(19) SCHWEIZERISCHE EIDGENOSSENSCHAFT
EIDGENÖSSISCHES INSTITUT FÜR GEISTIGES EIGENTUM

(11) **CH 708 199 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: 01026/13

(22) Anmeldedatum: 29.05.2013

(43) Anmeldung veröffentlicht: 15.12.2014

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

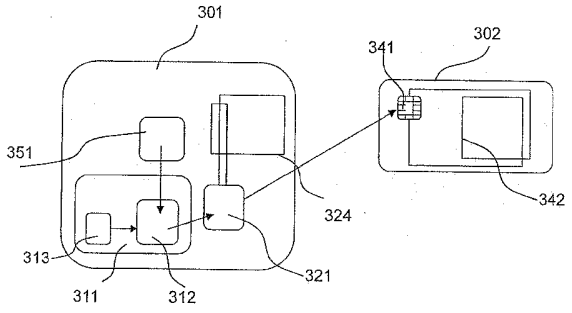
(72) Erfinder:
Paul Studerus, 8165 Oberweningen (CH)
André Lüscher, 8706 Feldmeilen (CH)

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

(54) Verfahren zur Verwaltung von Medien für die drahtlose Kommunikation.

(57) Gemäss einem Aspekt der Erfindung wird ein Verfahren zum Durchführen eines Schreib- und/oder -leseprozesses, unter Verwendung eines ersten, aktiv betriebenen Mediums (301), auf bzw. von einem passiv betriebenen zweiten Medium (302) zur Verfügung gestellt, wobei das erste Medium eine gesicherte Umgebung (311) aufweist, und das Verfahren folgende Schritte beinhaltet:

- Zur-Verfügung-Stellen eines Schreib- und/oder Leseapplets (312) in der gesicherten Umgebung (311),
- Zur-Verfügung-Stellen einer Applikation (351) ausserhalb der gesicherten Umgebung,
- Übermitteln eines Schreib- und/oder Lesebefehls durch die Applikation an das Applet,
- Umsetzen des Schreib- und/oder Lesebefehls in ein Schreib- und/oder Lesesignal durch das Applet, und
- Übermitteln des Schreib- und/oder Lesesignals an das passiv betriebene zweite Medium (302).



Beschreibung

[0001] Die Erfindung bezieht sich auf Verfahren und Vorrichtungen auf dem Gebiet der drahtlosen Kommunikation, insbesondere der Nahfeld-Kommunikation (NFC). 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. Die Erfindung betrifft in Aspekten jedoch auch andere Standards der kurzreichweitigen drahtlosen Kommunikation, bzw. Bluetooth, Millimetre Wave Gigabit Wireless (Wireless GIGE), wireless LAN, wireless USB, Infrarot etc.

[0002] NFC-Kommunikationsverbindungen sind standardisierte, kurzreichweitige Verbindungen, welche im Stand der Technik vielseitig und breit angewendet werden. Beispielsweise werden NFC-Kommunikationsverbindungen zur Überprüfung einer Zutrittsberechtigung vorgeschlagen oder gar schon benutzt, etwa für Skitickets an Skiliftzutrittseinrichtungen, für Kraftfahrzeugschlüsseln und dem entsprechenden Kraftfahrzeug, für Hotelzimmerschlüssel und Hotelzimmer oder bei Mitarbeiterausweisen an Türen und/oder an Arbeitszeiterfassungseinrichtungen. Aber auch für die Bezahlung von Kleinbeträgen an entsprechenden Zahlungseinrichtungen und zur Datenübertragung, etwa von Bildern von einem ersten Mobiltelefon zu einem zweiten Mobiltelefon, sind NFC-Systeme interessant.

[0003] Ein erster Aspekt der Erfindung betrifft Dienstmedien (bspw. in Schlössern eingebaute Lese- oder Schreib- und Leseeinrichtungen (Kontrollmodule) für die Zugangskontrolle oder Wertkarten-Abbuchgeräte, Ticketkontroll- und/oder Entwertungsgeräte etc.) und deren Verwaltung. Er betrifft insbesondere den Fall, in welchem solche Dienstmedien nicht online und unmittelbar über eine gesicherte Verbindung mit einem, Trusted Service Manager' (TSM) oder einer anderen vertrauenswürdigen Instanz verbunden sind, wie das in der Zugangskontrolle und bei einfacheren Lese- bzw. Schreib- und Lesegeräten oft der Fall ist, bspw. weil diese als batteriebetriebene Standalone-Geräte konzipiert sind.

[0004] Der erste Aspekt bezieht sich konkret auf ein Verfahren zur Verwaltung eines Dienstmediums durch eine Verwaltungsinstanz, insbesondere einen vertrauenswürdigen Vermittler (trusted service manager, TSM). Dieses zweite Medium kann bspw. eine zweite GU aufweisen, welche zu verwalten ist. Das zweite Medium weist ein Kommunikationsmodul auf.

[0005] Eine GU - die nachfolgend diskutierten Eigenschaften und Definitionen der GU und des TSM gelten für alle Aspekte der Erfindung - ist beispielsweise eine so genannte sichere Umgebung (Englisch: secure environment (SE); oft findet man auch den Begriff Secure-Element (SE) in der Literatur). Sichere Umgebungen (SEs) als Chips mit CPU und Speicher und mit normierten Sicherheitsstandards sind mit für unterschiedliche Anwendungen erhältlich.

[0006] Ein SE (im Sinne von «sicheres Element») 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.

[0007] 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.

[0008] 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, Micro-SD-Karte oder dergleichen) umfasst sein oder von anderen elektronischen Geräten wie z.B. Mobiltelephonen, Uhren, RFID-Karten, RFID-Lesegeräten, Schlüsseln mit Mikrochips, Schlössern, Verkaufsautomaten, Zahlungsterminals, portablen elektronischen Geräten wie etwa Tabletcomputern und Ähnlichem umfasst sein.

[0009] 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.

[0010] 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.

[0011] 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 vorhanden.

[0012] 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. Global-Plattform-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.

[0013] 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.

[0014] Ein vertrauenswürdiger Vermittler (trusted Service manager, TSM) ist eine an sich bekannte Einrichtung in Nahfeldkommunikationssystemen (NFC-Systemen). Der TSM ist befähigt, Secure Elements (bzw. allgemein GUs) zu verwalten, d.h. zu beschreiben. Beispielseise können Firmware-Updates, Schlüsselwechsel etc. durchgeführt werden.

[0015] In diesem Text erwähnte TSM erfüllen bspw. die Voraussetzungen gemäss dem NFC-Standard.

[0016] Ein TSM ist derart ausgebildet, dass er zu einer sicheren Übermittlung von Informationen in eine GU befähigt ist. Die Übermittlung erfolgt dabei gesichert und manipulationsgeschützt. Sie kann kontaktbehaftet oder - die häufigere Variante frei von physischem Kontakt zwischen TSM und GU erfolgen. Ein typisches Beispiel eines TSM ist ein Anbieter eines Mobiltelefonnetzes (mobile network operator MNO), welcher durch das Mobiltelefonnetz Daten frei von physischem Kontakt und gesichert an eine GU in einem Mobiltelefon übermittelt.

[0017] Zu diesem Zweck ist jedoch die genannte unmittelbare, meist kontaktlose Verbindung zum entsprechenden Medium mit dem SE nötig, was in den hier diskutierten Fällen nicht unbedingt der Fall ist.

[0018] Für die Wartung von Dienstmedien - bspw. mit GU - die nicht online sind, entsteht daher bei der Wartung, soweit diese überhaupt möglich ist, ein hoher Aufwand. Insbesondere sind Aktualisierungen (updaten) von Systemparametern und/oder Software (insbesondere von Firmware) und Reparatur aufwändig, zeitintensiv und kostspielig, da sich eine vertrauenswürdige Wartungsperson mit eigens dafür eingerichteten gesicherten Mitteln zum einem solchen Dienstmedium begeben muss.

[0019] Es ist deshalb Aufgabe des ersten Aspekts der Erfindung, ein Verfahren und ein Kommunikationssystem der eingangs genannten Art zu schaffen, welche mindestens einen Teil der oben genannten Nachteile mindestens teilweise vermeidet.

[0020] Das Verfahren gemäss dem ersten Aspekt der Erfindung umfasst folgende Schritte:

- Schritt 1: Übertragen einer ersten Verwaltungsinformation von einer Verwaltungsinstanz an eine von einem ersten, mobilen Medium umfasste erste GU,
- Schritt 2: Erstellen einer Kommunikationsverbindung zwischen einem vom ersten Medium umfassten ersten Kommunikationsmodul und dem zweiten Kommunikationsmodul,
- Schritt 3: Übertragen einer aus der ersten Verwaltungsinformation abgeleiteten zweiten Verwaltungsinformation von der ersten GU an das erste Kommunikationsmodul und über die Kommunikationsverbindung an das zweite Kommunikationsmodul.

[0021] Sofern das Dienstmedium eine (hier «zweite GU» genannte) gesicherte Umgebung aufweist und die die zu wartenden Teile des Dienstmediums in der zweiten GU sind, wird die zweite Verwaltungsinformation schliesslich an die zweite GU übertragen.

[0022] Dabei können die jeweiligen Kommunikationsmodule oder Teile davon Bestandteile der jeweiligen GUs sein, oder die Kommunikationsmodule können separat sein.

[0023] Die Verwaltungsinstanz kann insbesondere ein Trusted Service Manager sein.

[0024] Die Kommunikationsverbindung ist beispielsweise eine NFC-Kommunikationsverbindung.

[0025] Die zweite Verwaltungsinformation ist aus der ersten Verwaltungsinformation abgeleitet. Bspw. umfasst die erste Verwaltungsinformation die zweite Verwaltungsinformation. Insbesondere, können die erste und die zweite Verwaltungsinformation identisch sein. Es ist auch möglich, dass die zweite Verwaltungsinformation die erste Verwaltungsinformation umfasst. Insbesondere kann die erste Verwaltungsinformation die zweite Verwaltungsinformation sowie optional zusätzlichen Informationen wie etwa eine Identifikation des zu verwaltenden zweiten Mediums aufweisen. Auch andere Arten der Ableitung/Verarbeitung der ersten Verwaltungsinformation zur zweiten Verwaltungsinformation sind denkbar.

[0026] Weil das zweite Medium die zweite Verwaltungsinformation von der Verwaltungsinstanz (d.h. im hier diskutierten Beispiel vom TSM) über die erste Verwaltungsinformation und das erste Medium übermittelt bekommt, kann das Verfahren die oben beschriebenen Aufgaben erfüllen. Somit wird das zweite Medium also dank des oben beschriebenen Verfahrens durch den TSM verwaltet, ohne dass das zweite Medium online mit dem TSM verbindbar sein muss.

[0027] Das erste Medium kann insbesondere zur peer-to-peer Kommunikation über NFC befähigt sein, und es kann ein mobiles Gerät oder Teil eines mobilen Geräts, insbesondere ein Mobiltelefon sein.

[0028] Anstelle von peer-to-peer NFC kann auch eine andere Kommunikationsverbindung dazu dienen, die erste Verwaltungsinformation von der Verwaltungsinstanz an das erste Medium zu übermitteln, bspw. bluetooth, WLAN, Infrarot, etc.

Ergänzend oder alternativ dazu kann auch die Kommunikationsverbindung zwischen erstem und zweitem Medium über eine von NFC verschiedene Kommunikationsverbindung geschehen, bspw. bluetooth, WLAN, Infrarot etc. vorausgesetzt das zweite Medium ist dafür eingerichtet.

[0029] Somit erlaubt das Verfahren, auch ein zweites Medium mit einfachem Aufbau und ohne online-Kommunikationsmöglichkeit über Methoden und Protokolle zu verwalten, wie sie für die Verwaltung von SEs bspw. in Smartphones bekannt sind.

[0030] Von Vorteil ist auch, dass beispielsweise bei jedem Aufbau einer NFC-Kommunikationsverbindung zwischen dem zweiten Medium und einem beliebigen ersten Medium die Möglichkeit besteht, vom ersten Medium an das zweite Medium die zweite Verwaltungsinformation zu übermitteln. Somit kann die Verwaltung der zweiten GU durch zweite Medien etwa mit anderen Interaktionen zwischen dem ersten und dem zweiten Medium kombiniert werden. Die Verwaltung kann sozusagen nebenher bei sich ergebenden Gelegenheiten erfolgen.

[0031] Zur besseren Veranschaulichung sei folgendes Beispiel beschrieben: in einem Hotel sollen zweite Medien, welche als Kontrollmodule von Türschlössern ausgebildet sind, durch einen TSM mit nicht sicherheitsrelevanten Wartungsdaten (bspw. eine Anpassung eines auf einem Display anzuzeigenden Texts) versehen werden. Setzt das Hotel als Türschlüssel etwa eine emulierte RFID-Karte eines Mobiltelefons ein, kann das Mobiltelefon als erstes Medium benutzt werden. Der TSM übermittelt die erste Verwaltungsinformation in die vom Mobiltelefon umfasste erste GU. Beim Einsatz des Mobiltelefons als Schlüssel zum Öffnen der Hoteltür wird eine NFC-Kommunikationsverbindung verwendet, welche neben der primären Interaktion des Mobiltelefons mit dem Kontrollmodul des Türschlosses, zum Öffnen des Türschlosses, auch für die Übermittlung der Wartungsdaten des Türschlosses durch die Übermittlung der zweiten Verwaltungsinformation benutzt wird. In diesem Fall werden die Wartungsdaten des Türschlosses über das Mobiltelefon erneuert, wobei diese vom TSM stammen. Auf eine separate Interaktion zwischen TSM und zweiter GU oder zwischen erster GU und zweiter GU zum alleinigen Zweck der Verwaltung kann daher verzichtet werden. Auf diese Weise kann bei der Verwaltung der zweiten GU viel Aufwand und somit Zeit und/oder Geld gespart werden.

