- oder Transparentdatenbalisen am Gleisbett ermittelt werden.

Fig. 4 zeigt eine schematische Darstellung eines Schienenfahrzeugsicherungssystems 40. Das Schienenfahrzeugsicherungssystem 40 unterscheidet sich von dem Schienenfahrzeugsicherungssystem 30 in Fig. 3 dadurch, dass ein Hauptkommunikationsschlüssel 6 zwischen den KMCs 1a, 1b und 1c vorgesehen ist, von dem über eine Schlüsselableitungsfunktion eine Vielzahl von Kommunikationsschlüsseln 6a, 6b, 6c abgeleitet werden kann. In den Schritten 8b und 8c wird statt der Vielzahl von Kommunikationsschlüsseln 6a, 6b, 6c der Hauptkommunikationsschlüssel 6 an die KMCs 1b und 1c weitergegeben, die ihrerseits die Vielzahl von Kommunikationsschlüsseln 6a, 6b, 6c lokal ableiten können. Die Ableitung durch die KMCs kann beispielsweise in Abhängigkeit von einem zugspezifischen Parameter erfolgen, beispielsweise die Identifikationsnummer des Schienenfahrzeugs 4. Der Hauptkommunikationsschlüssel 6 kann dabei beispielsweise nur über einen bestimmten Zeitraum hinweg gültig sein.

Ebenso kann es vorgesehen sein, dass das Schienenfahrzeug 4 selbst mit dem Hauptkommunikationsschlüssel 6 versorgt wird, aus dem der Steuerrechner des Schienenfahrzeugs 4 die Vielzahl von Kommunikationsschlüsseln 6a, 6b, 6c selbst ableitet.

Die Ableitung der Vielzahl von Kommunikationsschlüsseln 6a, 6b, 6c von dem Hauptkommunikationsschlüssel 6 kann beispielsweise mittels einer Schlüsselableitungsfunktion (Key Derivation Function, KDF) wie HMAC (Hash Message Authentication Co-

de) oder auch AES-CBCMAC (Advanced Encryption Standard - Cipher Block Chaining Message Authentication Code) in Abhängigkeit von RBC-spezifischen Parametern wie Identifikationscode, Gebietscode, Streckenabschnittscode oder ähnlicher Parameter abgeleitet werden.

Der Vorteil dieser Vorgehensweise besteht darin, dass keine ständige Online-Verbindung zwischen den KMCs 1a, 1b, 1c bestehen muss, da jedes KMC selbstständig RBC-spezifische Kommunikationsschlüssel 6a, 6b, 6c aus dem einmalig übertragenen Hauptkommunikationsschlüssel 6 ableiten kann, ohne dass dazu eine erneute Kommunikation mit dem Heim-KMC 1a nötig ist. Ferner müssen bei einer Vielzahl von Schienenfahrzeugen 4 und RBCs 3 nur wenige Daten zwischen den KMCs 1a, 1b, 1c ausgetauscht werden.

Fig. 5 zeigt eine schematische Darstellung eines Schienenfahrzeugsicherungssystems 50. Das Schienenfahrzeugsicherungssystem 50 unterscheidet sich von dem Schienenfahrzeugsicherungssystem 40 in Fig. 4 dadurch, dass ein Hauptkommunikationsschlüssel 6 vorgesehen ist, von dem über eine Schlüsselableitungsfunktion eine Vielzahl von schienenfahrzeugspezifischen Kommunikationsschlüsseln 6a, 6b, 6c abgeleitet werden kann. Von einem der schienenfahrzeugspezifischen Kommunikationsschlüssel 6c, welches beispielsweise dem Schienenfahrzeug 4 in Fig. 5 zugeordnet ist, kann dann wiederum eine Vielzahl von RBC-spezifischen Kommunikationsschlüsseln 11 abgeleitet werden, welche an die verschiedenen RBCs 3 durch die jeweiligen KMCs 1a, 1b, 1c verteilt werden können. Dem Schienenfahrzeug 4 wird dann jeweils der schienenfahrzeugspezifische Kommunikationsschlüssel 6c sowie die RBC-spezifischen Kommunikationsschlüssel 11 bereitgestellt, so dass eine Kommunikation mit den jeweiligen RBCs 3 über eine Auswahl eines der RBC-spezifischen Kommunikationsschlüssel 11 erfolgen kann.

