(19) Deutsches Patent- und Markenamt

(10) **DE 10 2014 210 434 B4** 2021.08.26

(12) # Patentschrift

(21) Aktenzeichen: **10 2014 210 434.3**
(22) Anmeldetag: **03.06.2014**
(43) Offenlegungstag: **03.12.2015**
(45) Veröffentlichungstag der Patenterteilung: **26.08.2021**

(51) Int Cl.: ***H04L 9/32*** (2006.01)
G06F 21/33 (2013.01)
H04W 12/06 (2021.01)

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:
Rohde & Schwarz SIT GmbH, 12489 Berlin, DE

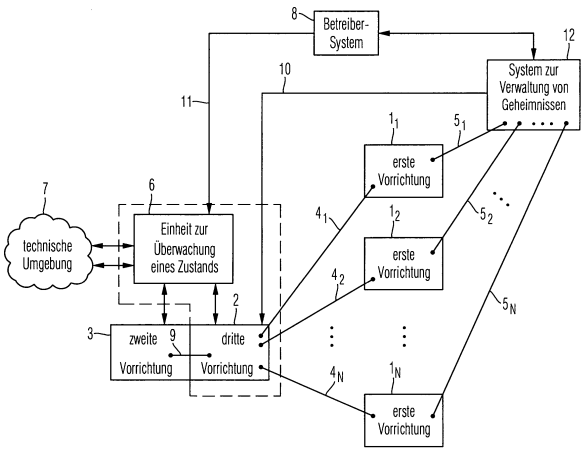
(74) Vertreter:
Mitscherlich, Patent- und Rechtsanwälte PartmbB, 80331 München, DE

(72) Erfinder:
Kultermann, Bernd, 13053 Berlin, DE; Grawunder, Torsten, 12589 Berlin, DE

(56) Ermittelter Stand der Technik:
WO 2014/ 080 780 A1

(54) Bezeichnung: **Verfahren und System zur Herstellung einer gesicherten Kommunikationsverbindung zwischen einer ersten und zweiten Vorrichtung**

(57) Hauptanspruch: Verfahren zur automatischen Herstellung von jeweils einer gesicherten Kommunikationsverbindung zwischen mindestens einer ersten Vorrichtung (1_1, 1_2, ..., 1_N) und einer zweiten Vorrichtung (3) mittels einer mit der zweiten Vorrichtung (3) untrennbar verbundenen dritten Vorrichtung (2) mit folgenden Verfahrensschritten:
• Aufbauen von jeweils einer gesicherten ersten Kommunikationsverbindung (4_1, 4_2,..., 4_N) zwischen der mindestens einen ersten Vorrichtung (1_1,1_2,...,1_N) und der dritten Vorrichtung (2),
• Vergabe eines ersten Identifikationsmerkmals an die mindestens eine erste Vorrichtung (1_1, 1_2,..., 1_N) über die jeweilige gesicherte erste Kommunikationsverbindung (4_1,4_2,..., 4_N) durch die dritte Vorrichtung (2) und
• Aufbauen einer gesicherten zweiten Kommunikationsverbindung (9) zwischen der dritten Vorrichtung und der zweiten Vorrichtung bei Identität zwischen dem von der jeweiligen ersten Vorrichtung (1_1, 1_2,...,1_N) über die jeweilige gesicherte erste Kommunikationsverbindung (4_1, 4_2,..., 4_N) übertragenen jeweiligen ersten Identifikationsmerkmal und einem zugehörigen, in der dritten Vorrichtung (2) gespeicherten ersten Referenz-Identifikationsmerkmal und bei Eintreten eines von der dritten Vorrichtung (2) überprüfbaren Zustandes; wobei die erste Vorrichtung (1_1), der von der dritten Vorrichtung (2) das erste Identifikationsmerkmal zuerst vergeben wird, das erste Identifikationsmerkmal über eine gesicherte dritte Kommunikationsverbindung (5_1) einem System ...



Beschreibung

[0001] Die Erfindung betrifft ein Verfahren und ein System zur Herstellung einer gesicherten Kommunikationsverbindung zwischen einer ersten und zweiten Vorrichtung.

[0002] Die Interaktion zwischen einem Anwender und einem Gerät bzw. einem System in einem sicherheitsrelevanten Bereich erfolgt typischerweise mittels einer Chipkarte, die dem Anwender vom Betreiber des Gerätes bzw. des Systems ausgestellt wird und über die sich der Anwender authentisieren kann. Eine erfolgreiche Authentisierung des Anwenders durch das Gerät bzw. das System ermöglicht es dem Anwender, mit dem Gerät bzw. dem System in eine gesicherte Kommunikationsverbindung zu treten.

[0003] Alternativ kann anstelle der Chipkarte auch ein Datenendgerät eingesetzt werden, für das dem Anwender vom Betreiber eine Zugangsberechtigung ausgestellt wurde und über das ebenfalls eine gesicherte Kommunikationsverbindung mit dem Gerät bzw. mit dem System aufgebaut werden kann.

[0004] Der Aufbau der gesicherten Kommunikationsverbindung und die weiteren Schritte der Authentisierung des Anwenders der Chipkarte bzw. des Datenendgeräts beim Gerät bzw. System des Betreibers erfolgt typischerweise über Identifikationsmerkmale und weitere Geheimnisse, die dem Anwender vom Betreiber vergeben werden und die auf der Chipkarte bzw. auf dem Datenendgerät abgespeichert sind. Diese Identifikationsmerkmale werden im Rahmen einer Authentifizierung des Anwenders mittels Referenz-Identifikationsmerkmalen beim Gerät bzw. System des Betreibers verifiziert.

[0005] Das Anwendungsspektrum derartiger sicherheitsbasierter Systeme ist vielfältig:

> Nachdem ein Anwender sich bei einem Verschlüsselungsgerät
>
> - einem so genannten Kryptogerät - mithilfe von Identifikationsmerkmalen auf einer ihm ausgestellten Chipkarte authentisiert hat, kann er beispielsweise eine programmierbare elektronische Schaltung innerhalb des Verschlüsselungsgeräts mit Konfigurationsdaten, die auf der Chipkarte gespeichert sind, kundenspezifisch, d.h. personalisiert, konfigurieren.

[0006] In einem anderen Beispiel kann sich ein Anwender über sein zugeordnetes Datenendgerät in einer Datenverarbeitungseinheit mit integrierter Datenbank, in der sensible Unternehmensdaten geschützt abgespeichert sind, authentisieren und die in der Unternehmensdatenbank enthaltenen sensiblen Unternehmensdaten abfragen.

[0007] Der Authentifizierung des Anwenders über seine Chipkarte bzw. über sein Datenendgerät beim Gerät bzw. System des Betreibers geht eine Initialisierung der Chipkarte bzw. des Datenendgeräts beim Gerät bzw. System des Betreibers voraus, in der zwischen der Chipkarte bzw. dem Datenendgerät und dem Gerät bzw. System des Betreibers gemeinsame Geheimnisse - beispielsweise gemeinsame Schlüssel, ein gemeinsames Verschlüsselungsverfahren und gemeinsame Identifikationsmerkmale - zum Aufbau einer gesicherten Kommunikationsverbindung und zur Identifizierung des Anwenders der Chipkarte bzw. des Datenendgeräts ausgetauscht werden. Der gemeinsame Schlüssel, das gemeinsame Verschlüsselungsverfahren und die Identifikationsmerkmale werden vom Betreiber vorgegeben und werden zwischen dem Gerät bzw. System des Betreibers und der Chipkarte bzw. dem Datenendgerät des zukünftigen Anwenders in einer Initialisierung typischerweise am Ende der Herstellungsphase des Geräts bzw. Systems des Betreibers und der Chipkarte bzw. des Datenendgeräts transferiert.

[0008] Diese Initialisierung der Chipkarte bzw. des Datenendgeräts wird auch als Personalisierung der Chipkarte bzw. des Datenendgeräts bezeichnet und ist in der US 2013/0166902 A1 beschrieben.

[0009] Durch die Initialisierung kommt es zu einer festen Bindung auf Dauer zwischen der Chipkarte bzw. dem Endgerät des Anwenders und dem Gerät bzw. System des Betreibers. Diese feste Bindung kann nachteilig weder durch den Anwender der Chipkarte bzw. des Endgeräts, der die Chipkarte bzw. das Endgerät nicht manipulieren kann, noch vom Betreiber des Geräts bzw. des Systems, der ebenfalls keine Eingriffsmöglichkeit in den sicherheitsrelevanten Bereich des Gerätes bzw. Systems besitzt, aufgelöst werden.

[0010] Die WO 2014/080780 A1 beschreibt ein Verfahren zur Authentifizierung einer Zugriffsanfrage von mindestens einem Terminal auf mindestens eine Ressource. Ein Authentifizierungsserver ist hierbei zuständig für die Authentifizierung von Geräten, die Zugriffe auf die Ressourcen anfordern. Ein Gateway ermöglicht einen Zugriff auf die Ressourcen durch authentifizierte Terminals. Dabei kann mehr als ein Gateway den authentifizierten Terminals einen Zugriff auf die Ressourcen ermöglichen. Zur Zugriffsabfrage werden von den Terminals Anfragen für einen Zugriff auf die Ressourcen an das Gateway übertragen. Das Gateway wiederum fragt beim Authentifizierungsserver an, ob die Terminals berechtigt sind, auf die Ressourcen zuzugreifen. Unter Umständen kann das Gateway für einige oder alle Terminals, die Zugriff auf die Ressourcen anfordern, auch auf eine Anforderung einer Authentifizierung durch den Authentifizierungsserver verzichten. Hierzu ermöglicht das Gateway den Aufbau einer sicheren direk-

ten Verbindung zwischen dem Terminal und dem Authentifizierungsserver. Diese Verbindung ermöglicht es dem Terminal, dem Authentifizierungsserver Informationen zur Identifizierung eines Teilnehmers, der das Terminal benutzt, zur Verfügung zu stellen. Der Authentifizierungsserver identifiziert diesen Empfänger und ruft verwandte Empfängerinformationen, wie z. B. Zugriffsrechte auf die Ressourcen, ab. Danach wird durch den Authentifizierungsserver mindestens eine Prüffunktion für das Terminal ermittelt und mindestens eine Authentifizierungsinformation bestimmt, die mit der ermittelten Prüffunktion verknüpft ist. Der Authentifizierungsserver überträgt nun mindestens eine bestimmte Prüffunktion oder deren Koeffizienten an das Gateway. Die Prüffunktionen sind daher mit der zweiten temporären Kennung verbunden. Der Authentifizierungsserver überträgt auch mindestens eine bestimmte Authentifizierungsinformation an das Terminal in der sicheren Verbindung. Jede Authentifizierungsinformation ist für einen Wert repräsentativ, sodass die Prüffunktionen bei der Eingabe in die jeweiligen Prüffunktionen einen vordefinierten Wert zurückgeben. Das Gateway empfängt nun eine Anforderung auf Zugriffsberechtigung eines Terminals auf die Ressourcen. Dabei wird die Anforderung in Verbindung mit einem Teil der Authentifizierungsinformation empfangen. Das Gateway ruft jetzt eine auf die empfangene Anforderung anwendbare Prüffunktion ab. Abschließend wird die Anforderung zum Erhalten von Zugriff auf die Ressourcen akzeptiert, wenn das Authentifizierungsergebnis gleich dem vordefinierten Wert ist. Andernfalls wird die Anforderung abgelehnt.