[0032] Beispielsweise bei einem Firmwarewechsel des Kontrollmoduls oder einem Schlüsselwechsel kann das erfindungsgemässe Vorgehen ebenfalls verwendet werden, wobei dieser Vorgang bevorzugt nicht mit dem Öffnen der Türe kombiniert wird, sondern durch Wartungspersonal mit einem ersten Medium durchgefühlt wird.

[0033] Die Sicherheit ist jederzeit gewährleistet, auch dann wenn die Betreiber der Schliessanlage (hier: das Hotel) keine lückenlose Kontrolle über das erste Medium ausüben können. Die Sicherheit ergibt sich daraus, dass die Verwaltungsinformation in der gesicherten Umgebung (im beschriebenen Beispiel beispielsweise der SIM-Karte) des ersten Mediums abgelegt sind und aus dieser konstruktionsgemäss nicht ohne weiteres ausgelesen werden können.

[0034] Optional erfolgt im beschriebenen Verfahren des ersten Aspekts der Erfindung Schritt 3 gleichzeitig mit Schritt 1, oder Schritt 3 folgt unmittelbar nach Schritt 1. Mit anderen Worten kann der erste Schritt online erfolgen, d.h. während die Kommunikationsverbindung zwischen dem ersten und dem zweiten Medium (bzw. von deren Kommunikationsmodulen) besteht.

[0035] In diesem Fall dient das erste Medium sozusagen als Verbindungspunkt einer Verbindung der Verwaltungsinstanz mit dem zweiten Medium. Die Verwaltungsinformation kann dabei von der Verwaltungsinstanz über den Umweg der ersten GU an das zweite Medium übertragen werden, ohne dass die Verwaltungsinformation in der ersten GU gespeichert wird (bzw. kann die Verwaltungsinformation nur kurz gespeichert werden). Die Verwendung der ersten GU des ersten Medium kann auch in diesen Aufführungsformen sinnvoll bzw. notwendig sein, wenn zum Beschreiben und/oder Auslesen des zweite Mediums eine GU nötig ist - d.h. unter anderem, wenn das zweite Medium eine GU aufweist, die beschrieben werden muss.

[0036] Als alternatives optionales Merkmal des Verfahrens erfolgt Schritt 1 zeitlich unabhängig von Schritt 2 und Schritt 3. Insbesondere erfolgt dabei Schritt 1 vorher, d.h. die Verwaltungsinformation wird im ersten Medium abgespeichert und später bei Bedarf und wenn die Kommunikationsverbindung steht an das zweite Medium (Dienstmedium) übertragen.

[0037] Indem Schritt 1 zeitlich unabhängig von Schritt 2 und Schritt 3 erfolgt, ist das Verfahren sehr flexibel und vielseitig anwendbar. Die erste Verwaltungsinformation kann von der Verwaltungsinstanz zu einem beliebigen Zeitpunkt an das erste Medium übermittelt werden. Dies kann dabei gleichzeitig mit einer anderen Interaktion zwischen der Verwaltungsinstanz und erster GU erfolgen und damit vorteilhaft kombiniert werden. Analog dazu kann die zweite Verwaltungsinformation von der ersten GU zu einem beliebigen Zeitpunkt an das zweite Medium übermittelt werden. Auch dies kann gleichzeitig mit einer anderen Interaktion zwischen erster GU und zweitem Medium oder allgemein zwischen dem ersten Medium und dem zweiten Medium erfolgen und folglich vorteilhaft damit kombiniert werden.

[0038] In beiden Fällen funktioniert das erste Medium - also bspw. das Mobiltelefon - als eine Art «Relais». Die bspw. langreichweitigen Kommunikationsmittel des ersten Mediums werden benutzt - aufgrund der Verwendung der ersten GU ohne dass bei der Sicherheit Kompromisse gemacht würden.

[0039] Der erste Aspekt der Erfindung bezieht sich neben dem oben beschriebenen Verfahren auch auf ein Kommunikationssystem zur Verwaltung des zweiten Mediums durch die Verwaltungsinstanz. Das entsprechende Kommunikationssystem umfasst dabei der Verwaltungsinstanz (bspw. einem TSM), ein erstes Medium und ein zweites Medium. Das erwähnte erste Medium umfasst eine erste GU und ein erstes Kommunikationsmodul. Das zweite Medium umfasst ein zweites

Kommunikationsmodul und bspw. eine zweite GU. Die erste GU ist derart ausgebildet, dass sie zu einem Empfang von gesicherten Daten in Form einer ersten Verwaltungsinformation von der Verwaltungsinstanz befähigt ist. Das erste Kommunikationsmodul und das zweite Kommunikationsmodul sind derart ausgebildet, dass sie zum Senden und zum Empfangen eines Signals durch eine Kommunikationsverbindung befähigt sind. Die erste GU ist derart ausgebildet, dass sie zu einem Übermitteln einer auf der ersten Verwaltungsinformation beruhenden zweiten Verwaltungsinformation über die NFC-Kommunikationsverbindung an das zweite Medium befähigt ist.

[0040] In den Fällen, in denen das zweite Medium eine GU («zweite GU») aufweist und die Verwaltungsinformationen diese betreffen, ist die zweite GU derart ausgebildet, dass sie zu einem Empfang einer auf der ersten Verwaltungsinformation beruhenden zweiten Verwaltungsinformation befähigt ist, wobei die zweite Verwaltungsinformation von der ersten GU im ersten Medium über die NFC-Kommunikationsverbindung an die zweite GU übermittelt wird.

[0041] Ein solches Kommunikationssystem kann die oben beschriebenen Verfahren ausführen und weist daher dieselben Vorteile wie die oben beschriebenen Verfahren auf. Dies gilt jeweils für alle möglichen Kombinationen von als optional beschriebenen Ausführungsformen dieses Verfahrens. Die entsprechend beschriebenen Vorteile der Verfahren sind auch Vorteile des jeweiligen sie anwendenden Kommunikationssystems.

[0042] Ebenfalls zum ersten Aspekt gehört ein Kommunikationsmedium, welches befähigt ist, als erstes Medium das vorstehend beschriebene Verfahren auszuführen. Insbesondere ist das Kommunikationsmedium befähigt, ein Verfahren mit folgenden Schritten auszuführen:

- Schritt 1: Empfangen einer ersten Verwaltungsinformation von der Verwaltungsinstanz (100) und übertragen an die erste gesicherte Umgebung (III),
- Schritt 2: Erstellen einer Kommunikationsverbindung zwischen dem ersten Medium (101) umfassten ersten Kommunikationsmodul (121) und einem Kommunikationsmodul (122) eines zweiten Mediums,
- Schritt 3: Übertragen einer aus der ersten Verwaltungsinformation abgeleiteten zweiten Verwaltungsinformation von der ersten gesicherten Umgebung (111) an das erste Kommunikationsmodul (121) und über die Kommunikationsverbindung an das zweite Kommunikationsmodul (122).

[0043] Ein zweiter Aspekt der Erfindung bezieht sich auf ein Verfahren zur sicheren Übermittlung von Daten durch eine NFC-Kommunikationsverbindung oder eine andere drahtlose Kommunikationsverbindung (bspw. Bluetooth, WLAN oder optisch über Infrarotstrahlung etc.) von einem ersten Medium an ein zweites Medium, wobei das erste und das zweite Medium aktiv betrieben werden. Der zweite Aspekt der Erfindung bezieht sich auch auf ein Kommunikationssystem zur sicheren Übermittlung von Daten durch eine NFC-Kommunikationsverbindung von einem ersten Medium an ein zweites Medium.

[0044] Im Stand der Technik wird eine Vielzahl von verschiedenen Techniken verwendet, um die Übermittlung von Daten durch eine solche Kommunikationsverbindung mehr oder weniger sicher vor unbefugtem Zugriff, insbesondere vor Abhören und/oder Manipulation zu gestalten. Je nach angewendeter Technik ist der Grad der Sicherheit eher hoch oder eher niedrig, wobei jede Technik mit spezifischen Nachteilen verbunden ist.

[0045] Aufgabe des zweiten Aspekts der Erfindung ist es daher, die Sicherheit der Übermittlung von Daten durch eine NFC-Kommunikationsverbindung zu erhöhen.

[0046] Das Verfahren gemäss dem zweiten Aspekt der Erfindung umfasst folgende Schritte:

- Schritt 1: Erstellen einer Kommunikationsverbindung zwischen einem vom ersten Medium umfassten ersten Kommunikationsmodul und einem vom zweiten Medium umfassten zweiten Kommunikationsmodul,
- Schritt 2: Übergabe der zu übermittelnden Daten an die erste GU
- Schritt 3: Verschlüsseln der zu übermittelnden Daten in der ersten GU mit einem in der ersten GU gespeicherten ersten Schlüssel,
- Schritt 4: Übergabe der verschlüsselten zu übermittelnden Daten von der ersten GU an das erste Kommunikationsmodul und Übermitteln der verschlüsselten Daten vom ersten Kommunikationsmodul an das zweite Kommunikationsmodul durch die Kommunikationsverbindung.

[0047] Die Schritte 2 und 3 können vorgängig zu Schritt 1, mindestens teilweise gleichzeitig oder anschliessend dran stattfinden.

[0048] Das Entschlüsseln der Daten im zweiten Medium kann in einer zweiten GU des zweiten Mediums mit einem zweiten Schlüssel erfolgen.

[0049] Vorgängig zum Kommunikationsverfahren können die in der GU geschützten Schlüssel (erster Schlüssel, ggf. zweiter Schlüssel) von einer Verwaltungsinstanz, bspw. einem TSM in die entsprechenden GUs geschrieben worden sein, d.h. heisst das Verfahren kann den vorgängigen Schritt des Übermitteins des ersten Schlüssels durch einen vertrauenswürdigen Vermittler (trusted Service manager, TSM) an die vom ersten Medium umfasste erste gesicherte Umgebung (abgekürzt GU) und ggf. das Übermitteln des zweiten Schlüssels vom TSM an eine vom zweiten Medium umfasste zweite GU umfassen.

[0050] Durch dieses Verfahren wird die Sicherheit der gesicherten Umgebung im entsprechenden Medium, bspw. in einem Mobiltelefon, für andere sichere Kommunikationsverfahren als die Kartenemulation genutzt. Dies kann insbesondere

für NFC-Kommunikation (bspw. Peer-to-Peer-NFG-Kommunikation), andere Funkverbindungen wie bspw. Bluetooth oder WLAN (z.B. nach IEEE-802.11), oder Infrarot etc. geschehen. Die Verschlüsselung wird vom an sich nicht sicheren aktiven Kommunikationsmodul wie Bluetooth oder ähnlich an die sichere GU delegiert. Das Kommunikationsmodul selbst kennt dann den Schlüssel nicht, und dieser kann daher auch nicht für einen Missbrauch aus dem ersten Medium (bspw. Mobiltelefon) geholt werden.

[0051] Auch die Personen, die das Kommunikationsmodul einrichten, kommen nicht an den Schlüssel. Das Verfahren ermöglicht also die Verwendung von weniger sicheren Kommunikationskanälen für die sicherere Kommunikation.

[0052] Weil die GU über einen vertrauenswürdigen Dienst, insbesondere einen TSM mit dem ersten Schlüssel (und ggf. zweiten Schlüssel) versehen werden kann/können, sind der erste und der zweite Schlüssel sicher übermittelbar. Indem der erste (und ggf. der zweite) Schlüssel die entsprechende GU nie verlassen und die GU an sich gut geschützt ist, ist eine hohe Sicherheit gewährleistet.

[0053] Die zu übertragenden Daten aus dem ersten Medium werden gemäss obigem Verfahren bspw. unverschlüsselt oder mittels eines weiteren Schlüssels verschlüsselt der ersten GU übermittelt. In der ersten GU werden die zu übertragenden Daten unter Verwendung des ersten Schlüssels verschlüsselt und an das erste Kommunikationsmodul übermittelt. Das erste Kommunikationsmodul übermittelt die verschlüsselten zu übertragenden Daten an das zweite Kommunikationsmodul und somit an das zweite Medium. Im zweiten Medium - bspw. ggf. in der zweiten GU -werden die verschlüsselten zu übertragenden Daten unter Verwendung des zweiten Schlüssels entschlüsselt und stehen danach dem zweiten Medium unverschlüsselt oder mittels eines weiteren Schlüssels verschlüsselt zur Verfügung.

[0054] Der erste und der zweite Schlüssel sind dabei miteinander korreliert. Mit anderen Worten können für die Verschlüsselung in der ersten GU und der Entschlüsselung bekannte Methoden verwendet werden. Der erste und zweite Schlüssel können identisch (symmetrische Verschlüsselung) oder auch voneinander verschieden sein, wie das für diverse drahtlose Datenübertragungsverfahren an sich bekannt ist, insbesondere ist auch eine asymmetrische Verschlüsselung möglich. Die Besonderheit des Verfahrens liegt darin, dass dem ersten und ggf. dem zweiten Medium eine besonders gesicherte Aufbewahrung der jeweiligen Schlüssel zur Verfügung steht, indem, die Verschlüsselung und ggf. die Entschlüsselung ebenfalls im jeweiligen GU erfolgt. Dies bringt eine zusätzliche Sicherheit insbesondere bei der Verwendung eines nicht sicher aufbewahrten ersten Mediums im Zusammenhang mit an sich wenig sicheren Kommunikationskanälen.