Es kann beispielsweise vorgesehen sein, dass auf zwei Schienenfahrzeugen unterschiedlicher Betreiber bzw. unterschiedli-

cher Heim-KMCs der gleiche schienenfahrzeugspezifische Kommunikationsschlüssel 6c installiert wird, so dass bei einer Kopplung der zwei Schienenfahrzeug eine sichere Schienenfahrzeugkommunikation ermöglicht wird.

Fig. 6 zeigt eine schematische Darstellung eines Verfahrens 60 zum Verteilen von Kommunikationsschlüsseln für die Verschlüsselung von Verkehrsleitnachrichten eines Schienenfahrzeugsicherungssystems. In einem ersten Schritt 61 erfolgt ein Erzeugen eines Kommunikationsschlüssels in einer ersten Schlüsselvergabestelle (KMC) eines ersten Streckenbetreibers in Abhängigkeit von einer geplanten Fahrtroute eines Schienenfahrzeugs. In einem zweiten Schritt 62 erfolgt ein Bereitstellen des Kommunikationsschlüssels an ein zweites KMC eines zweiten Streckenbetreibers. In einem dritten Schritt 63 erfolgt ein Bereitstellen des Kommunikationsschlüssels an das Schienenfahrzeug durch das erste KMC. In einem vierten Schritt 64 erfolgt ein Verschlüsseln von Verkehrsleitnachrichten des Schienenfahrzeugs mit dem Kommunikationsschlüssel zum manipulationssicheren Kommunizieren des Schienenfahrzeugs mit RBCs des ersten Streckenbetreibers und mit RBCs des zweiten Streckenbetreibers. Unter Verschlüsseln einer Verkehrsleitnachricht wird insbesondere verstanden, dass Nutzdaten und/oder Verwaltungsdaten, zum Beispiel Adressierungsinformationen, einer Verkehrsleitnachricht kryptographisch vor Abhören und/oder Manipulation geschützt werden, beispielsweise durch Ersetzen von Klartextdaten durch entsprechende verschlüsselte Cipher-Daten, und/oder durch Hinzufügen einer kryptographischen Integritätsprüfinformation (Message Authentication Code).

Patentansprüche

1. Verfahren zum Verteilen von Kommunikationsschlüsseln (6; 6a, 6b, 6c; 11) für die Verschlüsselung von Verkehrsleitnachrichten eines Schienenfahrzeugsicherungssystems, mit den Schritten:
Erzeugen eines Kommunikationsschlüssels (6; 6a, 6b, 6c; 11) in einer ersten Schlüsselvergabestelle (1a) eines ersten Streckenbetreibers in Abhängigkeit von einer geplanten Fahrtroute eines Schienenfahrzeugs (4);
Bereitstellen des Kommunikationsschlüssels (6; 6a, 6b, 6c; 11) an eine zweite Schlüsselvergabestelle (1b) eines zweiten Streckenbetreibers;
Bereitstellen des Kommunikationsschlüssels (6; 6a, 6b, 6c; 11) an das Schienenfahrzeug (4) durch die erste Schlüsselvergabestelle; und
Verschlüsseln von Verkehrsleitnachrichten des Schienenfahrzeugs (4) mit dem Kommunikationsschlüssel (6; 6a, 6b, 6c; 11) zum manipulationssicheren Kommunizieren des Schienenfahrzeugs (4) mit Streckenzentralen (3) des ersten Streckenbetreibers und mit Streckenzentralen (3) des zweiten Streckenbetreibers.

2. Verfahren nach Anspruch 1, weiterhin mit den Schritten:
Bereitstellen des Kommunikationsschlüssels (6; 6a, 6b, 6c; 11) an erste Streckenzentralen (2a; 3) durch den ersten Streckenbetreiber; und
Bereitstellen des Kommunikationsschlüssels (6; 6a, 6b, 6c; 11) an zweite Streckenzentralen (2b; 3) durch den zweiten Streckenbetreiber.

