(19) Deutsches Patent- und Markenamt

(10) **DE 10 2023 115 048 B4** 2024.12.19

(12) # Patentschrift

(21) Aktenzeichen: **10 2023 115 048.0**
(22) Anmeldetag: **07.06.2023**
(43) Offenlegungstag: **12.12.2024**
(45) Veröffentlichungstag der Patenterteilung: **19.12.2024**

(51) Int Cl.: ***H04L 9/30*** (2006.01)
H04L 9/32 (2006.01)

Innerhalb von neun Monaten nach Veröffentlichung der Patenterteilung kann nach § 59 Patentgesetz gegen das Patent Einspruch erhoben werden. Der Einspruch ist schriftlich zu erklären und zu begründen. Innerhalb der Einspruchsfrist ist eine Einspruchsgebühr in Höhe von 200 Euro zu entrichten (§ 6 Patentkostengesetz in Verbindung mit der Anlage zu § 2 Abs. 1 Patentkostengesetz).

(73) Patentinhaber:
SMA Solar Technology AG, 34266 Niestetal, DE

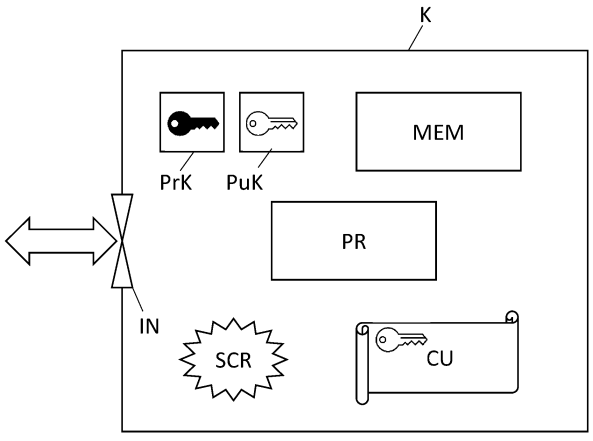
(72) Erfinder:
Hanke, Ingo, 37073 Göttingen, DE; Tuemmler, Joern, 34317 Habichtswald, DE; Wischer, Mirko, 36251 Bad Hersfeld, DE; Graf, Tobias, 34246 Vellmar, DE

(56) Ermittelter Stand der Technik:

US	**2021 / 0 184 864**	**A1**
WO	**2013/ 123 548**	**A2**

(54) Bezeichnung: **VERFAHREN ZUM AUFBAU EINER DEZENTRALEN DATENKOMMUNIKATIONSSTRUKTUR INNERHALB EINES SYSTEMS MIT EINER MEHRZAHL VON KOMPONENTEN**

(57) Zusammenfassung: Ein Verfahren zum Aufbau einer dezentralen Datenkommunikationsstruktur innerhalb eines Systems mit einer Mehrzahl von Komponenten (K), wobei jede Komponente einen privaten Schlüssel (PrK), einen zugehörigen öffentlichen Schlüssel (PuK), ein gegen Auslesen gesichertes Geheimnis (SCR) und im Ausgangszustand unsignierte, den öffentlichen Schlüssel (PuK) beinhaltende Zertifikatsinformationen (CU) enthält, umfasst die Schritte:
- Einrichten einer registrierenden Komponente (rK) der Mehrzahl von Komponenten (K), wobei das Einrichten ein Hinterlegen einer Liste von Validierungseinträgen umfasst,
- Aufbauen eines manipulationssicheren Kanals zwischen der registrierenden Komponente (rK) und einer ersten Komponente (K1) der anderen Komponenten (aK), und
- Authentisieren der ersten Komponente (K1) bei der registrierenden Komponente (rK) und Authentifizieren der ersten Komponente (K1) mittels der Liste von Validierungseinträgen über den manipulationssicheren Kanal. Das Authentifizieren umfasst ein Signieren der unsignierten Zertifikatsinformationen (CU) der ersten Komponente (K1) durch die registrierende Komponente (rK) über den manipulationssicheren Kanal. Ein System, insbesondere eine Energieerzeugungsanlage, mit einer Mehrzahl von Komponenten (K) ist eingerichtet zur Ausführung des Verfahrens.



Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zum Aufbau einer dezentralen Datenkommunikationsstruktur innerhalb eines Systems mit einer Mehrzahl von Komponenten, sowie ein System mit einer Mehrzahl von Komponenten, das zur Ausführung des Verfahrens eingerichtet ist.

[0002] Um kritische Infrastruktur, insbesondere Systeme zur Energieerzeugung und Einspeisung in ein öffentliches Netz, vor Cyberangriffen zu schützen, sind hohe Sicherheitsanforderungen zu erfüllen. Es wird daher gefordert, die Anbindung solcher Systeme an ein Datennetz auf das funktional notwendige Maß zu reduzieren oder darauf ganz zu verzichten. Dennoch müssen die Komponenten eines solchen Systems untereinander manipulationssicher und abhörsicher kommunizieren können, auch wenn ein Cyberangriff gegebenenfalls nur über einen direkten Zugriff auf eine der Komponenten beziehungsweise auf die Kommunikationsverbindung zwischen Komponenten möglich ist, der nur vor Ort durchgeführt werden kann. Hierzu sind Verfahren entwickelt worden, die auf der Existenz von bereits signierten Zertifikaten auf den Komponenten des Systems beruhen. Die Installation eines Systems, das die Voraussetzungen zur Ausführung solcher Verfahren bereitstellt, ist aber komplex, da es eine Verteilung dieser Zertifikate zu jeder der Komponenten auf sicherem Wege, bevorzugt bereits bei der Produktion der Komponente, andernfalls durch eine direkte Datenverbindung mit jeder der Komponenten des bereits installierten Systems, erfordert. Insbesondere ein Einsatz von Komponenten einer Mehrzahl von Herstellern in einem System wird dadurch mangels vorhandener Standards erschwert.