[0055] Diese Verschlüsselung und Entschlüsselung nach dem oben beschriebenen Verfahren ist dabei insbesondere kombinierbar mit allen anderen Methoden, die Kommunikationsverbindung zu betreiben und insbesondere zu sichern. Die Kommunikationsverbindung kann also beispielsweise mit einem hohen Sicherheitsstandard betrieben werden, etwa mit einem Authentisierungsprozess und einer ersten Verschlüsselung nach bekannten Verfahren. Das Verfahren gemäss dem zweiten Aspekt der Erfindung erlaubt es also, zusätzlich zu dieser ersten Verschlüsselung die zu übermittelnden Daten zusätzlich noch auf einer höheren Ebene zu verschlüsseln, indem die zu übermittelnden Daten durch eine zweite Verschlüsselung, also die Verschlüsselung in der ersten GU und der Entschlüsselung in der zweiten GU gemäss dem zweiten Aspekt der Erfindung, noch zusätzlich verschlüsselt werden. Dies resultiert in einer zusätzlichen Sicherheit und erfüllt somit die gestellte Aufgabe.

[0056] Optional erlaubt das Verfahren die sichere Übermittlung von Daten durch eine Kommunikationsverbindung sowohl vom ersten Medium an das zweite Medium als auch durch analoge Schritte vom zweiten Medium an das erste Medium.

[0057] Mit anderen Worten kann das Verfahren nicht nur zur sicheren Übermittlung von Daten vom ersten zum zweiten Medium, sondern auch durch entsprechende Schritte in die andere Richtung, d.h. bidirektional erfolgen.

[0058] Als weiteres optionales Merkmal umfasst der erste und/oder der zweite Schlüssel mindestens zwei Teilschlüssel, wobei im gegebenenfalls ausgeführten vorgängigen Schritt das Übermitteln des ersten Schlüssels und/oder des zweiten Schlüssels durch Übermitteln von mehreren Teilschlüsseln erfolgt.

[0059] Die Verwendung von mehreren Teilschlüsseln für einen Schlüssel erhöht die Sicherheit zusätzlich. Zudem kann die Übermittlung der Teilschlüssel gestaffelt erfolgen. Alternativ kann ein Schlüssel aber auch aus einer Einheit (also nicht aus Teilschlüsseln) bestehen und als Einheit übermittelt werden.

[0060] Das Kommunikationssystem gemäss dem zweiten Aspekt der Erfindung dient also einer sicheren Übermittlung von Daten durch eine NFC-Kommunikationsverbindung von einem ersten Medium an ein zweites Medium und umfasst ein erstes Medium und ein zweite Medium. Das erste Medium umfasst dabei eine erste gesicherte Umgebung (abgekürzt GU) und ein erstes Kommunikationsmodul. Das zweite Medium umfasst ein zweites Kommunikationsmodul und bspw. eine zweite GU. Das erste und das zweite Kommunikationsmodul sind derart ausgebildet, dass sie zum Senden und zum Empfangen von Daten durch eine insbesondere drahtlose Kommunikationsverbindung (NFC, bluetooth, etc.) zwischen dem ersten und dem zweiten Kommunikationsmodul befähigt sind. Die erste und ggf. die zweite GU sind derart ausgebildet, dass sie zum Abspeichern je eines Schlüssels befähigt sind. Ausserdem ist die erste GU derart ausgebildet ist, dass sie einerseits zum Abspeichern eines ersten Schlüssels und andererseits zum Verschlüsseln von Daten unter Verwendung dieses ersten Schlüssels befähigt ist.

[0061] Sofern das zweite Medium eine («zweite GU» genannte) GU aufweist, ist diese bevorzugt derart ausgebildet, dass sie einerseits zum Abspeichern eines' zweiten Schlüssels und andererseits zum Entschlüsseln von Daten unter Verwendung dieses zweiten Schlüssels befähigt ist. Als weiteres Merkmal ist das das Kommunikationssystem dann derart

ausgebildet, dass vom ersten Medium an das zweite Medium zu übermittelnde Daten in der ersten GU unter Verwendung des ersten Schlüssels verschlüsselt, danach vom ersten Kommunikationsmodul an das zweite Kommunikationsmodul übermittelt und schliesslich von der zweiten GU unter Verwendung des zweiten Schlüssels entschlüsselt werden.

[0062] Insbesondere kann/können die GU zum Empfang von Daten durch einen vertrauenswürdigen Vermittler (trusted service manager, abgekürzt TSM) eingerichtet sein, und der TSM kann zur Übermittlung des ersten bzw. zweiten Schlüssels verwendet werden.

[0063] Ein solches Kommunikationssystem kann die oben beschriebenen Verfahren gemäss zweiten Aspekt ausführen und weist daher dieselben Vorteile wie die oben beschriebenen Verfahren des zweiten Aspekts auf. Dies gilt jeweils für alle möglichen Kombinationen von als optional beschriebenen Ausführungsformen dieses Verfahrens. Die entsprechend beschriebenen Vorteile der Verfahren sind auch Vorteile des jeweiligen sie anwendenden Kommunikationssystems.

[0064] Ebenfalls zum zweiten Aspekt gehört ein Kommunikationsmedium, welches Mittel aufweist, als erstes Kommunikationsmedium ein Verfahren gemäss dem zweiten Aspekt durchzuführen.

[0065] Insbesondere weist ein solches Kommunikationsmedium ein Kommunikationsmodul und eine GU auf und ist befähigt, ein Verfahren mit folgenden Schritten durchzuführen:

- Schritt 1: Erstellen der Kommunikationsverbindung zwischen dem Kommunikationsmodul und einem Kommunikationsmodul eines anderen Mediums,
- Schritt 2: Übergabe der zu übermittelnden Daten an die erste gesicherte Umgebung,
- Schritt 3: Verschlüsseln der zu übermittelnden Daten in der ersten gesicherten Umgebung mit einem in der gesicherten Umgebung gespeicherten Schlüssel,
- Schritt 4: Übermitteln der verschlüsselten Daten vom ersten Kommunikationsmodul an das zweite Kommunikationsmodul durch die Kommunikationsverbindung.

[0066] Ein dritter Aspekt der Erfindung betrifft insbesondere passiv betriebene Medien und Schreib- und Lesevorgänge über NFC.

[0067] Aus dem Stand der Technik ist bekannt, dass RPID-Tags (dazu sind auch emulierte RFID-Tags in Mobiltelefonen zu rechnen) und andere passiv betriebene Medien für verschiedene Zwecke eingesetzt werden, darunter als Wertkarten, Tickets etc. Schreib- und Lesevorgänge müssen dabei über eine vertrauenswürdige Einrichtung, insbesondere einen Trusted Service Manager durchgeführt werden. Die für Schreibund Leseprozesse notwendigen Schlüssel dürfen nicht in einem ungesicherten Bereich vorhanden sein, weil ansonsten einfach Missbräuche getrieben werden können.

[0068] Es wäre jedoch wünschenswert, wenn die Benutzer von Zugangskontroll-, Wertkarten-, Ticketsystemen etc. einfach gewisse weniger sicherheitsrelevante Daten wie bspw. ein auf einer Wertkarte gespeichertes Guthaben auslesen könnten, bspw. mit einem Mobiltelefon. Auch für gewisse Schreibprozesse von nicht sicherheitsrelevanten Daten direkt durch einen Benutzer kann ein Bedarf vorhanden sein.

[0069] Es ist daher Aufgabe des dritten Aspekts der Erfindung ein Verfahren und ein System zum Lesen und Schreiben von Daten von bzw. auf Medien, insbesondere passiv betriebene Medien, zur Verfügung zu stellen, welches Benutzern einen einfacheren Zugriff auf gewisse Daten ermöglicht.

[0070] Diese Aufgabe wird gelöst durch ein Verfahren zum Durchfuhren eines Schreibund/oder -leseprozesses, unter Verwendung eines ersten, aktiv betriebenen Mediums, auf bzw. von einem passiv betriebenen zweiten Medium, wobei das erste Medium eine gesicherte Umgebung (GU) aufweist, mit den folgenden Schritten:

- Zur-Verfügung-Stellen eines Schreib- und/oder Leseapplets in der gesicherten Umgebung,
- Zur-Verfügung-Stellen einer Applikation ausserhalb der gesicherten Umgebung,
- Übermitteln eines Schreib- und/oder Lesebefehls durch die Applikation an das Applet,
- Umsetzen des Schreib- und/oder Lesebefehls in ein Schreib- und/oder Lesesignal durch das Applet, und
- Übermitteln des Schreib- und/oder Lesesignals an das passiv betriebene zweite Medium.

[0071] Das Schreib- und/oder Lesesignal entspricht dem Standard, gemäss dem das zweite Medium betrieben wird; bspw. kann es gemäss einer Norm (z.B. ISO 14443) ausgebildet sein. Es löst in diesem den Schreibprozess aus bzw. steht am Anfang eines Datenaustauschs, in welchem die gewünschten, zu lesenden Daten an das erste Medium übermittelt werden. Die Umsetzung des Schreib- und/oder Leseprozesses aufgrund des Schreib- und/oder Lesesignals im passiv betriebenen zweiten Medium bzw. zwischen dem ersten und dem zweiten Medium erfolgt also wie an sich bekannt und wird hier nicht weiter erläutert.

[0072] Unter «Applet» wird hier generell ein Programm oder Programmteil verstanden, welches einem Anwendungsprogramm (einer Applikation) zur Durchführung einer oder mehrerer spezifischer Aufgaben dient. Der Begriff «Applet» ist also nicht als auf eine bestimmte Programmiersprache eingeschränkt zu verstehen.

[0073] Die Applikation kann insbesondere im ersten Medium, aber eventuell auch ausserhalb der gesicherten Umgebung installiert sein. Alternativ kann sie auch ausserhalb des ersten Mediums installiert sein und das Applet - via ein Kommunikationsmodul des ersten Mediums - direkt ansteuern.

[0074] Das zweite Medium kann ein in Relation zum ersten Medium externes Medium sein, bspw. ein RFTD-Tag. Dann wird das Übermitteln des Schreib- und/oder Lesesignals die Teilschritte Übermitteln des Schreib- und/oder Lesesignals an ein Kommunikationsmodul des ersten Mediums und Übermitteln des Schreib- und/oder Lesesignals durch das Kommunikationsmodul an das zweite Medium beinhalten.

[0075] Alternativ kann das zweite Medium auch nur funktionell vom ersten Medium verschieden sein, indem es bspw. eine durch die gesicherte Umgebung des ersten Mediums emulierte RFID-Karte ist. In diesem Fall wird die Übermittlung des Schreib- und/oder Lesesignals an das zweite Medium ein Prozess im Innern der GU sein.

[0076] Durch dieses Vorgehen wird es nunmehr möglich, dass nicht sicherheitsrelevante Daten wie bspw. ein auf dem zweiten Medium gespeichertes Guthaben durch den Benutzer auslesbar sind, bspw. durch sein Mobiltelefon. Wenn die Wertkarte eine physische Wertkarte (insbesondere in Form eines RFID-Tags) ist, muss der Benutzer zu diesem Zweck lediglich die Wertkarte an sein Mobiltelefon halten und die betreffende Applikation ausführen, worauf das Mobiltelefon das Guthaben darstellen kann. Wenn das zweite Medium eine in der gesicherten Umgebung (bspw. auf der SIM-Karte) emuliertes Medium ist, kann der Ausleseprozess jederzeit durch die entsprechende Applikation stattfinden. Daraus resultiert ein beträchtlicher Komfortgewinn für den Benutzer; auch sind eventuelle Fehlbuchungen und dergleichen sofort erkennbar. Analoges gilt natürlich auch bei anderen Anwendungen als Wertkarten und für nicht sicherheitsrelevante Schreibprozesse.

[0077] Trotz dieses zusätzlichen Zugangs für den Benutzer und des daraus resultierenden Komfortgewinns ist die Sicherheit des Systems nicht beeinträchtigt. Die Schlüssel für Schreib- und Leseprozesse bleiben im Innern der GU gespeichert, stehen nur dem Applet (und nicht der Applikation selbst) zur Verfügung und werden niemals herausgegeben. Das Applet - das manipulationssicher ist, weil es in der GU vorhanden ist - kann so programmiert sein, dass es nur Befehle für nicht sicherheitsrelevante Schreib- bzw. Leseprozesse entgegennimmt. Optional kann auch vorgesehen sein, dass solche Prozesse unterschiedlicher Sicherheitsstufen abhängig von einer Authentifizierung der Applikation gegenüber dem Applet gemacht werden. So können die unkritischen Prozesse durch eine im nicht sicheren Bereich des Mobiltelefons gespeicherte (und daher für Missbrauch im Prinzip manipulierbare) Applikation durchgeführt werden, während für sicherheitsrelevantere Prozesse die Authentifizierung einer vertrauenswürdigen Instanz gegenüber dem Applet gefordert wird.

[0078] Das Applet selbst ist Manipulationen nicht zugänglich, da es in der gesicherten Umgebung abgespeichert ist.