[0011] Aufgabe der Erfindung ist es deshalb, ein Verfahren und ein System zu schaffen, mit dem die zwischen Chipkarte bzw. Endgerät eines oder mehrerer Anwender und dem Gerät bzw. System eines Betreibers nach der Initialisierung etablierte gesicherte Kommunikationsverbindung wieder auflösbar und von neuem reaktivierbar wird.

[0012] Die Aufgabe wird durch ein erfindungsgemäßes Verfahren zur Herstellung von jeweils einer gesicherten Kommunikationsverbindung zwischen mindestens einer ersten Vorrichtung und einer zweiten Vorrichtung mit den Merkmalen des Patentanspruchs 1 und durch ein erfindungsgemäßes System zur Herstellung von jeweils einer gesicherten Kommunikationsverbindung zwischen mindestens einer ersten Vorrichtung und einer zweiten Vorrichtung mit den Merkmalen des Patentanspruchs 17 gelöst. Vorteilhafte technische Erweiterungen sind in den jeweils abhängigen Patentansprüchen aufgeführt.

[0013] Erfindungsgemäß wird eine dritte Vorrichtung eingeführt, die bevorzugt mit der zweiten Vorrichtung - dem Gerät bzw. System des Betreibers - untrennbar verbunden ist, beispielsweise in einer festen mechanischen Verbindung steht. Zwischen dieser dritten Vorrichtung und mindestens einer ersten Vorrichtung - z.B. der Chipkarte bzw. dem Datenendgerät eines zukünftigen Anwenders - wird in einer Initialisierung - bevorzugt am Ende des Herstellungsprozesses - eine gesicherte erste Kommunikationsverbindung aufgebaut, indem der ersten Vorrichtung von der dritten Vorrichtung ein gemeinsames Geheimnis, bevorzugt ein verschlüsseltes gemeinsames Geheimnis, übertragen wird. Bei diesem gemeinsamen Geheimnis handelt es sich bevorzugt um einen gemeinsamen Schlüssel und ein gemeinsames Verschlüsselungsverfahren zum Verschlüsseln der über die gesicherte erste Kommunikationsverbindung übertragenen Daten.

[0014] Zusätzlich wird von der dritten Vorrichtung ebenfalls im Initialisierungsprozess über die gesicherte erste Kommunikationsverbindung zumindest einer ersten Vorrichtung jeweils zumindest ein erstes Identifikationsmerkmal - beispielsweise eine Identifikationsnummer - übertragen und in der jeweiligen ersten Vorrichtung abgespeichert. Die dritte Vorrichtung speichert die zu den jeweiligen ersten Identifikationsmerkmalen jeweils identischen Referenz-Identifikationsmerkmale ab.

[0015] Beabsichtigt der Anwender mit der ihm zugewiesenen ersten Vorrichtung einen gesicherten Zugriff auf die zweite Vorrichtung durchzuführen, so wird zwischen der ersten Vorrichtung und der dritten Vorrichtung eine gesicherte erste Kommunikationsverbindung aufgebaut und es werden über diese gesicherte erste Kommunikationsverbindung die ersten Identifikationsmerkmale von der ersten Vorrichtung zur dritten Vorrichtung übertragen und dort mit der für die jeweilige erste Vorrichtung abgespeicherten Referenz-Identifikationsmerkmalen auf Identität verglichen.

[0016] Stellt die dritte Vorrichtung eine Identität zwischen den von der ersten Vorrichtung übertragenen ersten Identifikationsmerkmalen und der in der dritten Vorrichtung abgespeicherten Referenz-Identifikationsmerkmalen fest, so wird zwischen der dritten Vorrichtung und der zweiten Vorrichtung eine gesicherte zweite Kommunikationsverbindung aufgebaut und damit eine gesicherte Kommunikation zwischen der jeweiligen ersten Vorrichtung und der zweiten Vorrichtung realisiert, falls erfindungsgemäß die dritte Vorrichtung zusätzlich das Eintreten eines überprüfbaren Zustands identifiziert hat.

[0017] Zum Aufbau der gesicherten zweiten Kommunikationsverbindung wird bevorzugt ein gemeinsames Geheimnis zwischen der dritten Vorrichtung und der zweiten Vorrichtung ausgetauscht. Auf diese Weise ist jeder Anwender, dem vom Betreiber jeweils eine erste Vorrichtung zugewiesen wurde, jeweils in der Lage, eine gesicherte Kommunikation und damit

einen gesicherten Zugriff auf die zweite Vorrichtung des Betreibers zu realisieren.

[0018] Durch die erfindungsgemäße zusätzliche Prüfung des Eintretens eines überprüfbaren Zustands durch die dritte Vorrichtung ist es möglich, durch „einen Dritten“ - d.h. durch eine technische Einrichtung oder durch eine autorisierte Person, die jeweils den überprüfbaren Zustand beeinflussen können - eine gesicherte Kommunikation zwischen einer ersten Vorrichtung und der zweiten Vorrichtung in Abhängigkeit des Vorliegens des Zustandes zu aktivieren, zu deaktivieren und/oder zu reaktivieren.

[0019] Der von der dritten Vorrichtung überprüfbare Zustand kann bevorzugt ein fehlerfreier Betrieb der zweiten Vorrichtung sein. Alternativ können aber auch Zustände von technischen Einrichtungen außerhalb der zweiten bzw. dritten Vorrichtung, die mit der zweiten Vorrichtung in einer technischen Beziehung stehen, von der dritten Vorrichtung überprüft werden. Schließlich kann der von der dritten Vorrichtung überprüfbare Zustand auch vom Betreiber der zweiten Vorrichtung als hierzu autorisierte Person beeinflussbar sein. Dies kann beispielsweise mittels eines so genannten „remote-zeroizing“ (deutsch: Nullzusetzen eines Zustands mittels Mobilfunksignal) erfolgen.

[0020] Neben dem Abbrechen, d.h. Sperren, der gesicherten zweiten Kommunikationsverbindung zwischen dritter und zweiter Vorrichtung werden durch die dritte Vorrichtung bei Eintreten des von der dritten Vorrichtung überprüfbaren Zustandes vorzugsweise sämtliche zu den ersten Vorrichtungen jeweils gehörigen ersten Referenz-Identifikationsmerkmale gelöscht. Auf diese Weise ist der durch die dritte Vorrichtung jeweils durchgeführte Vergleich zwischen von einer ersten Vorrichtung jeweils übertragenen ersten Identifikationsmerkmalen und den zur jeweiligen ersten Vorrichtung gehörigen Referenz-Identifikationsmerkmalen nicht mehr möglich. Dieser fehlende Vergleich kann durch die dritte Vorrichtung auch nicht mehr rückgängig gemacht werden und kann durch die dritte Vorrichtung auch nicht verhindert werden. Die gesicherte zweite Kommunikationsverbindung zwischen dritter und zweiter Vorrichtung bleibt somit gesperrt, so dass eine gesicherte Kommunikation zwischen der jeweiligen ersten Vorrichtung und der zweiten Vorrichtung bis auf weiteres nicht möglich ist.

[0021] Eine Reaktivierung der Kommunikation zwischen einer ersten Vorrichtung und der zweiten Vorrichtung ist bevorzugt erst wieder möglich, wenn der von der dritten Vorrichtung überprüfbare Zustand wieder eintritt. In diesem Fall vergibt die dritte Vorrichtung bevorzugt ein weiteres erstes Identifikationsmerkmal, das sich von dem ersten Identifikationsmerkmal unterscheidet, an mindestens eine erste Vorrichtung über die jeweilige gesicherte erste Kommunikation. Mit dem von der dritten Vorrichtung vergebenen weiteren ersten Identifikationsmerkmal überschreibt die jeweilige erste Vorrichtung das bisher gespeicherte erste Identifikationsmerkmal. Die dritte Vorrichtung speichert das zum weiteren ersten Identifikationsmerkmal gehörige Referenz-Identifikationsmerkmal ebenfalls ab.

[0022] In einer ersten bevorzugten erfindungsgemäßen Ausführungsform ist das erste Identifikationsmerkmal für jede erste Vorrichtung jeweils identisch. Ebenfalls ist in der ersten bevorzugten erfindungsgemäßen Ausführungsform ein weiteres erstes Identifikationsmerkmal für jede erste Vorrichtung jeweils identisch. Der Implementierungsaufwand ist hierbei minimiert, da nur ein erstes Referenz-Identifikationsmerkmal in der dritten Vorrichtung gespeichert werden muss und die Authentifizierung jeder ersten Vorrichtung durch die dritte Vorrichtung sich stark vereinfacht.

[0023] In einer ersten Variante der ersten bevorzugten erfindungsgemäßen Ausführungsform vergibt die dritte Vorrichtung während der Initialisierung am Herstellungsende der zweiten bzw. dritten Vorrichtung und einer ersten Vorrichtung über eine gesicherte erste Kommunikationsverbindung nur einer einzigen ersten Vorrichtung ein erstes Identifikationsmerkmal. Ein System zur Verwaltung von Geheimnissen baut mit dieser ersten Vorrichtung eine gesicherte dritte Kommunikationsverbindung auf und erhält über die gesicherte dritte Kommunikationsverbindung von dieser ersten Vorrichtung das zugehörige erste Identifikationsmerkmal und überträgt dieses erste Identifikationsmerkmal zu einem späteren Zeitpunkt - zum Zeitpunkt der Zuweisung der weiteren ersten Vorrichtungen an jeweils einen Anwender - ebenfalls in einer Initialisierung über jeweils eine gesicherte dritte Kommunikationsverbindung an jede weitere erste Vorrichtung.

[0024] In einer zweiten Variante der ersten bevorzugten erfindungsgemäßen Ausführungsform wird dieses erste Identifikationsmerkmal während der Initialisierung am Herstellungsende der zweiten bzw. dritten Vorrichtung und aller ersten Vorrichtungen von der dritten Vorrichtung über jeweils eine gesicherte erste Kommunikationsverbindung an jede erste Vorrichtung zur Speicherung übertragen.

[0025] In einer zweiten erfindungsgemäßen Ausführungsform wird von der dritten Vorrichtung jeder ersten Vorrichtung jeweils ein unterschiedliches erstes Identifikationsmerkmal und zu einem späteren Zeitpunkt jeweils ein unterschiedliches weiteres erstes Identifikationsmerkmal vergeben. Auf diese Weise ist es möglich, jeder ersten Vorrichtung nicht nur eine gesicherte Kommunikation und damit einen gesicherten Zugriff auf die zweite Vorrichtung zu er-

möglichen, sondern auch über die jeweils zugeordneten unterschiedlichen ersten Identifikationsmerkmale jeweils unterschiedliche Zugriffsrechte auf die einzelnen Hardware- und Software-Komponenten der zweiten Vorrichtung zuzuweisen.

[0026] Die Zuweisung von unterschiedlichen Zugriffsrechten in der zweiten Vorrichtung an die einzelnen ersten Vorrichtungen entsprechend der zweiten erfindungsgemäßen Ausführungsform kann in der ersten erfindungsgemäßen Ausführungsform bevorzugt dadurch gelöst werden, dass jeder ersten Vorrichtung jeweils zusätzlich zum ersten Identifikationsmerkmal ein unterschiedliches zweites Identifikationsmerkmal von der dritten Vorrichtung vergeben wird.