3. Verfahren nach Anspruch 2, wobei der Kommunikationsschlüssel eine Vielzahl von streckenzentralenspezifischen Kommunikationsschlüsseln (6a, 6b, 6c) umfasst, wobei das Bereitstellen des Kommunikationsschlüssels (6; 6a, 6b, 6c; 11) an die zweite Schlüsselvergabestelle (1b) das Be-

reitstellen einer Gruppe von streckenzentralenspezifischen Kommunikationsschlüsseln (6a, 6b, 6c), welche den zweiten Streckenzentralen (2b; 3) des zweiten Streckenbetreibers zugeordnet sind, an die zweite Schlüsselvergabestelle (1b) umfasst.

4. Verfahren nach Anspruch 3, wobei das Erzeugen des Kommunikationsschlüssels (6; 6a, 6b, 6c; 11) in einer ersten Schlüsselvergabestelle (1a) das Ableiten der streckenzentralenspezifischen Kommunikationsschlüssel (6a, 6b, 6c) von einem Hauptkommunikationsschlüssel (6) durch ein Schlüsselableitungsverfahren umfasst.

5. Verfahren nach Anspruch 4, wobei das Ableiten der streckenzentralenspezifischen Kommunikationsschlüssel (6a, 6b, 6c) von einem Steuerrechner des Schienenfahrzeugs (4) durchgeführt wird.

6. Verfahren nach Anspruch 4, wobei das Ableiten der streckenzentralenspezifischen Kommunikationsschlüssel (6a, 6b, 6c) von der ersten und zweiten Schlüsselvergabestelle (1a, 1b) durchgeführt wird.

7. Verfahren nach Anspruch 6, wobei das Ableiten der streckenzentralenspezifischen Kommunikationsschlüssel (6a, 6b, 6c) durch die erste Schlüsselvergabestelle (1a) nur für die ersten Streckenzentralen (2a; 3) und das Ableiten der streckenzentralenspezifischen Kommunikationsschlüssel (6a, 6b, 6c) durch die zweite Schlüsselvergabestelle (1b) nur für die zweiten Streckenzentralen (2b; 3) durchgeführt wird.

8. Verfahren nach Anspruch 2, wobei der Kommunikationsschlüssel eine Vielzahl von schienenfahrzeugspezifischen Kommunikationsschlüsseln (6a, 6b, 6c) umfasst, wobei das Bereitstellen des Kommunikationsschlüssels (6; 6a, 6b, 6c; 11) an das Schienenfahrzeug (4) das Bereitstellen ei-

nes für das Schienenfahrzeug (4) spezifischen Kommunikationsschlüssels aus der Vielzahl von schienenfahrzeugspezifischen Kommunikationsschlüsseln (11) umfasst.

9. Verfahren nach Anspruch 8, weiterhin mit den Schritten:
Ableiten jeweils einer Vielzahl von streckenzentralenspezifischen Kommunikationsschlüsseln (11) von der Vielzahl der schienenfahrzeugspezifischen Kommunikationsschlüssel (6a, 6b, 6c); und
Bereitstellen einer Gruppe von streckenzentralenspezifischen Kommunikationsschlüsseln (11) jeweils einer der Vielzahl von streckenzentralenspezifischen Kommunikationsschlüsseln (11), welche schienenfahrzeugspezifisch den zweiten Streckenzentralen (2b; 3) des zweiten Streckenbetreibers zugeordnet sind, an die zweite Schlüsselvergabestelle (1b).

10. Verfahren nach Anspruch 9, wobei das Ableiten der Vielzahl von streckenzentralenspezifischen Kommunikationsschlüsseln (11) von der Vielzahl der schienenfahrzeugspezifischen Kommunikationsschlüssel (6a, 6b, 6c) durch einen Steuerrechner des Schienenfahrzeugs (4) durchgeführt wird.

11. Verfahren nach einem der Ansprüche 1 bis 10, wobei die geplante Fahrtroute des Schienenfahrzeugs (4) von einem Leitsystem zur Fahrdienststeuerung bereitgestellt wird, und wobei die erste Schlüsselvergabestelle (1a) das Erzeugen und das Bereitstellen des Kommunikationsschlüssels (6; 6a, 6b, 6c; 11) automatisiert durchführt.