[0079] Der dritte Aspekt betrifft auch ein Kommunikationsmedium mit einer gesicherten Umgebung und einem Kommunikationsmodul, bei welchem in der gesicherten Umgebung ein Applet installiert ist und welches zur Durchführung des Verfahrens nach dem dritten Aspekt befähigt ist. Insbesondere ist das Kommunikationsmedium befähigt, folgendes Verfahren durchzuführen:

- Übermitteln eines Schreib- und/oder Lesebefehls einer» Applikation an das Applet,
- Umsetzen des Schreib- und/oder Lesebefehls in ein Schreib- und/oder Lesesignal durch das Applet, und
- Übermitteln des Schreib- und/oder Lesesignals an ein passiv betriebenes zweites Medium.

[0080] Der dritte Aspekt betrifft auch ein System, welches zur Durchführung dieses Verfahrens eingerichtet ist und nebst dem Kommunikationsmedium auch ein passiv betreibbares zweites Medium sowie die Applikation (auf dem ersten Medium oder extern laufend) aufweist.

[0081] Erste Anwendungen des Systems und des Verfahrens sind das erwähnte Auslesen von nicht sicherheitsrelevanten Daten aus dem zweiten Medium durch den Benutzer.

[0082] Eine weitere mögliche Anwendung ist das Delegieren von Zugangsrechten von einem Benutzer an den anderen. Bei dieser Anwendung - und weiteren vergleichbaren Anwendungen - wird das Applet (auch) einen Schreibprozess durchführen. Bspw. kann ermöglicht sein, dass ein Benutzer mit Zugang zu einem Hotelzimmer seinen elektronischen Zimmerschlüssel auf einen (physischen oder emulierten) RFID-Tag einer anderen Person kopiert, damit diese selbst auch einen Zimmerschlüssel hat - selbstverständlich mit den gleichen zeitlichen Beschränkungen wie die erste Person selbst.

[0083] Ähnliches kann auch für die Übertragung von kleineren Guthaben oder Tickets von einem Benutzer zum anderen vorgesehen sein.

[0084] Ein weiterer Anwendungsfall kann das direkte Generieren von Zugangskarten (bspw. elektronischen Hotelzimmerschlüsseln) mittels des ersten Mediums sein. Bspw. kann ein bereits angemeldeter Gast, der sein Zimmer reserviert hat, automatisch oder manuell ausgelöst einen solchen elektronischen Schlüssel anfordern, der dann vom elektronischen Buchungssystem des Hotels (nach erfolgreicher Authentifizierung, entsprechend den Standards des Hotels) zur Verfügung gestellt und durch das Mobiltelefon des Benutzers direkt mit dem erfindungsgemässen Verfahren auf den physischen oder virtuellen (im Mobiltelefon emulierten) RFID-Tag geschrieben wird.

[0085] Auch andere Anwendungen im Hotelumfeld sind denkbar, bspw. im Betrag limitierte Zahlungen, zum Beispiel das Belasten der Zimmerrechnung nach Restaurantkonsumation durch Schreiben direkt auf den RFID-Tag (Zimmerschlüssel).

[0086] Ein vierter Aspekt der Erfindung bezieht sich auf verbesserte NFC-Kommunikationsverbindung zwischen einem ersten (aktiven) Medium und einem zweiten, passiv betriebenen Medium.

[0087] 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 elektro-

nischen 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.

[0088] Der Stand der Technik weist den Nachteil auf, dass in gewissen Situationen die NFC-Kommunikationsverbindung eine ungenügende Qualität aufweist. Dies ist beispielsweise der Fall aufgrund von bauartbedingten Eigenheiten des Mediums (kleiner Induktionsschlaufe) oder aufgrund eines gewählten Betriebsmodus (bspw. bei einem Mobiltelefon mit emulierter RFID-Karte, wenn das Mobiltelefon ausgeschaltet ist). Auch eine räumliche Ausrichtung der Sende- und/oder Empfangseinrichtung oder eine grosse Distanz oder eine ändernde Distanz zwischen den Medien kann die Qualität der NFC-Kommunikationsverbindung beeinträchtigen. Insbesondere kann die Qualität der NFC-Kommunikationsverbindung auch abnehmen und die NFC-Kommunikationsverbindung dadurch abbrechen.

[0089] Es ist deshalb Aufgabe des vierten Aspekts der Erfindung, ein Verfahren und eine Vorrichtung (Kommunikationsmedium) der eingangs genannten Art zu schaffen, welche die Qualität der NFC-Kommunikationsverbindung verbessert.

[0090] Gemäss dem vierten Aspekt wird ein Verfahren zum Betreiben einer NFC-Kommunikationsverbindung zwischen einem ersten Medium und einem zweiten Medium zur Verfügung gestellt, wobei das erste Medium aktiv und das zweite Medium passiv betrieben wird (d.h. ein passives Medium ist oder als an sich zum aktiven Betrieb befähigtes Medium im Card Emulation Mode betrieben wird), wobei das Verfahren das Senden eines Abfragesignals vom ersten Medium an das zweite Medium beinhaltet. Die Erfindung gemäss dem vierten Aspekt zeichnet sich nun dadurch aus, dass eine Sendeleistung, mit welcher das Abfragesignal gesandt wird, adaptiv in Abhängigkeit eines für die Kommunikation charakteristischen Parameters gewählt wird.

[0091] Die Begriffe «Abfragesignal» und «Antwortsignal» sind nicht so zu verstehen, dass die aufgebaute Kommunikation (notwendigerweise) aus einer Frage und einer Antwort besteht. Vielmehr wird das Abfragesignal generell im Rahmen des Aufbaus einer Kommunikationsverbindung ausgesandt, wobei es die nötige Energie für das zweite, passiv betriebene Medium liefert. Es löst im Rahmen eines Ausleseprozesses ein Antwortsignal und/oder einen Schreibprozess im zweiten Medium aus; eine solche Kommunikationsverbindung kann, bspw. in der an sich bekannten Art nach ISO 14443 aufgebaut werden. Bspw. kann ein Antwortsignal aus einer Lastmodulation bestehen oder in Form von modulierter Rückstreuung zurückgesandt werden.

[0092] Dieser Parameter kann bspw. die Signalqualität des Antwortsignals sein. In dieser ersten Gruppe von Ausführungsformen fasst also das Verfahren die Schritte:

- Schritt 1: Senden eines Abfragesignals vom ersten Medium an das zweite Medium und Empfangen eines in Reaktion darauf vom zweiten Medium gesendeten Antwortsignals durch das erste Medium (3),
- Schritt 2: Auswerten einer Signalqualität des Antwortsignals durch das erste Medium (3),
- Schritt 3: Steuern einer Sendeleistung des Abfragesignals des ersten Mediums (3) in Abhängigkeit von Schritt 2, wobei eine Signalleistung des Abfragesignals erhöht wird, wenn in Schritt 2 festgestellt wird, dass das Antwortsignal ein NFC-Signal von ungenügender Signalqualität ist.

[0093] Der Parameter kann gemäss einer zweiten Gruppe von Ausführungsformen auch aus der Information bestehen (oder solche Informationen mindestens beinhalten), ob ein Lese- oder ein Schreibprozess ausgelöst werden soll. Sofern das zweite Medium beschrieben werden soll, wird die Sendeleistung höher gewählt als wenn nur ein Leseprozess stattfinden soll.

[0094] Gemäss einer dritten Gruppe von Ausführungsformen des vierten Aspekts kann der charakteristische Parameter auch in einer Identifikation des zweiten Mediums bestehen oder eine solche mindestens aufweisen. Ein passives Medium kann im Rahmen der Kommunikation durch das aktive Medium anhand einer ID identifiziert und einfach einer bestimmten Technologie zugeordnet werden. Wenn bspw. am Anfang nach Aufbau der Kommunikationsverbindung festgestellt wird, dass das zweite Medium ein im Card Emulation Mode betriebenes Mobiltelefon ist, wird die Sendeleistung höher gewählt, als wenn es sich um einen konventionellen RFID-«Tag» handelt.

[0095] Kombinationen dieser Möglichkeiten sind ohne weiteres denkbar, bspw. die Wahl der Sendeleistung sowohl in Abhängigkeit von der Signalqualität als auch davon ob ein Lese- oder Schreibprozess stattfinden soll, die Wahl der Sendeleistung sowohl in Abhängigkeit von der Signalqualität als auch davon, welcher Art das zweite Medium ist, die Wahl der Sendeleistung in Abhängigkeit davon, ob ein Lese- oder ein Schreibprozess durchgeführt werden soll als auch in Abhängigkeit von der Art des Mediums, oder eine Kombination aller drei Möglichkeiten.

[0096] Bei Beispielen von Ausführungsformen der ersten Gruppe (ggf. kombiniert mit der zweiten und/der dritten Gruppe) kann die Auswertung der Signalqualität die Auswertung einer messbaren Grösse des empfangenen Signals, beispielsweise etwa einer Amplitude und/oder Frequenz (und/oder deren Änderung) der empfangenen elektromagnetischen Strahlung, oder die Prüfung von einem Vorhandensein eines Kontrollsignals bzw. der Stimmigkeit einer Prüfgrösse beinhalten. Ebenfalls möglich ist die Messung einer Anzahl übertragener Informationseinheiten wie etwa Bits oder ein Verhältnis von Signalhöhe zu einer definierten Schwelle, beispielsweise etwa einem Schwellwert oder einen anderen geeigneten Test beinhalten. Eine weitere, oft besonders günstige Möglichkeit ist die Feststellung von Bitfehlern anhand eines Prüfsummentests (oder ähnlich).

[0097] Sobald die Auswertung zeigt, dass das Empfangene zwar ein NFC-Signal aber eines von ungenügender Signalqualität ist (bspw. indem es Bitfehler aufweist oder nur ein Teil einer «Message» empfangen wurde (vorzeitiger Abbruch)),

kann bei entsprechend gewählter vorbestimmter Signalcharakteristik auf eine tiefe/ ungenügende Qualität der NFC-Kommunikationsverbindung geschlossen werden. Als Reaktion auf die festgestellte tiefe Qualität der NFC-Kommunikationsverbindung ändert das erste Medium die Sendeleistung des ausgesendeten NFC-Signals von einer ersten Sendeleistung zu einer zweiten, höheren Sendeleistung.

[0098] Nach einer vorgegebenen Dauer und/oder nach einem beendeten Prozess (bspw. dem Abschluss einer Authentifizierung) ändert das erste Medium die Sendeleistung wieder zurück auf die erste, tiefere Sendeleistung, um Energie zu sparen, oder es geht direkt in einen Standby-Modus (Ruhezustand oder «polling»-Betrieb; periodisches Aussenden von kurzen Signalpulsen zum Feststellen, ob ein passiv betriebenes Medium in Reichweite ist).

[0099] Eine solche vorgegebene Dauer kann dabei ggf. beispielsweise auf eine durchschnittliche Dauer einer NFC-Kommunikationsverbindung ausgerichtet sein, beispielsweise für einen definierten Prozess von einheitlicher Länge, etwa einer Autorisierung zur Türöffnung oder dergleichen. Die vorgegebene Dauer kann aber auch so gewählt sein, dass ein bewusst kurz gehaltenes Zeitintervall eine Mehrzahl von Sendeleistungsänderungen bedingt, um einen Datentransfer zu erlauben.

[0100] Eine solche vorgegebene Dauer kann in einem Bereich von 0.3 bis 30 Sekunden liegen, insbesondere in einem Bereich von 0.5 bis 15 Sekunden. Die Dauer kann so gewählt werden, dass gleichzeitig eine Qualitätsverbesserung der NFC-Kommunikationsverbindung und ein energiesparender Betrieb des ersten Mediums ermöglicht werden.

[0101] Das Vorgehen gemäss dem vierten Aspekt der Erfindung ist insbesondere für folgenden Fall von Vorteil: Für batteriebetriebene erste Medien, die bspw. in Schlössern oder mobilen Geräten eingebaut sind, ist die Sendeleistung minimiert, um auf den Batterieverbrauch Rücksicht zu nehmen. Im Zusammenspiel mit passiven RFID-Karten funktioniert das gut, ebenfalls recht gut für Java-Karten und Mobiltelefone im Card Emulation Mode (Kartenemulationsmodus), wenn diese Geräte aktiv und batterieversorgt sind. Sofern jedoch das Mobiltelefon ausgeschaltet ist oder die Batterie leer ist, funktioniert der Ausleseprozess zwar immer noch. Er funktioniert aber sehr schlecht, weil die empfangene Leistung auch dazu dienen muss, gewisse Grundfunktionen des die RFID Karte emulierenden Chips (im Allgemeinen eines Secure Elements (SE), oft der SIM-Karte des Mobiltelefons) zu gewährleisten. Die Reichweite wird dann extrem kurz. Durch das Vorgehen gemäss dem vierten Aspekt der Erfindung ist für einen solchen Fall vorgesehen, dass die Sendeleistung des Abfragesignals zunimmt.

