(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 102 40 396 A1** 2004.01.15

(12) # Offenlegungsschrift

(21) Aktenzeichen: **102 40 396.1**
(22) Anmeldetag: **02.09.2002**
(43) Offenlegungstag: **15.01.2004**

(51) Int Cl.[7]: **G07C 9/00**
E05B 49/04

(66) Innere Priorität:
202 09 132.5 12.06.2002

(71) Anmelder:
SimonsVoss Technologies AG, 85774 Unterföhring, DE

(74) Vertreter:
Vossius & Partner, 81675 München

(72) Erfinder:
Meyerle, Herbert, 85774 Unterföhring, DE

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Vorrichtung und Verfahren zum Sichern von passiven Systemen gegen manipulatives Ansprechen**

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren und eine Vorrichtung zum Sichern von passiven Systemen gegen manipulatives Ansprechen. Derartige Vorrichtungen und Verfahren können zur Vermeidung einer mißbräuchlichen Abfrage von beispielsweise sicherheitsrelevanten Daten und/oder Informationen eingesetzt werden. Hierbei wird ein Transponder gegen ein unberechtigtes und/oder manipulatives Ansprechen gesichert, indem dem Transponder die Zustände bzw. Stati "Ansprechen zulässig" oder "Ansprechen unzulässig" zugewiesen werden. Das Verfahren und die Vorrichtung ermöglichen das Sichern eines Transponders gegen ungewollte Datenübertragung bzw. Datenabfrage und erhöhen somit die Sicherheit von transponderbasierten Zutritts- und Berechtigungskontrollen.

Beschreibung

[0001] Die vorliegende Erfindung betrifft eine Vorrichtung und ein Verfahren zum Sichern von passiven Systemen gegen manipulatives Ansprechen. Derartige Vorrichtungen und Verfahren können zur Vermeidung einer mißbräuchlichen Abfrage von beispielsweise sicherheitsrelevanten Daten und/oder Informationen eingesetzt werden.

Stand der Technik

[0002] Heutigen passive Systeme bzw. passive Kontrollsysteme basieren in der Regel auf der RFID ("Radio Frequency Identification") – Technologie. Sie weisen vorzugsweise eine Basisstation und einen entsprechenden Transponder auf. Der Transponder enthält die für den jeweiligen Anwendungszweck relevanten Daten, die mit Hilfe eines Readers (Basisstation) aus dem Transponder ausgelesen werden. Dieser Vorgang wird auch als Ansprechen oder Nutzung des Transponders bezeichnet. Der Reader erzeugt ein Hochfrequenzfeld, welches der Energieversorgung des Transponders dient und gleichzeitig die Daten überträgt. Hierzu ist keine direkte Verbindung, also auch kein Sichtkontakt erforderlich. Es können sogar nichtmetallische Materialien wie Glas oder Kunststoff zwischen Readerantenne und Tag sein. Metall wirkt in der Regel abschirmend.

[0003] Ein derartiges System weist in der Regel die Komponenten Reader, Antenne (angeschlossen am Reader) und Transponder, der sich an dem zu identifizierenden Gegenstand befindet, auf. Der Transponder selbst besteht wiederum aus einem Mikrochip und einer Antenne, vergossen in einer Einheit z.B. in einem Autoschlüssel, in Münzform, Stäbchenform (Glasröhrchen) oder als ISO Karte, die wiederum in einem Gehäuse untergebracht sein kann.

[0004] Die Reader enthalten meist eine Mikroprozessorelektronik mit serieller Schnittstelle oder sind als Hand-Held Terminal mit eingebautem Reader ausgeführt. Hinzu kommt eine eingebaute oder externe Antenne. Die Schreib-/Lesereichweiten hängen von der Bauform des Transponders ab und betragen bei einfachen Readermodulen (proximity reader) einige Zentimeter und bei long-range Readern bis zu 2 m. Zusammengefaßt gilt: je größer der Transponder, um so besser sind die Abstände.

[0005] Für die verschiedenen Arten von Tranpondern, mit unterschiedlich großen Datenspeichern oder als read-only bzw. read-write Transponder, sind bereits sogenannte „Multi-Standard" Reader entwickelt worden, die die verschiedenen Transponder-Arten lesen und/oder beschreiben können. In Europa sind derzeit RFID – Systeme, die auf 125 kHz oder auf 13,56 MHz arbeiten üblich.