12. Steuereinrichtung (7) in einer ersten Schlüsselvergabestelle (1a) eines ersten Schienennetzstreckenbetreibers zum Verteilen von Kommunikationsschlüsseln (6; 6a, 6b, 6c; 11) für die Verschlüsselung von Verkehrsleitnachrichten eines Schienenfahrzeugsicherungssystems, mit:

einer Erzeugungseinrichtung, welche dazu ausgelegt ist, einen Kommunikationsschlüssel (6; 6a, 6b, 6c; 11) in Abhängigkeit von einer geplanten Fahrtroute eines Schienenfahrzeugs (4) zu erzeugen; und

einer Bereitstellungseinrichtung, welche dazu ausgelegt ist, den erzeugten Kommunikationsschlüssel (6; 6a, 6b, 6c; 11) an eine zweite Schlüsselvergabestelle (1b) eines zweiten Streckenbetreibers und an das Schienenfahrzeug (4) bereitzustellen, wobei der Kommunikationsschlüssel (6; 6a, 6b, 6c; 11) zum Verschlüsseln von Verkehrsleitnachrichten des Schienenfahrzeugs (4) zum manipulationssicheren Kommunizieren des Schienenfahrzeugs (4) mit Streckenzentralen (2a; 3) des ersten Streckenbetreibers und mit Streckenzentralen (2b; 3) des zweiten Streckenbetreibers ausgelegt ist.

13. Schienenfahrzeugsicherungssystem (20; 30; 40; 50), mit:
einer Steuereinrichtung (7) nach Anspruch 12;
einer ersten Schlüsselvergabestelle (1a), in der die Steuereinrichtung (7) angeordnet ist;
einer Vielzahl von ersten Streckenzentralen (2a; 3), welche dazu ausgelegt sind, von der ersten Schlüsselvergabestelle (1a) mit einem von der Steuereinrichtung (7) erzeugten Kommunikationsschlüssel (6; 6a, 6b, 6c; 11) für die Verschlüsselung von Verkehrsleitnachrichten eines Schienenfahrzeugs (4) versorgt zu werden;
einer zweiten Schlüsselvergabestelle (1b); und
einer Vielzahl von zweiten Streckenzentralen (2b; 3), welche dazu ausgelegt sind, von der zweiten Schlüsselvergabestelle (1b) mit einem von der Steuereinrichtung (7) erzeugten Kommunikationsschlüssel (6; 6a, 6b, 6c; 11) für die Verschlüsselung von Verkehrsleitnachrichten eines Schienenfahrzeugs (4) versorgt zu werden.