[0102] Vorteil dieses vierten Aspekts ist es also, dass die Qualität der NFC-Kommunikationsverbindung verbessert wird, aber gleichzeitig kein übermässig grosser Energieverbrauch entsteht. Typischerweise werden in Medien Batterien (bspw. Akkumulatoren oder nicht wiederaufladbare Batterien) als Energiequellen eingesetzt, welche ein begrenztes Speichervermögen aufweisen. Darum gilt es, die vorhandene Energie möglichst sparsam einzusetzen. Das oben beschriebene Verfahren erlaubt es, die vorhandene Energie optimal einzusetzen, indem nur bei Bedarf eine hohe Sendeleistung eingesetzt wird. Der Mehrverbrauch durch die zweite, erhöhte Sendeleistung ist im Vergleich zum Verbrauch aus dem Dauerbetrieb (periodische Sendepulse, gegebenenfalls Echtzeituhr) moderat. Da typischerweise ein grosser Teil der vorhandenen Energie im ersten Medium im Ruhezustand (Standby-Modus) verbraucht wird, fällt eine kurzzeitige Erhöhung der Sendeleistung im aktiven Zustand im Vergleich dazu nicht sehr stark ins Gewicht. Der Zyklus, mit dem bspw. in Schlössern die Batterien ausgewechselt werden müssen, wird nicht oder höchstens unerheblich kürzer.

[0103] Beispielsweise sendet das erste Medium in einem Ruhezustand periodisch Signalpulse mit einer tiefen Sendeleistung aus, um festzustellen, ob sich ein zweites Medium im Kommunikationsbereich befindet (Medium im Feld). Wenn das der Fall ist, sendet das erste Medium ein Abfragesignal aus. Wenn das empfangene Antwortsignal ein einwandfrei lesbares NFC-Signal ist, wird dieser Betrieb fortgesetzt bis der Ausleseprozess beendet ist. Ist das empfangene Antwortsignal zwar als NFC-Signal erkennbar, aber ungenügend (bspw. wenn Bitfehler festgestellt werden), wird die Sendeleistung erhöht. Wenn das empfangene Antwortsignal nicht als NFC-Signal erkannt wird, geht das erste Medium bspw. zurück auf den Standby-Betrieb und sendet wieder periodische Signalpulse.

[0104] Der vierte Aspekt der Erfindung betrifft auch ein aktiv betreibbares NFC-Gerät, d.h. ein NFC-Kommunikationsmedium zur Durchführung des beschriebenen Verfahrens. Das Medium umfasst ein Kommunikationsmodul, und ist dazu befälligt, das Kommunikationsmodul ein NFC-Abfragesignal mit einer adaptiv wählbaren Leistung, d.h. mindestens mit einer ersten und einer zweiten, höheren Sendeleistung aussenden zu lassen.

[0105] Beispielsweise kann NFC-Kommunikationsmedium befähigt sein, ein Abfragesignal an ein zweites Medium zu senden und ein in Reaktion darauf vom zweiten Medium gesendeten Antwortsignals durch das erste Medium (3) zu empfangen, eine Signalqualität des Antwortsignals auszuwerten und eine Sendeleistung des Abfragesignals in Abhängigkeit der Resultate dieser Auswertung zu steuern.

[0106] Zu diesem Zweck kann die das Kommunikationsmedium eine Steuereinheit umfassen, welche die Leistung steuert.

[0107] Die beschriebene Vorrichtung erlaubt es, das oben beschriebene Verfahren des vierten Aspekts anzuwenden. Folglich weist die Vorrichtung auch die oben beschriebenen Vorteile auf. Zudem kann die Vorrichtung auch die oben genannten optionalen Merkmale aufweisen, was mit den oben beschriebenen Vorteilen verbunden ist.

[0108] Weitere bevorzugte Ausführungsformen gehen aus den abhängigen Patentansprüchen hervor. Dabei sind Merkmale der Verfahrensansprüche sinngemäss mit den Vorrichtungsansprüchen kombinierbar und umgekehrt.

[0109] Es sind auch Merkmale der verschiedenen Aspekte der Erfindung sinngemäss untereinander kombinierbar, d.h. es kann bspw. der vierte Aspekt mit dem ersten Aspekt kombiniert werden, z.B. durch Verwendung eines entsprechend dem vierten Aspekt eingerichteten Dienstmediums in einem Verfahren nach dem ersten Aspekt; und Kombinationen beider Aspekte zusammen oder je für sich allein mit dem zweiten Aspekt sind denkbar. Weiter sind Kombinationen aller Aspekte von und erwähnten Kombinationen von Aspekten mit dem dritten Aspekt denkbar.

[0110] Für alle Aspekte und Ausführungsformen sind Anwendungen einerseits beispielsweise in den Bereichen der Gebäudesicherung und Raumzutrittsberechtigung zu finden, sowohl in privaten als auch in halböffentlichen Gebäuden - bspw. Hotels; Vergabe von Zimmerschlüsseln etc. Weiter gibt es Anwendungen im Ticketing (Ticketkontrolle und/oder -entwertung Aufladen eines elektronischen Tickets auf ein mobiles Kommunikationsmedium, im Bereich Wertkartensysteme, aber auch in der direkten Kommunikation zwischen Mobilen Geräten, bspw. zum Austausch von persönlichen Informationen wie Adressen, zur Synchronisierung etc.).

[0111] Nebst den Kommunikationsmedien gehört zur Erfindung auch die Software, welche Kommunikationsmedien befähigt, die hier beschriebenen Verfahren auszuführen.

[0112] Im Folgenden wird der Erfindungsgegenstand anhand von bevorzugten Ausführungsbeispielen, welche in den beiliegenden Zeichnungen dargestellt sind, näher erläutert. Es zeigen jeweils schematisch:

Fig. 1	eine Vorrichtung zur Qualitätsverbesserung einer NFC-Kommunikationsverbindung gemäss dem vierten Aspekt der Erfindung;
Fig. 2	ein Ablaufdiagramm eines Verfahrens gemäss dem vierten Aspekt;
Fig. 3	ein Kommunikationssystem zur Verwaltung der zweiten GU des zweiten Mediums durch einen TSM gemäss dem ersten Aspekt der Erfindung;
Fig. 4	ein Kommunikationssystem zur sicheren Übermittlung von Daten durch eine NFC-Kommunikationsverbindung von einem ersten Medium an ein zweites Medium gemäss dem zweiten Aspekt der Erfindung; und
Fig. 5-7	je ein Kommunikationssystem gemäss dem dritten Aspekt.

[0113] 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.

[0114] Fig. 1 zeigt ein aktives NFC-Kommunikationsmedium 3 zur Durchführung des Verfahrens nach dem vierten Aspekt. Das Kommunikationsmedium 3 umfasst ein Kommunikationsmodul 1 und eine Steuereinheit 2 (die hier separat gezeichnet ist, die. aber im Kommunikationsmodul integriert realisiert sein kann). Das Kommunikationsmedium kann bspw. in die Steuerung der mechatronischen Elemente eines Türschlosses integriert sein, ein Lese/Schreibgerät für Wertkarten darstellen, zur Ticketkontrolle und/oder -entwertung, zum Aufladen eines elektronischen Tickets auf ein mobiles Kommunikationsmedium befähigt sein oder irgend ein anderes Gerät für die Kommunikation mittels NFC sein.

[0115] Fig. 1 zeigt auch ein passiv betriebenes zweites Medium 10, welches bspw. als passive RFID-Chipkarte oder aber als Mobiltelefon ausgebildet sein kann. Auch in Fällen, in denen das Mobiltelefon an sich zur aktiven NFC-Kommunikation befähigt ist, kann ein passiver Betrieb (Card Emulation Mode) möglich sein. Das zweite Medium wird unabhängig von seiner physischen Beschaffenheit eine der Ausgestaltung des Geräts angepasste Funktion aufweisen. Zum Beispiel bei der Anwendung «Zugangskontrolle» (das Gerät ist als Kontrollmodul in das Türschloss integriert) kann das zweite Medium bspw. die Funktion einer passiven Chipkarte haben, welche als Türschlüssel verwendet wird.

[0116] Mit «passiv» ist in diesem Zusammenhang gemeint, dass das entsprechende Gerät keine Leistung für die NFC-Kommunikation aufbringen muss, aber ausgelesen und u.U. auch beschrieben werden kann. Der passive NFC-Kommunikationspartner wird in dieser Funktion auch als Transponder bezeichnet, wenn er auf die oben beschriebene Weise vom aktiven NFC-Kommunikationspartner Energie bezieht.

[0117] Das Kommunikationsmodul 1 im ersten Medium (NFC-Kommunikationsmedium 3) ist dazu befähigt, ein Abfragesignal an ein zweites, passives Medium zu senden und ausserdem kann es bei Bedarf eingerichtet sein, auch Schreibprozesse mittels NFC-Signalen durchzuführen (auch die in diesem vierten Aspekt nicht zentrale Befähigung, in einem peer-to-peer-mode zu kommunizieren kann selbstverständlich eingerichtet sein).

[0118] Darüber hinaus ist das Kommunikationsmodul 1 dazu befähigt, ein NFC-Signal mit einer ersten Sendeleistung (L=l) zu senden oder mit einer zweiten Sendeleistung (L=2) zu senden.

[0119] Fig. 2 zeigt ein beispielhaftes Ablaufdiagramm eines Verfahrens der erfindungsgemässen Art. In einem Standby-Modus mit geringem Energieverbrauch wird das Kommunikationsmodul bspw. regelmässig sehr kurze Abfragepulse schicken um festzustellen, ob ein NFC-Medium im Empfangsbereich ist.

[0120] Sofern ein Antwortsignal festgestellt wird, welches als Antwortsignal eines NFC-Mediums interpretiert werden kann, wird das Kommunikationsmodul ganz aufgeweckt und sendet ein Abfragesignal mit der normalen ersten Sendeleis-

tung (L=l). Sofern das Antwortsignal als NFC-Signal interpretiert werden kann (wenn nicht, geht das erste Medium bspw. in den Standby-Modus zurück) wird erfindungsgemäss die Signalqualität ausgewertet.

[0121] Zu diesem Zweck ist die Steuereinheit 2 dazu befähigt, vorgegebene Kriterien auf das vom Kommunikationsmodul 1 empfangene NFC-Signal anzuwenden. Beispielsweise kann durch einen Prüfsummentests festgestellt werden ob und ggf. wie viele Bitfehler bei der Übertragung gemacht werden. Wenn zu viele Bitfehler festgestellt werden, wird die Qualität als ungenügend eingestuft.

[0122] Sofern Die Signalqualität genügt, wird das Abfragesignal weiterhin mit der ersten Sendeleistung ausgesandt, bis der gewünschte Prozess abgeschlossen ist («Stopp»), woraufhin das System bspw. wieder in den Standby-Modus («Periodische Signalpulse») zurückkehrt. Wenn nicht, wird die Sendeleistung des Abfragesignals auf den zweiten, höheren Wert (L=2) eingestellt und der Prozess mit diesem durchgeführt, bis er beendet ist («Stopp»). Auch in diesem Fall kann nach Abschluss des Prozesses das System in den Standby-Mode zurückkehren.

[0123] Es kann auch vorgesehen sein, dass die zweite Sendeleistung nur während einer vorbestimmten Zeit beibehalten wird und danach wieder zur ersten Sendeleistung (sofern der Prozess noch nicht abgeschlossen ist und/oder das zweite Medium im Empfangsbereich verbleibt) zurückgekehrt wird.

[0124] Ergänzend oder alternativ kann vorgesehen sein, dass eine Signalqualitätskontrolle permanent während des Lese bzw. Schreib- und Leseprozesses oder mindestens solange das System mit der ersten Sendeleistung sendet (gestrichelter Pfeil) durchgeführt wird.

[0125] Die erste Sendeleistung reicht in der Regel aus, um mit möglichen NFC-Kommunikationspartnern im üblichen Empfangsbereich des Kommunikationsmoduls 1 von maximal etwa 10cm zu kommunizieren. Die zweite Sendeleistung ist abweichend von der ersten Sendeleistung und von den gewohnten Sendeleistungen deutlich höher, bspw. um mindestens 50% höher, und bspw. mindestens doppelt so hoch. Die Abfragesignale sowohl mit der ersten als mit der zweiten Sendeleistung sind auf einer durch die Norm vorgegebenen Signalfrequenz, bspw. 13,56 MHz.

[0126] Fig. 3 zeigt ein Kommunikationssystem zur Verwaltung eines zweiten Mediums 102 durch einen TSM 100 gemäss dem ersten Aspekt der Erfindung. Das zweite Medium 102 umfasst ein zweites Kommunikationsmodul 122 sowie eine zweite GU 112. Das Kommunikationssystem umfasst neben dem TSM 100 und dem zweiten Medium 102 noch ein erstes Medium 101. Das erste Medium 101 umfasst eine erste GU 111 und ein erstes Kommunikationsmodul 121.

[0127] Es ist das Ziel der hier beschriebenen Ausführungsform des Verfahrens gemäss dem ersten Aspekt, welches hier an einer Vorrichtung gemäss des ersten Aspekts angewendet wird, eine vom TSM zur Verfügung gestellte Firmware der zweiten GU 112 zu aktualisieren (updaten der Firmware). Dazu übermittelt der TSM der ersten GU III und somit dem ersten Medium 101 eine erste Verwaltungsinformation. Die erste Verwaltungsinformation wird in der ersten GU 111 gespeichert. Diese erste Verwaltungsinformation umfasst einerseits die neue Firmwareversion für die zweite GU 112 sowie eine Information für die erste GU 111, dass diese neue Firmwareversion für die zweite GU 112 bestimmt ist. Ausserdem umfasst die erste Verwaltungsinformation eine Anweisung an die erste GU III, dass die erste Verwaltungsinformation nach einer Übermittlung der neuen Firmwareversion an die zweite GU 112 in der ersten GU gelöscht wird.

