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

(10) **DE 10 2004 018 367 A1** 2005.11.10

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2004 018 367.8**
(22) Anmeldetag: **13.04.2004**
(43) Offenlegungstag: **10.11.2005**

(51) Int Cl.[7]: **G06F 12/14**
G07C 11/00, G06F 17/60, H04L 9/32

(71) Anmelder:
Berthold, Oliver, 10829 Berlin, DE; Freytag, Johann-Christoph, 14532 Kleinmachnow, DE; Spiekermann, Sarah, 14057 Berlin, DE

(72) Erfinder:
Berthold, Oliver, 10829 Berlin, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Datenschutzgerechtes Radio Frequency Identification (RFID)-System durch Besitzer-kontrollierte RFID-Tag Funktionalität**

(57) Hauptanspruch: RFID-Tag mit einem Mittel zum Senden und Empfangen von Nachrichten eines Lesegerätes (Readers) mit der besonderen Eigenschaft Funktionen in Abhängigkeit davon auszuführen, dass
– das Lesegerät die Kenntnis eines Passwortes nachweist oder
– ein interner Zustand die Ausführung gestattet,
wobei das Passwort und der interne Zustand durch mindestens jeweils eine Funktionen geändert werden kann.

Beschreibung

[0001] Die Anmeldung betrifft eine Erweiterung der Funktionalität sogenannter RFID (Radio Frequency Identification) Systeme.

[0002] RFID-Tags und die notwendige Infrastruktur wie z.B. Lesegeräte sind dem Stand der Technik seit langem bekannt und werden beispielsweise zur Kennzeichnung von Gegenständen verwendet. RFID-Tags weisen normalerweise eine Sende- und Empfangsvorrichtung auf, mit der sie u.a. eine Kennzeichnung (Identifikationsnummer) an ein Lesegerät (Reader) übertragen können und andere vom Reader angewiesene (aufgerufene) Funktionen ausführen können, sobald sich ein RFID-Tag in dessen Wirkungsbereich befindet.

[0003] Die Kennzeichnung dient der Identifizierung der Tags und somit des damit verbundenen Gegenstandes.

[0004] In naher Zukunft sollen diese Tags die bisher verwendeten Barcodes auf Konsumprodukten ersetzen, um alle Logistikprozesse sowie die Prozesse im Supermarkt zu vereinfachen. Beispielsweise sind Selbstbedienungskassen geplant, da der Inhalt eines Einkaufwagens komplett in einem Schritt gescannt werden kann.

[0005] Die Erfindung adressiert die Privacy-Problematik dieser Technologie: Da jeder RFID-Tag eine eindeutige Seriennummer tragen soll, kann der Weg jedes Konsumprodukts – damit ist jedes einzelne Objekt gemeint – unbemerkt und auch noch nach Verlassen des Supermarktes ausgelesen werden. Dadurch sind Menschen anhand dieser Seriennummern verfolgbar und können zudem bezüglich aller mitgeführten Produkte (z.B. der Kleidung) durch jedermann gescannt werden. Sollten diese Daten, was zumindest zu befürchten ist, gesammelt und mit Hilfe von Datenbanken gespeichert und ausgewertet werden, wird das von Datenschützern und Privacy-Aktivisten befürchte Szenario vom „Gläsernen Menschen" Wirklichkeit.

Stand der Technik

[0006] Bisher setzt die Industrie dieser Vision nur eine sogenannte Kill-Funktion entgegen, mit der die Tags entgültig deaktiviert werden können. Leider verhindert die endgültige Deaktivierung der RFID-Tags eine Reihe von Anwendungen. Insbesondere sind Anwendungen betroffen, die normalerweise erst nach dem Kauf eines Produktes zum Einsatz kommen, wie beispielsweise eine intelligente Waschmaschine, welche Waschtemperatur und -programm anhand der eingeworfenen Kleidungsstücke automatisch ermittelt. RFID-Tags, welche eine solche Killfunktion zur Verfügung stellen, werden in den Spezifikationen Version 1.0 des EPC Global (http://epcglobalinc.org/standards_technologie/specifications.html) beschrieben.

Aufgabenstellung

[0007] Die Erfindung löst das beschriebene Privacy-Problem der bisherigen RFID-Technologie und ermöglicht im Unterschied zur bekannten Killfunktion zugleich eine Weiternutzung der Technologie für intelligente ggf. vernetzte Geräte mit einem RFID-Tag gemäß den Merkmalen des Anspruchs 1, einem Reader gemäß den Merkmalen des Anspruchs 29 sowie einem Verfahren nach den Merkmalen von Anspruch 42. Vorteilhafte Ausgestaltungen ergeben sich jeweils aus den abhängigen Ansprüchen.