FIG 1

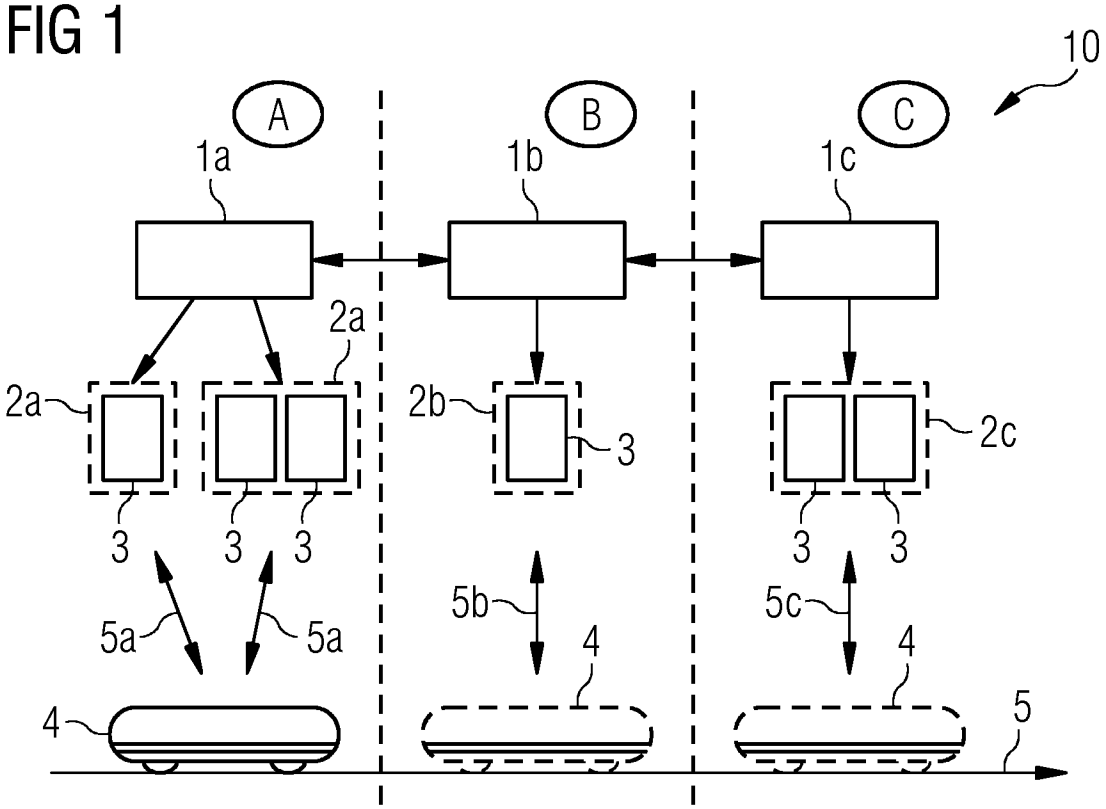

10
A
B
C
1a
1b
1c
2a
2a
2b
2c
3
3
3
3
3
3
3
5a
5a
5b
5c
4
4
4
4
5

FIG 2

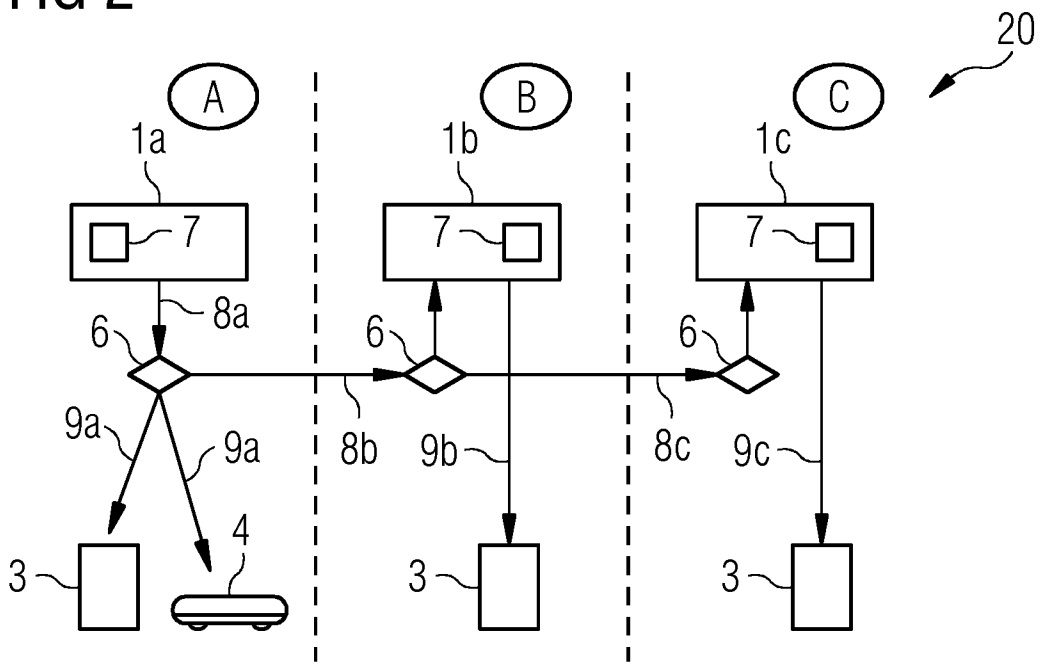

20
A
B
C