[0003] In dem Dokument US 2021/0184864 A1 ist ein Verfahren zum Aufbau einer Zertifikat-Infrastruktur in einem System mit gemischten Signierprotokollen offenbart. Hierbei werden unterschiedliche digitale Zertifikate für die verschiedenen Protokolle erzeugt. Weiterhin zeigt auch das Dokument WO 2013/123548 A2 ein Verfahren zur Bereitstellung von Schlüsseln für eine gesicherte Kommunikation zwischen zwei Nutzern in einem dezentralen Netzwerk beziehungsweise eine Anwendung zum Teilen von Informationen zwischen Nutzern über einen gemeinsamen Datenspeicher.

[0004] Andere Verfahren basieren darauf, dass die Komponenten ihre Zertifikate selbst signieren. Diese Verfahren sind leicht umsetzbar, haben aber den wesentlichen Nachteil, dass eine sichere Überprüfung der Identität dieses Gerätes durch andere Kommunikationspartner nicht möglich ist. Die Kommunikation zwischen zwei Geräten kann auf diese Weise zwar verschlüsselt werden, aber es kann keine korrekte gegenseitige Authentifizierung der Kommunikationsteilnehmer erfolgen. Dadurch ist ein Unterbrechen und Abhören der Kommunikation zwischen zwei Geräten durch einen unautorisierten Dritten („Man-in-the-Middle“) möglich.

[0005] Entsprechend ist es Aufgabe dieser Erfindung, ein Verfahren zum Aufbau einer dezentralen Datenkommunikationsstruktur innerhalb eines Systems mit einer Mehrzahl von Komponenten aufzuzeigen, das sicher und mit geringem Aufwand umsetzbar ist, und das den Einsatz effizienter und bewährter Standard-Kommunikationsprotokolle innerhalb der dezentralen Datenkommunikationsstruktur erlaubt.

[0006] Diese Aufgabe wird gelöst durch ein Verfahren mit den Merkmalen des unabhängigen Anspruchs 1. Bevorzugte Ausführungen des Verfahrens sowie Systeme, eingerichtet zur Ausführung des Verfahrens, sind Gegenstand der abhängigen Ansprüche.

[0007] In einem System mit einer Mehrzahl von Komponenten, wobei jede Komponente des Systems einen privaten Schlüssel, einen zugehörigen öffentlichen Schlüssel, ein gegen Auslesen gesichertes Geheimnis und im Ausgangszustand unsignierte, den öffentlichen Schlüssel beinhaltende Zertifikatsinformationen aufweist, umfasst ein erfindungsgemäßes Verfahren zum Aufbau einer dezentralen Datenkommunikationsstruktur innerhalb des Systems ein Einrichten einer registrierenden Komponente der Mehrzahl von Komponenten, ein Aufbauen eines manipulationssicheren Kanals zwischen der registrierenden Komponente und einer ersten Komponente der anderen Komponenten, ein Authentisieren der ersten Komponente bei der registrierenden Komponente, sowie ein Authentifizieren der ersten Komponente mittels der Liste von Einträgen über den manipulationssicheren Kanal. Das Authentifizieren umfasst ein Signieren der unsignierten Zertifikatsinformationen der ersten Komponente durch die registrierende Komponente über den manipulationssicheren Kanal. Das Einrichten umfasst ein Hinterlegen einer Liste von Validierungseinträgen.

[0008] Im Rahmen dieser Erfindung wird unter dem Begriff Validierungseintrag ein Eintrag verstanden, der aus den jeweiligen gerätespezifischen Geheimnissen der Mehrzahl von Komponenten erzeugt wurde und eine Prüfung der Kenntnis der gerätespezifischen Geheimnisse ohne deren Übertragung gestatten. Der Validierungseintrag kann das Geheimnis selbst enthalten oder daraus bestehen, es ist aber von Vorteil, dass der Validierungseintrag lediglich einen mittels des Geheimnisses errechneten Datensatz enthält, aus dem sich das Geheimnis selbst nicht zurückrechnen lässt. Der Validierungseintrag kann beispielsweise einen „gesalzenen“ Hashwert des Geheimnisses enthalten. Der Validierungseintrag kann aber auch einen Nonce oder eine

Mehrzahl von Nonces (zufällig erzeugte Datensätze) und zu jedem Nonce als erwartete Antwort einen zugehörigen Hashwert enthalten, der aus einer Kombination des Nonces und des Geheimnisses bestimmt wurde. Bei einer Mehrzahl von Nonces kann zur Steigerung der Cybersicherheit vorgesehen werden, dass jeder Nonce nur einmal verwendet wird oder erst wieder verwendet wird, nachdem die anderen Nonces verwendet wurden.

[0009] In einer vorteilhaften Ausgestaltung kann das Signieren eine Übertragung des öffentlichen Schlüssels der registrierenden Komponente über den manipulationssicheren Kanal umfassen. Wenn der öffentliche Schlüssel nur im Rahmen des Signierens übertragen wird, kann die Sicherheit der Datenkommunikationsstruktur gegen Cyberangriffe erhöht werden, weil der öffentliche Schlüssel hierbei nur an authentifizierte Komponenten übertragen wird.

[0010] Das Einrichten einer registrierenden Komponente der Mehrzahl von Komponenten kann beispielsweise durch einen Installateur als autorisierte Partei über eine verschlüsselte und manipulationsgesicherte Datenverbindung erfolgen. Die Validierungseinträge können hierbei erzeugt werden, indem der Installateur Seriennummern der in die dezentrale Datenkommunikationsstruktur aufzunehmenden Komponenten in ein Endgerät eingibt und dieses Endgerät hieraus die an die registrierende Komponente zu übertragenden Validierungseinträge identifiziert und überträgt. Die Identifikation kann über eine lokal auf dem Endgerät hinterlegte Datenbank oder durch Abruf der Validierungseinträge zu den Seriennummern aus einer entfernt hinterlegten Datenbank erfolgen. Die weiteren Komponenten des Systems müssen zu diesem Zeitpunkt nicht in Betrieb oder über eine Datenverbindung erreichbar sein.