[0008] Die Erfindung erweitert die Funktionalität der Tags um die Möglichkeit zur dynamischen Aktivierung, Deaktivierung oder Einschränkung der (Identifikations-)Funktionalität der RFID-Tags.

[0009] Konkret ist damit gemeint, dass anhand eines internen Zustandes entschieden wird, welche Funktionen ein RFID-Tag in welchem Umfang ausführt, wenn eine bestimmte Anforderung des Readers empfangen wird. Insbesondere soll ein Zustand vorgesehen sein, bei welchem der RFID-Tag keine der intern gespeicherten Daten, die üblicherweise eine Identifizierung ermöglichen, ausgibt.

[0010] Jedoch sollte der RFID-Tag in jedem Zustand die zwischen Reader und RFID-Tag gültigen Kommunikationsprotokolle soweit erfüllen, dass das Übermitteln und Empfangen von Daten und Befehlen möglich ist. Beispielsweise muss ein RFID-Tag seine Anwesenheit gegenüber einem Reader signalisieren und an einem sogenannten Singulation oder Anti-Collusion Protokoll teilnehmen, um überhaupt individuelle Befehle empfangen zu können. In den obigen ERC Global Spezifikationen wird ein Anti-Collusion Protokoll vorgestellt, welches ohne Verwendung der gespeicherten identifizierenden Daten auskommt. In DE10161302 werden Anti-Collusion-Protokolle vorgeschlagen, die auf regelmäßig neu generierten Zufallszahlen statt auf identifizierenden Daten basieren.

[0011] Der erfindungsgemäße RFID-Tags stellt eine Funktion zur Änderung des internen Zustandes zur Verfügung. Dabei wird diese Funktion nur ausgeführt, nachdem der die Funktion aufrufende Reader die Kenntnis eines geheimen Datums, einer auf dem RFID-Tag gespeicherten Bitfolge, nachgewiesen hat. Das geheime Datum wird im folgenden als Passwort bezeichnet. Die Nachweisfunktion wird im folgenden als Verifikation bezeichnet.

[0012] Der erfindungsgemäße RFID-Tag sieht einen wiederbeschreibbaren nichtflüchtigen Speicherplatz

für die Einspeicherung des Passwortes vor. Das erste Passwort kann dabei in vorteilhafter Weise beim Herstellungsprozess des Tags oder beim Verbinden des Produktes mit dem RFID-Tag gesetzt werden. Idealerweise sollte die Einschreibung des Passwortes zusammen mit der Einschreibung der Identifikationsdaten erfolgen, da beides in jedem Schritt der Logistikkette mit dem Produkt mitgesendet werden sollte.

[0013] Es werden zwei vorteilhafte Ausprägungen der Passwort-Verifikation bei den erfindungsgemäßen RFID-Systemen offenbart:
In der ersten Ausprägung wird zur Verifikation das Passwort vom Reader zum RFID-Tag gesendet. Der Vorteil dieser Methode der Verifikation ist eine sehr einfache Implementierbarkeit auf dem RFID-Tag. Es wird nur eine Vergleichsfunktion des gespeicherten mit dem erhaltenen Passwort benötigt. Der Nachteil ist, dass das Passwort von anderen Geräten durch Abhören der Funk-Kommunikation ermittelt werden kann.

[0014] In einer zweiten Ausprägung steht sowohl im RFID-Tag als auch im Reader ein Mittel (eine Funktion) zur Verfügung, welche das Passwort und einen weiteren Wert zu einem Prüfwert kombiniert. Zudem steht im RFID-Tag ein Mittel zur Erzeugung eines zufälligen Wertes (Zufallswert) zur Verfügung. Die Ausprägung des Mittels zur Erzeugung des Zufallswertes ist beliebig. Beispielsweise kann eine Rauschquelle mit einer Sampling-Schaltung verwendet werden oder auf einen bei der Herstellung individuell vergebenem Initialwert wiederholt eine Hashfunktion angewendet werden und die Zufallsfolge aus Teilen der jeweiligen Zwischenwerte gebildet werden.

[0015] Das Mittel zur Berechnung des Prüfwertes kann beliebig realisiert werden. Ideal wäre eine kryptographisch sichere Einwegfunktion oder eine symmetrische Verschlüsselungsfunktion, wobei einer der Eingabewerte als Schlüssel verwendet würde, da so die Umkehrung der Funktion bzw. die Ermittlung eines unbekannten dritten Werfe bei Kenntnis der beiden anderen schwer oder unmöglich ist. Die Realisierungsoptionen des Mittels beinhalten auch die Möglichkeit, die Berechnung nur auf Basis eines Eingabewertes durchzuführen, wobei entweder nur das Passwort verwendet wird oder ein weiteres beliebiges Mittel genutzt wird, um die Eingabewerte zu kombinieren. Die Realisierungsoptionen des Mittels beinhalten auch die Möglichkeit die Berechnung auf Basis von mehr als zwei Eingabewerten durchzuführen. Die Realisierungsoptionen des Mittels beinhalten auch die Möglichkeit mehr als einen Ausgabewert zu berechnen.