1a
1b
1c
7
7
7
8a
6
6
6
9a
9a
8b
9b
8c
9c
4
3
3
3

FIG 3

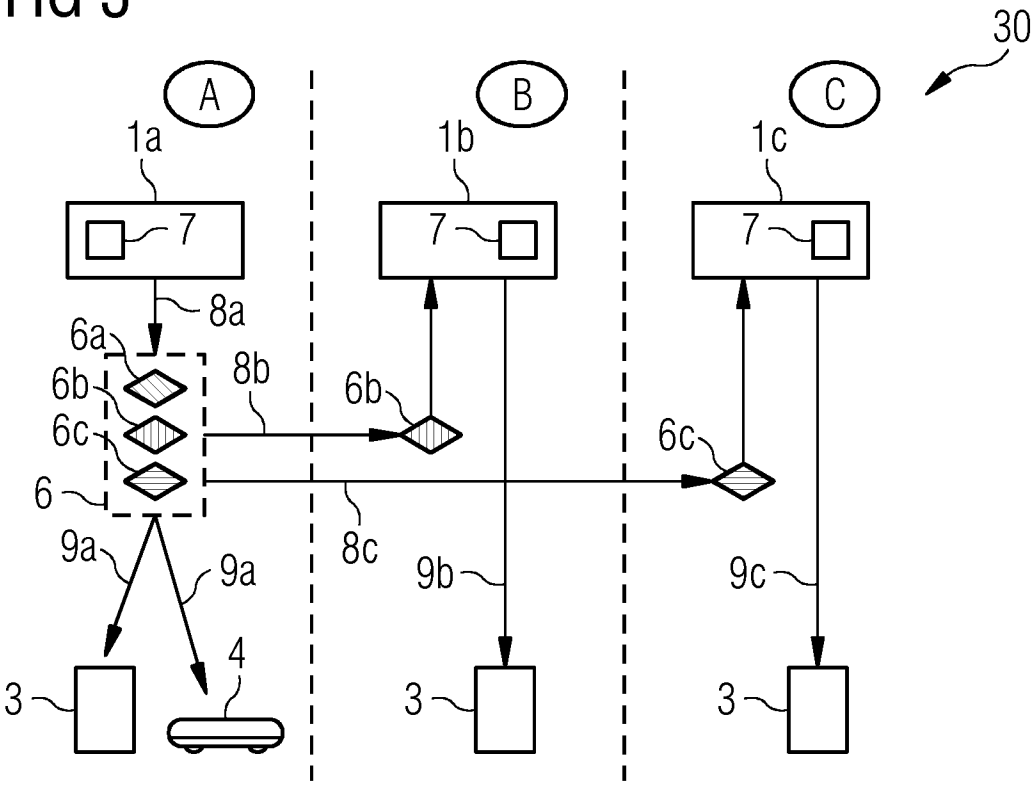

30
A
B
C
1a
1b
1c
7
8a
6a
6b
6c
6
8b
8c
9a
9b
9c
4
3

FIG 4