[0011] Das Aufbauen eines manipulationssicheren Kanals zwischen der registrierenden Komponente und einer ersten Komponente des Systems kann mit Hilfe eines Preshared Keys erfolgen. Es ist hierzu denkbar, dass die autorisierte Partei sich mit der ersten Komponente über eine verschlüsselte und manipulationsgesicherte Datenverbindung verbindet, und den Preshared Key, beispielsweise den öffentlichen Schlüssel der registrierenden Komponente, auf diese Weise überträgt. Ebenso ist denkbar, dass der Preshared Key bereits bei der Produktion gemeinsam mit dem gerätespezifischen Geheimnis in einem besonders gegen Auslesen gesicherten Speicherbereich abgelegt wird. Zusätzlich zur Absicherung gegen Manipulation der übertragenen Daten kann der Kanal auch verschlüsselt und/oder gegen ein erneutes, nicht autorisiertes Übertragen (sogenannte Replay-Attacke) gesichert sein.

[0012] Die Authentifizierung einer Komponente in Reaktion auf die Authentisierung kann über den manipulationssicheren Kanal erfolgen, indem die erste Komponente die unsignierte Zertifikatsinformation zur registrierenden Komponente überträgt. Weiterhin umfasst die Authentifizierung eine Prüfung, ob auf der ersten Komponente ein dem für diese Komponente in der Liste enthaltenen Validierungseintrag entsprechendes Geheimnis hinterlegt ist. Das Geheimnis sollte bei dieser Prüfung auf der ersten Komponente verbleiben und nicht übertragen werden. Dies kann beispielsweise dadurch erfolgen, dass die registrierende Komponente einen ersten Datensatz in Form eines im Validierungseintrag hinterlegten Nonces zur ersten Komponente überträgt, diese einen Hashwert einer Kombination des ersten Datensatzes und des hinterlegten Geheimnisses berechnet und diesen als zweiten Datensatz zurück an die registrierende Komponente überträgt. Nur bei Identität des zweiten Datensatzes mit einer zum ersten Datensatz zugehörigen erwarteten Antwort des Validierungseintrags wird das Signieren und die Rückübertragung der signierten Zertifikatsinformation vorgenommen. Das Signieren kann durch eine Verschlüsselung der unsignierten Zertifikatsinformation, eines Teils davon oder eines daraus berechneten Datensatzes, beispielsweise eines Hashwerts, mit dem privaten Schlüssel der registrierenden Komponente erfolgen. Jede Komponente kann dann die Vertrauenswürdigkeit der signierten Zertifikatsinformation mittels des öffentlichen Schlüssels der registrierenden Komponente überprüfen. Beim Signieren können der Zertifikatsinformation auch weitere Informationen durch die registrierende Komponente hinzugefügt werden. Insbesondere kann ein Gültigkeitszeitraum oder weitere Gültigkeitskriterien ergänzt werden, die erfüllt sein müssen, damit das signierte Zertifikat als vertrauenswürdig eingestuft werden kann.

[0013] Die unsignierte Zertifikatsinformation kann über den öffentlichen Schlüssel der zugehörigen Komponente hinaus weitere Bestandteile enthalten, beispielsweise Informationen zur Herstellung einer Datenverbindung mit der zugehörigen Komponente wie einem Domänen-Name oder eine IP-Adresse.

[0014] Die Authentifizierung kann für jede Komponente des Systems durchgeführt werden, um eine durch die registrierende Komponente signierte Zertifikatsinformationen zu erhalten, und nach Durchführung der Authentifizierung kann die Komponente mittels der signierten Zertifikatsinformation bei anderen Komponenten des Systems seine Vertrauenswürdigkeit nachweisen. Anschließend kann mittels bekannter Protokolle ein Sitzungsschlüssel mit den anderen Komponenten, die durch die registrierende Komponente signierte Zertifikatsinformationen bereitstellen, zum Aufbauen eines gesicherten Kommunikationskanals vereinbart werden. Der Kommunikationskanal

kann insbesondere durch eine symmetrische Verschlüsselung über den Sitzungsschlüssel gesichert sein. Das verwendete Protokoll kann ein TLS-Protokoll sein. Hierdurch können hohe Datenübertragungsraten mit geringem Aufwand erreicht werden.

[0015] Ein Nachweis der Vertrauenswürdigkeit einer signierten Zertifikatsinformation kann auf bekanntem Wege über den öffentlichen Schlüssel der registrierenden Komponente erfolgen. Dieser kann jederzeit bei der registrierenden Komponente abgefragt werden und kann auch über einen nicht gesicherten Kommunikationskanal übertragen werden, ohne die Integrität der Kommunikationsstruktur zu gefährden.

[0016] In einem weiteren Aspekt der Erfindung ist ein System mit einer Mehrzahl von Komponenten mit den vorstehend beschriebenen Merkmalen eingerichtet zur Ausführung des erfindungsgemäßen Verfahrens. Vorteilhafterweise weist eine Komponente der Mehrzahl von Komponenten eine Schnittstelle zum Login eines Systemnutzers auf, wobei die Schnittstelle zum Einrichten der einen Komponente als registrierende Komponente und zum Hinterlegen der Liste von Validierungseinträgen der anderen Komponenten des Systems eingerichtet ist. Die Schnittstelle kann bevorzugt eine Schnittstelle zur kabelgebundenen Kommunikation sein, beispielsweise eine LAN-Schnittstelle, an die ein Endgerät des Systemnutzers angeschlossen werden kann. Das System weist in einer vorteilhaften Ausführung einen Generator, einen Verbraucher, einen Wandler oder einen Speicher für elektrische Energie auf. Bevorzugt ist das System dazu eingerichtet, elektrische Leistung mit einem Energieübertragungsnetz auszutauschen.

[0017] Bevorzugt weist das System keine Datenverbindung mit einer Instanz außerhalb des Systems, beispielsweise keine Internetverbindung, auf. Hierdurch ist die Möglichkeit eines Datenzugriffs auf das System, insbesondere eines Cyber-Angriffs, von außen unmöglich. Alternativ ist nur genau eine der Komponenten mit einer solchen Datenverbindung ausgestattet. Diese Komponente kann besonders gegen Cyber-Angriffe gesichert sein und beispielsweise nur von ausgewählten Instanzen aus oder über eine besonders gesicherte Verbindung erreichbar sein.