[0016] In dieser Ausprägung der Verifikation erzeugt das RFID-Tag als erstes eine Zufallszahl speichert diese in einem beliebigen Speicher und sendet die Zufallszahl zudem an den Reader. Der Reader verwendet das Mittel zur Erzeugung des Prüfwertes wobei als Eingabe das Passwort und die empfangene Zufallszahl verwendet wird. Den Prüfwert sendet der Reader an den RFID-Tag. Der RFID-Tag berechnet einen zweiten Prüfwert anhand des gespeicherten Passwortes und der gespeicherten Zufallszahl und vergleicht beide Prüfwerte. Wenn beide Prüfwerte übereinstimmen, wird die durch die Verifikation geschützte Funktion ausgeführt. Alternativ kann das Mittel auf dem RFID-Tag die Berechnung auch umkehren, also aus dem Prüfwert und einem Eingabewert den jeweils anderen berechnen und diesen vergleichen. Der Vorteil der zweiten Ausprägung der Verifikation ist die Abhörsicherheit, Nachteil die höhere schaltungstechnische Komplexität des Tags.

[0017] Die Sicherheit des Verfahren, also der Schutz vor der Ermittelbarkeit des Passwortes durch Dritte ist abhängig von der kryptographischen Güte des Mittels zur Prüfwertberechnung (wie schwer ist die Umkehrung der Einwegfunktion oder die Ermittlung des unbekannten Wertes), der kryptographischen Güte des Zufallsgenerators und der Länge der verwendeten Bitfolgen für Passwort, Zufallswert und Prüfwert.

[0018] Des weiteren stellt ein erfindungsgemäßer RFID-Tag ein Mittel (eine Funktion) zum Ändern des Passwortes bereit. Diese Funktion wird dabei nur nach einer erfolgreichen Verifikation des bisherigen Passwortes ausgeführt. Dabei wird das neue Passwort vom Reader zum RFID-Tag übertragen.

[0019] Es werden zwei vorteilhafte Ausprägungen für die Übertragung eines Passwortes vom Reader zum RFID-Tag des erfindungsgemäßen RFID-Systemen offenbart:
In der ersten Ausprägung der Passwortübertragung wird das neue Passwort vom Reader zum RFID-Tag gesendet. Der Vorteil dieser Ausprägung der Erfindung ist die einfache Implementierbarkeit auf dem RFID-Tag. Der Nachteil ist die Möglichkeit des Abhörens durch ein anderes Gerät.

[0020] In der zweiten vorteilhaften Ausprägung der Passwortübertragung steht sowohl im RFID-Tag als auch im Reader jeweils ein Mittel zur Verfügung, welches aus zwei Eingabewerten einen dritten berechnen kann. Dieses Mittel kann beliebig realisiert werden, wobei die Berechnung in so fern umkehrbar sein muss, als dass ein Mittel existiert, welches aus einem der Eingabewerte und dem Ausgabewert den zweiten Eingabewert berechnen kann. Beispiel für solche Mittel sind beliebige symmetrische Verschlüsselungsfunktionen oder die bitweise XOR-Überlagerung der beiden Eingabewerte. Die Realisierungsoptionen der Mittel beinhalten auch die Möglichkeit die Berechnung auf Basis von mehr als zwei Eingabewerten durchzuführen. Die Realisierungsoptionen der Mittel beinhalten auch die Möglichkeit mehr als

einen Ausgabewert zu berechnen.

[0021] Der Vorteil dieser Ausprägung der Erfindung ist die höhere Abhörsicherheit, Nachteil die höhere schaltungstechnische Komplexität des Tags. Die Sicherheit des Verfahrens ist von kryptographischen Güte der verwendeten Mittel und von der Länge der verwendeten Werte abhängig, wobei die einfache bitweise XOR-Überlagerung (One-Time-Pad) bereits maximale Sicherheit bietet und somit optimal ist.

[0022] Damit das Passwort bzw. der Zustand des Tags geändert werden kann, ist es für den aktuellen Besitzer eines Tags notwendig, das jeweilige Passwort zu kennen.