[0006] Transponder werden in unterschiedlichsten Bereichen, wie z.B. der Produktkennzeichnung, Prozess- und Fertigungssteuerung, Prozess- und Fertigungskontrolle, Lagerverwaltung, Warensicherung, Warenverfolgung, Warenschutz, Ticketing, Zutritts- und Berechtigungskontrolle, Tier-Identifikation, Behälter-Identifikation, Sport-Timing oder Verkehrssteuerung angewandt.

[0007] Derartige System sind beispielsweise in der DE 199 02 797 C1 oder der DE 44 40 855 C2 offenbart.

[0008] DE 199 02 797 C1 beschreibt eine schlüssellose Zugangskontrolleinrichtung für Kraftfahrzeuge sowie ein Verfahren zum Durchführen einer schlüssellosen Zugangsberechtigungskontrolle bei Kraftfahrzeugen. Die Zugangskontrolleinrichtung umfaßt eine Steuervorrichtung, die mit zumindest einem dem Kraftfahrzeug zugeordneten Bedienelement kooperiert, und durch ein von dem Transponder nach Empfang des NF-Signals ausgesandtes ersten HF-Antwortsignal in einen Status versetzt ist, in dem das zumindest eine Bedienelement durch den Nutzer des Kraftfahrzeugs betätigbar ist und sich in Wirkverbindung mit einem mechanisch dem Bedienelement und elektrisch der Steuervorrichtung zugeordneten elektrischen Schalter befindet.

[0009] Die DE 44 40 855 C2 offenbart ein Kontrollsystem bei dem zwischen einer Basisstation und einem Transponder eine drahtlose Signalübermittlung zur Identifizierung des Transponders durch die Basisstation stattfindet.

[0010] Dem Stand der Technik ist zu entnehmen, daß auch zwischen einem Transponder und einem nicht zum System gehörigen Reader oder Basisgerät eine Datenübertragung stattfinden kann. Hierbei können die im Transponder enthaltenen Daten durch den nicht zum System gehörigen Reader ausgelesen werden, um anschließend die gewonnenen Informationen auf einen weiteren Transponder zu übertragen. Dieser kann nun beispielsweise dazu verwendet werden, im ursprünglichen System eine Berechtigung zu erhalten. Im Bereich der Zutritts- und Berechtigungskontrolle besteht somit das Risiko, daß Unbefugte durch Auslesen eines Transponders bzw. durch mißbräuchliches/ungewolltes Ansprechen eines Transponders einen widerrechtlichen Zutritt bzw. eine widerrechtliche Berechtigung bzw. Verwendung erzielen. Wie bereits angedeutet kommt dieser Gefahr vor allem im Bereich der Zutrittskontrolle, beispielsweise für Kraftfahrzeuge oder für bestimmte räumliche Bereiche, z.B. Labore, und im Bereich der Berechtigungskontrolle, beispielsweise Wegfahrsperren für Automobile, Alarmanlagen, Tresore oder sonstiger Systeme, eine besondere Bedeutung zu. Hinzu kommt, daß es mit den herkömmlichen Systemen nicht möglich ist, einen Transponder gegen ungewollte Datenübertragung bzw. Datenabfrage zu sichern.

Aufgabenstellung

[0011] Der vorliegenden Erfindung liegt daher die Aufgabe zugrunde, ein Verfahren und eine Vorrichtung bereitzustellen, mit dem bzw. mit der die be-

schriebenen Anforderungen erfüllt und die bestehenden Nachteile überwunden werden.

[0012] Diese Aufgabe wird mit den Merkmalen der Patentansprüche gelöst. Die Erfindung geht dabei von dem Grundgedanken aus, einen Transponder gegen ein unberechtigtes und/oder manipulatives Ansprechen zu sichern, indem dem Transponder die Zustände bzw. Stati „Ansprechen zulässig" oder „Ansprechen unzulässig" zugewiesen werden können.

[0013] In einer bevorzugten erfindungsgemäßen Ausführungsform weist der Transponder eine Vorrichtung und/oder ein Element auf, das den Transponder in einen Status „Ansprechen zulässig" oder „Ansprechen nicht zulässig" versetzt. Die Einstellung des jeweiligen Status kann beispielsweise über einen Taster, einen Schalter und/oder sonstige Betätigungselemente erfolgen. Die Betätigung des oder der Elemente, bzw. die Zuweisung des Status „Abfrage zulässig" ist die Vorraussetzung zur Durchführung einer erfolgreichen Autorisierung.

