(19) SCHWEIZERISCHE EIDGENOSSENSCHAFT
EIDGENÖSSISCHES INSTITUT FÜR GEISTIGES EIGENTUM

(11) CH 708 123 A2

(51) Int. Cl.: G06F 21/44 (2013.01)
E05B 47/00 (2006.01)

Patentanmeldung für die Schweiz und Liechtenstein
Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

(12) PATENTANMELDUNG

(21) Anmeldenummer: 01027/13

(22) Anmeldedatum: 29.05.2013

(43) Anmeldung veröffentlicht: 15.12.2014

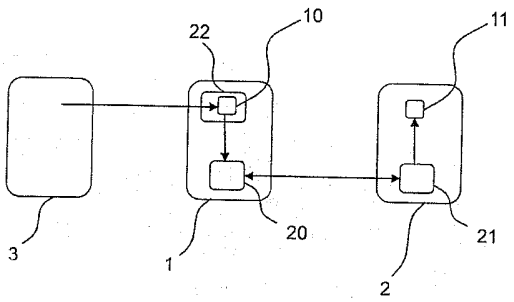
(71) Anmelder:
Kaba AG, Mühlebühlstrasse 23
8620 Wetzikon (CH)

(72) Erfinder:
Paul Studerus, 8165 Oberweningen (CH)
André Lüscher, 8706 Feldmeilen (CH)

(74) Vertreter:
Frei Patentanwaltsbüro AG, Postfach 1771
8032 Zürich (CH)

(54) Verfahren zur Verfügungsstellung einer gesicherten Zeitinformation.

(57) Die Erfindung betrifft ein Verfahren, um insb. für einen Authentifizierungsprozess eine gesicherte Zeitinformation (11) zur Verfügung zu stellen. Ein Benutzermedium (1) umfasst ein erstes Kommunikationsmodul (20) und eine erste gesicherte Umgebung (GU) (22), und ein zweites Medium (2) ein zweites Kommunikationsmodul (21). Das Verfahren umfasst in einem ersten Schritt das Übermitteln einer Referenzzeitinformation (10) an die erste gesicherte Umgebung (22), in einem zweiten Schritt das Erstellen einer Kommunikationsverbindung zwischen dem ersten Kommunikationsmodul (20) und dem zweiten Kommunikationsmodul (21) und in einem dritten Schritt das Übermitteln einer auf der Referenzzeitinformation (10) beruhenden gesicherten Zeitinformation (11) an das zweite Medium und/oder das Verwenden der auf der Referenzzeitinformation (10) beruhenden gesicherten Zeitinformation (11) für den Authentifizierungsprozess.



Beschreibung

[0001] Die Erfindung bezieht sich auf das Gebiet der Sicherheitstechnik und der sicheren Datenübertragung und insbesondere auf Medien welche zu einem Authentifizierungsprozess befähigt sind und welche dafür eine Zeitinformation verwenden.

[0002] Die Erfindung bezieht sich im Speziellen auf ein Verfahren, um für einen Authentifizierungsprozess zwischen einem Benutzermedium (bspw. einem NFC-fähigen Mobiltelefon) und einem zweiten Medium eine gesicherte Zeitinformation zur Verfügung zu stellen. Sie betrifft auch einen Authentifizierungsprozess, ein Kommunikationssystem und ein Kommunikationsmedium sowie Software dafür.

[0003] Derartige Verfahren und Kommunikationssysteme sind beispielsweise aus den Bereichen der Gebäudesicherung und Raumzutrittsberechtigung bekannt. In handelsüblichen Lösungen von Raumzutrittsberechtigungssystemen, beispielsweise in Hotels, kann ein Zimmerschlüssel in Form einer elektronischen Speicherkarte als Benutzermedium eingesetzt werden. Im Beispiel des Hotels berechtigt die elektronische Speicherkarte zum temporären Zutritt zu beispielsweise einem bestimmten Hotelzimmer. Das bestimmte Hotelzimmer ist mit einem Dienstmedium in Form eines Türschloss-Kontrollmoduls ausgestattet, welches mit der elektronischen Speicherkarte kommunizieren kann.

[0004] Eine weitere verbreitete Anwendung sind Schreib- und Leseprozesse von bzw. auf Wertkarten, elektronischen Tickets oder dergleichen. Auch für solche findet zunächst ein Authentifizierungsprozess statt.

[0005] Für die Zugangskontrolle oder andere Vorgänge, insbesondere Vorgänge, die einen Authentifizierungsprozess beinhalten, muss oft die genaue Zeit bekannt sein. Bspw. kann die Zeit als Parameter im Authentifizierungsprozess selbst eingehen, so für die Berechnung eines temporären elektronischen Schlüssels. Ergänzend oder alternativ dazu kann - im Dienstradium oder im Benutzermedium - ein Zeitfenster definiert sein, während welchem eine Berechtigung für den Prozess besteht. Bspw. kann bestimmt - sein, in welchem spezifischen Zeitfenster der Zutritt zum bestimmten Hotelzimmer erlaubt ist. Nur in diesem spezifischen Zeitfenster autorisiert das Türschloss die elektronische Speicherkarte nach einem Authentifizierungsprozess zum Öffnen des Türschlosses. Zu diesem Zweck bzw. zu diesen Zwecken muss das Türschloss über eine verlässliche Zeitinformation verfügen. Schliesslich kann die Zeit auch für die Protokollierung eines Prozesses wichtig sein, insbesondere wenn diese Protokollierung sicherheitsrelevant ist.

[0006] Um eine hohe Sicherheit gewährleisten zu können, ist dabei eine gesicherte Zeitinformation von Vorteil. Mit gesicherter Zeitinformation ist eine manipulationssichere Zeitinformation (Zeitangabe) gemeint, deren Ursprung eine vertrauenswürdige Quelle ist. Typischerweise verfügt dabei im Stand der Technik jedes Türschloss über eine eigene, manipulationsgesicherte Uhr und somit über eine eigene vertrauenswürdige Quelle für die gesicherte Zeitinformation. Diese Uhr ist dabei häufig als Echtzeituhr (real time clock, RTC) ausgebildet.

[0007] Ein anderes Beispiel ist ein Erstellen einer sicheren Kommunikationsverbindung. Häufig wird beim Einrichten einer Verschlüsselung ein Zeitsignal in der Berechnung mit verwendet. Dies dient unter anderem beispielsweise dazu, mindestens einem Schritt dieser Erstellung der sicheren Kommunikationsverbindung ein Alleinstellungsmerkmal durch eine Verwendung eines sich nicht wiederholenden Zahlenwerts, also eines Zeitwerts (insbesondere eines Absolutzeitwerts) zuzuordnen. Auch Zeitfenster für die Gültigkeit von Authentifizierungszertifikaten können beispielsweise definiert sein.

[0008] Die vorgenannten Beispiele finden in vielen Kombinationen auch beispielsweise gleichzeitig Verwendung und dienen lediglich der Illustration von ausgewählten Anwendungen aus einer Vielzahl von Anwendungsmöglichkeiten einer Zeitinformation in einem Dienstmedium.

[0009] Eine ständig laufende, genaue Echtzeituhr, bspw. mit Funkuhr-Funktionalität, ist jedoch verhältnismässig aufwändig und hat - was insbesondere für Standalone-Systeme mit Batteriespeisung ins Gewicht fällt - einen hohen Energieverbrauch. Neben der Herstellung sind auch Wartung und Reparatur aufwändig, zeitintensiv und kostspielig. Die verhältnismässig grosse Komplexität kann sich auch negativ auf Ausfallraten und technische Komplikationen auswirken. Der Stromverbrauch einer RTC fällt insbesondere dann ins Gewicht, wenn eine grosse Anzahl von räumlich verteilten Dienstmedien wie etwa Schlössern in weiträumigen Anlagen vorhanden ist.

[0010] Es ist deshalb Aufgabe der Erfindung, ein Verfahren und ein Kommunikationssystem der eingangs genannten Art zu schaffen, welche mindestens einen oben genannten Nachteile mindestens teilweise behebt.

[0011] Gemäss einem Aspekt der Erfindung geht es um ein Verfahren um insbesondere für einen Authentifizierungsprozess zwischen einem Benutzermedium und einem zweiten Medium (bspw. Dienstmedium) eine gesicherte Zeitinformation zur Verfügung zu stellen. Dabei weist das Benutzermedium ein erstes Kommunikationsmodul und eine erste gesicherte Umgebung und das zweite Medium ein zweites Kommunikationsmodul auf. Das Verfahren umfasst folgende Schritte:

- Schritt 1: Übermitteln einer Referenzzeitinformation an die erste gesicherte Umgebung - von einer vertrauenswürdigen Quelle ausserhalb des Benutzermediums,
- Schritt 2: Erstellen einer Kommunikationsverbindung zwischen dem ersten Kommunikationsmodul und dem zweiten Kommunikationsmodul,
- Schritt 3: Übermitteln einer auf der Referenzzeitinformation beruhenden gesicherten Zeitinformation an das zweite Medium und/oder Verwenden der auf der Referenzzeitinformation beruhenden gesicherten Zeitinformation für den Authentifizierungsprozess.

[0012] Dabei ist das Benutzermedium i.A. das mobile Medium, das vom Benutzer mitgetragen wird. Das zweite Medium ist oft ortsfest oder fest mit einer Einrichtung (bspw. Fahrzeug oder Terminal) verbunden und fest mit dem Dienst verknüpft, der in Anspruch genommen werden soll. Oft ist ein Authentifizierungsprozess so, dass sich das Benutzermedium gegenüber dem zweiten Medium authentifiziert, wobei der Benutzer Zugang zu einem Dienst begehrt, zu dem der Zugang via das zweite Medium führt.

[0013] Das Verfahren gemäss einem Aspekt der Erfindung zeichnet sich dadurch aus, dass erstens das Benutzermedium als eine Art Vermittler der Zeitinformation verwendet wird. Die Zeit wird also nicht direkt von der vertrauenswürdigen Quelle an das zweite Medium übertragen, sondern eben über das Benutzermedium - oder alternativ wird die Zeitinformation sonstwie im Authentifizierungsprozess verwendet, bspw. wenn dieser durch das Benutzermedium selbst durchgeführt wird. Zweitens zeichnet sich das Vorgehen dadurch aus, dass eine Gesicherte Umgebung (GU) des Benutzermediums für die Speicherung und ggf. Ermittlung der Zeit verwendet wird.

[0014] Eine GU ist beispielsweise eine so genannte sichere Umgebung (Englisch: secure environment (SE); oft findet man dafür auch den Begriff Secure dement (SE) in der Literatur). Sichere Umgebungen (SEs) als Chips mit CPU und Speicher und mit normierten Sicherheitsstandards sind mit für unterschiedliche Anwendungen erhältlich.