Ausführungsbeispiel

[0023] In der oben genannten EPC Global Spezifikation wird vorgeschlagen jedem RFID-Tag ein individuelles Passwort zu geben. Idealerweise sollte diese Passwörter auf dem Weg in den Supermarkt dem jeweiligen aktuellen Besitzer übergeben werden, bzw. direkt vom Hersteller zum jeweiligen Supermarkt übertragen werden. Die Erfindung will nicht dieses Problem lösen, da bereits für die Kill-Funktion die Übermittlung eines ähnlichen Passwortes notwendig ist, welches hierfür verwendet werden kann.

[0024] Im Gegensatz zur bisherigen Lösung auf Basis der Killfunktion wird das Passwort an oder nach der Supermarktkasse an den Kunden übergeben. Dadurch erhält der Kunde die vollständige Kontrolle über die Funktionalität seiner Tags.

[0025] Durch Änderung des Passwortes übernimmt der jeweilige Besitzer die alleinige Kontrolle über die Funktionalität eines RFID-Tags, da die bisherigen Besitzer nunmehr ein falsches Passwort in Ihren Datenbanken haben.

[0026] Die Erfindung betrifft auch ein vorteilhaftes Verfahren zum Ändern der Passwörter, welches das Problem löst, das Tags, die sich in einem deaktivierten Zustand befinden, nicht identifiziert werden können und somit deren Passwort nicht ermittelt werden kann.

[0027] Das vorteilhafte Verfahren beinhaltet, dass ein Besitzer allen in seinem Besitz befindlichen Tags das gleiche Passwort einspeichert. Erst danach oder dabei erfolgt die Deaktivierung.

[0028] Idealerweise sollte dieses Verfahren bereits an der Supermarktkasse durchgeführt werden.

[0029] Der Wechsel des Besitzers eines Tags, beispielsweise an der Kasse eines Supermarktes, sollte in zwei Schritten erfolgen:

1. Der bisherige Besitzer ändert das Passwort der zu übergebendes Tags auf einen zufällig gewählten Wert. Bei Übergabe des Objektes teilt der alte Besitzer dem neuen Besitzer das verwendete Passwort mit.
2. Der neue Besitzer führt möglichst außerhalb der Funk-Reichweite (in seinem Vertrauensbereich) eine zweite Passwortänderung durch, wobei der Besitzer üblicherweise ein gemeinsames Passwort für alle seine Tags verwendet.

[0030] Eine vorteilhafte Schrittfolge an der Supermarktkasse ist:

1. Wahl eines zufälligen Wertes als neues Passwort durch den Reader.
2. Auslesen der Identifikation eines Tags
3. Ändern des Passwortes des Tags auf den neuen Wert, das jeweilig notwendige bisherige Passwort erhält der Reader durch Abfrage einer Datenbank, beispielsweise der Produkt-Bestandsdatenbank des Supermarktes.
4. Deaktivieren des Tags.
5. Wenn weitere Tags vorhanden sind, fortfahren mit Schritt 2.
6. Übergabe des Passwortes für diesen Einkauf an den neuen Besitzer der Produkte, beispielsweise durch Drucken auf den Kassenzettel oder durch übertragen an ein sich im Besitz des Kunden befindliches Gerät (z.B. Chipkarte)

[0031] Damit alle in Besitz einer Person/eines Haushalts befindlichen Tags das gleiche Passwort enthalten, sollte die Passwortänderung durch einen Reader im Vertrauensbereich der Person wiederholt werden.

[0032] Dabei kann eine ähnliche Schrittfolge verwendet werden, mit dem Unterschied, dass Schritt 1 nur einmal durchgeführt und das einmal im Gerät gespeicherte Passwort für alle Tags verwendet wird. Das bisherige Passwort, notwendig in Schritt 3 steht dem Nutzer durch Schritt 6 vorherigen Passwortänderung zur Verfügung und muss ggf. an den Reader übermittelt werden. Schritt 6 fällt weg.

[0033] Es werden drei Möglichkeiten vorgeschlagen, wie das Zwischenpasswort dem Nutzer mitgeteilt werden kann:

1. Übertragen an irgend ein elektronisches Gerät im Besitz des Kunden (z.B. Handy).
2. Direkt übertragen (senden) an das Haussystem des Kunden (insbesondere für Fernabsatz/Internet-Bestellung)
3. Drucken auf den Kassenzettel: Die dritte Möglichkeit könnte in der Ausbauphase besonders wichtig, sein, wenn nur wenige Kunden intelligente Haushaltsgeräte haben. Man könnte sozusagen wichtige Tags nachträglich migrieren, wenn ein solches Gerät angeschafft wurde. Andererseits ist Einkaufen so auch ohne das elektronische Gerät möglich, welches die Passwörter speichert.