[0014] Die Vorrichtung und/oder das Element zur Statuszuweisung ist in einer bevorzugten Ausführungsform in Reihe zur Antenne angeordnet. Die Abfrage, welcher Status gesetzt ist, erfolgt in einer erfindungsgemäßen Ausführungsform durch den Transponder selbst. In einer weiteren bevorzugten Ausführungsform erfolgt die Abfrage durch den Reader bzw. die Basisstation.

[0015] Das Element zur Statuseinstellung ist in einer bevorzugten erfindungsgemäßen Ausführungsform als Taster ausgebildet, der in unbeeinflußtem Zustand einen Status „Autorisierung unzulässig" bewirkt und der beim Anordnen des Transponders an einem vorgesehen Ort in einer vorgesehen Art und Weise betätigt wird und einen Status „Autorisierung zulässig" zuweist. Ein oben beschriebener Taster kann beispielsweise an Schlüsseln mit zusätzlicher Transponderfunktion so untergebracht sein, daß er beim Einführen in das Gegenstück, bzw. Schloß automatisch betätigt wird.

[0016] In einer weiteren erfindungsgemäßen Ausführungsform weist der Transponder einen Lichtsensor auf, der vom Transponderchip abgefragt wird und für erfolgreiche Autorisierung erforderlich ist. Der Lichtsensor reagiert auf die Helligkeit der Umgebung und vergibt den Status „Autorisierung zulässig" nur dann, wenn er einem bestimmten Licht oder einer bestimmten Helligkeit ausgesetzt ist. Somit wird gewährleistet, daß der Transponder nicht aus einer Tasche, wie z.B. einer Hosen oder einer Handtasche, heraus abfragbar ist. Diese Ausführungsform ist von Vorteil bei Autoschlüsseln, die im Regelfall in einer Tasche aufbewahrt werden. Ein in einem Autoschlüssel angeordneter Transponder kann somit nicht unbefugt angesprochen und/oder ausgelesen werden, wenn er sich in einer Tasche bzw. in einer dunklen Umgebung befindet.

[0017] In weiteren bevorzugten Ausführungsformen weist der Transponder alternative abschaltbare Störmechanismen bzw. nicht abschaltbare Störmechanismen auf.

[0018] In einer bevorzugten erfindungsgemäßen Ausführungsform, in der der Transponder Kartenform aufweist, weist der Kartenhalter einen gut leitenden Ring parallel zur Kartenantenne auf. Diese Anordnung erwirkt eine starke Dämpfung der Kommunikation. In einer weiteren bevorzugten Ausführungsform der Erfindung kann der leitende Ring durch einen Taster bzw. eine sonstige Vorrichtung unterbrochen werden und damit bewußt eine Kommunikation ermöglicht werden. Dieser Ansatz hat den Vorteil, daß am passiven Transponder kein Eingriff vorgenommen werden muß. Die beschriebene Ausführungsform ist vorzugsweise nachrüstbar ausgeführt. Dies ist aufgrund der weiten Verbreitung transponderbasierter Systeme erstrebenswert.

[0019] In einer weiteren bevorzugten Ausführungsform ist der Störmechanismus als Gehäuse oder als Aufnahmevorrichtung ausgeführt, so daß die Karte bzw. der Transponder zur Betätigung bzw. Nutzung entnommen werden muß. Derartige Ausführungsformen sind bevorzugt nachrüstbar ausgebildet.

[0020] Weitere erfindungsgemäße Ausführungsformen enthalten eine programmierbare und/oder softwareunterstützte Umsetzung der beschriebenen Ausführungsformen. Weiterhin wird in einer bevorzugten Ausführungsform eine Unterscheidung zwischen berechtigter und unberechtigter Datenübertragung bzw. Datenabfrage ermöglicht, indem die Basisstation bzw. der Reader eine bestimmte Information und/oder Kennung an den Transponder überträgt, die Vorraussetzung für eine erfolgreiche Abfrage des Transponders ist.

[0021] Weitere bevorzugte Ausführungsformen weisen eine Kombination der beschriebenen und/oder in den Ansprüchen aufgeführten Ausführungsformen auf.

[0022] Vorzugsweise sind die beschriebenen erfindungsgemäßen Ausführungsformen so ausgeführt, daß sie kostengünstig realisierbar und/oder bei bestehenden Systemen einfach nachrüstbar sind.