[0027] Jedes Identifikationsmerkmal - erstes Identifikationsmerkmal, jedes weitere erste Identifikationsmerkmal und das zweite Identifikationsmerkmal - wird bevorzugt in der dritten Vorrichtung als Zufallszahl nach den üblichen Methoden der Generierung einer Zufallszahl gewonnen.

[0028] Als zweites Identifikationsmerkmal kann alternativ zur Zufallszahl auch eine nach klassischen Methoden gewonnenes Identifikationsmerkmal zur Authentifizierung eines Anwenders - beispielsweise ein Benutzername, eine PIN-Nummer, ein Pass-Wort oder ein Zertifikat - verwendet werden, das außerhalb der dritten Vorrichtung, beispielsweise im System zur Verwaltung von Geheimnissen oder in einer akkreditierten Zertifizierungsstelle, gewonnen wird und zur dritten Vorrichtung über eine gesicherte Kommunikationsverbindung transferiert wird.

[0029] Die einzelnen Identifikationsmerkmale werden auf der jeweiligen ersten Vorrichtung entweder gesichert, d.h. verschlüsselt, oder ungesichert, d.h. unverschlüsselt, abgespeichert. Äquivalent werden die zugehörigen Referenz-Identifikationsmerkmale auf der dritten Vorrichtung entweder gesichert oder ungesichert gespeichert.

[0030] In den einzelnen gesicherten Kommunikationsverbindungen werden die Daten verschlüsselt übertragen. Hierzu werden zwischen den Kommunikationspartnern der jeweiligen gesicherten Kommunikationsverbindung gemeinsame Geheimnisse (englisch: secrets) ausgetauscht. Bei den gemeinsamen Geheimnissen handelt es sich um die bei der Verschlüsselung der Daten verwendeten Schlüssel und Verschlüsselungsverfahren. Hierbei kann eine symmetrische oder asymmetrische Verschlüsselung zur Anwendung kommen.

[0031] In einer weiteren ersten Ausprägung der Erfindung werden für die erste gesicherte Kommunikationsverbindung zwischen der dritten Vorrichtung und jeder ersten Vorrichtung jeweils identische Geheimnisse verwendet. In einer weiteren zweiten Ausprägung der Erfindung werden dagegen für jede erste gesicherte Kommunikationsverbindung jeweils unterschiedliche Geheimnisse verwendet. Mit der zweiten Ausprägung der Erfindung wird somit die Übertragungssicherheit und damit die Integrität der verschlüsselten Daten in jeder ersten gesicherten Kommunikationsverbindung vor einer Manipulation durch Dritte zusätzlich erhöht.

[0032] Optional wird zur Freischaltung der zweiten gesicherten Kommunikationsverbindung zwischen dritter und zweiter Vorrichtung zusätzlich von der dritten Vorrichtung das Zustandekommen einer korrekten ersten gesicherten Kommunikationsverbindung zwischen der jeweiligen ersten Vorrichtung und der dritten Vorrichtung geprüft.

[0033] Ausführungsformen der Erfindung werden im Folgenden im Detail anhand der Zeichnung erläutert. Die Figuren der Zeichnung zeigen:

Fig. 1 ein Blockdiagramm eines Ausführungsbeispiels des erfindungsgemäßen Systems zur Herstellung von jeweils einer gesicherten Kommunikationsverbindung zwischen einer ersten Vorrichtung und einer zweiten Vorrichtung und

Fig. 2 ein Flussdiagramm eines Ausführungsbeispiels des erfindungsgemäßen Verfahrens zur Herstellung von jeweils einer gesicherten Kommunikationsverbindung zwischen einer ersten Vorrichtung und einer zweiten Vorrichtung.

[0034] Ein Ausführungsbeispiel des erfindungsgemäßen Verfahrens zur Herstellung von jeweils einer gesicherten Kommunikationsverbindung zwischen mindestens einer ersten Vorrichtung und einer zweiten Vorrichtung gemäß dem Flussdiagramm in **Fig. 2** wird im Folgenden in Kombination mit einem Ausführungsbeispiel des erfindungsgemäßen Systems zur Herstellung von jeweils einer gesicherten Kommunikationsverbindung zwischen mindestens einer ersten Vorrichtung und einer zweiten Vorrichtung gemäß dem Blockdiagramm in **Fig. 1** im Detail erläutert.

[0035] Im ersten Verfahrensschritt **S10** wird zwischen einer ersten Vorrichtung $\mathbf{1}_1$ oder mehreren ersten Vorrichtungen $\mathbf{1}_1$, $\mathbf{1}_2$,..., $\mathbf{1}_N$ und einer dritten Vorrichtung **2** jeweils eine gesicherte erste Kommunikationsverbindung $\mathbf{4}_1$, $\mathbf{4}_2$,..., $\mathbf{4}_N$ aufgebaut.

[0036] Die dritte Vorrichtung **2** ist untrennbar beispielsweise mittels einer fixen mechanischen Verbindung mit einer zweiten Vorrichtung **3** verbunden. Bei der zweiten Vorrichtung **3** handelt es sich um ein individuelles Gerät bzw. ein individuelles System eines Betreibers. Dies kann beispielsweise ein Verschlüsselungsgerät - ein so genanntes Kryptogerät - mit sehr hohen Sicherheitsvorkehrungen gegen Manipulationen durch Dritte oder ein Überwachungssystem

für eine Anlage mit hohen Sicherheitsauflagen oder ein Datenverarbeitungssystem mit integrierter Datenbank, die hochsensible Daten speichert, sein. Im Wesentlichen handelt es sich bei der zweiten Vorrichtung **3** um ein beliebiges zu einem Betreiber gehöriges Gerät bzw. System mit hohen Sicherheitsanforderungen.

[0037] Die ersten Vorrichtungen $\mathbf{1_1}$ bis $\mathbf{1_N}$ stellen jeweils eine Vorrichtung dar, die vom Betreiber der zweiten Vorrichtung **3** jeweils einem Anwender zugewiesen werden, damit dieser Anwender mittels der jeweiligen ersten Vorrichtung $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$ einen autorisierten Zugriff auf die zweite Vorrichtung **3** ausführen kann. Typischerweise handelt es sich bei einer ersten Vorrichtung $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$ um eine Chipkarte (englisch: smartcard) oder um ein Datenendgerät, die jeweils dem jeweiligen Anwender zugewiesen werden und die jeweils über eine Schnittstelle eine Kommunikationsverbindung mit der zweiten Vorrichtung **3** aufbauen können. Alternativ können als erste Vorrichtung $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$ beispielsweise auch eine RFID-Karte oder ein USB-Stick mit Tresor zur gesicherten Speicherung von Geheimnissen verwendet werden und sind von der Erfindung ebenfalls mit abgedeckt.

[0038] Bei der Schnittstelle, über die die Chipkarte mit der zweiten Vorrichtung **3** kommuniziert, handelt es sich typischerweise um einen in der dritten Vorrichtung **2** vorgesehenen Steckplatz mit hohen Sicherheitsvorkehrungen, in die die Chipkarte vom Anwender eingeführt werden kann. Die Schnittstelle, über die das Datenendgerät mit der zweiten Vorrichtung **3** kommuniziert, ist z.B. ein Hochsicherheits-Datennetz auf Festnetz- oder Mobilfunknetz-Basis zwischen dem Datenendgerät und der dritten Vorrichtung **2**. Die Kommunikation zwischen der dritten Vorrichtung **2** und der zweiten Vorrichtung **3** erfolgt über eine weitere noch zu beschreibende gesicherte Kommunikationsverbindung.

[0039] Der Aufbau einer gesicherten ersten Kommunikationsverbindung $\mathbf{4_1}$, $\mathbf{4_2}$,..., $\mathbf{4_N}$ zwischen einer der ersten Vorrichtungen $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ und der dritten Vorrichtung **2** erfolgt in einer Initialisierungsphase, die typischerweise am Herstellungsende der jeweiligen ersten Vorrichtung $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ und der mit der zweiten Vorrichtung **3** untrennbar verbundenen dritten Vorrichtung **2** erfolgt. Hierzu wird vom Hersteller in Kooperation mit dem Betreiber ein gemeinsames Geheimnis zwischen der jeweiligen ersten Vorrichtung $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$ und der dritten Vorrichtung **2** erzeugt. Beim gemeinsamen Geheimnis handelt es sich typischerweise um den verwendeten Schlüssel und das verwendete Verschlüsselungsverfahren, mit denen die Verschlüsselung der Daten verschlüsselt werden, die zwischen der jeweiligen ersten Vorrichtung **11**, **12**,..., **1N** und der dritten Vorrichtung **2** über die jeweilige gesicherte erste Kommunikationsverbindung $\mathbf{4_1}$, $\mathbf{4_2}$,..., $\mathbf{4_N}$ ausgetauscht werden.

[0040] Der verwendete Schlüssel und das verwendete Verschlüsselungsverfahren werden vom Hersteller über ein Datenterminal und eine Datenverbindung in die dritte Vorrichtung **2** transferiert und dort gespeichert. Die Speicherung von Schlüssel und Verschlüsselungsverfahren in der dritten Vorrichtung **2** kann entweder ungesichert, d.h. unverschlüsselt, oder gesichert, d.h. mit einem weiteren Schlüssel und einem weiteren Verschlüsselungsverfahren verschlüsselt, erfolgen.

[0041] Die in der dritten Vorrichtung **2** gespeicherten gemeinsamen Geheimnisse - d.h. verwendeter Schlüssel und verwendetes Verschlüsselungsverfahren - werden von der dritten Vorrichtung **2** über die jeweilige erste Kommunikationsverbindung $\mathbf{4_1}$, $\mathbf{4_2}$,..., $\mathbf{4_N}$ zur jeweiligen ersten Vorrichtung $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$ in einer erstmalig zwischen diesen beiden Kommunikationspartnern stattfindenden Kommunikation (so genanntes „Pairen“; deutsch: „sich paaren“) übertragen und dort ebenfalls ungesichert oder gesichert abgespeichert.

[0042] Nach der Speicherung der gemeinsamen Geheimnisse in der jeweiligen ersten Vorrichtung $\mathbf{1_1}$, $\mathbf{1_2}$,...1_N ist eine verschlüsselte Übertragung von Daten zwischen der jeweiligen ersten Vorrichtung $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$ und der dritten Vorrichtung **2** möglich und damit eine jeweilige gesicherte erste Kommunikationsverbindung $\mathbf{4_1}$, $\mathbf{4_2}$,..., $\mathbf{4_N}$ zwischen der jeweiligen ersten Vorrichtung $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$ und der dritten Vorrichtung **2** etabliert.

[0043] In einer ersten erfindungsgemäßen Ausprägung sind die gemeinsamen Geheimnisse - d.h. verwendeter Schlüssel und verwendetes Verschlüsselungsverfahren - für jede gesicherte erste Kommunikationsverbindung $\mathbf{4_1}$, $\mathbf{4_2}$,..., $\mathbf{4_N}$ jeweils identisch. Dies ist die bevorzugte Realisierung einer gesicherten Kommunikationsverbindung, da Betreiber und Hersteller nur einen einzigen gemeinsamen Schlüssel und ein einziges gemeinsames Verschlüsselungsverfahren generieren, anwenden und speichern müssen.