[0018] Im Folgenden wird die Erfindung mithilfe von Figuren dargestellt, von denen

Fig. 1 eine Datenstruktur einer Komponente eines erfindungsgemäßen Systems,

Fig. 2 ein Ablaufdiagramm eines erfindungsgemäßen Verfahrens,

Fig. 3 einen Teilschritt des Ablaufdiagramms aus **Fig.** 2, und

Fig. 4 ein erfindungsgemäßes System nach Ausführung des erfindungsgemäßen Verfahrens zeigen.

[0019] **Fig.** 1 zeigt eine Datenstruktur einer Komponente K eines Systems, das zum Aufbau einer dezentralen Datenkommunikationsstruktur eingerichtet ist. Die Komponente K weist eine Schnittstelle IN zur Datenkommunikation mit anderen Komponenten auf. Weiterhin umfasst die Komponente K einen Prozessor PR und einen Speicher MEM, mit dem wesentliche Funktionen der Komponente bereitgestellt werden. Neben einem Schlüsselpaar, gebildet durch einen privaten Schlüssel PrK und einen zugehörigen öffentlichen Schlüssel PuK zur Verschlüsselung und Entschlüsselung von Daten, weist die Komponente K in einem gegen Auslesen von außen gesicherten Speicherbereich ein Geheimnis SCR auf. Auch der private Schlüssel PrK kann in dem von gegen Auslesen von außen gesicherten Speicherbereich abgelegt sein. Das Schlüsselpaar kann beispielsweise bei der Produktion der Komponente erzeugt und abgelegt werden, oder die Komponente kann das Schlüsselpaar mithilfe von zufällig erzeugten Daten bei der Inbetriebnahme oder aufgrund eines über die Schnittstelle IN empfangenen Befehls erzeugen. Das Geheimnis wird bevorzugt während der Produktion der Komponente erzeugt und eine Kopie des Geheimnisses wird in einer Datenbank beim Produzenten der Komponente gespeichert. Alternativ kann das Geheimnis aus der Seriennummer der Komponente bestimmt werden oder lesbar auf der Komponente angebracht oder in den mit der Komponente mitgelieferten Unterlagen enthalten sein.

[0020] Zusätzlich umfasst die Komponente K ein zunächst unsigniertes Zertifikat CU, in dem eine Kopie des öffentlichen Schlüssels PuK der Komponente K enthalten ist, was durch das Schlüsselsymbol in dem Zertifikat CU angedeutet werden soll. Das Zertifikat CU kann weitere Informationen enthalten, beispielsweise eine Adresse, unter der die Komponente K über die Schnittstelle IN angesprochen werden kann. Ein System wird durch eine Mehrzahl von Komponenten K mit einer solchen Struktur gebildet, zwischen denen eine gegenüber Zugriff oder Manipulation von außen gesicherte, dezentrale Datenkommunikationsstruktur aufgebaut werden soll. Das System kann eine Energieerzeugungsanlage sein, die an ein Versorgungsnetz angeschlossen ist.

[0021] In einem in **Fig.** 2 gezeigten Verfahren zum Aufbau einer dezentralen Datenkommunikationsstruktur innerhalb eines Systems mit einer Mehrzahl von Komponenten umfasst ein erster Schritt S1 ein Einrichten einer registrierenden Komponente der Mehrzahl von Komponenten. Grundsätzlich kann jede der Komponenten des Systems als registrierende Komponente ausgewählt werden. Das Einrich-

ten kann durch einen Installateur im Rahmen der Inbetriebnahme des Systems durchgeführt werden. Das Einrichten umfasst ein Hinterlegen einer Liste von Validierungseinträgen im Speicher der registrierenden Komponente, durch die festgelegt wird, welche Authentisierungen von anderen Komponenten des Systems von der registrierenden Komponente akzeptiert werden. Die Liste von Validierungseinträgen kann aus einer Liste von gerätespezifischen Geheimnissen erzeugt werden, wobei die Gerätegeheimnisse dem Gerät in gedruckter Form oder abgedruckt auf dem Typenschild beigelegt werden können. Zur Erzeugung der Validierungseinträge kann eine Abfrage des zu dem jeweiligen Gerät zugehörigen Geheimnisses in der Datenbank des Produzenten notwendig sein. Die Auswahl einer Komponente als registrierende Komponente kann im Speicher der registrierenden Komponente hinterlegt werden.

[0022] In einem zweiten Schritt S2 kann dann eine andere Komponente einen gegen Manipulation gesicherten Kanal mit der registrierenden Komponente aufbauen. Ein solcher Aufbau kann über bekannte Verfahren wie dem Diffie-Hellman-Verfahren erfolgen. Hierzu ist noch nicht der Nachweis einer Vertrauenswürdigkeit zwischen den Kommunikationspartnern erforderlich.

[0023] In einem dritten Schritt authentisiert sich die andere Komponente bei der registrierenden Komponente. Dies ist in **Fig.** 3 näher aufgegliedert. Hierzu überträgt die andere Komponente in einem ersten Teilschritt S3.1 ihr zunächst unsigniertes Zertifikat an die registrierende Komponente. Die registrierende Komponente prüft die Berechtigung der anderen Komponente mittels der Validierungseinträge. Beispielsweise kann die Prüfung in einem zweiten Teilschritt S3.2 ein Senden eines Eintrages aus den Validierungseinträgen von der registrierenden Komponente an die andere Komponente umfassen, die aus dem Eintrag und dem bei der anderen Komponente hinterlegten Geheimnis eine Antwort errechnet und in einem dritten Teilschritt S3.3 an die registrierende Komponente zurückschickt. Stimmt die Antwort in einem vierten Teilschritt S3.4 mit einem der erwarteten Antwort zugeordneten Eintrag in der Liste der Validierungseinträge überein, authentifiziert die registrierende Komponente in einem fünften Teilschritt S3.5 die andere Komponente, andernfalls verweigert sie die Authentifizierung in einem sechsten Teilschritt S3.6. Die Authentifizierung umfasst ein Signieren der unsignierten Zertifikatsinformationen der anderen Komponente mittels des privaten Schlüssels der registrierenden Komponente und eine Rücksendung des signierten Zertifikats über den gesicherten Kanal. Bevorzugt wird bei der Rücksendung auch der öffentliche Schlüssel der registrierenden Komponente mit verschickt, der eine spätere Prüfung der Vertrauenswürdigkeit des Zertifikats erlaubt. Alternativ kann der öffentliche Schlüssel auch zu einem anderen Zeitpunkt, insbesondere nach gegenseitiger Authentifizierung beider Kommunikationspartner, übertragen werden. So kann sichergestellt werden, dass der öffentliche Schlüssel der registrierenden Komponente auch tatsächlich von dieser stammt.