[0023] Das Verfahren und die Vorrichtung ermöglichen das Sichern eines Transponders gegen ungewollte Datenübertragung bzw. Datenabfrage und erhöhen somit die Sicherheit von transponderbasierten Zutritts- und Berechtigungskontrollen. Des weiteren ermöglichen die Vorrichtung und das Verfahren eine kostengünstige und einfache Nachrüstung bestehender Systeme.

Patentansprüche

1. Vorrichtung zum Sichern von passiven Systemen gegen unberechtigtes und/oder manipulatives Ansprechen, **dadurch gekennzeichnet**, daß die Vorrichtung mindestens ein betätigbares Element aufweist, dessen Betätigung dem Transponder einen Status „Ansprechen zulässig" oder „Ansprechen nicht zulässig" zuweist, wobei nur im Status „Ansprechen zulässig" eine erfolgreiche Autorisierung, der

Empfang und/oder die Abgabe von Daten und Informationen möglich ist.

2. Vorrichtung nach Anspruch 1, wobei mindestens betätigbares Element ein Taster und/oder Schalter ist.

3. Vorrichtung nach Anspruch 1 oder 2, wobei die Betätigung bzw. die Nicht-Betätigung des Elements vom Transponder selbst abgefragt wird.

4. Vorrichtung nach einem der Ansprüche 1 bis 3, wobei das betätigbare Element in Reihe zur Antenne angeordnet ist und deren Anschluß bei Betätigung herstellt.

5. Vorrichtung nach einem der Ansprüche 1 bis 4, wobei das Element an Schlüsseln mit zusätzlicher Transponderfunktion angeordnet ist.

6. Vorrichtung nach Anspruch 5, wobei das Element so angeordnet ist, daß es beim Einführen des Schlüssels in das Gegenstück automatisch betätigt wird.

7. Vorrichtung zum Sichern von passiven Systemen gegen unberechtigtes und/oder manipulatives Ansprechen, dadurch gekennzeichnet, daß die Vorrichtung mindestens einen Sensor aufweist, von dem Daten abgefragt werden, wobei eine erfolgreiche Autorisierung, die Möglichkeit des Empfangs und/oder der Abgabe von Daten und Informationen von den von dem mindestens einen Sensor aufgenommenen Informationen abhängig ist.

8. Vorrichtung nach Anspruch 7, wobei mindestens ein Sensor ein Lichtsensor ist.

9. Vorrichtung nach Anspruch 7, wobei mindestens ein Sensor ein Tastsensor ist.

10. Vorrichtung nach einem der Ansprüche 7 bis 9, wobei der mindestens eine Sensor von einem Transponderchip abgefragt wird und wobei eine erfolgreiche Autorisierung, die Möglichkeit des Empfangs und/oder der Abgabe von Daten und Informationen von den Sensordaten abhängig ist.

11. Vorrichtung nach Anspruch 8 oder 10, wobei eine erfolgreiche Autorisierung, die Möglichkeit des Empfangs und/oder der Abgabe von Daten und Informationen nur ab einem bestimmten Helligkeitswert möglich ist.

12. Vorrichtung zum Sichern von passiven Systemen gegen unberechtigtes und/oder manipulatives Ansprechen, wobei die Vorrichtung ein dämpfendes Element aufweist, dadurch gekennzeichnet, daß es deaktivierbar ist.

13. Vorrichtung nach Anspruch 12, wobei das dämpfende Element ringförmig ist.

14. Vorrichtung nach Anspruch 12 oder 13, wobei das dämpfende Element im wesentlichen parallel zur Antenne angeordnet ist.

15. Vorrichtung nach einem der Ansprüche 12 bis 14, wobei das dämpfende Element unterbrechbar ist, um eine Kommunikation zu ermöglichen.

16. Vorrichtung nach Anspruch 15, wobei die Unterbrechung durch einen oder mehrere Taster, Schalter und/oder Sensoren erfolgt.

17. Vorrichtung zum Sichern von passiven Systemen gegen unberechtigtes und/oder manipulatives Ansprechen, dadurch gekennzeichnet, daß die Vorrichtung alternativ abschaltbare und/oder nicht abschaltbare Störmechanismen aufweist, durch die eine Kommunikation ermöglicht oder verhindert wird.