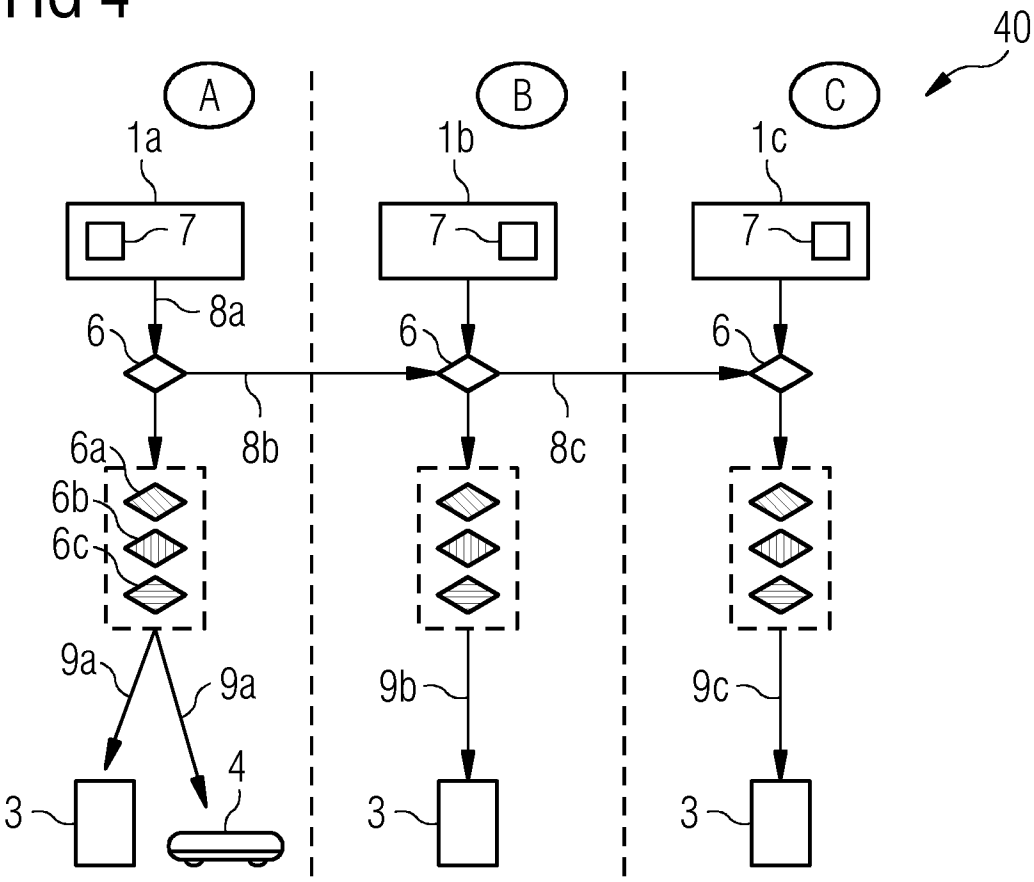

40
A
B
C
1a
1b
1c
7
8a
6
8b
8c
6a
6b
6c
9a
9b
9c
4
3

FIG 5

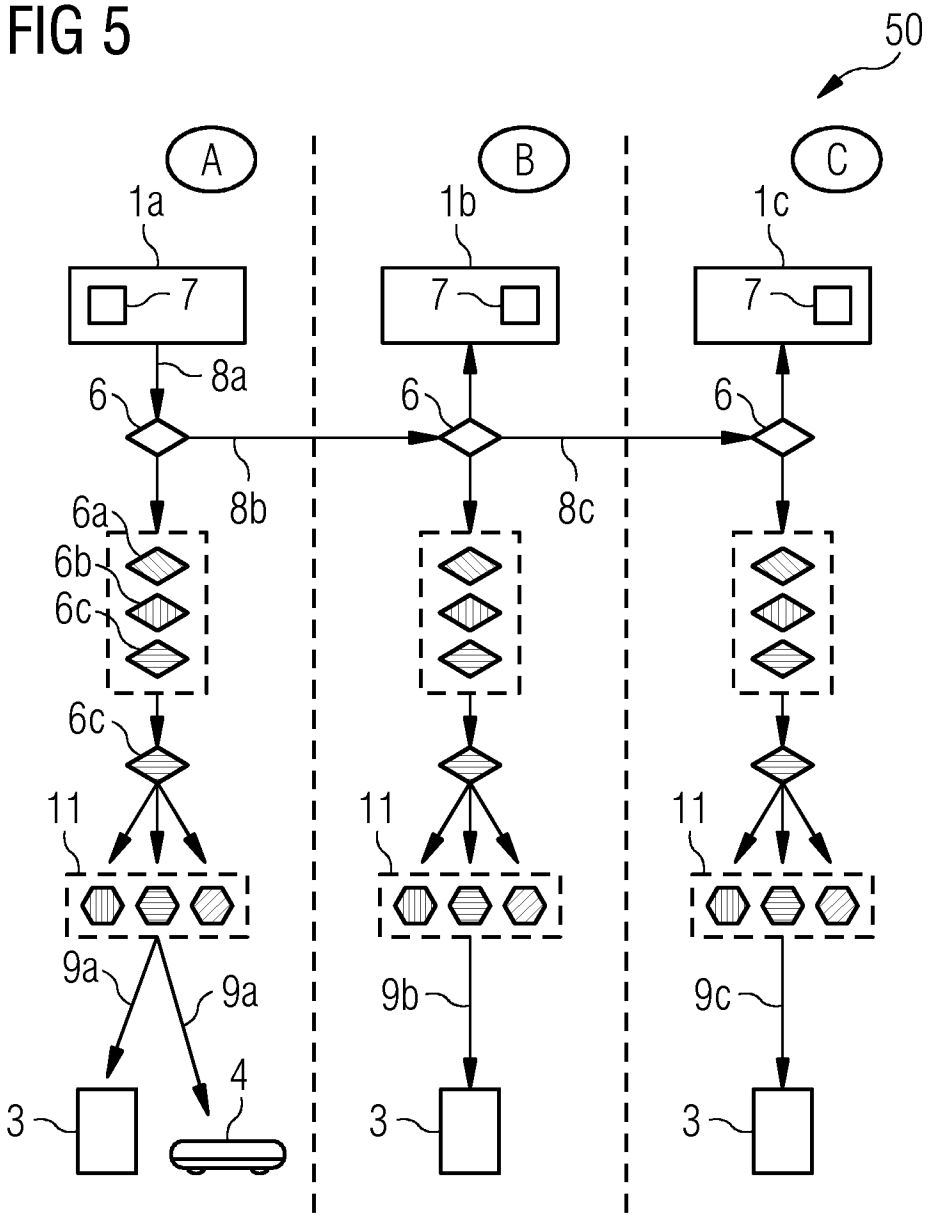
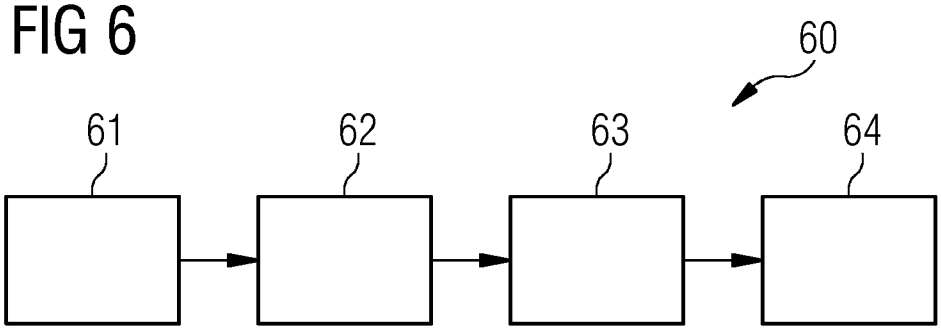