[0034] In einer weiteren vorteilhaften Ausprägung der Erfindung erfolgt der Besitzerwechsel nur durch Übergabe des bisherigen Passwortes. Diese Möglichkeit ist u.U. an der Supermarkt-Kasse praktikabel, da die Tags bei der Herstellung ein individuelles Passwort zugewiesen bekommen. Für die Weitergabe aus einem Vertrauensbereich in einen anderen ist diese Vorgehensweise jedoch nicht zu empfehlen, da dem neuen Besitzer in diesem Fall das gemeinsame Passwort aller RFID-Tags des vorherigen Besitzers mitgeteilt werden müsste.

[0035] Die beschriebenen Privacy-Probleme der RFID-Technologie, welche auf alle Vorgänge nach verlassen des Supermarktes beziehen, werden durch die Erfindung gelöst, da sich deaktivierte Tags sich nur noch gegenüber autorisierten Scannern identifizieren.

[0036] Aufgrund der auf einem Passwort basierenden Möglichkeit der Zugriffbeschränkung auf die Tagfunktionalität wird u.a. erreicht, dass ein RFID-Tag nur von verifizierten Readern vollständig kontrolliert werden kann. Durch das Ändern des Passwortes kann die Kontrolle des Tags auf den aktuellen Besitzer beschränkt werden. Zudem kann der Besitzer den Zugriff unautorisierter beliebig beschränken. Folgende beispielhaften Beschränkungen wären denkbar:

– Vollständige Anonymisierung: Ein unverifizierter Reader erhält keinen Teil der Kennzeichnung, d.h. der RFID-Tag ist nicht identifizierbar.

– Anonymisierung der Seriennummer: RFID-Tags können so verwendet werden, dass sie eine EPC (Electronic Product Code) ausgeben, der aus einer Produktkennung und einer Seriennummer des einzelnen Objektes besteht. In dieser Ausprägung würde nur die Produktkennung ausgegeben. Welches konkrete Objekt des Produktes vorliegt, bleibt verborgen.

– Anonymisierung der Identifikationsnummer aber Offenlegung anderer Informationen: Die Ausgabe der Identifikationsnummer wird auf verifizierte Reader beschränkt, aber beliebige andere Informationen die in einer Ausprägung der Erfindung von einem verifizierten Reader geändert werden können, abrufbar über zusätzliche Funktionen, werden allgemein zur Verfügung gestellt. Dies ermöglicht beispielsweise Recycling-Informationen über die chemischen Bestandteile lesbar zu gestalten oder für Information für Rücknahmeautomaten pfandpflichtiger Verpackungen.

[0037] Eine weitere vorteilhafte Ausprägung der Erfindung sieht ein Mittel vor welches aus zwei Eingabewerten einen Prüfwert berechnet. Beispiele für die Realisierung eines solchen Mittels sind eine kryptographische Hash-Funktion (Einwegfunktion) oder eine symmetrische Verschlüsselungsfunktion. Mit Hilfe eine Challenge-Response Verfahrens und unter Mitwirkung des RFID-Tag- oder Produktherstellers kann die Echtheit des Tags und somit unter Einschränkungen auch die Echtheit des Produktes überprüft werden.

[0038] Hintergrund der Ausprägung der Erfindung ist die Tatsache, dass es problemlos möglich ist, freiprogrammierbare Tags herzustellen – aus produktionstechnischen Gründen dürften sogar nahezu alle RFID-Tags ohne konkrete Identifikationsnummer hergestellt werden und diese statt dessen erst am Produkt die erste und endgültige Programmierung erhalten. RFID-Tags ohne verifizierbare Identifikationsnummer werden daher Produktfälschungen eher erleichtern statt zu erschweren.

[0039] Für diese Ausprägung muss im erfindungsgemäßen RFID-Tag neben dem Passwort ein weiterer geheimer Wert gespeichert werden, der in einem nicht wiederbeschreibbaren Speicher abgelegt sein kann. Zudem muss im Computersystem des Produkt- oder RFID-Tag-Herstellers ein Mittel vorgesehen sein, welches die Berechnung des Mittels im RFID-Tag wiederholen oder umkehren kann. Zudem benötigt der Reader i.d.R. eine Online-Verbindung zu dem Computersystem des Herstellers. Der Hersteller benötigt außerdem eine Datenbank, die zu jedem RFID-Tag zumindest die Identifikationsnummer und den auch im RFID-Tag abgelegten geheimen Wert speichert.

[0040] In einer Ausprägung des beanspruchten Verfahrens übersendet der Reader dem RFID-Tag einen zufälligen Wert. Der RFID-Tag berechnet mit Hilfe des Mittels den Prüfwert, wobei die Zufallszahl und der im RFID-Tag gespeicherte geheime Wert als Eingabe verwendet werden. Der Prüfwert wird an den Reader zurückgesendet. Der Reader sendet die Kombination aus RFID-Tag-Identifikationsdaten, Zufallswert und Prüfwert an den Hersteller. Der Hersteller überprüft die Korrektheit mit Hilfe seines Mittels und dem in seiner Datenbank gespeicherten geheimen Wert für den angefragten RFID-Tag. Dabei werden je nach Ausprägung des Mittels zwei der drei Werte (Zufallswert, Prüfwert und geheimer Wert des Tags) als Eingabewerte verwendet und das Ergebnis mit dem dritten Wert verglichen. Der Hersteller meldet das Ergebnis des Vergleiches an den Reader.