[0044] In einer zweiten erfindungsgemäßen Ausprägung sind die gemeinsamen Geheimnisse für jede gesicherte erste Kommunikationsverbindung $\mathbf{4_1}$, $\mathbf{4_2}$,..., $\mathbf{4_N}$ jeweils unterschiedlich. Der Aufwand für Betreiber und Hersteller zur Erzeugung, Anwendung und Speicherung aller verwendeten Schlüssel und aller verwendeten Verschlüsselungsverfahren ist entsprechend höher. Auch ist der Implementierungsaufwand in der dritten Vorrichtung **2** für das Ver- und Entschlüsseln der Daten über die einzelnen ersten Kommunikationsverbindungen $\mathbf{4_1}$,$\mathbf{4_2}$,...,$\mathbf{4_N}$ entsprechend höher, da in der dritten Vorrichtung **2** ein entsprechend höherer Speicherbedarf für die Speicherung aller Schlüssel und Verschlüsselungsverfahren erforderlich ist und die dritte Vorrichtung **2** beim Ver- und

Entschlüsseln der Daten erst den korrekten Schlüssel und das korrekte Verschlüsselungsverfahren ermitteln muss.

[0045] Hinsichtlich der verwendeten Schlüssel und der verwendeten Verschlüsselungsverfahren sind prinzipiell alle gängigen symmetrischen und asymmetrischen Verschlüsselungen für die Realisierung einer ersten gesicherten Kommunikationsverbindung $\mathbf{4_1}$, $\mathbf{4_2}$,..., $\mathbf{4_N}$ geeignet.

[0046] In einer ersten bevorzugten Variante der Erfindung wird der Aufbau einer gesicherten ersten Kommunikationsverbindung zwischen einer ersten Vorrichtung und der dritten Vorrichtung **2** lediglich für eine einzige erste Vorrichtung $\mathbf{1_1}$ in einer Initialisierung am Herstellungsende der dritten Vorrichtung **2** und der einzig hergestellten ersten Vorrichtung $\mathbf{1_1}$ realisiert. Für weitere erste Vorrichtungen $\mathbf{1_2}$,..., $\mathbf{1_N}$, die u.U. erst zu einem späteren Zeitpunkt hergestellt werden und vom Betreiber einem Anwender zugewiesen werden, werden in einer später vom Betreiber und nicht vom Hersteller durchgeführten Initialisierung eine jeweilige gesicherte erste Kommunikationsverbindung $\mathbf{4_2}$,..., $\mathbf{4_N}$ zur dritten Vorrichtung **2** realisiert.

[0047] Hierzu wird für den Fall der ersten erfindungsgemäßen Ausprägung - identische gemeinsame Geheimnisse für alle gesicherten ersten Kommunikationsverbindungen $\mathbf{4_1}$, $\mathbf{4_2}$,..., $\mathbf{4_N}$ - zwischen der bereits beim Hersteller mit gemeinsamen Geheimnissen versehenen ersten Vorrichtung $\mathbf{1_1}$ und einem beim Betreiber befindlichen und mit dem Betreiber-System **8** verbundenen System **12** zur Verwaltung von Geheimnissen eine gesicherte dritte Kommunikationsverbindung $\mathbf{5_1}$ aufgebaut.

[0048] Das System **12** zur Verwaltung von Geheimnissen erhält hierbei von der bereits initialisierten ersten Vorrichtung $\mathbf{1_1}$ typischerweise in verschlüsselter Form - d.h. mit einem weiteren Schlüssel und einem weiteren Verschlüsselungsverfahren verschlüsselt - die in der bereits initialisierten ersten Vorrichtung $\mathbf{1_1}$ abgespeicherten gemeinsamen Geheimnisse und speichert diese ebenfalls gesichert oder ungesichert ab. Mit diesen abgespeicherten gemeinsamen Geheimnissen baut das System **12** zur Verwaltung von Geheimnissen mit allen zukünftig hergestellten und jeweils einem Anwender zuzuweisenden ersten Vorrichtungen $\mathbf{1_2}$,...,$\mathbf{1_N}$ jeweils eine gesicherte dritte Kommunikationsverbindung $\mathbf{5_2}$,..., $\mathbf{5_N}$ auf, indem sie der jeweiligen ersten Vorrichtung $\mathbf{1_2}$,...,$\mathbf{1_N}$ die gemeinsamen Geheimnisse der zuerst initialisierten ersten Vorrichtung $\mathbf{1_1}$ verschlüsselt oder unverschlüsselt überträgt. Die jeweilige erste Vorrichtung $\mathbf{1_2}$,...,$\mathbf{1_N}$ speichert die gemeinsamen Geheimnisse der zuerst initialisierten ersten Vorrichtung $\mathbf{1_1}$ gesichert oder ungesichert intern ab und baut wiederum mit der dritten Vorrichtung **2** auf der Basis der abgespeicherten gemeinsamen Geheimnisse jeweils eine gesicherte erste Kommunikationsverbindung $\mathbf{4_2}$,...,$\mathbf{4_N}$ auf.

[0049] Für den Fall der zweiten erfindungsgemäßen Ausprägung - jeweils unterschiedliche gemeinsame Geheimnisse für jede gesicherte erste Kommunikationsverbindung $\mathbf{4_1}$, $\mathbf{4_2}$,..., $\mathbf{4_N}$ - werden bei Anwendung der ersten bevorzugten Variante der Erfindung die von der bereits initialisierten ersten Vorrichtung $\mathbf{1_1}$ über eine gesicherte dritte Kommunikationsverbindung $\mathbf{5_1}$ transferierten gemeinsamen Geheimnisse im System **12** zur Verwaltung von Geheimnissen bei der Erzeugung von jeweils unterschiedlichen gemeinsamen Geheimnisse für die jeweiligen gesicherten ersten Kommunikationsverbindungen $\mathbf{4_2}$,...,$\mathbf{4_N}$ zwischen den jeweils übrigen ersten Vorrichtungen $\mathbf{1_2}$,...,$\mathbf{1_N}$ und der dritten Vorrichtung **2** berücksichtigt.

[0050] Sobald die übrigen ersten Vorrichtungen $\mathbf{1_2}$,...,$\mathbf{1_N}$ hergestellt sind und einem Anwender jeweils zuzuweisen sind, überträgt das System **12** zur Verwaltung von Geheimnissen die jeweils erzeugten unterschiedlichen gemeinsamen Geheimnisse verschlüsselt über die jeweils zu erzeugende gesicherte dritte Kommunikationsverbindung $\mathbf{5_2}$,..., $\mathbf{5_N}$ an die jeweilige erste Vorrichtung $\mathbf{1_2}$,..., $\mathbf{1_N}$. Die jeweilige erste Vorrichtung $\mathbf{1_2}$,...,$\mathbf{1_N}$ speichert die jeweils zugeführten gemeinsamen Geheimnisse gesichert oder ungesichert intern ab und überträgt sie zum Aufbau der jeweils zugeordneten gesicherten ersten Kommunikationsverbindung $\mathbf{4_2}$,...,$\mathbf{4_N}$ über die jeweilige erste Kommunikationsverbindung $\mathbf{4_2}$,...,$\mathbf{4_N}$ an die dritte Vorrichtung **2**, die sie jeweils intern abspeichert.

[0051] In einer zweiten Variante der Erfindung werden am Herstellungsende der dritten Vorrichtung **2** und aller ersten Vorrichtungen $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ die gemeinsamen Geheimnisse über die jeweilige erste Kommunikationsverbindung $\mathbf{4_1}$, $\mathbf{4_2}$,..., $\mathbf{4_N}$ an die jeweilige erste Vorrichtung $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ verschlüsselt übertragen und dort gesichert oder ungesichert abgespeichert. Hierbei werden im Fall der ersten erfindungsgemäßen Ausprägung jeweils identische gemeinsame Geheimnisse für alle gesicherten ersten Kommunikationsverbindungen $\mathbf{4_1}$, $\mathbf{4_2}$,..., $\mathbf{4_N}$ und im Fall der zweiten erfindungsgemäßen Ausprägung jeweils unterschiedliche gemeinsame Geheimnisse für jede einzelne gesicherte erste Kommunikationsverbindung $\mathbf{4_1}$, $\mathbf{4_2}$,..., $\mathbf{4_N}$ zur jeweiligen ersten Vorrichtung $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$ übertragen.

[0052] In der zweiten Variante der Erfindung ist folglich das System **12** zur Verwaltung von Geheimnissen nicht im Einsatz.

[0053] Im nächsten Verfahrensschritt **S20** werden den einzelnen ersten Vorrichtungen $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ Identifikationsmerkmale zur Authentifizierung der jewei-

ligen ersten Vorrichtung $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ bei der zweiten Vorrichtung **3** vergeben.

[0054] Als Identifikationsmerkmal wird typischerweise eine Zufallszahl verwendet, die üblicherweise in einem Zufallszahlengenerator nach dem Stand der Technik generiert wird.

[0055] In Äquivalenz zur Vergabe von gemeinsamen Geheimnissen zum Aufbau einer gesicherten Kommunikationsverbindung zwischen zwei Kommunikationspartnern werden die Identifikationsmerkmale in einer ersten bevorzugten Variante der Erfindung während der Initialisierungsphase am Herstellungsende der dritten Vorrichtung **2** und der ersten Vorrichtung $\mathbf{1_1}$ lediglich für eine einzige erste Vorrichtung $\mathbf{1_1}$ in einem in der dritten Vorrichtung integrierten Zufallszahlengenerator erzeugt und über die gesicherte erste Kommunikationsverbindung $\mathbf{4_1}$ zur ersten Vorrichtung $\mathbf{1_1}$ verschlüsselt übertragen und dort entweder gesichert oder ungesichert abgespeichert.

[0056] In einer ersten erfindungsgemäßen Ausführungsform wird als Identifikationsmerkmal für jede erste Vorrichtung $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ jeweils ein identisches erstes Identifikationsmerkmal verwendet. Mit diesem ersten Identifikationsmerkmal wird jede erste Vorrichtung $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$ bei der dritten Vorrichtung **2** authentifiziert und somit autorisiert, einen Zugriff auf die zum Betreiber gehörige zweite Vorrichtung **3** durchzuführen.

[0057] Dieses erste Identifikationsmerkmal wird bei der ersten bevorzugten Variante der Erfindung von der ersten Vorrichtung $\mathbf{1_1}$ über die gesicherte dritte Kommunikationsverbindung $\mathbf{5_1}$ verschlüsselt dem System **12** zur Verwaltung von Geheimnissen zugeführt und dort gesichert oder ungesichert abgespeichert. Werden zu einem späteren Zeitpunkt zusätzliche erste Vorrichtungen $\mathbf{1_2}$,...,$\mathbf{1_N}$ hergestellt und vom Betreiber einzelnen Anwendern zur Verfügung gestellt, so überträgt das System **12** zur Verwaltung von Geheimnissen dieses gespeicherte erste Identifikationsmerkmal, das für jede weitere erste Vorrichtung $\mathbf{1_2}$,...,$\mathbf{1_N}$ identisch ist, über die jeweilige gesicherte dritte Kommunikationsverbindung $\mathbf{5_2}$,..., $\mathbf{5_N}$ verschlüsselt an die übrigen ersten Vorrichtungen $\mathbf{1_2}$,..., $\mathbf{1_N}$, wo es entweder gesichert oder ungesichert abgespeichert wird.