[0024] Nacheinander kann sich dann auf diese Weise jede der anderen Komponenten ebenfalls bei der registrierenden Komponente authentifizieren und so ein von der registrierenden Komponente signiertes Zertifikat erhalten. Daher kann das Verfahren beendet werden, wenn in einem vierten Schritt S4 festgestellt wird, dass alle Komponenten des Systems erfolgreich authentifiziert worden sind. Hierdurch ist sichergestellt, dass in der Folge jede Komponente des Systems ein von der registrierenden Komponente signiertes Zertifikat und den öffentlichen Schlüssel der registrierenden Komponente besitzt und mit diesen Informationen zu jeder anderen Komponente des Systems mit bekannten Protokollen, beispielsweise dem TLS (Transport-Layer-Security) Protokoll, einen Sitzungsschlüssel vereinbaren und damit eine gesicherte und vertrauenswürdige Datenverbindung herstellen kann. Ebenso ist ausgeschlossen, dass fremde Komponenten eine solche Verbindung mit Komponenten des Systems aufbauen oder in diese unbemerkt eingreifen können, da eine fremde Komponente keine Authentifizierung durch die registrierende Komponente erzielen kann, weil sie kein zu der Liste der Validierungseinträge passendes Geheimnis besitzt. Die mit den erfindungsgemäßen Verfahren aufgebaute dezentrale Datenkommunikationsstruktur ist daher eine geschlossene Struktur.

[0025] Bei Bedarf kann das Verfahren jederzeit erneut ausgeführt werden, um eine vermutete Kompromittierung auszuschließen. Hierzu ist es lediglich erforderlich, dass die registrierende Komponente ein neues Schlüsselpaar, also einen neuen privaten und öffentlichen Schlüssel, erzeugt und den alten öffentlichen Schlüssel im System durch den neu erzeugten öffentlichen Schlüssel ersetzt. Die anderen Komponenten können dann erkennen, dass eine erneute Authentisierung ihrer Zertifikate erforderlich ist und dies bei der registrierenden Komponente anstoßen.

[0026] Ebenso ist es leicht möglich, weitere Komponenten später in das System aufzunehmen, indem die Liste der Validierungseinträge um einen Validierungseintrag der neuen Komponente erweitert wird. Die weitere Komponente kann sich dadurch ebenfalls erfolgreich bei der registrierenden Komponente authentisieren.

[0027] In **Fig.** 4 ist ein System nach Ausführung des erfindungsgemäßen Verfahrens gezeigt. Sowohl eine registrierende Komponente rK als auch eine Anzahl anderer Komponenten aK sind dazu einge-

richtet, über einen Bus BUS miteinander zu kommunizieren und sind auch mit diesem über eine Schnittstelle IN verbunden. Dies kann eine kabelgebundene oder auch eine nicht kabelgebundene Verbindung, beispielsweise eine Funkverbindung, sein. Nach Ausführung des erfindungsgemäßen Verfahrens weist jede Komponente ein von der registrierenden Komponente rK signiertes Zertifikat CS auf. Dies ist durch das Symbol des öffentlichen Schlüssels der der registrierenden Komponente rK im signierten Zertifikat CS angedeutet. Die der registrierende Komponente rK weist hierbei ein selbst signiertes Zertifikat CS auf. Die anderen Bestandteile der Komponenten des Systems, wie der Prozessor PR, der Speicher MEM, das eigene Schlüsselpaar PrK, PuK, sowie das Geheimnis SCR entsprechen den namensgleichen Bestandteilen der **Fig.** 1.

[0028] Durch Bereitstellung des eigenen Zertifikats einer ersten Komponente an eine zweite, andere Komponente des Systems als gewünschtem Kommunikationspartner kann die zweite Komponente den öffentlichen Schlüssel der ersten Komponente erhalten und mittels bekannter Verfahren auf Vertrauenswürdigkeit prüfen, sowie das eigene signierte Zertifikat als Antwort zur Kontaktaufnahme zurücksenden. Dieses kann die erste Komponente auf gleiche Weise auf Vertrauenswürdigkeit prüfen. Nach erfolgreicher gegenseitiger Zusicherung der Vertrauenswürdigkeit kann mittels der öffentlichen Schlüssel leicht ein temporärer Schlüssel für eine gesicherter Kommunikation vereinbart werden. Das Kommunikationsverfahren kann beispielsweise das TLS-Verfahren oder ein SSL (Secure Socket Layer) Verfahren sein, das hohe Datenraten und geringen Rechenaufwand für die Prozessoren PR der beteiligten Kommunikationspartner bei hoher Cybersicherheit ermöglicht.

Bezugszeichenliste

K, K1, K2, aK	Komponente
rK	registrierende Komponente
PrK	privater Schlüssel
PuK	öffentlicher Schlüssel
CU	unsigniertes Zertifikat
CS	signiertes Zertifikat
PR	Prozessor
MEM	Speicher
SCR	Gerätespezifisches Geheimnis
S1-S4	Schritt
S3.1 - S3.6	Schritt

Patentansprüche

1. Verfahren zum Aufbau einer dezentralen Datenkommunikationsstruktur innerhalb eines Systems mit einer Mehrzahl von Komponenten (K), wobei jede Komponente einen privaten Schlüssel (PrK), einen zugehörigen öffentlichen Schlüssel (PuK), ein gegen Auslesen gesichertes Geheimnis (SCR) und im Ausgangszustand unsignierte, den öffentlichen Schlüssel (PuK) beinhaltende Zertifikatsinformationen (CU) enthält, umfassend:
- Einrichten einer registrierenden Komponente (rK) der Mehrzahl von Komponenten (K), wobei das Einrichten ein Hinterlegen einer Liste von Validierungseinträgen umfasst,
- Aufbauen eines manipulationssicheren Kanals zwischen der registrierenden Komponente (rK) und einer ersten Komponente (K1) der anderen Komponenten (aK), und
- Authentisieren der ersten Komponente (K1) bei der registrierenden Komponente (rK) und Authentifizieren der ersten Komponente (K1) mittels der Liste von Validierungseinträgen über den manipulationssicheren Kanal, wobei das Authentifizieren ein Signieren der unsignierten Zertifikatsinformationen (CU) der ersten Komponente (K1) durch die registrierende Komponente (rK) über den manipulationssicheren Kanal umfasst.