[0041] In einer anderen vorteilhaften Ausprägung des Verfahrens erhält der Reader bereits vorab eine oder mehrere gültige Kombination aus Zufallswert und Prüfwert für einen bestimmten RFID-Tag. Die Überprüfung der Echtheit des Tags kann dann lokal erfolgen, ohne dass eine Online-Verbindung notwendig wäre, indem der in der Kombination erhaltene Zufallswert an den RFID-Tag gesendet wird und die Antwort des Tags mit dem Prüfwert verglichen wird.

[0042] Bestandteile der Anmeldung sind zudem

(vernetzte) Reader mit folgenden besonderen Funktionalitäten:

– Funktion zum Verifizieren (Senden des Passwortes bzw. Durchführen des Challenge-Response Verfahrens und der entsprechenden Mittel zum Nachweis der Kenntnis des Passwortes
– Aufrufen von Funktion nach Verifikation des Passwortes
– Funktion zum Ändern des Zustandes
– Funktion zum Ändern des Passwortes
– Methode das gemeinsame Passwort zu speichern und nur an bekannte vertrauenswürdige andere Geräte weiterzugeben
– Methode neue RFID-Tags unter Angabe der jeweiligen Passwörter durch Änderung der Passwörter auf das gemeinsame Passwort in Besitz zu nehmen.

Patentansprüche

1. RFID-Tag mit einem Mittel zum Senden und Empfangen von Nachrichten eines Lesegerätes (Readers) mit der besonderen Eigenschaft Funktionen in Abhängigkeit davon auszuführen, dass
– das Lesegerät die Kenntnis eines Passwortes nachweist oder
– ein interner Zustand die Ausführung gestattet,
wobei das Passwort und der interne Zustand durch mindestens jeweils eine Funktionen geändert werden kann.

2. RFID-Tag nach Anspruch 1, bei dem ein wiederbeschreibbarer Speicher zum Einspeichern eines Passwortes vorgesehen ist.

3. RFID-Tag nach Anspruch 2, bei dem ein Mittel zum Vergleichen zweier Werte vorgesehen ist.

4. RFID-Tag nach Anspruch 3 welcher das Mittel aus Anspruch 3 verwendet, um einen empfangenen Wert mit dem gespeicherten Passwort zu vergleichen.

5. RFID-Tag nach Anspruch 3; bei dem weiterhin ein Mittel zur Erzeugung von Zufallswerten vorgesehen ist.

6. RFID-Tag nach Anspruch 5, bei dem weiterhin ein Mittel zur Berechnung eines oder mehrerer Prüfwerte aus mindestens zwei Eingabewerten vorgesehen ist.

7. RFID-Tag nach Anspruch 6, bei dem eine Challenge-Response Funktion zum vergleichen des Passwortes vorgesehen ist.

8. RFID-Tag nach Anspruch 5, bei dem ein flüchtiger oder nichtflüchtiger wiederbeschreibbarer Speicher zum Zwischenspeichern einer Zufallszahl (Anspruch 5) vorgesehen ist.

9. RFID-Tag nach Anspruch 8, bei dem eine Anfrage des Readers zum Vergleichen des Passwortes mit den Zwischenspeichern (Anspruch 8) und Aussenden einer mit dem Mittel aus Anspruch 5 generierten Zufallszahl beantwortet wird.

10. RFID-Tag nach Anspruch 9, bei dem die Antwort auf das Aussenden (Anspruch 9) verglichen wird mit dem Ergebnis des Mittels aus Anspruch 6, wobei die Werte aus dem Speicher der Zufallszahl (Anspruch 8) und aus dem Speicher des Passwortes (Anspruch 2) als Eingabe verwendet werden.

11. RFID-Tag nach Anspruch 9, bei dem die Antwort auf das Aussenden (Anspruch 9) der Wert aus dem Speicher des Passwortes (Anspruch 2) als Eingabe für das Mittel aus Anspruch 6 verwendet wird und das Ergebnis der Berechnung des Mittels mit Zufallszahl (Anspruch 8) mit Hilfe des Mittels aus Anspruch 3 verglichen wird.

12. RFID-Tag nach Anspruch 4,10 oder 11 bei dem bei einem positiven Ausgang des Vergleiches die Passwort-Verifikation als erfolgreich andernfalls als erfolglos bewertet wird.