[0058] In einer zweiten erfindungsgemäßen Ausführungsform, in der jeder ersten Vorrichtung $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ jeweils ein unterschiedliches erstes Identifikationsmerkmal vergeben wird, ist es möglich, neben einer individuellen Authentifizierung - d.h. einer Personalisierung - der einzelnen ersten Vorrichtungen $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ bei der dritten Vorrichtung **2** und damit indirekt bei der zweiten Vorrichtung **3** auch jeder einzelnen Vorrichtung $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ über das unterschiedliche erste Identifikationsmerkmal individuelle Zugriffsrechte auf die zweite Vorrichtung **3**, wie im einzelnen noch weiter unten im Detail beschrieben wird, vom Betreiber zu gewähren.

[0059] Das der ersten Vorrichtung $\mathbf{1_1}$ von der dritten Vorrichtung **2** vergebene erste Identifikationsmerkmal wird über die gesicherte dritte Kommunikationsverbindung $\mathbf{5_1}$ dem System **12** zur Verwaltung von Geheimnissen von der ersten Vorrichtung $\mathbf{1_1}$ verschlüsselt übertragen und dort in einem integrierten Speicher zur Verwaltung abgelegt. Für die zu einem späteren Zeitpunkt hergestellten weiteren ersten Vorrichtungen $\mathbf{1_2}$,...,$\mathbf{1_N}$ werden vom System **12** zur Verwaltung von Geheimnissen in einem integrierten Zufallszahlengenerator jeweils unterschiedliche erste Identifikationsmerkmale erzeugt und der jeweiligen ersten Vorrichtung $\mathbf{1_2}$,...,$\mathbf{1_N}$ über die jeweilige gesicherte dritte Kommunikationsverbindung $\mathbf{5_2}$,..., $\mathbf{5_N}$ verschlüsselt übertragen, wo sie entweder gesichert oder ungesichert intern abgespeichert werden.

[0060] Werden alle ersten Vorrichtungen $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ zur selben Zeit mit der dritten Vorrichtung **2** bzw. der zweiten Vorrichtung **3** hergestellt, so können in einer zweiten Variante der Erfindung die den einzelnen ersten Vorrichtungen $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ jeweils zugewiesenen ersten Identifikationsmerkmale - sowohl im Fall von für alle erste Vorrichtungen $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$ jeweils identischen ersten Identifikationsmerkmalen gemäß der ersten erfindungsgemäßen Ausführungsform als auch im Fall von verschiedenen ersten Identifikationsmerkmalen für jede erste Vorrichtung $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ gemäß der zweiten erfindungsgemäßen Ausführungsform - von einem in der dritten Vorrichtung **2** integrierten Zufallsgenerator erzeugt werden und den einzelnen ersten Vorrichtungen $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$ über die jeweilige gesicherte erste Kommunikationsverbindung $\mathbf{4_1}$, $\mathbf{4_2}$,..., $\mathbf{4_N}$ verschlüsselt übertragen werden, wo sie entweder gesichert oder ungesichert intern abgespeichert werden.

[0061] Im Falle von identischen ersten Identifikationsmerkmalen für alle ersten Vorrichtungen $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ können jeder ersten Vorrichtung $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ jeweils unterschiedliche zweite Identifikationsmerkmale zusätzlich zum ersten identischen Identifikationsmerkmal zugewiesen werden, mit der die jeweilige erste Vorrichtung $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$ bei der dritten Vorrichtung **2** und damit indirekt bei der zweiten Vorrichtung **3** individuell authentifiziert wird und zugleich individuelle Zugriffsrechte in der zweiten Vorrichtung **3** erhält.

[0062] Die Erzeugung und die Übertragung des zweiten Identifikationsmerkmals an die einzelnen ersten Vorrichtungen $\mathbf{1_1}$, $\mathbf{1_2}$, ..., $\mathbf{1_N}$ erfolgt in Äquivalenz zur Erzeugung und Übertragung des ersten Identifikationsmerkmals entweder unter Zwischenschaltung des Systems **12** zur Verwaltung von Geheimnissen gemäß der ersten bevorzugten Variante

der Erfindung oder einzig mithilfe der dritten Vorrichtung **2** gemäß der zweiten Variante der Erfindung.

[0063] Ebenfalls im Verfahrensschritt **S20** erfolgt parallel zur Erzeugung und zur Übertragung des ersten und optional zweiten Identifikationsmerkmals eine Speicherung eines zum jeweiligen ersten Identifikationsmerkmal und optional zum jeweiligen zweiten Identifikationsmerkmal jeweils identischen ersten Referenz-Identifikationsmerkmal bzw. zweiten Referenz-Identifikationsmerkmal in einem internen, in **Fig. 1** nicht dargestellten Speicher der dritten Vorrichtung **2**.

[0064] Während die ersten beiden Verfahrensschritte **S10** und **S20** für jede erste Vorrichtung $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ jeweils einmalig in einer Initialisierungsphase durchgeführt werden, können die nun folgend beschriebenen Verfahrensschritte **S30** bis **S100** ein- oder mehrmalig auftreten, je nachdem wie oft die einzelnen ersten Vorrichtungen $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$ jeweils einen Zugriff auf die zweite Vorrichtung **3** ausüben.

[0065] Der nächste Verfahrensschritt **S30** erfolgt, sobald ein Anwender, dem vom Betreiber der zweiten Vorrichtung **2** eine erste Vorrichtung $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$ ausgestellt bzw. zur Verfügung gestellt wurde, einen Zugriff auf die zweite Vorrichtung **3** beabsichtigt. Die jeweilige erste Vorrichtung $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$ baut jeweils eine zugeordnete gesicherte ersten Kommunikationsverbindung $\mathbf{4_1}$, $\mathbf{4_2}$,..., $\mathbf{4_N}$ zur dritten Vorrichtung auf. Der Aufbau und die korrekte Funktion der jeweiligen gesicherten ersten Kommunikationsverbindung $\mathbf{4_1}$, $\mathbf{4_2}$,..., $\mathbf{4_N}$ wird von der dritten Vorrichtung **3** geprüft. Sobald die jeweilige gesicherte erste Kommunikationsverbindung $\mathbf{4_1}$,$\mathbf{4_2}$,...,$\mathbf{4_N}$ einen korrekten Betrieb ermöglicht, überträgt die jeweilige erste Vorrichtung $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ über die jeweils zugeordnete gesicherte erste Kommunikationsverbindung $\mathbf{4_1}$,$\mathbf{4_2}$,...,$\mathbf{4_N}$ das ihr zugeordnete und intern abgespeicherte erste und optionale zweite Identifikationsmerkmal an die dritte Vorrichtung **2**.

[0066] Zur Authentifizierung der jeweils anfragenden ersten Vorrichtung $\mathbf{1_1}$, $\mathbf{1_2}$, ..., $\mathbf{1_N}$ bei der zweiten Vorrichtung **3** überprüft die dritte Vorrichtung **2** das empfangene erste und optionale zweite Identifikationsmerkmal mit dem zugehörigen und internen abgespeicherten ersten und optionale zweiten Referenz-Identifikationsmerkmal.

[0067] Schließlich wird im selben Verfahrensschritt **S30** von einer Einheit **6** zur Überwachung eines Zustandes, die entweder in der dritten Vorrichtung **2**, wie in **Fig. 1** gestrichelt dargestellt ist, integriert ist oder mit der dritten Vorrichtung **2** verbunden ist, ein bestimmter, vorab definierter Zustand der zweiten Vorrichtung **3** oder einer in **Fig. 1** als Wolke dargestellte technische Umgebung **7**, mit der die zweite Vorrichtung **3** in einer technischen Interaktion steht, überprüft.

[0068] Bevorzugt handelt es sich bei dem zu überprüfenden Zustand um den korrekten Betrieb der gesamten zweiten Vorrichtung **3**, den korrekten Betrieb einzelner vorab definierter Hardware- und/oder Software-Komponenten der zweiten Vorrichtung **3** oder um den korrekten Betrieb der technischen Umgebung **7**, mit der die zweite Vorrichtung **3** in einer technischen Beziehung steht. Bei der technischen Umgebung **7** kann es sich beispielsweise um eine technische Anlage oder ein technisches Aggregat handeln, dessen korrekte Funktionsweise die zweite Vorrichtung **3** als Überwachungseinrichtung überwacht.

[0069] Schließlich kann der von der Einheit **6** zur Überwachung eines Zustandes zu überwachende Zustand ein vom Betreiber-System **8** aktiviertes und der Einheit **6** zur Überwachung eines Zustandes über eine Datenverbindung **11** zugeführtes Signal sein. Mit diesem aktivierten Signal ist es dem Betreiber möglich, jederzeit die zweite Vorrichtung **3** und jedes andere zum Betreiber gehörige Gerät bzw. System für einen Zugriff durch einen Anwender, dem vom Betreiber jeweils eine erste Vorrichtung $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ zugewiesen wurde, zu sperren (so genanntes „remotezeroizing“; deutsch: „über die Luftschnittstelle zurücksetzen“).

[0070] Ist von der dritten Vorrichtung **2** gleichzeitig eine korrekt funktionierende gesicherte erste Kommunikationsverbindung $\mathbf{4_1}$,$\mathbf{4_2}$,...,$\mathbf{4_N}$ zu derjenigen ersten Vorrichtung $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$, die einen Zugriff auf die zweite Vorrichtung **3** beabsichtigt, eine korrekte Authentifizierung der jeweiligen ersten Vorrichtung $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ anhand von deren ersten und optional zweiten Identifikationsmerkmal und das Eintreten eines von der Vorrichtung **6** zur Überwachung eines Zustandes überprüfbaren Zustandes ermittelt und festgestellt worden, so wird von der dritten Vorrichtung **2** eine gesicherte zweite Kommunikationsverbindung **9** zwischen der dritten Vorrichtung **2** und der zweiten Vorrichtung **3** aufgebaut.

[0071] Hierzu werden gemeinsame Geheimnisse, d.h. ein gemeinsamer Schlüssel und ein gemeinsames Verschlüsselungsverfahren, von der dritten Vorrichtung **2** verschlüsselt über die Kommunikationsverbindung **9** zur zweiten Vorrichtung **3** übertragen und dort intern abgespeichert.

[0072] Nach dem Aufbau der gesicherten zweiten Kommunikationsverbindung **9** besteht eine gesicherte Kommunikationsmöglichkeit zwischen der jeweiligen ersten Vorrichtung $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$, deren Anwender einen Zugriff auf die zweite Vorrichtung **3** beabsichtigt, und der zweiten Vorrichtung **3**.

[0073] Im nächsten Verfahrensschritt **S40** erfolgt eine gesicherte Kommunikation von Daten zwischen der jeweiligen ersten Vorrichtung $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$, deren Anwender einen Zugriff auf die zweite Vorrichtung **3** beabsichtigt, und der zweiten Vorrichtung **3** über die jeweilige gesicherte erste Kommunikationsverbindung $\mathbf{4_1}$, $\mathbf{4_2}$,..., $\mathbf{4_N}$ und die gesicherte zweite Kommunikationsverbindung **9** unter Zwischenschaltung der mit der zweiten Vorrichtung **3** untrennbar verbundenen dritten Vorrichtung **2**.