[0015] Ein SE umfasst einen eigenen sicheren Prozessor und einen eigenen sicheren Speicher. Beispielsweise kann der sichere Speicher eines SE verschiedene Teile umfassen, etwa einen Arbeitsspeicher und einen Datenspeicher. Ein SE ist typischerweise in Form eines Sicherheitschips ausgebildet. Dabei ist unter Sicherheitschip ein integrierter Schaltkreis zu verstehen, also eine elektronische Schaltung auf einem Substrat. Ein Sicherheitschip ist beispielsweise ein monolithisches Halbleitersubstrat mit elektronischen Elementen und Leitungen. Ein SE kann dabei insbesondere aus mehreren räumlich getrennt angeordneten aber funktional verbundenen Bereichen bzw. Teilen des Sicherheitschips bestehen, um unbefugtes Auslesen zu erschweren.

[0016] Als Alternative zu einem dedizierten Chip kann eine GU auch als sogenannte «Trusted Zone» ausgebildet sein, d.h. als Bereich eines Chips (bspw. umfassend mindestens einen CPU-Kern und Speicher), welcher funktional einem SE entspricht. Auch in dieser umfasst die GU sichere Prozessormittel und sichere Speichermittel.

[0017] Ein SE bzw. eine «Trusted Zone» kann beispielsweise von einer SIM-Karte umfasst sein, von einer Speicherkarte (so genannte memory card, wie z.B. einer SD-Karte, MicroSD-Karte oder dergleichen) umfasst sein oder von anderen elektronischen Geräten wie z.B. Mobiltelephonen, Uhren, RPID-Karten, RFID-Lesegeräten, Schlüsseln mit Mikrochips, Schlössern, Verkaufsautomaten, Zahlungsterminals, portablen elektronischen Geräten wie etwa Tabletcomputern und Ähnlichem bzw. deren Modulen umfasst sein.

[0018] Ein SE bzw. eine, Trusted Zone kann dabei Anforderungen an die Vertrauenswürdigkeit nach verschiedenen bekannten Normen erfüllen bzw. Anforderungen von bekannten Sicherheitslevels erfüllen. Beispielsweise kann ein SE ein bestimmtes so genanntes EAL (Evaluation Assurance Level) aufweisen. Diese EALs existieren in sieben Stufen (von EAL1 bis EAL7). Die gesicherten Umgebungen für die verschiedenen Aspekte der Erfindung entsprechen bspw. mindestens EAL2, mindestens EAL3 oder mindestens EAL4.

[0019] Eine GU kann beispielsweise aber auch mindestens teilweise ausserhalb eines dedizierten Chips eines SE - bzw. einer Trusted Zone - ausgebildete Elemente umfassen. Eine GU kann ganz allgemein sichere Prozessormittel und einen eigenen sicheren Speicher umfassen. Beispielsweise umfasst der sichere Speicher einer GU verschiedene Teile, etwa einen Arbeitsspeicher und einen Datenspeicher. Eine GU ' kann dabei insbesondere aus mehreren räumlich getrennt angeordneten aber funktional verbundenen Elementen bestehen, um unbefugtes Auslesen zu erschweren.

[0020] Es sind auch Lösungen mit virtualisierten gesicherten Umgebungen möglich (bspw. im Rahmen einer «Cloud»-Lösung), wobei auch eine solche physisch nicht im Medium angeordnete sichere Umgebung einem Medium eineindeutig zugeordnet ist und denselben Sicherheitsanforderungen entspricht wie die physisch in einem monolithisch integrierten Prozessor vorhandenen gesicherten Umgebungen.

[0021] Eine GU ist ganz allgemein als funktionelle Einheit zu verstehen, welche für ein manipulationssicheres und lesegeschütztes Aufbewahren und Verarbeiten von Daten eingerichtet ist und also funktionell einem «Secure Element» gemäss NFC-Standards, bspw. GlobalPlatform-Spezifikationen, entspricht. Eine GU kann demnach eine funktionelle Einheit sein, welche befähigt ist, als «Secure Element» gemäss NFC-Standards und/oder als «Teilnehmer-Identitätsmodul» (Subscriber Identity Module (SIM)) eines mobilen Endgeräts in einem Mobiltelefonnetz zu dienen.

[0022] In der GU sind insbesondere bspw. die Daten gespeichert, welche im Rahmen eines Authentifizierungsprozesses das Medium mit der GU (z.B. Benutzermedium) gegenüber einem anderen Medium (z.B. Dienstmedium) identifizieren.

[0023] Beim vorstehend beschriebenen Verfahren kann Schritt 2 nach Schritt 1, mindestens teilweise gleichzeitig oder vor Schritt 1 erfolgen.

[0024] Unter «Medium» ist dabei erstens ein elektronisches Gerät (Hardware) zu verstehen, welches ein Datenverarbeitungsmittel umfasst. Das Datenverarbeitungsmittel kann dabei als Software und/oder als mindestens ein Teil des elektronischen Geräts ausgebildet sein. Zweitens kann ein Medium auch ein emuliertes Medium sein, d.h. eine Entität, die durch auf einem Rechnersystem Eigenschaften eines elektronischen Gerätes nachbildet.

[0025] Sowohl das das zweite Medium als auch das Benutzermedium sind je ein Medium in diesem Sinn. Ein Medium kann keine, eine oder mehrere GU umfassen. Umfasst ein Medium mehr als eine GU in einer physisch verbundenen (d.h. durch Kontaktschluss miteinander verbundenen) funktionalen Einheit, so ist das Medium als eine mehrere GU umfassende Einheit zu verstehen. Beispielsweise sind eine erste GU in einer SIM-Karte und eine zweite GU in einem diese SIM-Karte umfassenden Mobiltelephon als Teil eines einzigen Mediums zu verstehen, nämlich des Mobiltelephons.

[0026] Ein Authentifizierungsprozess ist ein Erbringen eines Nachweises, also eine Verifizierung, einer behaupteten Eigenschaft eines Kommunikationspartners. Typischerweise wird eine Identität, eine Zahlungsberechtigung bzw. -fähigkeit, eine Bezugsberechtigung und/oder eine Zugangsberechtigung eines Kommunikationspartners verifiziert. Bei erfolgreicher Authentifizierung erfolgt eine abschliessende Bestätigung. Diese abschliessende Bestätigung wird auch als Autorisierung bezeichnet Gemäss einer Gruppe von Ausführungsformen wird als vertrauenswürdige Quelle ein vertrauenswürdiger Vermittler (trusted Service manager, TSM) verwendet. Trusted Service Managers sind aus dem Gebiet der Nahfeldkommunikation (NFC) bekannt und haben fest definierte Eigenschaften, bspw. gemäss GlobalPlatform, GSM Association, oder NFC Forum.

[0027] Ein vertrauenswürdiger Vermittler (trusted service manager, TSM) ist derart ausgebildet, dass er zu einer sicheren Übermittlung von Informationen in eine GU befähigt ist. Die Übermittlung erfolgt dabei gesichert und manipulationsgeschützt. Die Übermittlung kann dabei über physischen Kontakt zwischen TSM und GU erfolgen, oder die Übermittlung kann frei von physischem Kontakt zwischen TSM und GU erfolgen. Ein typisches Beispiel eines TSM ist ein von einem Anbieter eines Mobiltelephonnetzes (mobile network operator MNO) zur Verfügung gestellter entsprechender Server, welcher durch das Mobiltelephonnetz Daten frei von physischem Kontakt und gesichert an eine GU in einem Mobiltelephon übermittelt.

[0028] Die Referenzzeitinformation umfasst eine Zeitangabe, welche einer sicheren und manipulationsgeschützten, zuverlässigen Zeitquelle entstammt. Sicherheit, Manipulationsschutz und Zuverlässigkeit dieser Zeitquelle entsprechen dabei je nach Anwendung verschiedenen Kriterien. Die Referenzzeitinformation kann dabei der vertrauenswürdigen Quelle zur Verfügung gestellt werden, oder diese kann eine genaue Uhr aufweisen und die Referenzzeitinformation von sich aus zur Verfügung stellen.

[0029] In dem Verfahren gemäss einem Aspekt der Erfindung wird eine Referenzzeitinformation an eine erste GU eines Benutzermediums übermittelt. Eine solche Referenzzeitinformation kann bspw. eine einfache, genaue Angabe der aktuellen Zeit sein. Nach dieser Übermittlung verfügt das Benutzermedium, und darin die erste GU, über eine Zeitangabe, welche einer sicheren und manipulationsgeschützten, zuverlässigen Zeitquelle entstammt.

[0030] Indem eine für den Authentifizierungsprozess verwendbare gesicherte Zeitinformation mit dem hier beschriebenen Verfahren via Benutzermedium zur Verfügung gestellt wird, können die gestellten Aufgaben erfüllt werden. So kann ohne Funkuhr-Funktionalität und ohne direkte Kommunikationsverbindung zwischen dem Dienstmedium und einem sicheren Server stets gewährleistet sein, dass eine Uhr im Dienstmedium die richtige Zeit aufweist. Dies kann auch dann der Fall sein, wenn die Uhr im Dienstmedium nicht ständig läuft, sondern bspw. erst für den Authentifizierungsprozess in Gang gesetzt wird.

[0031] Das erfindungsgemässe Vorgehen kann sogar so genutzt werden, dass das Dienstmedium beispielsweise gar keine eigene Echtzeituhr und gar keinen Zeitgeber aufweisen muss.

[0032] Als andere alternative Möglichkeit kann der Authentifizierungsprozess auch im Benutzermedium selbst durchgeführt werden. Das zweite Medium (Dienstmedium) kann dann in Vertauschung der Rollen rein passiv ausgestaltet sein, bspw. als so genannter «Tag». Indem Authentifizierungsprozess und erfindungsgemäss die gesicherte Zeitinformation in der GU lokalisiert sind, ist die Authentifizierung auch dann manipulationssicher, wenn das Benutzermedium nicht kontrolliert ist.

[0033] Ganz allgemein ein Vorteil dieses Verfahrens ist eine hohe Manipulationssicherheit der Zeitinformation. Obwohl das Benutzermedium in den Händen eines Benutzers ist und also an sich auch Manipulationsversuchen ausgesetzt sein kann, wird durch die Nutzung der GU sichergestellt, dass die Zeitinformation sicher ist.

[0034] Somit erlaubt das Verfahren, ein Dienstmedium mit einfachem Aufbau zu verwenden; welches schnell, einfach und kostengünstig hergestellt werden kann und einfach und weniger häufig gewartet werden muss. Auch können ausfallsichere und wenig störanfällige Dienstmedien verwendet werden.

[0035] In Ausführungsformen kann beispielsweise bei jedem Aufbau der Kommunikationsverbindung zwischen dem ersten und dem zweiten Kommunikationsmodul die Möglichkeit bestehen, vom Benutzermedium an das Dienstmedium eine gesicherte Zeitinformation zu übermitteln. Somit kann etwa bei jeder Kommunikation zwischen Benutzermedium und Dienstmedium das Dienstmedium vom Benutzermedium erneut mit der gesicherten Zeitinformation versehen werden.