13. RFID-Tag nach Anspruch 1, bei dem ein Speicher zum Einspeichern von Identifikationsdaten vorgesehen ist.

14. RFID-Tag nach Anspruch 13, bei dem ein Mittel zum Aussenden von Teilen der Identifikationsdaten (Anspruch 13) vorgesehen ist.

15. RFID-Tag nach Anspruch 14, bei dem ein Speicher zum Einspeichern eines Zustandes vorgesehen ist, der festlegt, ob und welche Teile der Identifikationsdaten (Anspruch 13) ausgegeben werden dürfen.

16. RFID-Tag nach Anspruch 14 und 15, bei dem die Funktion zum Aussenden von Teilen der Identifikationsdaten (Anspruch 14), abhängig von dem Zustand (Anspruch 15) ausgeführt wird.

17. RFID-Tag nach Anspruch 12 und 14, bei dem das Aussenden der Identifikationsdaten (Anspruch 14) nur durchgeführt wird, wenn eine vorherige Passwort-Verifikation erfolgreich war (Anspruch 12), wobei im Erfolgsfall die Identifikationsdaten vollständig ausgesendet werden.

18. RFID-Tag nach Anspruch 16 und 17, bei dem die Aussendung von Teilen der Identifikationsnummer entweder nach den Bedingungen nach Anspruch 16 oder nach den Bedingungen von Anspruch 17 erfolgt.

19. RFID-Tag nach Anspruch 12 und 15, bei dem eine Funktion zum Ändern des Zustandes aus An-

spruch 15 vorgesehen ist, die nur nach einer erfolgreichen Passwort-Verifikation (Anspruch 12) durchgeführt wird.

20. RFID-Tag nach Anspruch 2, bei dem ein Mittel zum berechnen eines neuen Passwortes aus zwei Eingabewerten, einem empfangenen Wert und dem Wert aus dem Speicher des Passwortes (Anspruch 2) vorgesehen ist.

21. RFID-Tag nach Anspruch 2, bei dem das neue Passwort direkt empfangen wird.

22. RFID-Tag nach Anspruch 20 oder 21, bei dem eine Möglichkeit zum Ändern des Passwortes vorgesehen ist, wobei das durch das Mittel von Anspruch 20 oder direkt empfangene Passwort (Anspruch 21) in den Speicher aus Anspruch 2 abgelegt wird.

23. RFID-Tag nach Anspruch 22, bei dem die Funktion zum Ändern des Passwortes (Anspruch 22) nur durchgeführt wird, wenn eine vorherige Passwort-Verifikation (Anspruch 12) erfolgreich war.

24. RFID-Tag mit der besonderen Eigenschaft, dass die Echtheit der von einem RFID-Tag ausgesendeten Identifikationsdaten (z.B. die aus Anspruch 13) unter Mitwirkung des Herstellers verifiziert werden können.

25. RFID-Tag nach Anspruch 24, bei dem ein nichtflüchtiger und nichtwiederbeschreibbarer oder wiederbeschreibbarer Speicher zum Einspeichern eines Verifikationswertes vorgesehen ist.

26. RFID-Tag nach Anspruch 25, bei dem ein Mittel vorgesehen ist, welches aus zwei Eingabewerten einen Prüfwert ermittelt.

27. RFID-Tag nach Anspruch 26, bei dem eine Challenge-Response Funktion zum verifizieren der Identifikationsdaten (Anspruch 13) vorgesehen ist.

28. RFID-Tag nach Anspruch 27, bei dem eine Funktion zum verifizieren der Identifikationsdaten (Anspruch 13) vorgesehen ist, indem ein empfangener Wert und der Verifikationswert (Anspruch 25) als Eingabe des Mittels aus Anspruch 26 verwendet und das Ergebnis ausgesendet wird.

29. Gerät (Reader) mit Mittel zum Kommunizieren mit RFID-Tags nach Ansprüchen 1–28, mit den besonderen Eigenschaften die Kenntnis eines im RFID-Tag gespeicherten Passwortes (Anspruch 2) nachweisen, gespeicherte Daten (Anspruch 13) abfragen, den Zustand des Tags ändern und das Passwort des Tags ändern zu können.

30. Reader nach Anspruch 29, bei dem ein Speicher zum Einspeichern eines Passwortes vorgesehen ist. 31. Reader nach Anspruch 30, bei dem ein Mittel zum Berechnen eines Prüfwertes vorgesehen ist, wobei dieses Mittel die gleiche oder die umgekehrte Berechnung realisiert wie das Mittel aus Anspruch 6.