[0074] Der Zugriff auf die zweite Vorrichtung **3** kann in Abhängigkeit der der jeweiligen ersten Vorrichtung $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ jeweils zugewiesenen Zugriffsrechte, die entweder an das der jeweiligen ersten Vorrichtung $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ zugeordnete individuelle erste Identifikationsmerkmal oder an das der jeweiligen ersten Vorrichtung $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ individuelle zweiten Identifikationsmerkmal gekoppelt ist, ein lesender Zugriff und/oder ein schreibender Zugriff sein.

[0075] Die an das jeweilige individuelle erste oder zweite Identifikationsmerkmal der jeweiligen ersten Vorrichtung $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$ jeweils gekoppelten Zugriffsrechte werden bevorzugt vom System **12** zur Verwaltung von Geheimnissen verwaltet und werden der dritten Vorrichtung **2** typischerweise verschlüsselt über eine Mobilfunk- oder Festnetzverbindung **10** bekannt gegeben.

[0076] Ein schreibender Zugriff kann beispielsweise die Übertragung von Konfigurationsdaten, die in der jeweils zugreifenden ersten Vorrichtung $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$, d.h. im Speicher des Datenendgeräts oder auf dem Speicherchip der Chipkarte, gespeichert sind, in die zweite Vorrichtung **3** zur Konfiguration, d.h. zur Programmierung, einer in der zweiten Vorrichtung **3** befindlichen programmierbaren elektronischen Schaltung sein. Die Konfigurationsdaten zur Programmierung der elektronischen Schaltung in der zweiten Vorrichtung **3** sind typischerweise in allen ersten Vorrichtungen $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$ identisch.

[0077] Hierbei werden die übertragenen Konfigurationsdaten nach der Konfiguration der programmierbaren elektronischen Schaltung in der zweiten Vorrichtung **3** gelöscht. Eventuell in der dritten Vorrichtung **2** zwischengespeicherte Konfigurationsdaten werden ebenfalls nach der Konfiguration der programmierbaren elektronischen Schaltung in der zweiten Vorrichtung **3** auf Anweisung der zweiten Vorrichtung **3** in der dritten Vorrichtung **2** gelöscht.

[0078] Ein weiteres Beispiel für einen schreibenden Zugriff ist die gesicherte Übertragung und die gesicherte Aktivierung eines bestimmten Steuerbefehls in einer als Überwachungseinrichtung agierenden zweiten Vorrichtung **3**, mit der eine bestimmte, mit der zweiten Vorrichtung **3** in einer technischen Interaktion stehende technische Umgebung **7** mit hohen Sicherheitsstandards, d.h. beispielsweise eine technische Anlage oder ein technisches Aggregat in einem für den Menschen gefährlichen Umfeld, in einem bestimmten Betriebszustand gefahren wird.

[0079] Ein beispielhafter lesender Zugriff ist das Auslesen von sensiblen Daten aus einer in einer Datenverarbeitungseinrichtung integrierten Datenbank - beispielsweise Betriebsgeheimnisse eines Unternehmens, die nur einem begrenzten Personenkreis zugänglich sein sollen - und das gesicherte Übertragen dieser sensiblen Daten zu einem Datenendgerät, das einer Person aus dem begrenzten Personenkreis zugewiesen ist.

[0080] Die Zuweisung von individuellen Zugriffsrechten entsprechend der individuellen ersten oder zweiten Identifikationsmerkmale jeder ersten Vorrichtung $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$ ermöglicht auch eine gestaffelte oder hierarchische Zuweisung von Zugriffsrechten. Bestimmte Anwender, beispielsweise Systemadministratoren des Betreibers, erhalten über ihre erste Vorrichtung $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ lesende und/oder schreibende Zugriffsrechte auf alle Hardware- und/oder Software-Komponenten der zweiten Vorrichtung **3**, während andere Anwender, beispielsweise Kunden des Betreibers, beispielsweise nur lesende Zugriffsrechte auf eine stark begrenzte Anzahl von Hardware- und/oder Softwarekomponenten der zweiten Vorrichtung **3** zugewiesen bekommen.

[0081] Die Zuweisung von individuellen ersten oder zweiten Identifikationsmerkmalen an jede einzelne erste Vorrichtung $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$ ermöglicht weiterhin eine an das individuelle erste oder zweite Identifikationsmerkmal gekoppelte Sperrung von bestimmten Hardware- und/oder Softwarekomponenten der zweiten Vorrichtung **3** im Fall eines weiter unten noch beschriebenen Identifikationsmerkmals eines Nichteintretens eines von der dritten Vorrichtung **2** überprüfbaren Zustandes.

[0082] Zusätzlich ist es mit der Zuweisung von individuellen ersten oder zweiten Identifikationsmerkmalen an jede einzelne erste Vorrichtung $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$ möglich, in einem lesenden Zugriff eine an das individuelle erste oder zweite Identifikationsmerkmal gekoppelte Anzahl von Daten aus der Gesamtanzahl von in der zweiten Vorrichtung **3** zu lesenden Daten zu lesen und/oder in einem schreibenden Zugriff eine an das individuelle erste oder zweite Identifikationsmerkmal gekoppelte Anzahl von in die zweite Vorrichtung **3** zu schreibende Daten aus der Gesamtanzahl von zu schreibenden Daten zu schreiben.

[0083] Schließlich können für das zweite Identifikationsmerkmal anstelle von Zufallszahlen alternativ jeweils auch nach klassischen Methoden gewonnene Identifikationsmerkmale zur Authentifizierung eines Anwenders - beispielsweise ein Benutzername, eine

PIN-Nummer, ein Pass-Wort oder ein Zertifikat - verwendet werden. Diese alternativen zweiten Identifikationsmerkmale werden außerhalb der dritten Vorrichtung, beispielsweise im System **12** zur Verwaltung von Geheimnissen oder in einer akkreditierten Zertifizierungsstelle gewonnen und zur dritten Vorrichtung über eine gesicherte Kommunikationsverbindung transferiert.

[0084] Wird im darauffolgenden Verfahrensschritt **S50** von der dritten Vorrichtung **2** festgestellt, dass die gesicherte Übertragung von Daten zwischen der jeweils einen Zugriff anfordernden ersten Vorrichtung $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ und der zweiten Vorrichtung **3** abgeschlossen ist, so wartet die dritte Vorrichtung **2** auf einen weiteren Zugriffswunsch einer ersten Vorrichtung $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ auf die zweite Vorrichtung **3**. Sobald dieses Ereignis mit der Übertragung eines ersten und optional zweiten Identifikationsmerkmals von einer der ersten Vorrichtungen $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ eingetreten ist, erfolgt im wiederaufgenommenen Verfahrensschritt **S20** die Authentifizierung der jeweils anfragenden ersten Vorrichtung $\mathbf{1_1}$, $\mathbf{1_2}$, ..., $\mathbf{1_N}$ durch die dritte Vorrichtung **2**.

[0085] Solange im Verfahrensschritt **S50** die dritte Vorrichtung **2** keinen Abschluss der gesicherten Übertragung von Daten zwischen der jeweiligen zugreifenden ersten Vorrichtung $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$ und der zweiten Vorrichtung **3** festgestellt hat, wird im nächsten Verfahrensschritt **S60** von der dritten Vorrichtung **2** ermittelt, ob der von der Einheit **6** zu überwachende Zustand - beispielsweise ein korrekter Betrieb der zweiten Vorrichtung **3** - weiterhin vorliegt.

[0086] Ist dies der Fall, so werden in Verfahrensschritt **S40** weiterhin die Daten gesichert zwischen der zweiten Vorrichtung **3** und der jeweiligen ersten Vorrichtung $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$ übertragen, bis die Übertragung abgeschlossen ist.

[0087] Liegt der von der Einheit **6** zu überwachende Zustand nicht mehr vor, falls beispielsweise die Funktionsweise der zweiten Vorrichtung **3** zwischenzeitlich gestört ist, so wird im darauf folgenden Verfahrensschritt **S70** die aktuelle gesicherte Übertragung von Daten zwischen der jeweiligen ersten Vorrichtung $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$ und der zweiten Vorrichtung **3** und die gesicherte zweite Kommunikationsverbindung **9** zwischen der zweite Vorrichtung **3** und der dritten Vorrichtung **2** abgebrochen. Außerdem werden im selben Verfahrensschritt **S70** sämtliche in der dritten Vorrichtung **2** gespeicherten ersten und zweiten Referenz-Identifikationsmerkmale gelöscht.

[0088] Alternativ zur Löschung der ersten und zweiten Referenz-Identifikationsmerkmale können von der dritten Vorrichtung **2** auch die für die gesicherte Übertragung in den gesicherten ersten Kommunikationsverbindungen $\mathbf{4_1}$,$\mathbf{4_2}$,...,$\mathbf{4_N}$ und/oder die für die gesicherte Übertragung in der gesicherten zweiten Kommunikationsverbindung **9** jeweils erforderlichen und in der dritten Vorrichtung **2** gespeicherten gemeinsamen Geheimnisse - d.h. gemeinsame Schlüssel und gemeinsames Verschlüsselungsverfahren - gelöscht werden.

[0089] Auf diese Weise wird unwiderruflich sichergestellt, dass eine Authentifizierung von zukünftig hinsichtlich eines Zugriffes auf den zweiten Vorrichtung **3** anfragenden ersten Vorrichtungen $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ durch die dritte Vorrichtung **2** fehlschlägt und damit der jeweils anfragenden ersten Vorrichtung $\mathbf{1_1}$,$\mathbf{1_2}$,...,$\mathbf{1_N}$ kein Zugriff auf die zweite Vorrichtung **3** gewährt wird, solange die dritte Vorrichtung **3** kein erneutes Eintreten des zu überprüfenden Zustandes - beispielsweise kein erneutes Eintreten eines ungestörten Betriebes der zweiten Vorrichtung **3** - identifiziert.

[0090] Außerdem ist gewährleistet, dass weder die zweite Vorrichtung **3** bzw. die mit der zweiten Vorrichtung **3** untrennbar verbundene dritte Vorrichtung **2** noch eine der ersten Vorrichtungen $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$ die Freigabe bzw. die Sperrung der gesicherten Übertragung und damit den Zugriff auf die zweite Vorrichtung **3** beeinflussen können. Eine Freigabe oder eine Sperrung der gesicherten Übertragung kann einzig durch eine gezielte Aktivierung bzw. gezielte Deaktivierung des Betreibers im Rahmen eines „remote-zeroizing“ und/oder durch eine Reparatur bzw. eine Störung der zweiten Vorrichtung **2** oder einer mit der zweiten Vorrichtung **2** technisch interagierenden technischen Umgebung **7** erfolgen.

[0091] Wird im darauffolgenden Verfahrensschritt **S80** von der dritten Vorrichtung **2** ein Wiedereintreten des zu überprüfenden Zustandes - beispielsweise ein sich wieder einstellender korrekter Betrieb der zweiten Vorrichtung **3** - festgestellt, so werden im darauf folgenden Verfahrensschritt **S90** von der dritten Vorrichtung **2** den einzelnen ersten Vorrichtungen $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$ jeweils ein weiteres erstes Identifikationsmerkmal über die jeweiligen gesicherten ersten Kommunikationsverbindungen $\mathbf{4_1}$, $\mathbf{4_2}$,..., $\mathbf{4_N}$ vergeben und die zugehörigen ersten Referenz-Identifikationsmerkmale in einem internen Speicher der dritten Vorrichtung **2** abgelegt.