[0036] Somit kann das Dienstmedium beispielsweise frei von einer eigenen Zeitquelle oder Uhr ausgebildet sein und die gesicherte Zeitinformation bei jeder Kommunikation zwischen Benutzermedium und Dienstmedium erneut von der ersten GU zur Verfügung gestellt bekommen - oder wie erwähnt kann der Authentifizierungsprozess gleich im Benutzermedium stattfinden.

[0037] Die gesicherte Zeitinformation kann wie folgt auf der Referenzzeitinformation beruhen: die gesicherte Zeitinformation umfasst eine Zeitangabe, welche in einem Zusammenhang mit der Referenzzeitinformation steht und auf dieser be-

ruht. Dadurch steht die gesicherte Zeitinformation in einem eindeutigen Zusammenhang mit der Zeitangabe, welche der sicheren und manipulationsgeschützten, zuverlässigen Zeitquelle entstammt. Die gesicherte Zeitinformation umfasst daher eine Zeitangabe, welche gesichert und manipulationsgeschützt ist und einer vertrauenswürdigen Zeitquelle entstammt.

[0038] In einer ersten Gruppe von Ausführungsformen («online»-Ausführungsformen) besteht eine Kommunikationsverbindung zwischen der vertrauenswürdigen Zeitquelle und dem Benutzermedium einerseits und zwischen dem Benutzermedium und dem zweiten Medium («Dienstmedium») andererseits gleichzeitig. In dieser Gruppe von Ausführungsformen hat das Benutzermedium die Rolle eines Relais, welches die Information über die Zeit im Wesentlichen einfach weitergibt, wobei optional ein Verarbeitungsschritt stattfinden kann.

[0039] Beispielsweise kann die gesicherte Zeitinformation die Referenzzeitinformation sein bzw. diese umfassen. Optional kann auch ein zeitlicher Offset vorgesehen sein, der bspw. einer vorbekannten Verarbeitungszeit (zeitlicher Abstand zwischen Schritten 1 und 3) entsprechen kann. Damit kann im Dienstmedium beispielsweise ein gesicherter aktueller Zeitpunkt relativ zur Referenzzeitinformation nachvollzogen werden. Auch damit kann im Dienstmedium ein gesicherter aktueller Zeitpunkt relativ zur Referenzzeitinformation nachvollzogen werden. In einer Ausführungsform des Verfahrens kann die gesicherte Zeitinformation der Referenzzeitinformation entsprechen, insbesondere wenn die Zeitdifferenz zwischen Schritt 1 und Schritt 3 klein ist oder keine entsprechende Zeitdifferenz besteht.

[0040] Als optionales Merkmal umfasst im oben beschriebenen Verfahren demnach die gesicherte Zeitinformation die Referenzzeitinformation, und Schritt 3 erfolgt entweder gleichzeitig mit Schritt 1 oder unmittelbar nach Schritt 1.

[0041] Je kleiner der Zeitunterschied zwischen den beiden Übermittlungen ist, desto kleiner ist ein möglicher Fehler in der gesicherten Zeitinformation.

[0042] Vereinfach ausgedrückt erlaubt dieses optionale Merkmal, dass das Dienstmedium zeitlich direkt oder fast direkt mit der Quelle der Zeitinformation verbunden ist und über das Benutzermedium eine gesicherte Zeitinformation zur Verfügung gestellt bekommt. Das Benutzermedium dient dabei als Verbindung zur Quelle, welche ohne zeitliche Verzögerung oder mit nur einer minimalen zeitlichen Verzögerung funktioniert. Daher ist ein Risiko, dass die gesicherte Zeitinformation mit einem zeitlichen Fehler behaftet ist, relativ gering. Zudem muss das Benutzermedium den zeitlichen Unterschied zwischen Schritt 1 und Schritt 3 nicht zeitlich präzis bemessen an das Dienstmedium weitergeben. Es können auch Mechanismen vorgesehen sein, die das Resultat der Authentifizierung verwerfen oder eine solche gar nicht erlauben, wenn nicht verifiziert ist, dass das Benutzermedium mit der vertrauenswürdigen Quelle in Kommunikationsverbindung steht oder wenn der zeitliche Zusammenhang zwischen Schritten 1 und 3 nicht verifiziert ist.

[0043] Beispielsweise kann in dieser Ausführungsform das Benutzermedium die Referenzzeitinformation direkt verarbeiten und die entsprechende gesicherte Zeitinformation an das Dienstmedium übermitteln, ohne die Referenzzeitinformation und/oder die gesicherte Zeitinformation zu speichern und/oder weiterzuverarbeiten. Dies erlaubt eine einfache und schlanke Struktur des Benutzermediums.

[0044] In der ersten Gruppe von Ausführungsformen ist das Benutzermedium bevorzugt mit Mitteln für die mobile Kommunikation versehen, bspw. über ein Mobiltelefon-(Mobilfunk-) Netz und/oder über ein WLAN. Insbesondere kann das Benutzermedium in dieser wie auch in anderen Ausführungsformen als Mobiltelefon ausgestaltet sein.

[0045] In einer zweiten Gruppe von Ausführungsformen kann das Übermitteln der Referenzzeitinformation quasi «offline» geschehen, d.h. das Benutzermedium muss während Schritt 3, bzw. unmittelbar davor, nicht mit dem TSM in Kommunikationsverbindung stehen.

[0046] In Ausführungsform dieser Gruppe erfolgt Schritt 1 zeitlich unabhängig von Schritt 2 und Schritt 3, insbesondere können Schritt 2 und Schritt 3 zu einem anderen Zeitpunkt als Schritt 1 erfolgen. Dabei hängt die gesicherte Zeitinformation funktional mit einem zeitlichen Unterschied zwischen einer Ausführung von Schritt 1 und einer Ausführung von Schritt 3 zusammen.

[0047] Durch dieses Vorgehen ist das Benutzermedium nicht darauf angewiesen, zeitgleich oder zeitnah sowohl mit der vertrauenswürdigen Quelle als auch mit dem Dienstmedium in Kontakt zu stehen. Dies erlaubt einen zeitlich und verfahrenstechnisch flexiblen Einsatz des Verfahrens.

[0048] In dieser Gruppe von Ausführungsformen umfasst die erste GU einen Zeitgeber, insbesondere eine Echtzeituhr (RTC), wobei die Echtzeituhr mindestens einen Teil der gesicherten Zeitinformation liefert. Insbesondere wird dabei der Zeitgeber in Schritt 1 mittels der Referenzzeitinformation zeitlich synchronisiert.

[0049] Je nachdem wie die- gesicherte Zeitinformation auf der Referenzzeitinformation beruht, kann dabei der Zeitgeber (der in Schritt 1 durch die Referenzzeitinformation synchronisiert wurde, wodurch die von ihm gemessene Zeit auf letzterer beruht) die gesicherte Zeitinformation liefern.

[0050] Wie genau die Verarbeitung der Referenzzeitinformation in die gesicherte Zeitinformation erfolgt ist sekundär: Der Zeitgeber kann bspw. auch ohne das erwähnte Synchronisieren betrieben werden und nur den zeitlichen Abstand zwischen Schritt 1 und Schritt 3 liefern. Die gesicherte Zeitinformation wird dann anderswo in der GU aus der gespeicherten Referen2zeitinformation und diesem zeitlichen Abstand berechnet.

[0051] Ein Zeitgeber in der GU ist insbesondere dann von Vorteil, wenn Schritt 1 zeitlich unabhängig von Schritt 2 und Schritt 3 erfolgt. Auf diese Weise wird das Verfahren unabhängig von einer Verbindung zur vertrauenswürdigen Quelle.

Die Übermittlung der genauen gesicherten Zeitinformation an das Dienstmedium bzw. der Authentifizierungsprozess kann jederzeit stattfinden, ohne dass durch die fehlende zeitliche Koinzidenz zwischen Schritt 1 und Schritt 3 ein systematischer Fehler entstünde. Je nach Verfügbarkeit kann dabei die Quelle in kurzen oder langen zeitlichen Abständen die Referenzzeitinformation aktualisieren bzw. den Zeitgeber synchronisieren.

[0052] Auch in Ausführungsformen der zweiten Gruppe dient das Benutzermedium als eine Art Relais zur Übermittlung der Zeit mit den vorstehend diskutierten Vorteilen, allerdings mit dem zusätzlichen Vorteil, dass das Verfahren nicht von einer gleichzeitigen Verbindung mit TSM und Dienstmedium abhängig ist.

[0053] Es kann in Ausführungsformen der zweiten Gruppe vorgesehen sein, dass die Zeitinformation auf dem Benutzermedium periodisch justiert werden muss, mit einer an die Genauigkeit des Zeitgebers im Benutzermedium angepassten Periode. Wenn diese Synchronisation über eine gewisse Zeit nicht möglich ist oder wenn das Benutzermedium neu gestartet wird, so wird in diesen Ausführungsformen die Zeit solange als ungültig betrachtet bis wieder eine Synchronisation erfolgt ist.

[0054] Als weiteres optionales Merkmal des Verfahrens in verschiedenen Ausführungsformen (darunter online-Ausführungsformen und «offline»-Ausführungsformen) umfasst das Dienstmedium eine zweite GU, und das zweite Kommunikationsmodul übermittelt in Schritt 3 die gesicherte Zeitinformation an die zweite GU.

[0055] Die zweite GU im Dienstmedium bietet den Vorteil einer hohen Sicherheit der gesicherten Zeitinformation und insbesondere einer hohen Manipulationssicherheit auch vor Manipulationen direkt am Dienstmedium.

[0056] Ein anderes optionales Merkmal des Verfahrens ist, dass das Dienstmedium einen Zeitgeber umfasst. Ein solcher kann in Schritt 3 mittels der gesicherten Zeitinformation zeitlich synchronisiert werden; oder alternativ kann mittels diesem bei einem später stattfindenden Authentifizierungsprozess aus der Referenzzeitinforation die aktuelle Zeit berechnet werden.

[0057] Ein solcher Zeitgeber im Dienstmedium kann dabei mindesten teilweise oder auch vollständig von der zweiten GU, falls vorhanden, umfasst sein. Dies hat den Vorteil einer hohen Sicherheit und insbesondere einer hohen Manipulationssicherheit der Zeitangabe.