31. Reader nach Anspruch 30, bei dem eine Funktion zum Senden des Passwortes vorgesehen ist.

32. Reader nach Anspruch 31 bei dem eine Funktion vorgesehen ist, die einen empfangenen Zufallswert und das Passwort (Anspruch 30) als Eingabe für das Mittel aus Anspruch 31 verwendet und das Ergebnis an einen RFID-Tag absendet.

33. Reader nach Anspruch 32 oder 33, bei dem eine Funktion zum Abfragen der Identifikationsdaten eines RFID-Tags (Anspruch 13) nach Verifizieren des Passwortes (Anspruch 32 oder 33) vorgesehen ist.

34. Reader nach Anspruch 32 oder 33, bei dem eine Funktion zum Ändern des Zustandes auf dem RFID-Tag (Anspruch 15,19) nach Verifizieren des Passwortes (Anspruch 32 und 33) vorgesehen ist.

35. Reader nach Anspruch 32 oder 33, bei dem eine Funktion zum Ändern des Passwortes auf dem RFID-Tag (Anspruch 5) nach Verifikation des bisherigen Passwortes (Anspruch 32 oder 33) vorgesehen ist, wobei das neue Passwort im Klartext gesendet wird oder mit Hilfe eines Mittels aus dem bisherigen und dem neuen Passwort ein Prüfwert berechnet und an das RFID-Tag gesendet wird.

36. Verfahren eines Readers nach Anspruch 29 zum Verifizieren des Identifikationswertes eines RFID-Tags (Ansprüche 13), wobei der Reader eine Zufallszahl an den RFID-Tag und die erhaltene Antwort (Prüfwert), die Zufallszahl und den Identifikationswert an den Hersteller des Produkts sendet, welches den RFID-Tag trägt. Der Hersteller antwortet mit „wahr", wenn die Verifikation erfolgreich war.

37. Verfahren nach Anspruch 37, bei dem der Reader vorab eine gültige Kombination aus Zufallswert und Prüfwert für einen Identifikationswert vom Hersteller erfragt und die Antwort des Tags mit dem in der Kombination enthaltenen Prüfwert vergleicht.

38. Datenbank eines Produktherstellers nach Anspruch 37 oder 38 mit der besonderen Eigenschaft, zu den Identifikationswerten (Anspruch 13) aller hergestellten Produkte auch die Verifikationswerte (Anspruch 25) zu speichern.

39. Verfahren der Datenbank eines Produktherstellers nach Anspruch 39, bei dem eine Funktion vorgesehen ist, die eine Anfrage nach Identifikations-

nummer, Zufallszahl und vom RFID-Tag berechneter Antwort auf Korrektheit testen und das Ergebnis an den anfragenden zu übermitteln. Dazu wird ein Mittel verwendet welches aus dem empfangenen Zufallswert und dem Verifikationswert einen Prüfwert berechnet.

40. Verfahren nach Anspruch 40, bei dem vorgesehen ist Kombinationen aus Identifikationswert, Zufallszahl und Prüfwert mit Hilfe eines Mittels zu Erzeugen von Zufallszahlen und des Mittels aus Anspruch 40 zu erstellen.

41. Verfahren zum Ändern eines auf einem RFID-Tag nach Ansprüchen 1–23 gespeicherten Passwortes, wobei ein Reader zuerst die Kenntnis des bisherigen Passwortes nachweist (Anspruch 32 oder 33) und danach das neue Passwort entsprechend Anspruch 36 übermittelt.

42. Verfahren nach Anspruch 42 zum Ändern der Passwörter aller in einem Zeitraum von einem Reader kontaktierter RFID-Tags nach Ansprüchen 1–23 auf ein gemeinsames Passwort, welche entweder vorgegeben oder zu Beginn des Verfahrens zufällig gewählt wird. gemeinsame Passwort kontrolliert werden kann.

43. Verfahren nach Anspruch 42 zum Wechsel des Besitzers eines oder mehrerer RFID-Tags nach Ansprüchen 1–23, wobei pro RFID-Tag zweimal eine Passwortänderung nach Anspruch 42 durchgeführt wird, wobei ein zufällig gewähltes Zwischenpasswort verwendet wird.

44. RFID-Tag nach Ansprüchen 1–23 mit der besonderen Eigenschaft, dass Funktionen vorgesehen sind, die nur bei bestimmten Zuständen (Anspruch 15) oder nach Verifikation des Passwortes (Anspruch 12) ausgeführt werden.

45. RFID-Tag nach Anspruch 1–23 mit der besonderen Eigenschaft, dass zusätzliche Speicher vorgesehen sind, die nur bei bestimmten Zuständen (Anspruch 15) oder nach Verifikation des Passwortes (Anspruch 12) zugegriffen werden können.

Es folgt kein Blatt Zeichnungen