[0128] Sofern das erste Kommunikationsmodul 121 eine NFC-Kommunikationsverbindung mit einem Kommunikationspartner eingeht, wird von der ersten GU eine Identifikation des Kommunikationspartners geprüft. Handelt es sich beim Kommunikationspartner um das zweite Medium 102, welche die zweite GU 112 umfasst für welche die neue Firmwareversion bestimmt ist, so übermittelt die erste GU 111 dem ersten Kommunikationsmodul 121 eine zweite Verwaltungsinformation. Das erste Kommunikationsmodul 121 übermittelt diese zweite Verwaltungsinformation an das zweite Kommunikationsmodul 122, welches die zweite Verwaltungsinformation wiederum an die zweite GU 112 übermittelt. Die zweite Verwaltungsinformation umfasst die neue Firmwareversion sowie eine Anweisung zur Installation derselben in der zweiten GU 112. Nach der Übermittlung der neuen Firmwareversion in der zweiten Verwaltungsinformation an die zweite GU 112 löscht die erste GU 111 die erste Verwaltungsinformation. Auf diese Art gelangt die neue Firmwareversion vom TSM in die zweite GU 112 und wird dort auch installiert.

[0129] Updates der Firmware von anderen Komponenten des zweiten Mediums (bzw. eines zweiten Mediums ohne GU) können analog vorgenommen werden, wobei dann der letzte Schritt «Übermitteln der Verwaltungsdaten an die zweite GU» durch die Übermittlung an die entsprechende Komponente ersetzt wird bzw. bei einem Update des zweiten Kommunikationsmoduls ganz entfällt.

[0130] Fig. 4 zeigt ein Kommunikationssystem gemäss dem zweiten Aspekt der Erfindung und dient einer sicheren Übermittlung von Daten durch eine Kommunikationsverbindung von einem ersten Medium 201 an ein zweites Medium 202. Dieses Kommunikationssystem erlaubt es, das Verfahren des zweiten Aspekts der Erfindung anzuwenden. Das Kommunikationssystem umfasst ein erstes Medium 201 und ein zweites Medium 202. Das erste Medium 201 umfasst eine erste gesicherte Umgebung (abgekürzt GU) 211 und ein erstes Kommunikationsmodul 221. Das zweite Medium 202 umfasst eine zweite GU 212 und ein zweites Kommunikationsmodul 222.

[0131] Das erste Kommunikationsmodul 221 und das zweite Kommunikationsmodul 222 sind derart ausgebildet, dass sie zum Senden und zum Empfangen von Daten durch eine peer-to-peer NFC-Kommunikationsverbindung (im hier beschriebenen Beispiel; dieses lässt sich ohne Weiteres auf andere Kommunikationsverbindungen wie bluetooth, andere NFC-Kommunikationsverbindung etc. übertragen) zwischen dem ersten Kommunikationsmodul 221 und dem zweiten Kommu-

nikationsmodul 222 befähigt sind. Die erste GU 211 und die zweite GU 212 sind derart ausgebildet, dass sie zum Empfang von Daten durch einen vertrauenswürdigen Vermittler (trusted service manager, abgekürzt TSM) 200 befähigt sind.

[0132] Die erste GU 211 ist dabei befähigt, durch ein Mobiltelefonnetz einen ersten Schlüssel 231 vom TSM 200 zu empfangen. Die zweite GU 212 ist analog dazu befähigt, durch ein Mobiltelefonnetz einen zweiten Schlüssel 232 vom TSM 200 zu empfangen. Der erste Schlüssel 231 und der zweite Schlüssel 232 werden nach dem Empfangen in der jeweiligen GU 211, 212 gespeichert.

[0133] Die erste GU ist ausserdem derart ausgebildet, dass sie zu einem Verschlüsseln von Daten unter Verwendung dieses ersten Schlüssels 231 befähigt ist. Die Verschlüsselung von Daten erfolgt dabei in einem von der ersten GU 211 umfassten ersten Prozessor 241. Und die zweite GU ist derart ausgebildet, dass sie zu einem Entschlüsseln von Daten unter Verwendung des zweiten Schlüssels 232 befähigt ist. Die Entschlüsselung von Daten erfolgt dabei in einem von der zweiten GU 212 umfassten zweiten Prozessor 242.

[0134] Das beschriebene Kommunikationssystem ist derart ausgebildet, dass vom ersten Medium 201 an das zweite Medium 202 zu übermittelnde Daten als eine Startinformation 251 dem ersten Medium 201 zur Verfügung stehen. Nachdem die zu übermittelnden Daten sicher an das zweite Medium 202 übermittelt worden sind, stehen sie dem zweiten Medium 202 als eine Zielinformation 252 zur Verfügung. Dies erfolgt durch eine Anwendung des Verfahrens gemäss dem zweiten Aspekt der Erfindung.

[0135] Vorgängig, bspw. bei einem einmaligen Initialisierungsprozess, übermittelt der TSM 200 der ersten GU 211 den ersten Schlüssel 231 und der zweiten GU 212 den zweiten Schlüssel 232.

[0136] Sobald zwischen dem ersten Kommunikationsmodul 221 und dem zweiten Kommunikationsmodul 222 eine NFC-Kommunikationsverbindung besteht, ist das Kommunikationssystem bereit für eine sichere Datenübermittlung. Die NFC-Kommunikationsverbindung ist dabei bereits durch eine erste Verschlüsselung, bspw. nach an sich bekanntem Schema, verschlüsselt.

[0137] Die Daten in der Startinformation 251 sollen nun sicher vom ersten Medium 201 an das zweite Medium 202 übermittelt werden. Dafür werden die zu übermittelnden Daten 251 in die erste GU 211 und an den ersten Prozessor 241 übermittelt. Der erste Prozessor 241 verschlüsselt diese Daten 251 unter Verwendung des ersten Schlüssels 231. Der erste Prozessor 241 übermittelt dann die verschlüsselten Daten an das erste Kommunikationsmodul 221, welches diese über die NFC-Kommunikationsverbindung an das zweite Kommunikationsmodul 222 und somit an das zweite Medium übermittelt.

[0138] Das zweite Kommunikationsmodul 222 übermittelt die verschlüsselten Daten danach an den zweiten Prozessor 242. Der zweite Prozessor 242 entschlüsselt die verschlüsselten Daten unter Verwendung des zweiten Schlüssels 232. Die entschlüsselten Daten werden vom zweiten Prozessor 242 an einen Bereich des zweiten Mediums 202 ausserhalb der zweiten GU 212 übermittelt und dort als entschlüsselte Daten 252 dem zweiten Medium bspw. unverschlüsselt zur Verfügung gestellt. Auf diese Weise gelangt ein Inhalt der zu übermittelnden Daten 251 im ersten Medium 201 auf eine besonders sichere Weise in das zweite Medium 202, welchem er als Zielinformation 252 zur Verfügung steht. Selbst wenn der gesicherten NFC-Kommunikationsverbindung durch eine Manipulation Daten entnommen werden sollten, sind diese aber immer noch zusätzlich verschlüsselt und daher um eine zusätzliche Stufe sicherer.

[0139] Der erste Schlüssel 231 und der zweite Schlüssel 232 verlassen nie ihre entsprechende GU 211, 212 und sind daher gut geschützt, was die Sicherheit der Übermittlung der zu übermittelnden Daten erhöht. Der erste Schlüssel 231 und der zweite Schlüssel 232 stehen dabei in einem funktionalen Zusammenhang, welcher durch die verwendete Verschlüsselungs- und Entschlüsselungsmethode vorgegeben ist.

[0140] Anhand von Fig. 5 wird eine Möglichkeit für die Umsetzung des dritten Aspekts der Erfindung beschrieben. Das erste Medium 301 umfasst eine GU 311 und ein Kommunikationsmodul 321, welches befähigt ist, über eine Funkverbindung, insbesondere über NFC, mit weiteren Medien zu kommunizieren (in der Fig. 5 ist eine zugehörige Antenne 324 schematisch dargestellt). Die GU 311 umfasst in Fig. 5 nicht dargestellte Prozessor- und Speichermittel, durch die unter anderem ein Applet 312 implementiert ist. Dieses nimmt von einer Applikation 351, die ausserhalb der GU angeordnet ist, Schreib- und/oder Lesebefehle entgegen. Unter Verwendung eines Schlüssels 313, der ebenfalls nur innerhalb der GU 311 zur Verfügung steht, kann das Applet ein Schreib- und/oder Lesesignal erzeugen, welches es an das Kommunikationsmodul 321 weitergibt.

[0141] Fig. 5 zeigt auch ein zweites Medium 302, welches hier eine rein passive RFID-Karte ist. Das (in Bezug auf das erste Medium externe) zweite Medium kann auch ein zum aktiven Betrieb befähigtes Medium sein, das im hier beschriebenen Verfahren passiv betrieben wird.

[0142] Das zweite Medium weist einen Chip 341 auf, in welchem Prozessor- und Speichermittel angelegt sind; in Fig. 5 ist auch eine RFID-Antenne 342 schematisch illustriert.

[0143] Das hier beschriebene Verfahren sieht nun vor, dass das vom Applet erzeugte Schreib- und/oder Lesesignal durch das Kommunikationsmodul 321 an das zweite Medium übermittelt wird und dort den gewünschten Schreib- und/oder Leseprozess auslöst. Physikalisch kann die Signalübermittlung bspw. durch Lastmodulation geschehen.

[0144] Fig. 6 zeigt eine Variante, bei welcher das Verfahren analog abläuft, wobei das zweite Medium 303 jedoch ein in der GU 311 emuliertes und kein physikalisches Medium ist. Für den Schreib- und oder Leseprozess greift das von der

Applikation 321 angesteuerte Applet 312 daher das in der GU 311 emulierte zweite Medium 303 an. Das Kommunikationsmodul 321 wird für das Verfahren nicht benötigt und ist optional, wobei es im Allgemeinen trotzdem vorhanden sein wird, bspw. für Anwendungen, in denen das erste Medium 303 nach aussen kommuniziert.

[0145] Die Variante gemäss Fig. 7 unterscheidet sich dadurch, dass die Applikation 361, die den Schreib- und/oder Leseprozess durchführen möchte, nicht auf dem ersten Medium läuft, sondern extern. Die Applikation kann bspw. auf einem anderen Medium laufen, bspw. auf einem mobilen Medium (Mobiltelefon, Laptop, Tablet-Computer etc.), auf einem Desktop-Computer, einem Server, bspw. von einer zentralen Einheit, etc. Die Kommunikation mit dem ersten Medium kann über das Kommunikationsmodul 321 oder über einen anderen Kanal drahtlos oder kontaktbehaftet stattfinden; der entsprechenden Möglichkeiten gibt es viele.

[0146] Auch eine Kombination der Konzepte von Fig. 7 und Fig. 5 sind denkbar, d.h. die Kommunikation einer externen Applikation mit einem physikalischen zweiten Medium über das Applet.

[0147] In den Ausführungsbeispielen der verschiedenen Aspekte der Erfindung können die involvieren aktiv betriebenen Medien insbesondere batteriebetrieben sein (Standalone-Lösungen). Dies gilt sowohl bei den mobilen Geräten (Mobiltelefonen; bei diesen ist standardmässig ein Akku die Energiequelle) als auch bei den Dienstmedien, bspw. in Schlössern eingebaut. Die verschiedenen Aspekte der Erfindung eignen sich besonders gut für solche Standalone-Dienstmedien, da sie entsprechende Lösungen für deren spezifische Probleme bieten.

Patentansprüche

1. Verfahren zur Verwaltung eines zweiten Mediums (102), durch eine Verwaltungsinstanz wobei das zweite Medium (102) ein zweites Kommunikationsmodul (122) umfasst, dadurch gekennzeichnet, dass das Verfallen folgende Schritte umfasst:
   Schritt 1: Übertragen einer ersten Verwaltungsinformation von der Verwaltungsinstanz (100) an eine von einem ersten Medium (101) umfasste erste gesicherte Umgebung (111),
   Schritt 2: Erstellen einer Kommunikationsverbindung zwischen einem vom ersten Medium (101) umfassten ersten Kommunikationsmodul (121) und dem zweiten Kommunikationsmodul (122),
   Schritt 3: Übertragen einer aus der ersten Verwaltungsinformation abgeleiteten zweiten Verwaltungsinformation von der ersten gesicherten Umgebung (111) an das erste Kommunikationsmodul (121) und über die Kommunikationsverbindung an das zweite Kommunikationsmodul (122).
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Kommunikationsverbindung eine NFC-Kommunikationsverbindung ist.
3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass die Verwaltungsinstanz (100) ein vertrauenswürdiger Vermittler (Trusted Service Manager, TSM, 100).
4. Verfahren gemäss einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass Schritt 3 gleichzeitig mit Schritt 1 erfolgt oder unmittelbar nach Schritt 1 erfolgt.
5. Verfahren gemäss einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass Schritt 1 zeitlich unabhängig von Schritt 2 und Schritt 3 erfolgt und dass Schritt 1 insbesondere zeitlich versetzt und vor Schritt 2 und Schritt 3 erfolgt.
6. Verfahren gemäss einem, der vorangehenden Ansprüche, dadurch gekennzeichnet, dass die erste Verwaltungsinformation die zweite Vewaltungsinformation umfasst.
7. Verfahren gemäss einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass das zweite Medium eine zweite gesicherte Umgebung aufweist und dass die zweite Verwaltungsinformation in Schritt 3 oder nach Schritt 3 vom zweiten Kommunikationsmodul an die zweite gesicherte Umgebung (112) übertragen wird.
8. Kommunikationsmedium, wobei das Kommunikationsmedium Mittel aufweist als erstes Medium ein Verfahren nach einem der vorangehenden Ansprüche durchzuführen.
9. Kommunikationssystem zur Verwaltung eines zweiten Mediums (102) durch eine Verwaltungsinstanz (100), insbesondere nach einem Verfahren gemäss einem der Ansprüche 1-7, umfassend die Verwaltungsinstanz (100), ein erstes Medium (101) und das zweite Medium (102), wobei
   – das erste Medium (101) eine erste gesicherte Umgebung (111) und ein erstes Kommunikationsmodul (121) umfasst,
   – das zweite Medium (102) eine zweite gesicherte Umgebung (112) und ein zweites Kommunikationsmodul (122) umfasst,
   – die erste gesicherte Umgebung (111) derart ausgebildet ist, dass sie zu einem Empfang von gesicherten Daten von der Verwaltungsinstanz (100) befähigt ist, und das erste Kommunikationsmodul (121) und das zweite Kommunikationsmodul (122) derart ausgebildet sind, dass sie zum Senden und zum Empfangen eines NFC-Signals durch eine NFC-Kommunikationsverbindung befähigt sind, dadurch gekennzeichnet, dass
   die erste gesicherte Umgebung (111) derart ausgebildet ist, dass sie zum Empfang einer ersten Verwaltungsinformation von der Verwaltungsinstanz (100) befähigt ist,