FIG 6



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2012/055460

A. CLASSIFICATION OF SUBJECT MATTER
INV. B61L15/00 B61L27/00
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
B61L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 10 2007 041177 A1 (SIEMENS AG [DE]) 5 March 2009 (2009-03-05) paragraph [0049] - paragraph [0054] figures 1-5	1,2,8, 12,13
X	BRANDENBURG D ET AL: "Effektive ETCS-Schlüsselverwaltung mit KEY.connect", SIGNAL + DRAHT, TELZLAFF VERLAG GMBH. DARMSTADT, DE, vol. 102, no. 4, 1 April 2010 (2010-04-01) , pages 44-48, XP001552658, ISSN: 0037-4997 the whole document	1,2,8, 12,13
A	EP 2 039 583 A1 (HITACHI LTD [JP]) 25 March 2009 (2009-03-25) paragraph [0029] - paragraph [0038]	1-13

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 June 2012	03/07/2012

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Janhsen, Axel

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2012/055460

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 102007041177 A1	05-03-2009	DE 102007041177 A1	05-03-2009
		WO 2009027380 A1	05-03-2009
EP 2039583 A1	25-03-2009	AT 518718 T	15-08-2011
		CN 101391616 A	25-03-2009
		EP 2039583 A1	25-03-2009
		JP 4471996 B2	02-06-2010
		JP 2009067357 A	02-04-2009

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2012/055460

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. B61L15/00 B61L27/00
ADD.

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
B61L

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

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

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	DE 10 2007 041177 A1 (SIEMENS AG [DE]) 5. März 2009 (2009-03-05) Absatz [0049] - Absatz [0054] Abbildungen 1-5	1,2,8, 12,13
X	BRANDENBURG D ET AL: "Effektive ETCS-Schlüsselverwaltung mit KEY.connect", SIGNAL + DRAHT, TELZLAFF VERLAG GMBH. DARMSTADT, DE, Bd. 102, Nr. 4, 1. April 2010 (2010-04-01) , Seiten 44-48, XP001552658, ISSN: 0037-4997 das ganze Dokument	1,2,8, 12,13
A	EP 2 039 583 A1 (HITACHI LTD [JP]) 25. März 2009 (2009-03-25) Absatz [0029] - Absatz [0038]	1-13

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

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
21. Juni 2012	03/07/2012

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

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2012/055460

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 102007041177 A1	05-03-2009	DE 102007041177 A1	05-03-2009
		WO 2009027380 A1	05-03-2009
EP 2039583 A1	25-03-2009	AT 518718 T	15-08-2011
		CN 101391616 A	25-03-2009
		EP 2039583 A1	25-03-2009
		JP 4471996 B2	02-06-2010
		JP 2009067357 A	02-04-2009