[0092] Alternativ können weitere, für die gesicherte Übertragung in den gesicherten ersten Kommunikationsverbindungen $\mathbf{4_1}$,$\mathbf{4_2}$,...,$\mathbf{4_N}$ und/oder die für die gesicherte Übertragung in der gesicherten zweiten Kommunikationsverbindung **9** jeweils erforderlichen gemeinsamen Geheimnisse von neuem von der dritten Vorrichtung **2** vergeben werden. Diese werden im Rahmen eines Reinitialisierungsprozesses mit den jeweiligen ersten Vorrichtungen $\mathbf{1_1}$, $\mathbf{1_2}$,..., $\mathbf{1_N}$ bzw. der zweiten Vorrichtung **3** zum Aufbau einer erneut gesicherten ersten Kommunikationsverbindungen $\mathbf{4_1}$,

4_2,..., **4_N** und einer erneut gesicherten zweiten Kommunikationsverbindung **9** ausgetauscht.

[0093] Auf diese Weise ist es möglich, dass Anwender, die jeweils einen Zugriff auf die zweite Vorrichtung **3** zukünftig beabsichtigen, über die ihnen jeweils zugewiesene erste Vorrichtung **1_1**, **1_2**, ..., **1_N** mit dem neu vergebenen weiteren ersten Identifikationsmerkmal sich gemäß Verfahrensschritt **S30** bei der dritten Vorrichtung **2** erfolgreich authentifizieren lassen können und somit erneut einen Zugriff auf die zweiten Vorrichtung **3** gemäß Verfahrensschritt **S40** gewährt bekommen.

[0094] Bevor eine erneute Authentifizierung des Anwenders bzw. der dem Anwender zugewiesenen ersten Vorrichtung **1_1**, **1_2**, ..., **1_N** in Verfahrensschritt **S30** erfolgt, wird im darauffolgenden Verfahrensschritt **S100** von der dritten Vorrichtung **2** ermittelt, ob vom Betreiber ein Betrieb der zweiten Vorrichtung **3** noch vorgesehen ist. Hierzu erhält die dritte Vorrichtung **2** vom Betreiber-System **8** bevorzugt über die Datenverbindung **10** typischerweise in verschlüsselter Form eine Information zur Signalisierung eines aktivierten Betriebs der zweiten Vorrichtung **3**.

[0095] Wird der Betrieb der zweiten Vorrichtung **3** durch das Betreiber-System **8** gesperrt, so wird dies der dritten Vorrichtung **2** über die Datenverbindung **10** mitgeteilt und das erfindungsgemäße Verfahren ist beendet. Ist dagegen der Betrieb der zweiten Vorrichtung **3** durch das Betreiber-System **8** weiterhin noch freigegeben, so wird mit der Authentifizierung einer zukünftig einen Zugriff auf die zweite Vorrichtung **3** anfragenden ersten Vorrichtung **1_1**,**1_2**,...,**1_N** in Verfahrensschritt **S30** fortgefahren.

[0096] Wird in Verfahrensschritt **S80** von der dritten Vorrichtung **2** kein Wiedereintreten des zu überprüfenden Zustands - beispielsweise ein sich wieder einstellender korrekter Betrieb der zweiten Vorrichtung **3** - ermittelt, so verharrt die dritte Vorrichtung **2** in Verfahrensschritt **S80**, bis ein Wiedereintreten des zu überprüfenden Zustands von der dritten Vorrichtung **2** diagnostiziert wird.

[0097] Die Erfindung ist nicht auf die dargestellten Ausführungsformen, Ausprägungen und Varianten beschränkt. Von der Erfindung sind insbesondere alle Kombinationen aller in den einzelnen Patentansprüchen jeweils beanspruchten Merkmale, aller in der Beschreibung offenbarten Merkmale und aller in den einzelnen Figuren der Zeichnung jeweils dargestellten Merkmale mit abgedeckt.

Patentansprüche

1. Verfahren zur automatischen Herstellung von jeweils einer gesicherten Kommunikationsverbindung zwischen mindestens einer ersten Vorrichtung (1_1, 1_2, ..., 1_N) und einer zweiten Vorrichtung (3) mittels einer mit der zweiten Vorrichtung (3) untrennbar verbundenen dritten Vorrichtung (2) mit folgenden Verfahrensschritten:
• Aufbauen von jeweils einer gesicherten ersten Kommunikationsverbindung (4_1, 4_2,..., 4_N) zwischen der mindestens einen ersten Vorrichtung (1_1,1_2,...,1_N) und der dritten Vorrichtung (2),
• Vergabe eines ersten Identifikationsmerkmals an die mindestens eine erste Vorrichtung (1_1, 1_2,..., 1_N) über die jeweilige gesicherte erste Kommunikationsverbindung (4_1,4_2,...,4_N) durch die dritte Vorrichtung (2) und
• Aufbauen einer gesicherten zweiten Kommunikationsverbindung (9) zwischen der dritten Vorrichtung und der zweiten Vorrichtung bei Identität zwischen dem von der jeweiligen ersten Vorrichtung (1_1, 1_2,..., 1_N) über die jeweilige gesicherte erste Kommunikationsverbindung (4_1, 4_2,..., 4_N) übertragenen jeweiligen ersten Identifikationsmerkmal und einem zugehörigen, in der dritten Vorrichtung (2) gespeicherten ersten Referenz-Identifikationsmerkmal und bei Eintreten eines von der dritten Vorrichtung (2) überprüfbaren Zustandes; wobei die erste Vorrichtung (1_1), der von der dritten Vorrichtung (2) das erste Identifikationsmerkmal zuerst vergeben wird, das erste Identifikationsmerkmal über eine gesicherte dritte Kommunikationsverbindung (5_1) einem System (12) zur Verwaltung von Geheimnissen überträgt, das das erste Identifikationsmerkmal an jede weitere erste Vorrichtung (1_2,...,1_N) über jeweils eine gesicherte dritte Kommunikationsverbindung (5_2,..., 5_N) vergibt.

2. Verfahren nach Patentanspruch 1, **dadurch gekennzeichnet**, dass der von der dritten Vorrichtung (2) überprüfbare Zustand ein von der dritten Vorrichtung (2) überprüfbarer fehlerfreier Betrieb der zweiten Vorrichtung (3) ist.

3. Verfahren nach Patentanspruch 1 oder 2, **dadurch gekennzeichnet**, dass jedes erste Referenz-Identifikationsmerkmal in der dritten Vorrichtung (2) gelöscht wird und die gesicherte zweite Kommunikationsverbindung (9) abgebrochen wird, falls der überprüfbare Zustand nicht mehr eintritt.

4. Verfahren nach Patentanspruch 3, **dadurch gekennzeichnet**, dass bei Löschung jedes ersten Referenz-Identifikationsmerkmals in der dritten Vorrichtung (2) die dritte Vorrichtung (2) an mindestens eine erste Vorrichtung (1_1, 1_2,..., 1_N) jeweils ein weiteres erstes Identifikationsmerkmal vergibt und zumindest eine zur jeweiligen weiteren ersten Identifikation jeweils identisches weiteres erstes Referenz-Identifikationsmerkmal speichert, wenn der von der dritten Vorrichtung (2) überprüfbare Zustand wieder eintritt.

5. Verfahren nach einem der Patentansprüche 1 bis 4, **dadurch gekennzeichnet**, dass die dritte Vorrichtung (2) zur Generierung des ersten Identifikati-

onsmerkmals und/oder jedes weiteren ersten Identifikationsmerkmales jeweils einen Zufallswert ermittelt.

6. Verfahren nach einem der Patentansprüche 1 bis 5, **dadurch gekennzeichnet**, dass für jede erste Vorrichtung (1_1,1_2,...,1_N) das erste Identifikationsmerkmal jeweils identisch ist und/oder die weiteren ersten Identifikationsmerkmale jeweils identisch sind.

7. Verfahren nach einem der Patentansprüche 1 bis 6, **dadurch gekennzeichnet**, dass bei Vergabe eines identischen ersten Identifikationsmerkmals an jede erste Vorrichtung (1_1, 1_2,..., 1_N) jeweils ein zweites Identifikationsmerkmal von der dritten Vorrichtung (2) vergeben wird und die zweite gesicherte Kommunikationsverbindung (9) zwischen der dritten Vorrichtung (2) und der zweiten Vorrichtung (3) aufgebaut wird, sobald zusätzlich eine Identität zwischen dem der jeweiligen ersten Vorrichtung (1_1, 1_2,..., 1_N) jeweilig vergebenen zweiten Identifikationsmerkmal und einem zugehörigen in der dritten Vorrichtung (2) gespeicherten zweiten Referenz-Identifikationsmerkmal besteht.

8. Verfahren nach einem der Patentansprüche 1 bis 5, **dadurch gekennzeichnet**, dass für jede erste Vorrichtung (1_1,1_2,..., 1_N) das erste Identifikationsmerkmal jeweils unterschiedlich ist und/oder jedes weitere erste Identifikationsmerkmal jeweils unterschiedlich ist.

9. Verfahren nach Patentanspruch 7, **dadurch gekennzeichnet**, dass mit der Vergabe eines zweiten Identifikationsmerkmals oder eines jeweils unterschiedlichen ersten Identifikationsmerkmals an die jeweilige erste Vorrichtung (1_i,1_2,...,1_N) an das zweite bzw. erste Identifikationsmerkmal jeweils gekoppelte Zugriffsrechte auf einzelne Hardware- und/oder Software-Komponenten der zweiten Vorrichtung (3) vergeben werden.

10. Verfahren nach einem der Patentansprüche 1 bis 9, **dadurch gekennzeichnet**, dass die jeweilige erste Vorrichtung (1_1, 1_2,..., 1_N) jeweils das erste Identifikationsmerkmal und/oder die weiteren ersten Identifikationsmerkmale solange speichert, bis die dritte Vorrichtung (2) der jeweiligen ersten Vorrichtung (1_1,1_2,...,1_N) ein weiteres erstes Identifikationsmerkmal vergibt.

11. Verfahren nach einem der Patentansprüche 1 bis 10, **dadurch gekennzeichnet**, dass das erste Identifikationsmerkmal und/oder jedes weitere erste Identifikationsmerkmal jeweils verschlüsselt über die jeweilige gesicherte erste Kommunikationsverbindung (4_1,4_2,...,4_N) bzw. über die jeweilige gesicherte dritte Kommunikationsverbindung (5_1, 5_2,..., 5_N) zur jeweiligen ersten Vorrichtung (1_1,1_2,...,1_N) übertragen wird.

12. Verfahren nach einem der Patentansprüche 1 bis 11, **dadurch gekennzeichnet**, dass zum Aufbauen der jeweiligen gesicherten ersten Kommunikationsverbindung (4_1,4_2,...,4_N) zwischen der dritten Vorrichtung (2) und der jeweiligen ersten Vorrichtung (1_1, 1_2,..., 1_N) und/oder zum Aufbauen der gesicherten zweiten Kommunikationsverbindung (9) zwischen der dritten Vorrichtung (2) und der zweiten Vorrichtung (39 jeweils ein gemeinsames Geheimnis ausgetauscht wird.