18. Vorrichtung nach Anspruch 16, wobei der Störmechanismus die Form einer Hülle oder eines Gehäuses aufweist, der bzw. dem der Transponder und/oder die Karte zur Betätigung entnommen werden muß.

19. Verfahren zum Sichern von passiven Systemen gegen unberechtigtes und/oder manipulatives Ansprechen, dadurch gekennzeichnet, daß dem System nur dann einen Status „Ansprechen zulässig" zugewiesen ist, bzw. daß das System nur dann für eine Autorisierung freigegeben ist und/oder die Abgabe von Daten und Informationen möglich ist, wenn mindestens ein betätigbares Element betätigt wird.

20. Verfahren nach Anspruch 19, wobei mindestens ein betätigbares Element ein Taster und/oder Schalter ist.

21. Verfahren nach Anspruch 19 oder 20, wobei die Betätigung bzw. die Nicht-Betätigung des Elements vom Transponder selbst abgefragt wird.

22. Verfahren nach einem der Ansprüche 19 bis 21, wobei betätigbare Element in Reihe zur Antenne angeordnet ist und deren Anschluß bei Betätigung unterbricht.

23. Verfahren nach einem der Ansprüche 19 bis 22 zum Einsatz an Schlüsseln mit zusätzlicher Transponderfunktion.

24. Verfahren nach Anspruch 23, wobei das betätigbare Element beim Einführen des Schlüssels in das Gegenstück automatisch betätigt wird.

25. Verfahren zum Sichern von passiven Systemen gegen unberechtigtes und/oder manipulatives

Ansprechen, dadurch gekennzeichnet, daß Informationen durch mindestens einen Sensor aufgenommen werden und dadurch, daß Daten des mindestens einen Sensors abgefragt werden und eine erfolgreiche Autorisierung, die Möglichkeit des Empfangs und/oder die Abgabe von Daten und Informationen von den von dem mindestens einem Sensor aufgenommenen Informationen und/oder Daten abhängig ist.

26. Verfahren nach Anspruch 25, wobei mindestens ein Sensor ein Lichtsensor ist.

27. Verfahren nach Anspruch 25, wobei mindestens ein Sensor ein Tastsensor ist.

28. Verfahren nach einem der Ansprüche 25 bis 27, wobei der Sensor von einem Transponderchip abgefragt wird und wobei eine erfolgreiche Autorisierung, die Möglichkeit des Empfangs und/oder die Abgabe von Daten und Informationen von den Sensordaten abhängig ist.

29. Verfahren nach einem der Ansprüche 26 oder 28, wobei eine erfolgreiche Autorisierung, die Möglichkeit des Empfangs und/oder die Abgabe von Daten und Informationen nur ab einer bestimmten Helligkeit möglich ist.

30. Verfahren zum Sichern von passiven Systemen gegen unberechtigtes und/oder manipulatives Ansprechen, wobei das System eine Antenne aufweist und wobei ein leitendes Element im Bezug zur Antenne so angeordnet werden kann, daß eine Dämpfung der Kommunikation bewirkt wird.

31. Verfahren nach Anspruch 30, wobei ein ringförmiges leitendes Element verwendet wird.

32. Verfahren nach Anspruch 30 oder 31, bei dem das leitende Element im wesentlichen parallel zur Antenne angeordnet wird.

33. Verfahren nach einem der Ansprüche 28 bis 30, bei dem das leitende Element zum Ermöglichen einer Kommunikation unterbrechbar ist.

34. Verfahren nach Anspruch 33, bei dem die Unterbrechung durch einen oder mehrere Taster, Schalter und/oder Sensoren erfolgt.

35. Verfahren zum Sichern von passiven Systemen gegen unberechtigtes und/oder manipulatives Ansprechen, dadurch gekennzeichnet, daß eine Kommunikation durch mindestens einen alternativ abschaltbaren und/oder nicht abschaltbaren Störmechanismus ermöglicht oder verhindert wird.

36. Verfahren nach Anspruch 35, bei dem der Störmechanismus die Form einer Hülle oder eines Gehäuses aufweist, der bzw. dem der Transponder und/oder die Karte zur Betätigung entnommen werden muß.

37. Verfahren nach einem der Ansprüche 35 oder 36, wobei der Transponder in der Nähe des Störmechanismus so angeordnet ist, daß nach Entfernen des Transponders bzw. des Störmechanismus keine Störung vorliegt.

Es folgt kein Blatt Zeichnungen