[0058] Ein Zeitgeber im Dienstmedium hat den Vorteil, dass das Dienstmedium jederzeit über eine Zeitinformation verfügt. Durch die vom Benutzermedium erhaltene gesicherte Zeitinformation kann ein solcher Dienstmedium-Zeitgeber jederzeit die aktuelle Zeit bestimmen. Die Zeitinformation kann auch für nachfolgende Authentifizierungsprozesse mit Benutzermedien verwendbar sein, welche nicht über eine gesicherte Zeitinformation verfügen. Beispielsweise kann in einem komplexen System vorgesehen sein, dass nur gewisse Benutzer (bspw. der Nachtwächter, der regelmässige Kontrollen durchführt oder eine Wartungsperson) das erfindungsgemässe Verfahren ausführen, während sich für alle anderen nichts ändert.

[0059] In einem anderen Beispiel kann im Dienstmedium etwa die vom ersten GU zur Verfügung gestellte gesicherte Zeitinformation mit der Zeitinformation aus der Echtzeituhr des Dienstmediums verglichen werden, wobei je nach Resultat des Vergleichs bestimmte Schritte eingeleitet werden. Diese Schritte können beispielsweise darin bestehen, dass eine Fehlfunktionswarnung ausgelöst wird und/oder eine Warnung wegen unzureichender Stromzufuhr (beispielsweise Batterien mit ungenügender Leistung) ausgelöst wird.

[0060] Optional wird die Kommunikationsverbindung in Schritt 2 nach einem bekannten Standard erstellt. Insbesondere wird die Kommunikationsverbindung in Schritt 2 als NFC-, Bluetooth- oder andere kurzreichweitige Kommunikationsverbindung erstellt.

[0061] NFC ist dabei eine Abkürzung des englischen Begriffs Near Field Communication. und bezeichnet einen internationalen Übertragungsstandard zum kontaktlosen Austausch von Daten über kurze Strecken von bis zu 10 cm und einer Datenübertragungsrate von maximal 424 kBit/s.

[0062] Eine Verwendung von bekannten Standards macht die Benutzer- und/oder Dienstmedien vielseitig verwendbar. Die Kommunikationsmodule können dabei auch für weitere Zwecke als der Übermittlung der Referenzzeitinformation bzw. der gesicherten Zeitinformation verwendet werden. Zudem kann das Verfahren beispielsweise auch einfacher auf bereits vorhandene Geräte angewendet werden, wenn das Verfahren und die vorhandenen Geräte bekannte Standards verwenden.

[0063] Als weitere Option wird die Kommunikationsverbindung in Schritt 2 nach einem bekannten gesicherten Standard erstellt, wobei die Kommunikation über die Kommunikationsverbindung insbesondere verschlüsselt erfolgt.

[0064] Wenn die Kommunikationsverbindung einen bekannten Standard verwendet, welcher zudem eine Sicherheit der Kommunikationsverbindung gewährleistet, resultiert dies in einer hohen Sicherheit des gesamten beschriebenen Verfahrens. Insbesondere eine Verschlüsselung der Kommunikationsverbindung bietet den Vorteil einer hohen Sicherheit und insbesondere hohen Manipulationssicherheit des Verfahrens.

[0065] Die Erfindung betrifft auch einen Authentifizierungsprozess zwischen einem Benutzermedium und einem Dienstmedium, wobei zunächst nach dem Verfahren gemäss obiger Beschreibung dem Dienstmedium durch das Benutzermedium eine gesicherte Zeitinformation zur Verfügung gestellt wird und anschliessend die gesicherte Zeitinformation durch das Dienstmedium für die Authentifizierung des Benutzermediums verwendet wird.

[0066] Ein solcher Authentifizierungsprozess hat den Vorteil, dass sowohl das Benutzermedium als auch das Dienstmedium mindestens kurzzeitig über aktuelle Zeitinformationen verfügen, welche manipulationssicher und zuverlässig sind. Dies erlaubt eine hohe Sicherheit beim Authentisieren bei gleichzeitig allen oben erwähnten Vorteilen des Verfahrens, um einem Dienstmedium via ein Benutzermedium eine gesicherte Zeitinformation zur Verfügung zu stellen.

[0067] In einer besonderen Ausführungsform des Authentifizierungsprozesses weist das Dienstmedium keinen Zeitgeber oder mindestens keine Echtzeituhr auf. Die Vorteile eines Dienstmediums ohne Echtzeituhr sind bereits weiter oben beschrieben.

[0068] Weiter betrifft die Erfindung ein Kommunikationssystem, welches ein Benutzermedium und ein zweites Medium (insbesondere Dienstmedium oder bei der Authentifizierung die passive («Benutzer»-) Rolle einnehmendes Medium) umfasst. Das Benutzermedium umfasst dabei ein erstes Kommunikationsmodul und eine erste gesicherte Umgebung (GU), und das zweite Medium umfasst ein zweites Kommunikationsmodul. Zudem ist das Dienstmedium dazu eingerichtet, einen Authentifizierungsprozess durchzuführen. Die erste GU ist dabei derart ausgebildet, dass sie zu einem Empfang von gesicherten Daten von einer vertrauenswürdigen Quelle (bspw. einem trusted Service manager, TSM) befähigt ist. Die erste GU ist zudem funktional mit dem ersten Kommunikationsmodul verknüpft, und das erste und das zweite Kommunikationsmodul sind derart ausgebildet, dass sie zu einem Aufbau einer Kommunikationsverbindung zwischen sich befähigt sind. Ausserdem ist die erste GU derart ausgebildet, dass sie zu einem Übermitteln einer auf der Referenzzeitinformation beruhenden gesicherten Zeitinformation über die Kommunikationsverbindung an das zweite Medium befähigt oder befähigt ist, einen Authentifizierungsprozess anhand von Daten durchzufuhren, welche vom zweiten Medium empfangen wurden.

[0069] Ein solches Kommunikationssystem kann die oben beschriebenen Verfahren ausführen und weist daher dieselben Vorteile wie die oben beschriebenen Verfahren auf. Dabei sind sowohl die Verfahren, um eine gesicherte Zeitinformation für einen Authentifizierungsprozess zur Verfügung zu stellen gemeint als auch die Authentifizierungsprozesse selbst. Dies gilt jeweils für alle möglichen Kombinationen von als optional beschriebenen Ausführungsformen dieser Verfahren. Die entsprechend beschriebenen Vorteile der Verfahren sind auch Vorteile des jeweiligen sie anwendenden Kommunikationssystems.

[0070] Bestimmte spezifisch ausgebildete Kommunikationssysteme eignen sich gut zum Anwenden verschiedener der oben beschriebenen Verfahren. Dies gilt insbesondere für Kommunikationssysteme umfassend die nachstehend genannten optionalen Merkmale.

[0071] Optional kann dass die erste GU derart ausgebildet sein, dass sie zum Empfang der Referenzzeitinformation von der vertrauenswürdigen Quelle und gleichzeitig oder unmittelbar danach zum Übermitteln einer auf der Referenzzeitinformation beruhenden gesicherten Zeitinformation von der ersten GU durch die Kommunikationsverbindung an das Dienstmedium oder zum Durchführen eines Authentifizierungsprozesses befähigt ist.

[0072] Alternativ dazu kann die erste GU optional derart ausgebildet ist, dass sie zum Empfang der Referenzzeitinformation vom TSM und davon zeitlich unabhängig zum Übermitteln einer auf der Referenzzeitinformation beruhenden gesicherten Zeitinformation von der ersten GU durch die Kommunikationsverbindung an das Dienstmedium bzw. zum Durchführen eines Authentifizierungsprozesses befähigt ist.

[0073] In einer optionalen Ausführungsform umfasst das Benutzermedium einen Zeitgeber, bspw. eine Echtzeituhr (RTC). Insbesondere umfasst dabei die erste GU den Zeitgeber vollständig. Eine RTC kann auch teilweise von der ersten GU umfasst sein.

[0074] Eine andere Option ist, dass das zweite Medium als Dienstmedium eine zweite GU umfasst, wobei die zweite GU funktional mit dem zweiten Kommunikationsmodul verknüpft ist.

[0075] Optional umfasst das Dienstmedium einen Zeitgeber, bspw. eine Echtzeituhr. Insbesondere ist die RTC im Dienstmedium dabei mindestens teilweise oder auch vollständig von der zweiten GU umfasst.

[0076] Als weitere Option sind das erste und das zweite Kommunikationsmodul derart ausgebildet, dass sie zu einem Aufbau einer insbesondere sicheren Kommunikationsverbindung miteinander nach einem bekannten Standard befähigt sind. Dabei sind das erste und das zweite Kommunikationsmodul insbesondere zum Aufbau einer Kommunikationsverbindung nach NFC, Bluetooth oder anderen bekannten kurzreichweitigen Standards befähigt.

[0077] Als eine weitere optionale Möglichkeit umfasst die erste GU im Benutzermedium einen ersten Schlüssel und die zweite GU umfasst im Dienstmedium einen zweiten Schlüssel.

[0078] Die Schlüssel in den GUs können zum Aufbau einer gesicherten Kommunikationsverbindung und/oder zur Verschlüsselung der übermittelten Informationen benutzt werden. Dadurch wird das Kommunikationssystem sicher und ist insbesondere von Manipulation geschützt. Der erste und/oder zweite Schlüssel kann dabei insbesondere aus mehreren Teilschlüsseln mit unterschiedlicher Herkunft bestehen. Dies erhöht die Sicherheit zusätzlich. Entsprechende Verfahren und Konfigurationen sind bekannt.

[0079] In einer optionalen Ausführungsform des Kommunikationssystems ist das Dienstmedium dazu eingerichtet, einen Authentifizierungsprozess durchzuführen, bei welchem das Dienstmedium das Benutzermedium authentifiziert.

[0080] Bei erfolgreicher Authentifizierung erfolgt durch das Dienstmedium eine abschliessende Bestätigung an das Benutzermedium. Diese abschliessende Bestätigung wird auch als Autorisierung bezeichnet.

[0081] Optional umfasst das Kommunikationssystem ein Managermedium, welches funktional mit der ersten GU verknüpft ist. Dabei ist die erste GU derart ausgebildet, dass sie zum Empfangen einer Authentifizierungsinformation vom Managermedium befälligt ist.

[0082] Unter Managermedium ist dabei ein Medium zu verstehen, welches derart ausgebildet ist, um zu einer Kommunikation mit der ersten GU befähigt zu sein. Das Managermedium wird beispielsweise auch als application backend oder Anwendungsanbietermedium bezeichnet. Dieses Managermedium ist insbesondere dazu befähigt, eine Authentifizierungsinformation von einem TSM zu empfangen. Die Authentifizierungsinformation ist eine Information im ersten GU, welche einen Authentifizierungsprozess zwischen Benutzermedium und Dienstmedium beeinflusst. Dadurch kann das Managermedium im ersten GU zeitlich befristete Berechtigungen bzw. Autorisierungen eintragen, verändern und/oder löschen.