die erste gesicherte Umgebung (111) derart ausgebildet ist, dass sie zu einem Übermitteln einer auf der ersten Verwaltungsinformation beruhenden zweiten Verwaltungsinformation über die NFC-Kommunikationsverbindung an das zweite Medium (122) befähigt ist und
die zweite gesicherte Umgebung (112) derart ausgebildet ist, dass sie zu einem Empfang der zweiten Verwaltungsinformation befähigt ist T wobei die zweite Verwaltungsinformation von der ersten gesicherte Umgebung (111) im ersten Medium (101) über die NFC-Kommunikationsverbindung an die zweite gesicherte Umgebung (112) übermittelt wird.

10. Verfahren zur sicheren Übermittlung von zu übermittelnden Daten durch eine Kommunikationsverbindung von einem ersten aktiv betriebenen Medium (201) mit einer ersten gesicherten Umgebung (211) an ein zweites aktiv betriebenes Medium (202), umfassend folgende Schritte:
– Schritt 1: Erstellen der Kommunikationsverbindung zwischen einem vom ersten Medium (201) umfassten ersten Kommunikationsmodul (221) und einem vom zweiten Medium (202) umfassten zweiten Kommunikationsmodul (222),
– Schritt 2: Übergabe der zu übermittelnden Daten an die erste gesicherte Umgebung (211),
– Schritt 3: Verschlüsseln der zu übermittelnden Daten in der ersten gesicherten Umgebung (211) mit einem ersten, in der gesicherten Umgebung gespeicherten Schlüssel (231),
– Schritt 4: Übermitteln der verschlüsselten Daten vom ersten Kommunikationsmodul (221) an das zweite Kommunikationsmodul (222) durch die Kommunikationsverbindung.

11. Verfahren gemäss Anspruch 10, dadurch gekennzeichnet, dass das Verfahren die sichere Übermittlung von Daten durch die Kommunikationsverbindung sowohl vom ersten Medium (201) an das zweite Medium (202) als auch durch analoge Schritte vom zweiten Medium (202) an das erste Medium (201) erlaubt.

12. Verfahren gemäss Anspruch 10 oder 11, dadurch gekennzeichnet, dass in einem Initialisierungsschritt vor Schritt 1 der erste Schlüssel (231) und/oder ein zweiter Schlüssel (232) einer zweiten gesicherten Umgebung des zweiten Mediums von einem vertrauenswürdigen Vermittler die erste bzw. zweite gesicherte Umgebung geschrieben wird, wobei der erste bzw. zweite Schlüssel beispielsweise mindestens zwei Teilschlüssel umfasst, die getrennt geschrieben werden.

13. Verfahren nach einem der Ansprüche 10 bis 12, dadurch gekennzeichnet, dass die Kommunikationsverbindung eine NFC-Verbindung, eine bluetooth-Kommunikationsverbindung, eine WLAN-Kommunikationsverbindung, eine Kommunikationsverbindung über eine Infrarotschnittstelle, oder eine drahtgebundene Kommunikationsverbindung ist.

14. Kommunikationsmedium mit einer gesicherten Umgebung, wobei das Kommunikationsmedium Mittel aufweist als erstes Medium ein Verfahren nach einem der Ansprüche 10-13 durchzuführen.

15. Kommunikationssystem zur sicheren Übermittlung von Daten durch eine Kommunikationsverbindung von einem ersten Medium (201) an ein zweites Medium (202), insbesondere nach einem Verfahren gemäss einem der Ansprüche 18 bis 21, umfassend ein erstes Medium (201) und ein zweites Medium (202), wobei
das erste Medium (201) eine erste gesicherte Umgebung (GU, 211) und ein erstes Kommunikationsmodul (221) umfasst,
das zweite Medium (202) ein zweites Kommunikationsmodul umfasst (222), und
das erste Kommunikationsmodul (221) und das zweite Kommunikationsmodul (222) derart ausgebildet sind, dass sie zum Senden und zum Empfangen von Daten durch eine Kommunikationsverbindung zwischen dem ersten Kommunikationsmodul (221) und dem zweiten Kommunikationsmodul (222) befähigt sind,
dadurch gekennzeichnet, dass
die erste gesicherte Umgebung (211) derart ausgebildet ist, dass sie einerseits zum Abspeichern eines ersten Schlüssels (231) und andererseits zum Verschlüsseln von Daten unter Verwendung dieses ersten Schlüssels (231) befähigt ist, und
dass das Kommunikationssystem derart ausgebildet ist, dass vom ersten Medium (201) an das zweite Medium (202) zu übermittelnde Daten in der ersten gesicherten Umgebung (211) unter Verwendung des ersten Schlüssels (231) verschlüsselt und danach vom ersten Kommunikationsmodul (221) an das zweite Kommunikationsmodul (222) übermittelt werden.

16. Kommunikationssystem nach Anspruch 15, wobei das zweite Medium (202) eine zweite gesicherte Umgebung (212) mit einem zweiten Schlüssel aufweist, wobei die zweite gesicherte Umgebung derart ausgebildet ist, dass sie zum Entschlüsseln der vom ersten Medium empfangenen Daten unter Verwendung dieses zweiten Schlüssels (232) befähigt ist.

17. Verfahren zum Durchführen eines Schreib- und/oder -leseprozesses, unter Verwendung eines ersten, aktiv betriebenen Mediums (301), auf bzw. von einem passiv betriebenen zweiten Medium (302, 303), wobei das erste Medium eine gesicherte Umgebung (GU, 311) aufweist, mit den folgenden Schritten:
– zur-Verfügung-stellen eines Schreib- und/oder Leseapplets (312) in der gesicherten Umgebung (311),
– zur-Verfügung-stellen einer Applikation (351, 361) ausserhalb der gesicherten Umgebung, Übermitteln eines Schreib- und/oder Lesebefehls durch die Applikation an das Applet,
– Umsetzen des Schreib- und/oder Lesebefehls in ein Schreib- und/oder Lesesignal durch das Applet, und
– Übermitteln des Schreib- und/oder Lesesignals an das zweite Medium (302, 303).

18. Verfahren nach Anspruch 17, wobei die Applikation (351) auf dem ersten Medium, aber ausserhalb der gesicherten Umgebung installiert ist.
19. Verfahren nach Anspruch 17 oder 18, wobei die Applikation (361) mindestens teilweise ausserhalb des ersten Mediums installiert ist, wobei das erste Medium ein Kommunikationsmodul aufweist, über welches die Applikation oder ein Teil der Applikation mit dem ersten Medium kommuniziert.
20. Verfahren nach einem der Ansprüche 17 bis 19, wobei das zweite Medium (302) ein passives Medium ist und das erste Medium befähigt ist, über RFID mit dem zweiten Medium zu kommunizieren.
21. Verfahren nach einem der Ansprüche 17 bis 19, wobei das zweite Medium (303) ein in der gesicherten Umgebung des ersten Mediums emuliertes Medium ist.
22. Kommunikationsmedium (301) mit einer gesicherten Umgebung (311) und einem Kommunikationsmodul (321), wobei das Kommunikationsmedium Mittel aufweist als erstes Medium ein Verfahren nach einem der Ansprüche 17 bis 21 durchzuführen.
23. Verfahren zum Betreiben einer NFC-Kommunikationsverbindung zwischen einem ersten Medium (3) und einem zweiten Medium, wobei das erste Medium aktiv betrieben wird und das zweite Medium passiv betrieben wird, wobei das Verfahren das Senden eines Abfragesignals vom ersten Medium an das zweite Medium beinhaltet, und wobei das Verfahren das Wählen einer Sendeleistung, mit welcher das Abfragesignal gesandt wird, adaptiv in Abhängigkeit eines für die NFC-Kommunikationsverbindung charakteristischen Parameters umfasst.
24. Verfahren nach Anspruch 23, dadurch gekennzeichnet, dass der charakteristische Parameter eine Signalqualität eines in Reaktion auf das Abfragesignal durch das zweite Medium gesandten Antwortsignals ist, und wobei das Verfahren folgende Schritte umfasst:
Schritt 1: Senden des Abfragesignals vom ersten Medium an das zweite Medium und Empfangen des in Reaktion darauf vom zweiten Medium gesendeten Antwortsignals durch das erste Medium (3), Schritt 2: Auswerten einer Signalqualität des Antwortsignals durch das erste Medium (3),
Schritt 3: Steuern einer Sendeleistung des Abfragesignals des ersten Mediums (3) in Abhängigkeit von Schritt 2, wobei eine Signalleistung des Abfragesignals erhöht wird, wenn in Schritt 2 festgestellt wird, dass das Antwortsignal ein NFC-Signal von ungenügender Signalqualität ist.
25. Verfahren gemäss Anspruch 24, dadurch gekennzeichnet, dass Schritt 2 ein Feststellen von Bitfehlern beim als NFC-Signal identifizierten Antwortsignal umfasst.
26. Verfahren gemäss einem der Ansprüche 24 oder 25, dadurch gekennzeichnet, dass Schritt 2 ein das Feststellen eines Signalabbruchs als NFC-Signal identifizierten Antwortsignal umfasst.
27. Verfahren gemäss einem der Ansprüche 24 bis 26 dadurch gekennzeichnet, dass das Senden des Abfragesignals abgebrochen wird, wenn in Schritt 2 das Antwortsignal nicht als NFC-Signal identifiziert wird.
28. Verfahren gemäss einem der Ansprüche 23-27, dadurch gekennzeichnet, dass der Parameter Informationen darüber beinhaltet, ob ein Schreib- oder ein Leseprozess ausgelöst werden soll, wobei die Sendeleistung höher gewählt wird, wenn ein Schreibprozess ausgelöst werden soll als wenn nur ein Leseprozess ausgelöst werden soll.
29. Verfahren gemäss einem der Ansprüche 23-28, dadurch gekennzeichnet, dass der charakteristische Parameter eine Identifikation des zweiten Mediums aufweist, wobei die Sendeleistung in Abhängigkeit von der Art des zweiten Mediums gewählt wird.
30. NFC-Kommunikationsmedium, insbesondere zur Verwendung in einem Verfahren gemäss einem der Ansprüche 23 bis 29, umfassend ein Kommunikationsmodul (1), welches dazu befähigt ist, an ein passiv betriebenes zweites Medium ein Abfragesignal für eine NFC-Kommunikationsverbindung zu senden und ein entsprechendes Antwortsignal zu empfangen, dadurch gekennzeichnet, dass das Kommunikationsmodul (1) dazu befähigt ist, das Abfragesignal in Abhängigkeit eines für die NFC-Kommunikationsverbindung charakteristischen Parameters mit einer ersten Sendeleistung zu senden oder mit einer zweiten Sendeleistung zu senden.
31. NFC-Kommunikationsmedium nach Anspruch 30, dadurch gekennzeichnet, dass das Kommunikationsmedium befähigt ist, eine Signalqualität des Antwortsignals auszuwerten und eine Sendeleistung des Abfragesignals in Abhängigkeit eines Resultats der Auswertung zu wählen.
32. Computerprogramm, welches auf ein Kommunikationsmedium ladbar ist, und welches bei Ausführung das Kommunikationsmedium ein Verfahren nach einem der Ansprüche 1 bis 7, 10 bis 14, 17 bis 21 oder 23 bis 29 ausführen lässt.
33. Datenträger, enthaltend ein Computerprogramm gemäss Anspruch 32.