13. Verfahren nach Patentanspruch 12, **dadurch gekennzeichnet**, dass das gemeinsame Geheimnis für alle gesicherten ersten Kommunikationsverbindungen (4_1,4_2, ..., 4_N) jeweils unterschiedlich ist.

14. Verfahren nach Patentanspruch 12 oder 13, **dadurch gekennzeichnet**, dass das jeweilige gemeinsame Geheimnis jeweils ein gemeinsamer Schlüssel und ein gemeinsames Verschlüsselungsverfahren ist.

15. Verfahren nach einem der Patentansprüche 1 bis 14, **dadurch gekennzeichnet**, dass zum Aufbau einer gesicherten zweiten Kommunikationsverbindung (9) zwischen der dritten Vorrichtung (2) und der zweiten Vorrichtung (3) das Zustandekommen einer korrekten gesicherten ersten Kommunikationsverbindung (4_1, 4_2,..., 4_N) zwischen der jeweiligen ersten Vorrichtung (1_1,1_2,..., 1_N) und der zweiten Vorrichtung (3) überprüft wird.

16. Verfahren nach einem der Patentansprüche 1 bis 15, **dadurch gekennzeichnet**, dass die erste Vorrichtung (1_1, 1_2,..., 1_N) eine Chipkarte oder ein Datenendgerät ist.

17. System zur Herstellung von jeweils einer gesicherten Kommunikationsverbindung zwischen mindestens einer ersten Vorrichtung (1_1,1_2, ..., 1_N) und einer zweiten Vorrichtung (3) mittels einer mit der zweiten Vorrichtung (3) untrennbar verbundenen dritten Vorrichtung (2),
wobei das System so ausgebildet ist, dass jeweils eine gesicherte erste Kommunikationsverbindung (4_1,4_2,..., 4_N) zwischen jeder ersten Vorrichtung (1_1,1_2,...,1_N) und der dritten Vorrichtung (2) besteht,
wobei das System so ausgebildet ist, dass eine gesicherte zweite Kommunikationsverbindung (9) zwischen der dritten Vorrichtung (2) und der zweiten Vorrichtung (3) besteht, sobald eine Vergabe jeweils eines ersten Identifikationsmerkmals an die mindestens eine erste Vorrichtung (1_1,1_2,...,1_N) über die jeweilige gesicherte erste Kommunikationsverbindung (4_1,4_2,...,4_N) durch die dritte Vorrichtung (2) erfolgt ist, eine Identität zwischen dem von der jeweiligen ersten Vorrichtung (1_1,1_2,...,1_N) über die jeweilige gesicherte erste Kommunikationsverbindung (4_1, 4_2,..., 4_N) übertragenen jeweiligen ersten Identifikationsmerkmal und einem zugehörigen, in der dritten Vorrich-

tung (3) gespeicherten ersten Referenz-Identifikationsmerkmal besteht und ein von der dritten Vorrichtung (2) überprüfbarer Zustand eingetreten ist und wobei das System so ausgebildet ist, dass jeweils eine gesicherte dritte Kommunikationsverbindung (5_1, 5_2,..., 5_N) zwischen einem System (12) zur Verwaltung von Geheimnissen und jeweils einer ersten Vorrichtung (1_1,1_2, ..., 1_N) besteht.

18. System nach Patentanspruch 17, **dadurch gekennzeichnet**, dass eine Einheit (6) zur Überwachung eines Zustands der zweiten Vorrichtung in der dritten Vorrichtung (2) integriert ist oder mit der dritten Vorrichtung (2) verbunden ist.

Es folgen 2 Seiten Zeichnungen

Anhängende Zeichnungen

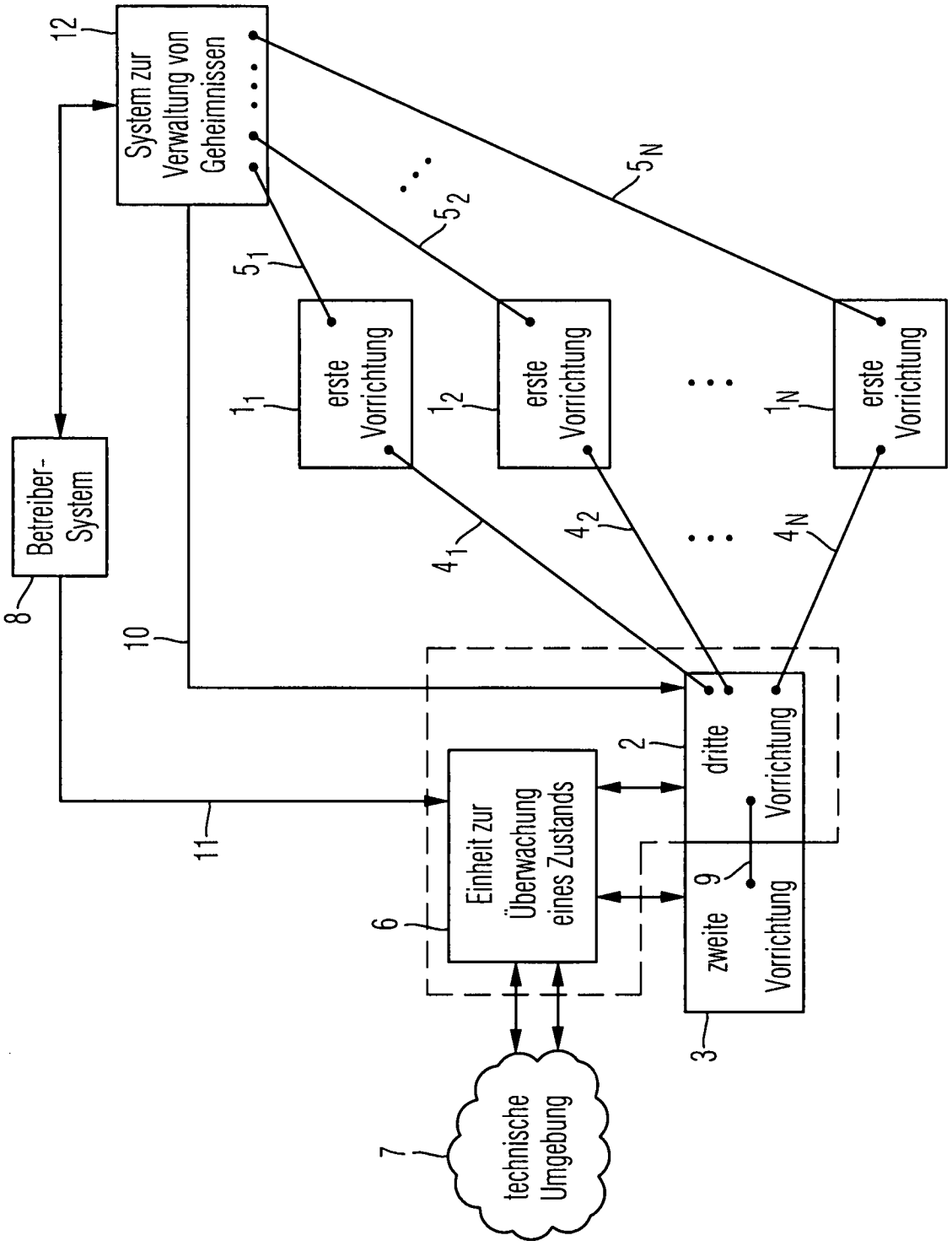


Fig. 1

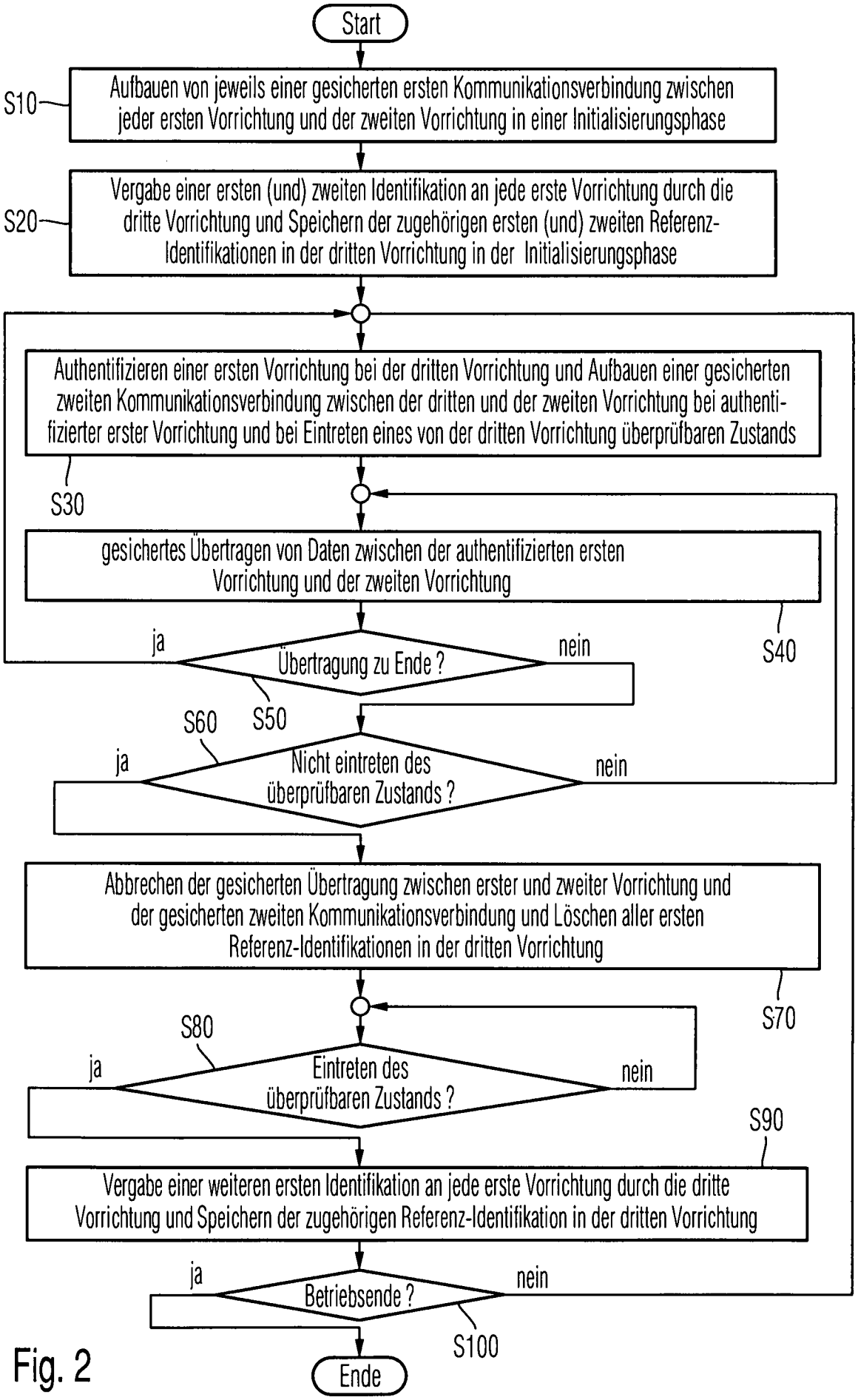


Fig. 2