[0083] Das Managermedium kann dabei über den TSM mit dem ersten GU verbunden sein. Alternativ ist das Managermedium unabhängig vom TSM mit dem ersten GU verbunden; zu diesem Zweck kann es selbst eine GU aufweisen, über welche die Kommunikation mit dem GU des Benutzer- und/oder Dienstmediums läuft. Die Verbindung des Managermediums mit der ersten GU ist aber je nach gewünschtem Sicherheitsstandard nicht dazu befähigt, die von der ersten GU empfangene Referenzzeitinformation zu beeinflussen. Optional kann das TSM auch dem Managermedium eine Zeitangabe übermitteln, welche einer sicheren und manipulationsgeschützten, zuverlässigen Zeitquelle entstammt. Insbesondere kann das TSM dem Managermedium auch die Referenzzeitinformation übermitteln.

[0084] Ein Managermedium ist einem Beispiel eines Raumzutrittsberechtigungssystems eines Hotels ein Gerät zum Beschreiben und/oder Löschen von Benutzermedien. Dabei sind elektronische Speicherkarten die Benutzermedien und Türschlösser die Dienstmedien. Insbesondere können in diesem Beispiel die Benutzermedien aber auch als Mobiltelephon, virtuelle Speicherkarte und/oder andere Medien ausgebildet sein.

[0085] Weitere bevorzugte Ausführungsformen gehen aus den abhängigen Patentansprüchen hervor. Dabei sind Merkmale der Verfahrensansprüche sinngemäss mit den Vorrichtungsansprüchen kombinierbar und umgekehrt.

[0086] Im Folgenden wird der Erfindungsgegenstand anhand von bevorzugten Ausführungsbeispielen, welche in den beiliegenden Zeichnungen dargestellt sind, näher erläutert. Es zeigen jeweils schematisch:

Fig. 1 ein Kommunikationssystem;

Fig. 2 ein Kommunikationssystem wie in Fig. 1 aber zusätzlich mit einer zweiten GU;

Fig. 3 ein Kommunikationssystem wie in Fig. 1 aber zusätzlich mit einer RTC im Benutzermedium;

Fig. 4 ein Kommunikationssystem wie in Fig. 3 aber zusätzlich einer zweiten GU und einem ersten und zweiten Schlüssel;

Fig. 5 ein Kommunikationssystem wie in Fig. 4 aber zusätzlich mit einem Managermedium;

Fig. 6 ein Kommunikationssystem, bei welchem das zweite Medium bei der Authentifizierung eine passive Rolle hat.

[0087] Die in den Zeichnungen verwendeten Bezugszeichen und deren Bedeutung sind in der Bezugszeichenliste zusammengefasst aufgelistet. Grundsätzlich sind in den Figuren gleiche Teile mit gleichen Bezugszeichen versehen.

[0088] Die Fig. 1 zeigt ein Kommunikationssystem mit einem Benutzermedium 1 und einem zweiten Medium 2, nämlich einem Dienstmedium. Das Benutzermedium 1 umfasst ein erstes SE 22, welches eine erste GU bildet. Dem ersten SE 22 kann eine Referenzzeitinformation 10 übermittelt werden. Die Referenzzeitinformation 10 wird dem ersten SE 22 von einer vertrauenswürdigen Quelle, hier einem TSM 3 durch ein Mobiltelephonnetz übermittelt; alternativ zum Mobiltelephonnetz könnte bspw. auch ein WLAN benutzt werden. Das Benutzermedium 1 umfasst ausserdem ein erstes Kommunikationsmodul 20, welches sich ausserhalb des ersten SE 22 befindet.

[0089] Das Dienstmedium 2 umfasst ein zweites Kommunikationsmodul 21. Das erste Kommunikationsmodul 20 und das zweite Kommunikationsmodul 21 sind derart ausgebildet, dass sie zum Aufbau einer NFC-Kommunikationsverbindung miteinander befähigt sind.

[0090] Dem Dienstmedium 2 wird hier ein gesichertes Zeitsignal 11 zur Verfügung gestellt, indem zuerst die NFC-Kommunikationsverbindung zwischen dem ersten Kommunikationsmodul 20 und dem zweiten Kommunikationsmodul 21 etabliert wird. Danach übermittelt der TSM 3 die Referenzzeitinformation 10 in das erste SE22. Sobald die Referenzzeitinformation 10 im ersten SE 22 empfangen worden ist, wird eine der Referenzzeitinformation 10 entsprechende gesicherte Zeitinformation 11 vom ersten SE 22 an das erste Kommunikationsmodul 20 und über die NFC-Kommunikationsverbindung zum zweiten Kommunikationsmodul 21 an das Dienstmedium 2 übermittelt. Somit ist dem Dienstmedium 2 eine gesicherte Zeitinformation 11 zur Verfügung gestellt.

[0091] Diese gesicherte Zeitinformation 11 benutzt nun das Dienstmedium 2, um in einem Authentifizierungsprozess zwischen dem Dienstmedium 2 und dem Benutzermedium 1 basierend auf der gesicherten Zeitinformation 11 zu entscheiden, ob eine Autorisierung des Benutzermediums 2 erfolgen darf oder nicht.

[0092] Beispielsweise kann im Dienstmedium festgelegt sein, dass das Benutzermedium nur während einem gewissen Zeitfenster autorisiert ist. Nur wenn die aktuelle, gesicherte Zeit in diesem Zeitfenster liegt, erfolgt eine Freigabe. Alternativ dazu kann eine im Benutzermedium vorhandene Autorisierungsinformation (bspw. ein elektronischer Hotelzimmerschlüssel oder ein zeitlich in seiner Gültigkeit beschränktes Ticket) nur zu gewissen Zeiten gültig sein, wobei die Gültigkeit durch das Dienstmedium bei Vorhandensein einer Zeitinformation verifizierbar bzw. falsifizierbar ist.

[0093] Das Dienstmedium 2 ist einfach aufgebaut und deswegen gleichzeitig wartungsarm und wenig störanfällig sowie kostengünstig in Produktion, Betrieb und Wartung sein.

[0094] In Fig. 2 ist ein weiteres Kommunikationssystem beschrieben. Als einzigen in der Figur dargestellten Unterschied zum Kommunikationssystem in Fig. 1 umfasst im Kommunikationssystem von Fig. 2 das Dienstmedium 2 eine zweite GU, welche als zweites SE 23 ausgebildet ist. Die gesicherte Zeitinformation 11 wird nach dem Empfang durch das zweite Kommunikationsmodul 21 innerhalb des Dienstmediums 2 an das zweite SE 11 übermittelt. Dadurch ist die gesicherte Zeitinformation 11 zusätzlich geschützt und vor Manipulation gesichert; der Authentifizierungsprozess kann in der zweiten GU oder ausserhalb davon ablaufen.

[0095] Dem Dienstmedium 2 in Fig. 2 wird ein gesichertes Zeitsignal 11 zur Verfügung gestellt, indem zuerst eine NFC-Kommunikationsverbindung zwischen dem ersten Kommunikationsmodul 20 und dem zweiten Kommunikationsmodul 21 etabliert wird. Danach übermittelt der TSM 3 die Referenzzeitinformation 10 in das erste SE22. Sobald die Referenzzeitinformation 10 im ersten SE 22 empfangen worden ist, wird eine der Referenzzeitinformation 10 entsprechende gesicherte Zeitinformation 11 vom ersten SE 22 an das erste Kommunikationsmodul 20 und über die NFC-Kommunikationsverbindung und nach bekannten Methoden verschlüsselt zum zweiten Kommunikationsmodul 21 und schlussendlich vom zweiten Kommunikationsmodul 21 an das zweite SE 23 im Dienstmedium 2 übermittelt. Somit ist dem Dienstmedium 2 und etwas genauer gesagt der zweiten SE 23 eine gesicherte Zeitinformation zur Verfügung gestellt worden. In diesem Fall ist die gesicherte Zeitinformation 11 auf eine nur durch eine SE entschlüsselbare Weise verschlüsselt übermittelt worden, was eine zusätzliche Sicherheit der gesicherten Zeitinformation bedeutet. Noch weiter erhöht wird die Sicherheit des Kommunikationssystems in Fig. 2 durch den Umstand, dass die gesicherte Zeitinformation 11 in die zweite SE 23 übermittelt wird.

[0096] Der Authentifizierungsprozess zwischen dem Dienstmedium 2 und dem Benutzermedium 1 wird analog zum Kommunikationssystem in Fig. 1 vorgenommen.

[0097] Fig. 3 zeigt ein Kommunikationssystem mit einem Zeitgeber, nämlich einer Echtzeituhr RTC 24 im Benutzermedium. Als einzigen dargestellten Unterschied zum Kommunikationssystem in Fig. 1 umfasst hier das erste SE 22 zusätzlich zur vom TSM 3 empfangenen Referenzinformation 10 noch eine RTC 24.

[0098] Dem Dienstmedium 2 in Fig. 3 wird ein gesichertes Zeitsignal 11 zur Verfügung gestellt, indem zuerst der TSM 3 die Referenzzeitinformation 10 in das erste SE 22 übermittelt. Sobald die Referenzzeitinformation 10 im ersten SE 22 empfangen worden ist, wird diese an die RTC 24 weitergeleitet, damit die RTC 24 mit der in der Referenzzeitinformation 11 enthaltenen Zeitangabe synchronisiert werden kann. Die RTC 24 im ersten SE 22 ist nun mit einer zuverlässigen Zeitquelle synchronisiert. Somit verfügt das Dienstmedium 2 über eine RTC 24, welche dazu befähigt ist, eine Zeitangabe zur Verwendung in der gesicherten Zeitinformation 11 zur Verfügung zu stellen.

[0099] Nachdem die RTC 24 im Benutzermedium 1 mindestens einmal durch die Referenzzeitinformation 10 synchronisiert worden ist, wird zeitlich unabhängig (typischerweise Minuten, Stunden oder unter Umständen auch Tage später) von der Synchronisation der RTC 24 die NFC-Kommunikationsverbindung zwischen dem ersten Kommunikationsmodul 20 und dem zweiten Kommunikationsmodul 21 etabliert. Danach wird eine dem RTC 24 entstammende Zeitangabe als gesicherte Zeitinformation 11 verwendet und diese gesicherte Zeitinformation 11 vom ersten SE 22 an das erste Kommunikationsmodul 20 und über die NFC-Kommunikationsverbindung zum zweiten Kommunikationsmodul 21 an das Dienstmedium 2 übermittelt. Somit ist dem Dienstmedium 2 eine gesicherte Zeitinformation 11 zur Verfügung gestellt.

[0100] Alternativ zu diesem Vorgehen kann auch der Zeitgeber im Benutzermedium eine relative Zeit herausgeben, und die Berechnung der aktuellen Zeit erfolgt bei der Authentifizierung anhand der abgespeicherten Referenzzeitinformation und dieser relativen Zeit ausserhalb des Zeitgebers aber bevorzugt innerhalb der GU.