2. Verfahren nach Anspruch 1, wobei das Signieren eine Übertragung des öffentlichen Schlüssels (PuK) der registrierenden Komponente (rK) über den manipulationssicheren Kanal umfasst.

3. Verfahren nach einem der vorangehenden Ansprüche, weiterhin umfassend:
- Aufbauen eines manipulationssicheren Kanals zwischen der registrierenden Komponente (RK) und einer zweiten Komponente (K2) der anderen Komponenten (aK), und
- Authentisieren der zweiten Komponente (K2) bei der registrierenden Komponente (rK) und Authentifizieren der zweiten Komponente (K2) mittels der Liste von Einträgen über den manipulationssicheren Kanal, wobei das Authentifizieren ein Signieren der unsignierten Zertifikatsinformationen (CU) der zweiten Komponenten (K2) durch die registrierende Komponente (rK) über den manipulationssicheren Kanal umfasst.

4. Verfahren nach Anspruch 3, weiterhin umfassend ein Aufbauen eines gesicherten Kommunikationskanals zwischen der ersten Komponente (K1) und der zweiten Komponente (K2) durch Austauschen der signierten Zertifikatsinformationen der ersten und der zweiten Komponente und Übertragung eines mittels einem der signierten Zertifikatsinformationen verschlüsselten Sitzungsschlüssels für den gesicherten Kommunikationskanal.

5. Verfahren nach Anspruch 4, wobei der gesicherte Kommunikationskanal eine symmetrische Verschlüsselung über den übertragenen Sitzungsschlüssel aufweist.

6. Verfahren nach Anspruch 4 oder 5, wobei der gesicherte Kommunikationskanal ein TLS-Protokoll verwendet.

7. Verfahren nach einem der Ansprüche 4 bis 6, wobei das Aufbauen des gesicherten Kommunikationskanals ein Abfragen bei der registrierenden Komponente (rK) nach deren öffentlichen Schlüssel (PuK) und ein Überprüfen der signierten Zertifikatsinformationen mittels des abgefragten öffentlichen Schlüssels (PuK) umfasst.

8. Verfahren nach einem der vorangehenden Ansprüche, wobei das Signieren der unsignierten Zertifikatsinformationen (CU) ein Signieren mit einer zeitlich begrenzten Gültigkeit umfasst.

9. System mit einer Mehrzahl von Komponenten (K), eingerichtet zur Ausführung des Verfahrens nach einem der vorangehenden Ansprüche.

10. System nach Anspruch 9, wobei eine Komponente der Mehrzahl von Komponenten eine Schnittstelle zum Login eines Systemnutzers aufweist, wobei die Schnittstelle zum Einrichten der einen Komponente als registrierende Komponente und zum Hinterlegen der Liste von Validierungseinträgen eingerichtet ist.

11. System nach Anspruch 9 oder 10, wobei eine der Komponenten einen Generator, einen Verbraucher, einen Wandler oder einen Speicher für elektrische Energie aufweist.

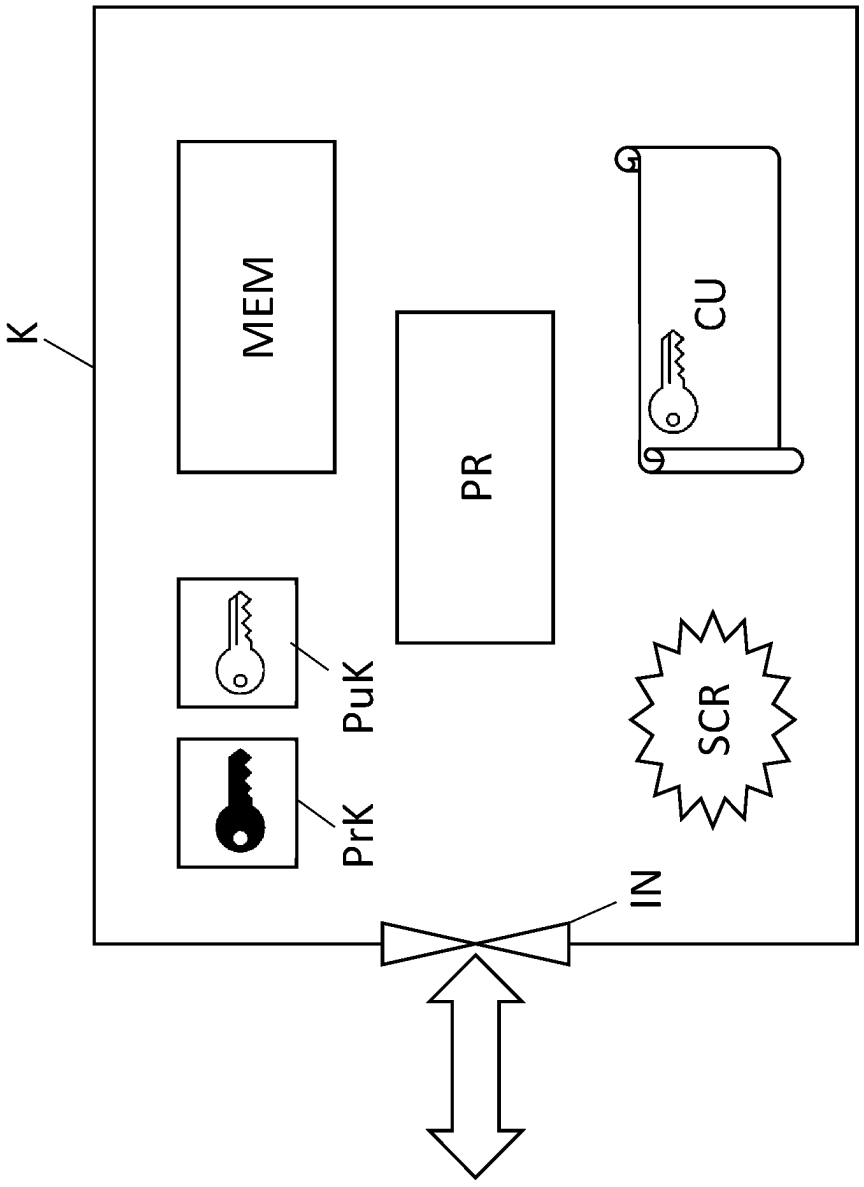
12. System nach einem der Ansprüche 9 bis 11, wobei das System keine Datenverbindung mit einer Instanz außerhalb des Systems aufweist.