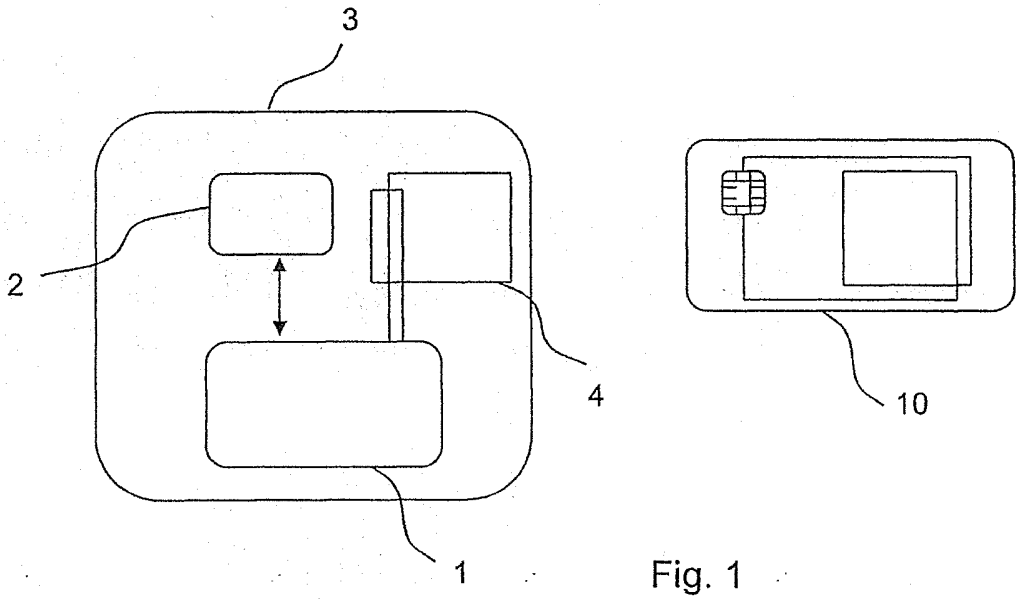

3
2
4
1
10

Fig. 1

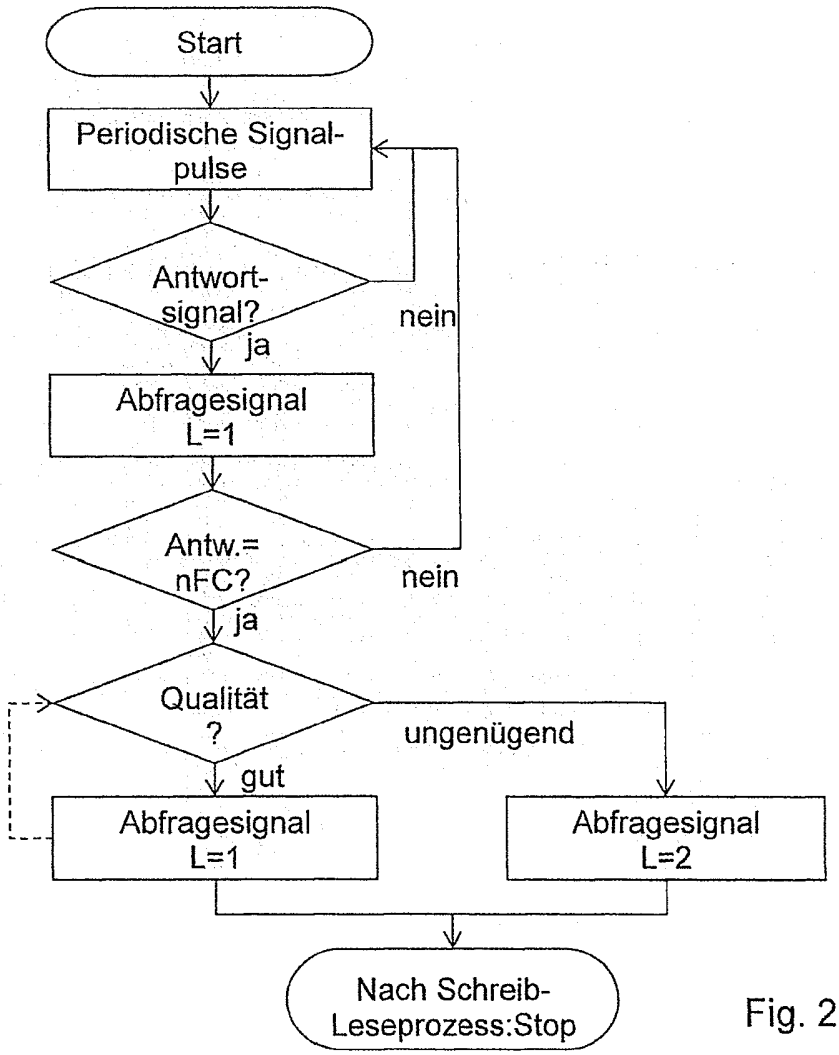

Start
Periodische Signal-pulse
Antwort-signal?
nein
ja
Abfragesignal L=1
Antw.= nFC?
nein
ja
Qualität ?
ungenügend
gut
Abfragesignal L=1
Abfragesignal L=2
Nach Schreib-Leseprozess:Stop

Fig. 2

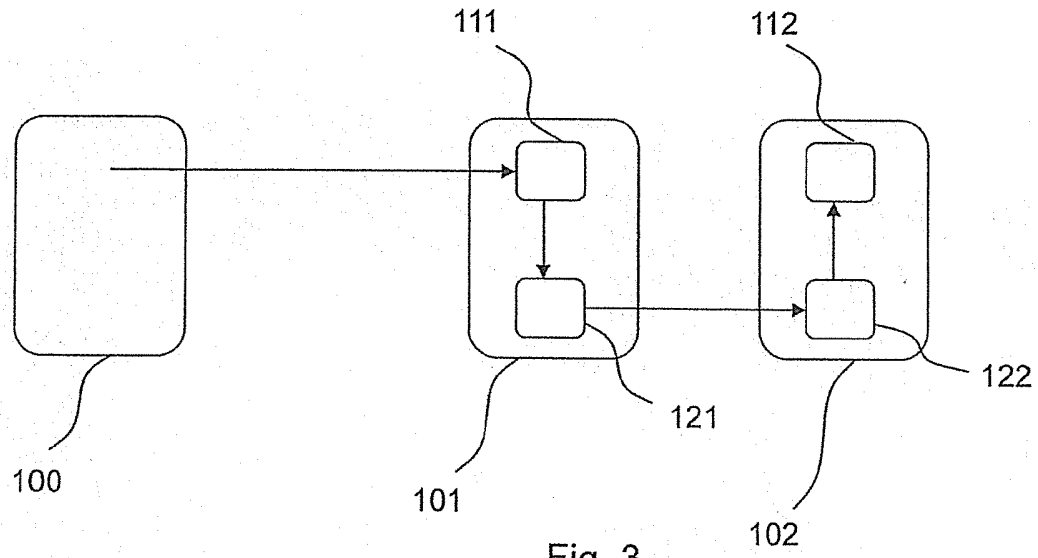

111
112
100
101
121
122
102

Fig. 3

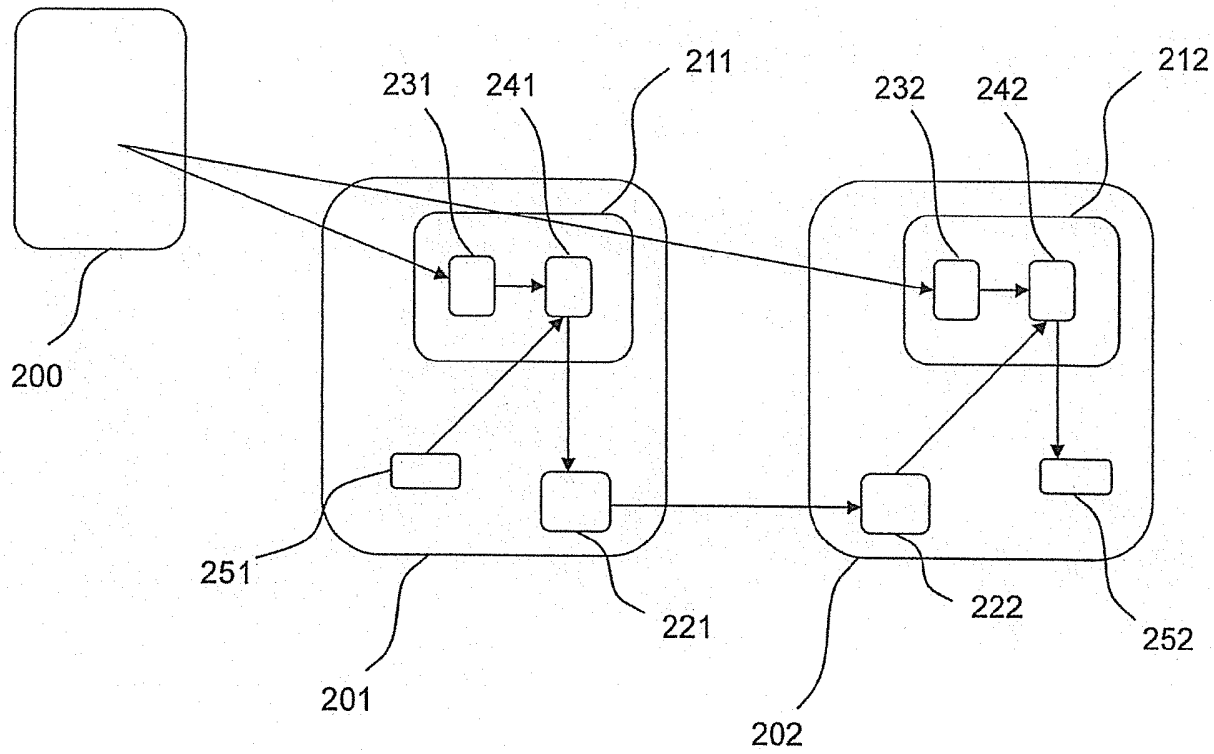

231
241
211
232
242
212
200
251
221
222
252
201
202

Fig. 4

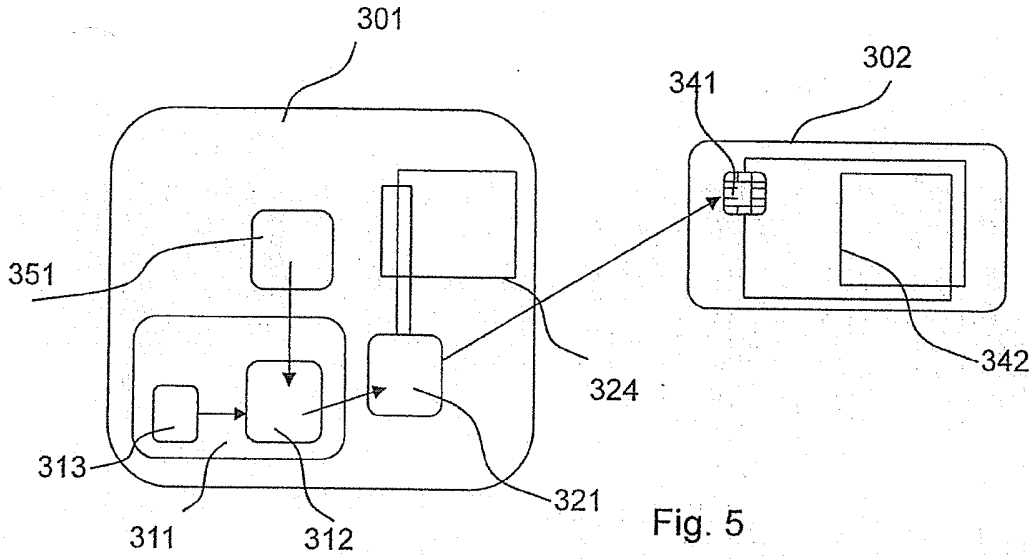


Fig. 5

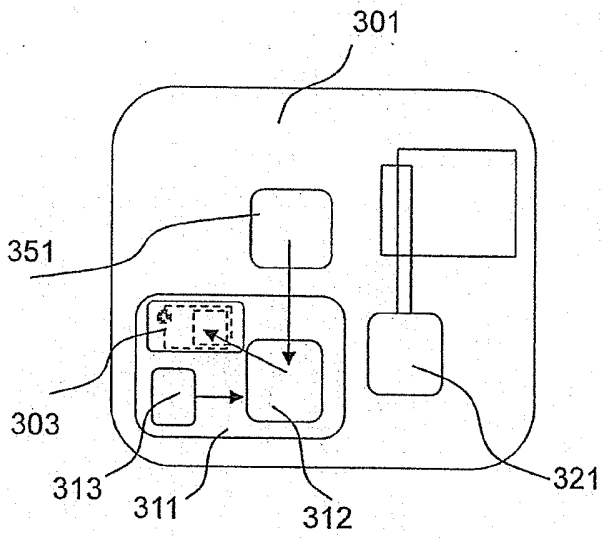


Fig. 6

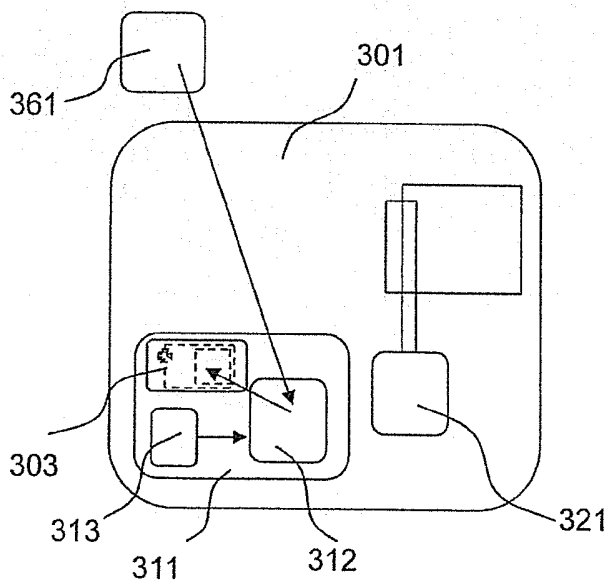


Fig. 7