[0101] Der Authentifizierungsprozess in Fig. 3 zwischen dem Dienstmedium 2 und dem Benutzermedium 1 wird analog zum Kommunikationssystem in Fig. 1 vorgenommen.

[0102] Die Synchronisierung des RTC - oder allgemeiner die Übermittlung der Referenzzeitinformation an das Benutzermedium - kann in den, offline'-Ausführungsformen (d.h. den Ausführungsformen, bei denen kein gleichzeitiger Kontakt zwischen Quelle und Benutzermedium einerseits und Benutzermedium und zweitem Medium andererseits vorausgesetzt wird und das Benutzermedium dafür einen Zeitgeber aufweist - bspw. jeweils beim Aufladen eines elektronischen Schlüssels oder Tickets oder dergleichen geschehen. Ergänzend oder alternativ kann es in regelmässigen Abständen geschehen, bzw. dann, wenn eine Verbindung zwischen der vertrauenswürdigen Quelle und dem Benutzermedium vorhanden ist.

[0103] Fig. 4 zeigt ein Kommunikationssystem wie in Fig. 3 aber zusätzlich mit einer zweiten GU und einem ersten und zweiten Schlüssel. Dieses Kommunikationssystem unterscheidet sich von demjenigen in Fig. 3 also dadurch, dass das Dienstmedium 2 analog zu Fig. 2 eine zweite GU in Form eines zweiten SE 23 aufweist. Zudem umfasst das erste SE 22 einen ersten Schlüssel 30, und das zweite SE 23 umfasst einen zweiten Schlüssel 31 (im Falle von symmetrischer Verschlüsselung sind der erste und der zweite Schlüssel identisch). Wie an sich von SEs bekannt, können der erste und zweite Schlüssel Sicherheitsschlüssel sein, welche vom Erzeuger des SE implementiert sind und dem Betreiber selbst nicht bekannt sind. In Fig. 4 ist zusätzlich in jedem SE jeweils ein eigener sicherer Prozessor dargestellt, da mindestens ein sicherer Prozessor definitionsgemäss von jedem SE umfasst wird. Somit sind in Fig. 4 im ersten SE 22 ein sicherer Prozessor 32 des ersten SE 22 und im zweiten SE 23 ein sicherer Prozessor 33 des zweiten SE 23 dargestellt.

[0104] Grundsätzlich verläuft in Fig. 4 das Verfahren, dem Dienstmedium 2 das gesicherte Zeitsignal 11 zur Verfügung zu stellen, analog zum entsprechenden Verfahren wie bereits zu Fig. 3 beschrieben. Im Unterschied zu Fig. 3 wird aber in Fig. 4 die gesicherte Zeitinformation 11, welche der RTC 24 entstammt, vor einem Verlassen des ersten SE 22 unter Verwendung des ersten Schlüssels 30 verschlüsselt und erst danach an das erste Kommunikationsmodul 20 übermittelt. Das Verschlüsseln erfolgt im sicheren Prozessor 32 des ersten SE 22. Die verschlüsselte, gesicherte Zeitinformation wird dann über die NFC-Kommunikationsverbindung an das zweite Kommunikationsmodul 21 und schliesslich in das zweite SE 23 übermittelt. Im zweiten SE 23 entschlüsselt der sichere Prozessor 33 unter Verwendung des zweiten Schlüssels 31 die verschlüsselte gesicherte Zeitinformation, wodurch schlussendlich die gesicherte Zeitinformation 11 im zweiten SE 23 verfügbar ist.

[0105] Vorteil von dieser Methode ist eine sehr hohe Manipulationssicherheit des Verfahrens und des Kommunikationssystems, da die gesicherte Zeitinformation 11 ausserhalb einer GU nicht unverschlüsselt zugänglich ist. Somit ist eine Manipulation selbst innerhalb des Benutzermediums 1 und/oder des Dienstmediums 2 erschwert oder verunmöglicht.

[0106] Die Verschlüsselung und Entschlüsselung durch die sicheren Prozessoren der jeweiligen SE unter Verwendung von Schlüsseln erfolgen dabei nach bekannten Methoden. Da die Schlüssel von den jeweiligen SE umfasst sind, sind diese in einem hohen Masse gesichert. Das Zusammenspiel der Schlüssel und das zur Verfügung stellen der Schlüssel erfolgt ebenfalls nach bekannten Methoden. Die Schlüssel bestehen beispielsweise je aus verschiedenen Quellen stammenden Teilschlüsseln, was eine hohe Sicherheit des Verfahrens und des Kommunikationssystems zur Folge hat.

[0107] Auch der Authentifizierungsprozess in Fig. 4 zwischen dem Dienstmedium 2 und dem Benutzermedium 1 wird analog zum Kommunikationssystem in Fig. 1 vorgenommen.

[0108] Fig. 5 zeigt ein Kommunikationssystem wie in Figur 4, welches aber zusätzlich ein Managermedium 4 umfasst. In Fig. 5 verläuft das Verfahren, dem Dienstmedium 2 das gesicherte Zeitsignal 11 zur Verfügung zu stellen, analog zum entsprechenden Verfahren wie bereits zu Fig. 4 beschrieben. Zusätzlich ist in Fig. 5 ein Managermedium 4 dargestellt, welches dazu befähigt ist, dem ersten SE 22 eine Authentifizierungsinformation 12 zu übermitteln. Dabei übermittelt das Managermedium 4 dem ersten SE 22 die Authentifizierungsinformation 12 auf eine bekannte Weise analog zum TSM 3, wobei aber die Übermittlung vom Managermedium 4 an das erste SE 22 unabhängig von der Übermittlung vom TSM 3 an das erste SE 22 erfolgen kann.

[0109] Die Authentifizierungsinformation 12 umfasst einen zeitlich nur beschränkt gültigen elektronischen Schlüssel bzw. ein zeitlich nur beschränkt gültiges elektronisches Ticket oder einen definierten Zeitraum und dazugehörige Angaben über eine Identität mindestens eines Dienstmediums 2. Während dieses definierten Zeitraums sind die mittels der Angaben über die Identität eindeutig festgelegten Dienstmedien 1 dazu befähigt, ein ihnen diese Authentifizierungsinformation 12 übermittelndes Benutzermedium 1 im Authentifizierungsprozess als ein zur Autorisation berechtigtes Benutzermedium 1 zu erkennen. Mit anderen Worten ist das Benutzermedium 1 während dieses definierten Zeitraums zur Autorisierung freigegeben.

[0110] Im Authentifizierungsprozess benutzt das Dienstmedium 2 also die ihm durch das Benutzermedium 1 (und schlussendlich durch den TSM 3) zur Verfügung gestellte gesicherte Zeitinformation 11, um zwischen dem Dienstmedium 2 und dem Benutzermedium 1 basierend auf der gesicherten Zeitinformation 11 zu entscheiden, ob eine Autorisierung des Benutzermediums 2 erfolgen darf oder nicht.

[0111] Die Authentifizierungsinformation 12 wird dabei analog zur gesicherten Zeitinformation 11 vor einem Verlassen des ersten SE 22 unter Verwendung des ersten Schlüssels 30 verschlüsselt und erst danach an das erste Kommunikationsmodul 20 übermittelt. Die Verschlüsselung, Übermittlung und Entschlüsselung der Authentifizierungsinformation 12 erfolgen dabei analog zu denselben Schritten für die gesicherte Zeitinformation. Daher weisen die analogen Schritte auch dieselben Vorteile auf.

[0112] In Fig. 6 ist eine Ausführungsform dargestellt, bei welcher die Authentifizierung im SE 20 des Benutzermediums 1 stattfindet. Bei dieser Ausführungsform sind bei der Authentifizierung die Rollen von Benutzermedium 1 und zweitem Medium 2 vertauscht, das zweite Medium nimmt quasi für die Authentifizierung die Rolle des «Benutzers» ein.

[0113] Das zweite Medium 2 beinhaltet eine Identifikationsinformation 51, anhand welcher das Benutzermedium 1 feststellt, ob und ggf. in welchem Umfang das Benutzermedium 1 berechtigt ist, zum aktuellen Zeitpunkt einen durch das zweite Medium identifizierten Dienst zu beanspruchen. Dadurch, dass der Authentifizierungsprozess im Benutzermedium im SE stattfindet, ist trotzdem sichergestellt, dass der Träger bzw. aktuelle Inhaber des Benutzermediums sich nicht Rechte

verschaffen kann, die ihm eigentlich nicht zustehen. Das SE ist wie an sich bekannt so eingerichtet, dass nur autorisierte Institutionen - bspw-. ein Netzbetreiber, wenn das SE eine SIM-Karte oder ein Teil einer SIM-Karte ist -Umkonfigurierungen oder Umprogrammierungen vornehmen können.

[0114] In der Ausführungsform gemäss Fig. 6 hat das zweite Medium eine rein passive Rolle: es dient lediglich der Identifikation des verlangten Dienstes. Entsprechend kann das zweite Medium optional rein passiv ausgestaltet sein, d.h. bspw. als RFID-Tag ohne eigene Energiequelle. Aber auch die Ausgestaltung als aktiv betriebenes, d.h. Signale mit eigener Signalleistung aussendendes Medium ist möglich in dieser Ausführungsform, bspw. dann, wenn die Reichweite der Kommunikation mit passiven Tags nicht ausreicht.

[0115] Das Prinzip der Ausführungsform von Fig. 6 (Authentifizierung im SE des Benutzermediums) kann sowohl für online- als auch für Offline-Ausführungsformen - letztere mit Zeitgeber im SE bzw. in einer anderen GU des Benutzermediums -verwendet werden.

[0116] Auch darüber hinaus sind viele weitere Ausführungsformen denkbar. Bspw. ist die Verwendung eines TSM als vertrauenswürdige Quelle keine Bedingung. Je nach gewähltem Sicherheitsstandard kann auch eine andere Quelle -bspw. ein dafür vorgesehener Server einer Applikation - verwendet werden, welche sich bspw. gegenüber der entsprechenden GU authentifizieren muss.

[0117] In allen Ausführungsformen kann das Benutzermedium physisch ein Mobiltelefon mit GU sein. Es ist auch möglich, die hier beschriebenen Funktionen der GU auf mehrere gesicherte Umgebungen (insbesondere SEs) zu verteilen. Bspw. kann in der Ausführungsform der Fig.6 der Authentifizierungsprozess im Prinzip in einer anderen GU durchgeführt werden als der GU, in welcher die gesicherte Zeitinformation aufbewahrt bzw. aus der Referenzzeitinformation ermittelt wird. Durch eine Benutzermedium-interne verschlüsselte Kommunikationsverbindung wird dann die gesicherte Zeitinformation für den Authentifizierungsprozess übermittelt.