13. System nach einem der Ansprüche 9 bis 11, wobei genau eine der Komponenten (K) eine Datenverbindung mit einer Instanz außerhalb des Systems aufweist.

Es folgen 4 Seiten Zeichnungen

Anhängende Zeichnungen

Fig. 1



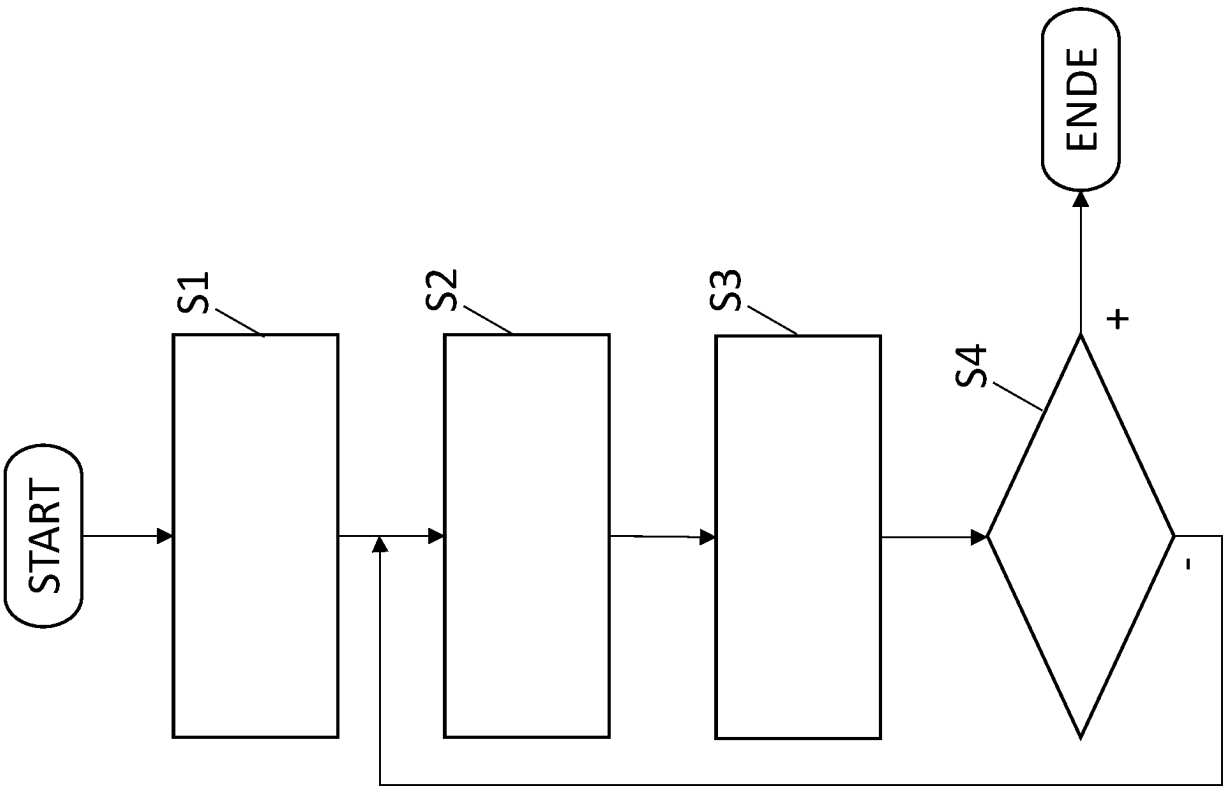


Fig. 2

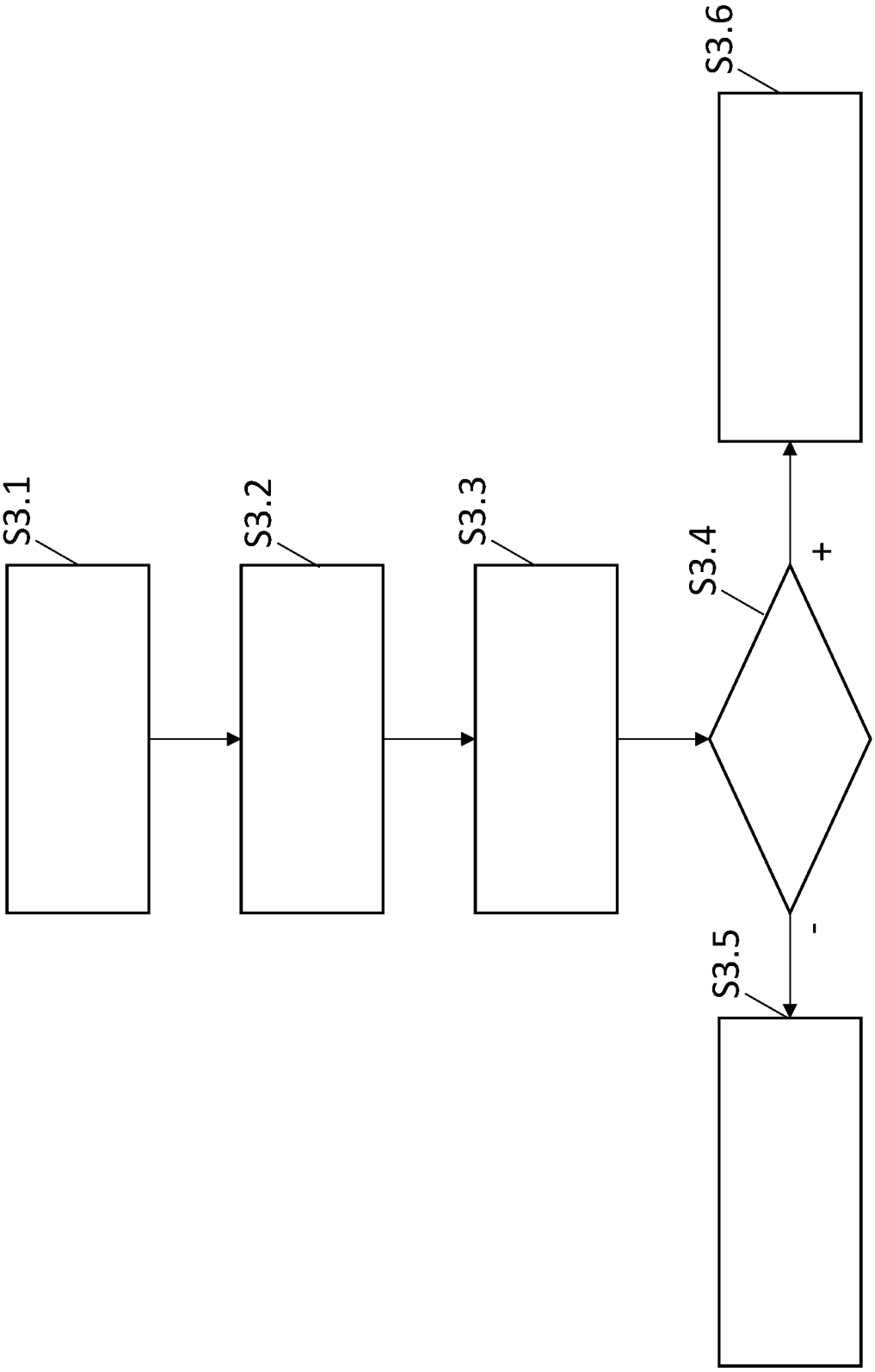


Fig. 3

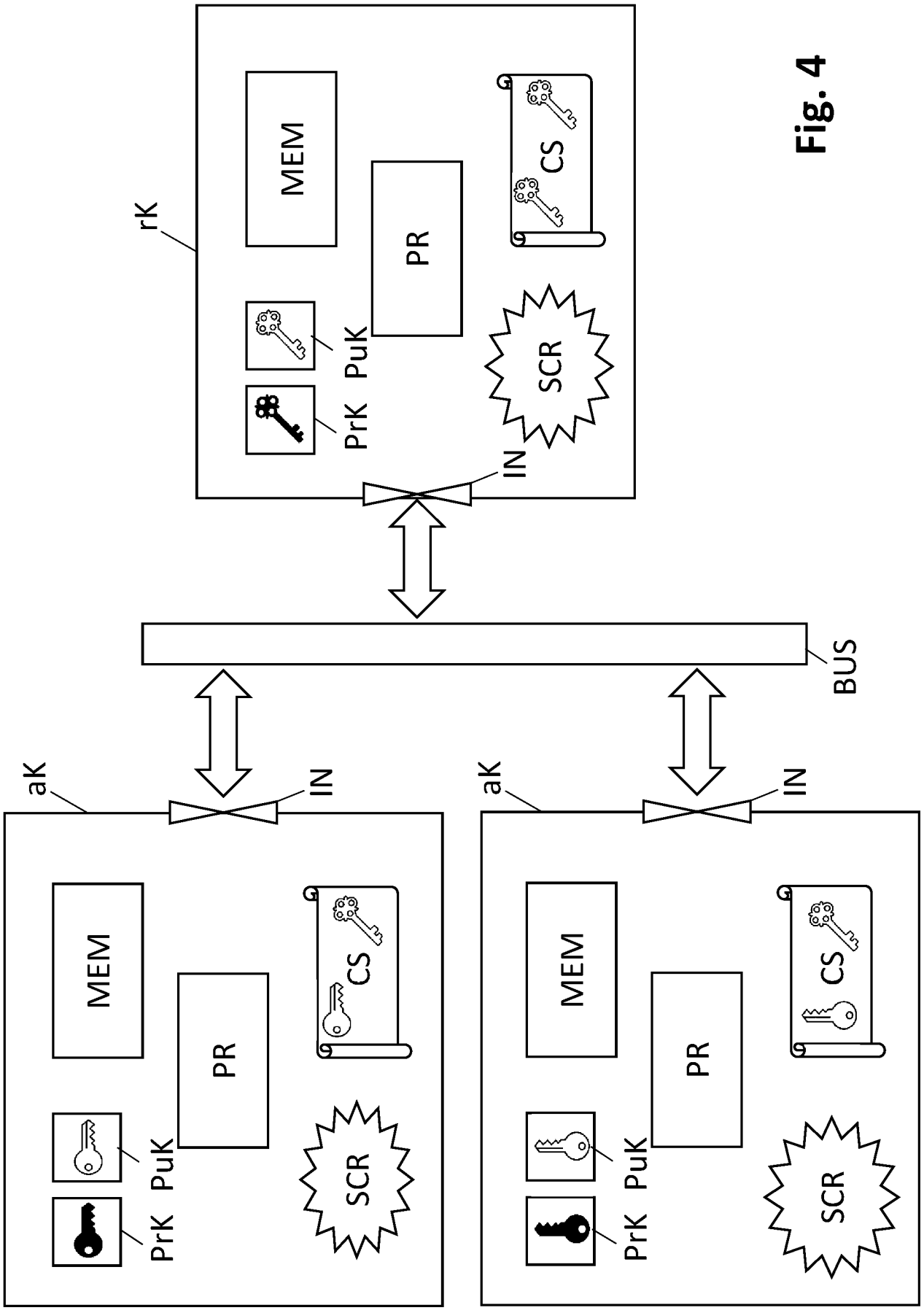


Fig. 4