Patentansprüche

1. Verfahren, um insbesondere für einen Authentifizierungsprozess zwischen einem Benutzermedium (1) und einem zweiten Medium eine gesicherte Zeitinformation (11) zur Verfügung zu stellen, wobei das Benutzermedium (1) ein erstes Kommunikationsmodul (20) und eine erste gesicherte Umgebung (22) und das zweite Medium (2) ein zweites Kommunikationsmodul (21) aufweist, umfassend folgende Schritte:
   Schritt 1: Übermitteln einer Referenzzeitinformation (10) an die erste gesicherte Umgebung (22),
   Schritt 2: Erstellen einer Kommunikationsverbindung zwischen dem ersten Kommunikationsmodul (20) und dem zweiten Kommunikationsmodul (21),
   Schritt 3: Übermitteln einer auf der Referenzzeitinformation (10) beruhenden gesicherten Zeitinformation (11) an das zweite Medium und/oder Verwenden der auf der Referenzzeitinformation (10) beruhenden gesicherten Zeitinformation (11) für den Authentifizierungsprozess.
2. Verfahren gemäss Anspruch 1, dadurch gekennzeichnet, dass die gesicherte Zeitinformation (11) die Referenzzeitinformation (10) umfasst und Schritt 3 gleichzeitig mit Schritt 1 erfolgt oder innerhalb eines vorbestimmten Zeitraums nach Schritt 1 erfolgt.
3. Verfahren gemäss einem der Ansprüche 1 bis 2, dadurch gekennzeichnet, dass Schritt 1 zeitlich unabhängig von Schritt 2 und Schritt 3 erfolgt, wobei die gesicherte Zeitinformation (11) funktional zusammenhängt mit einem zeitlichen Unterschied zwischen einer Ausführung von Schritt 1 und einer Ausführung von Schritt 3.
4. Verfahren gemäss einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass das Benutzermedium (1) einen Zeitgeber (24), umfasst, wobei die gesicherte Zeitinformation aus der Referenzzeitinformation (10) und Angaben des Zeitgebers ermittelt wird, beispielsweise indem der Zeitgeber eine Echtzeituhr ist, die in Schritt 1 mittels der Referenzzeitinformation (24) zeitlich synchronisiert wird.
5. Verfahren gemäss einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass das zweite Medium (2) eine zweite gesicherte Umgebung (23) umfasst und in Schritt 3 das zweite Kommunikationsmodul (21) die gesicherte Zeitinformation (11) an die zweite gesicherte Umgebung (23) übermittelt.
6. Verfahren gemäss einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass das zweite Medium (2) eine Echtzeituhr aufweist, welche in Schritt 3 mittels der gesichelten Zeitinformation (11) zeitlich synchronisiert wird.
7. Verfahren gemäss einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass in Schritt 2 die Kommunikationsverbindung nach einem bekannten Standard erstellt wird und insbesondere als NFC, Bluetooth oder andere kurzreichweitige Kommunikationsverbindungen erstellt wird.
8. Verfahren gemäss einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass in Schritt 2 die Kommunikationsverbindung nach einem bekannten gesicherten Standard erstellt wird und die Kommunikation über die Kommunikationsverbindung insbesondere verschlüsselt erfolgt.
9. Verfahren gemäss einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass die vertrauenswürdige Quelle die Voraussetzungen für einen Trusted Service Manager gemäss Standards der Nahfeldkommunikation erfüllt.

10. Authentifizierungsprozess zwischen einem Benutzermedium (1) und einem zweiten Medium (2), wobei zunächst nach dem Verfahren gemäss einem der vorangehenden Ansprüche eine gesicherte Zeitinformation zur Verfügung gestellt wird und anschliessend eine davon funktional abhängige Zeitinformation zur Authentifizierung unter Verwendung von Daten des Benutzermediums und des zweiten Mediums verwendet wird.

11. Authentifizierungsprozess gemäss Anspruch 10, wobei die Authentifizierung durch das zweite Medium erfolgt und die gesicherte Zeitinformation direkt als die Zeitinformation verwendet wird, wobei das zweite Medium bspw. keinen Zeitgeber aufweist.

12. Authentifizierungsprozess gemäss Anspruch 10, wobei die Authentifizierung durch das zweite Medium erfolgt, das zweite Medium einen Zeitgeber aufweist und das zweite Medium die funktional abhängige Zeitinformation mittels des Zeitgebers aus der gesicherten Zeitinformation ermittelt.

13. Authentifizierungsprozess gemäss Anspruch 10, wobei die Authentifizierung durch das Benutzermedium erfolgt und die gesicherte Zeitinformation direkt als die Zeitinformation verwendet wird, wobei das zweite Medium bspw. keinen Zeitgeber aufweist.

14. 14. Kommunikationssystem, umfassend
- ein Benutzermedium (1), welches ein erstes Kommunikationsmodul (20) und eine erste gesicherte Umgebung (GU, 22) umfasst, und
- ein zweites Medium (2), welches ein zweites Kommunikationsmodul (21) umfasst, wobei
- das Benutzermedium und/oder das zweite Medium eingerichtet ist, einen Authentifizierungsprozess durchzuführen, in welchem das eine Berechtigung des Benutzermediums gegenüber dem Dienstmedium geprüft wird
- die erste gesicherte Umgebung (22) derart ausgebildet ist, dass sie zu einem Empfang von gesicherten Daten befähigt ist,
- die erste gesicherte Umgebung (22) funktional mit dem ersten Kommunikationsmodul (20) verknüpft ist,
- das erste Kommunikationsmodul (20) und das zweite Kommunikationsmodul (21) derart ausgebildet sind, dass sie zu einem Aufbau einer Kommunikationsverbindung zwischen sich befähigt sind,
dadurch gekennzeichnet, dass
- die erste gesicherte Umgebung (22) derart ausgebildet ist, dass sie zu einem Übermitteln einer auf der Referenzzeitinformation (10) beruhenden gesicherten Zeitinformation (11) über die Kommunikationsverbindung an das zweite Medium (2) befähigt ist, oder
- das Benutzermedium befähigt ist, in der ersten gesicherten Umgebung einen Authentifizierungsprozess anhand von vom zweiten Medium (2) empfangenen Daten und auf der Referenzzeitinformation (10) beruhenden gesicherten Zeitinformation (11) durchzuführen.

15. Kommunikationssystem gemäss Anspruch 14 dadurch gekennzeichnet, dass die erste gesicherte Umgebung (22) derart ausgebildet ist, dass sie zum Empfang der Referenzzeitinformation (10) und gleichzeitig oder unmittelbar danach zum Übermitteln der gesicherten Zeitinformation (11) von der ersten gesicherten Umgebung (22) durch die Kommunikationsverbindung an das zweite Medium (2) oder zum Durchführen des Authentifizierungsprozesses befähigt ist.

16. Kommunikationssystem gemäss einem der Ansprüche 14 bis 15, dadurch gekennzeichnet, dass die erste gesicherte Umgebung (22) einen Zeitgeber beinhaltet und derart ausgebildet ist, dass sie zum Empfang der Referenzzeitinformation (10) und davon zeitlich unabhängig zum Übermitteln der gesicherten Zeitinformation (11) bzw. zum Durchführen des Authentifizierungsprozesses befähigt ist.

17. Kommunikationssystem gemäss einem der Ansprüche 14 bis 16, dadurch gekennzeichnet, dass das zweite Medium (2) eine zweite gesicherte Umgebung (23) umfasst, wobei die zweite gesicherte Umgebung (23) funktional mit dem zweiten Kommunikationsmodul (21) verknüpft ist.

18. Kommunikationssystem gemäss einem der Ansprüche 14 bis 17, dadurch gekennzeichnet, dass das zweite Medium (2) einen Zeitgeber umfasst.

19. Kommunikationssystem gemäss einem der Ansprüche 14 bis 18, dadurch gekennzeichnet, dass das zweite Medium (2) eingerichtet ist, einen Authentifizierungsprozess durchzuführen, bei welchem das zweite Medium (2) das Benutzermedium (1) authentifiziert.

20. Kommunikationssystem gemäss einem der Ansprüche 14 bis 19, dadurch gekennzeichnet, dass das Kommunikationssystem ferner ein Managermedium (4) umfasst, welches funktional mit der ersten gesicherten Umgebung (22) verknüpft ist und dass die erste gesicherte Umgebung (22) derart ausgebildet ist, dass sie zum Empfangen einer Authentifizierungsinformation (12) vom Managermedium (4) befähigt ist.

21. Benutzermedium, eingerichtet für einen Authentifizierungsprozess mit einem zweiten Medium, insbesondere über RFID, aufweisend ein erstes Kommunikationsmodul (20) und eine erste gesicherte Umgebung (GU, 22), wobei das Benutzermedium eingerichtet ist, ein Verfahren mit folgenden Schritten durchzuführen:
- Schritt 1: Empfangen einer Referenzzeitinformation (10) von einer ausserhalb des Benutzermediums angeordneten vertrauenswürdigen Quelle und Übergabe an die erste gesicherte Umgebung (22),

- Schritt 2: Erstellen einer Kommunikationsverbindung zwischen dem ersten Kommunikationsmodul (20) einem Kommunikationsmodul (21) des zweiten Mediums,
- Schritt 3: Obermitteln einer auf der Referenzzeitinformation (10) beruhenden gesicherten Zeitinformation (11) an das zweite Medium und/oder Durchführen des Authentifizierungsprozesses unter Verwendung der auf der Referenzzeitinformation (10) beruhenden gesicherten Zeitinformation (11) für den Authentifizierungsprozess.

22. Computerprogramm, welches auf ein Kommunikationsmedium mit einem ersten Kommunikationsmodul und einer ersten gesicherten Umgebung ladbar ist, und welches bei Ausführung das Kommunikationsmedium ein Verfahren mit den folgenden Schritten ausführen lässt:
- Schritt 1: Empfangen einer Referenzzeitinformation (10) von einer ausserhalb des Benutzermediums angeordneten vertrauenswürdigen Quelle und Übergabe an die erste gesicherte Umgebung (22),
- Schritt 2: Erstellen einer Kommunikationsverbindung zwischen dem ersten Kommunikationsmodul (20) einem Kommunikationsmodul (21) des zweiten Mediums,
- Schritt 3: Übermitteln einer auf der Referenzzeitinformation (10) beruhenden gesicherten Zeitinformation (11) an das zweite Medium (2) und/oder Durchführen des Authentifizierungsprozesses unter Verwendung der auf der Referenzzeitinformation (10) beruhenden gesicherten Zeitinformation (11) für den Authentifizierungsprozess.

23. Datenträger, enthaltend ein Computerprogramm gemäss Anspruch 22.

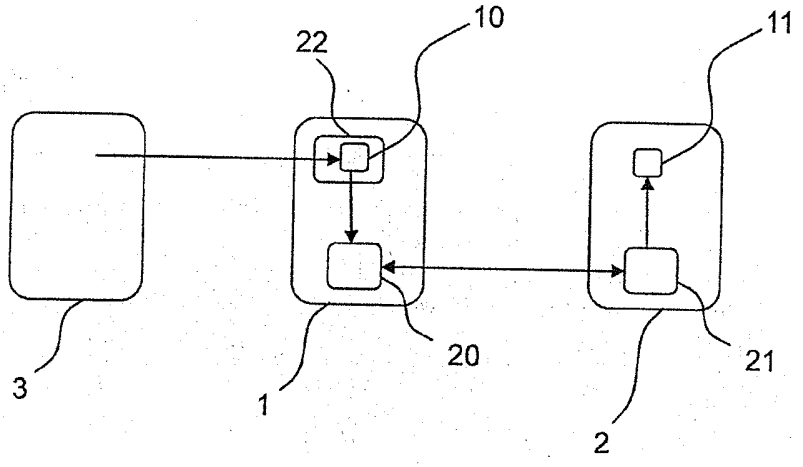


Fig. 1

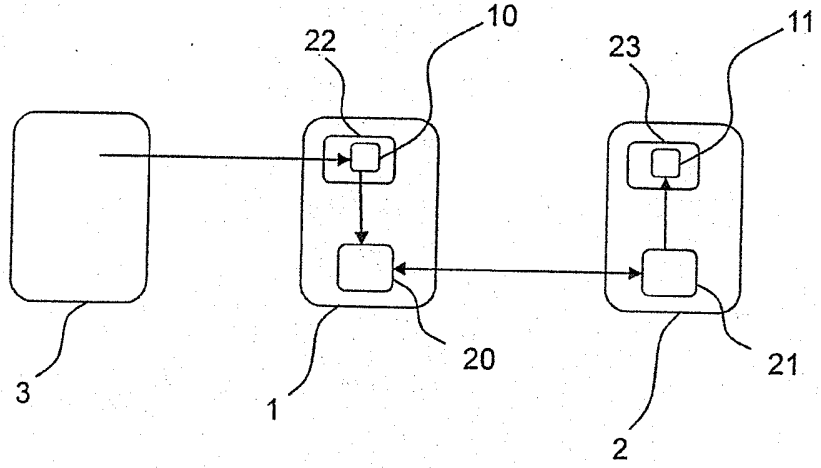


Fig. 2

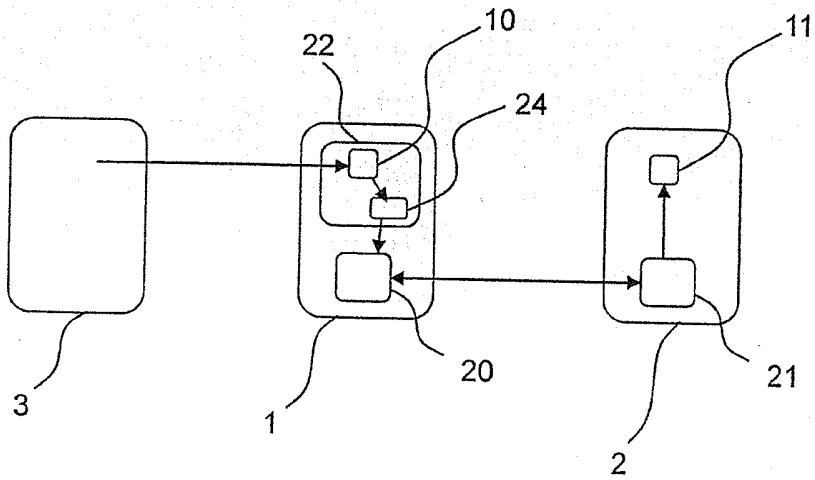


Fig. 3

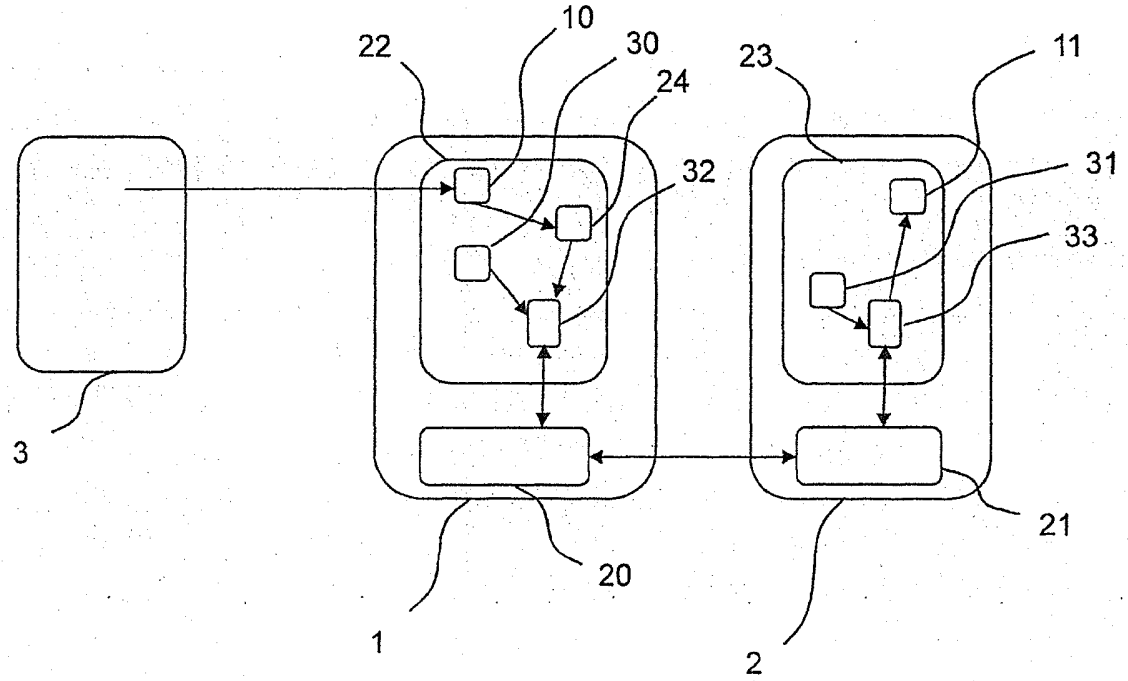

10
22
30
24
23
11
32
31
33
3
21
20
1
2

Fig. 4

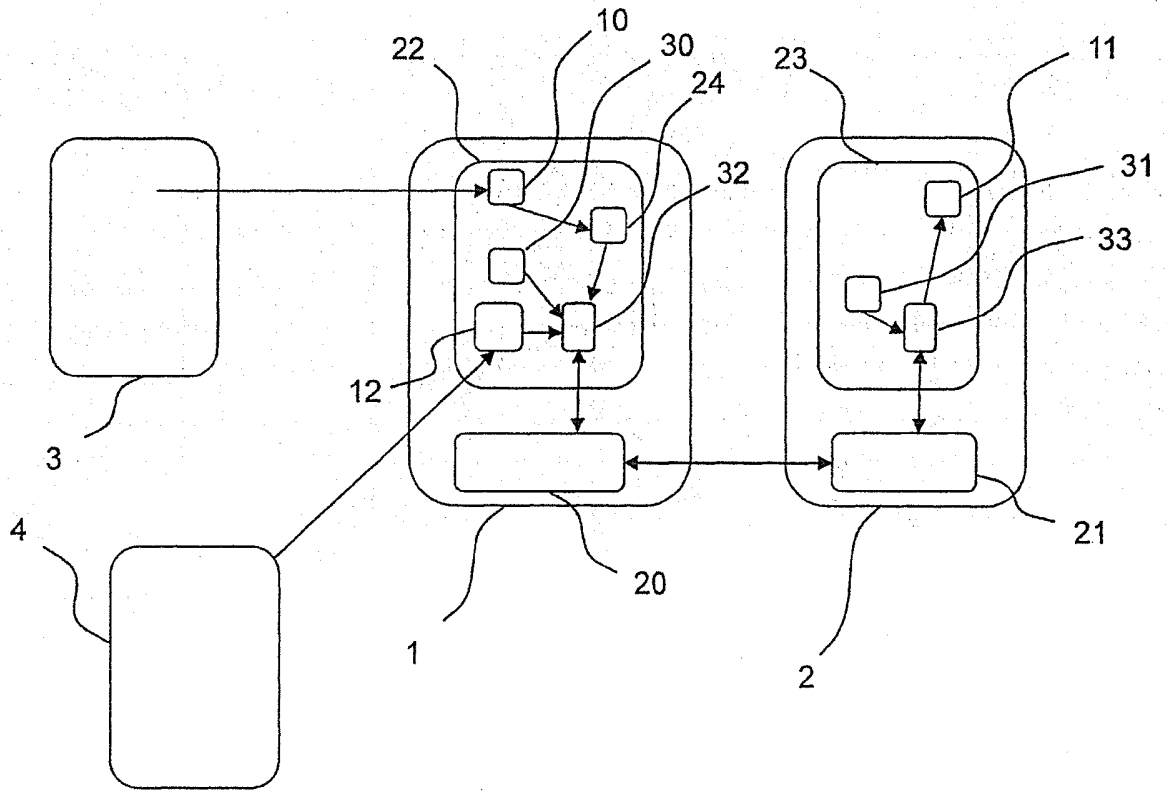

10
22
30
24
23
11
32
31
33
12
3
4
21
20
1
2

Fig. 5

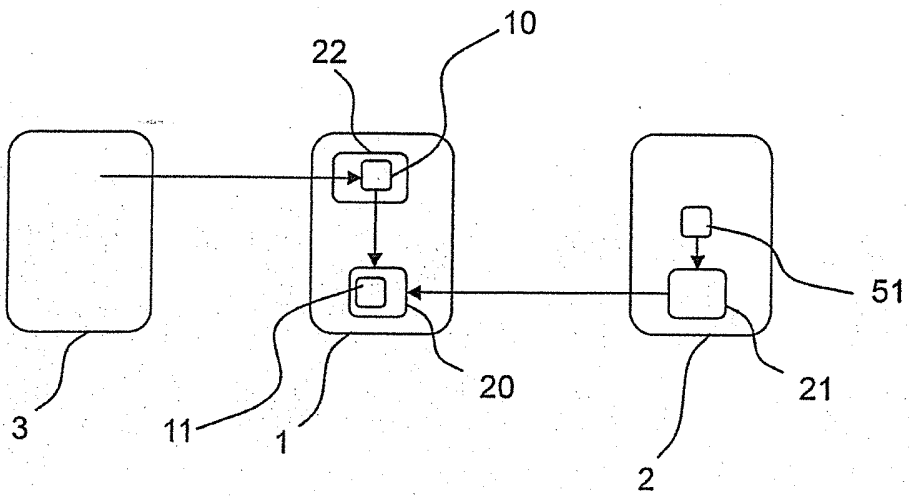


Fig. 6