(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 0 825 316 B2**

(12) **NEUE EUROPÄISCHE PATENTSCHRIFT**

(45) Veröffentlichungstag und Bekanntmachung des Hinweises auf die Entscheidung über den Einspruch:
06.02.2008 Patentblatt 2008/06

(45) Hinweis auf die Patenterteilung:
28.07.2004 Patentblatt 2004/31

(21) Anmeldenummer: **97202546.4**

(22) Anmeldetag: **19.08.1997**

(51) Int Cl.:
E05B 49/00 *(2006.01)* ***G07C 9/00*** *(2006.01)*

(54) Verfahren und System zum Einschreiben einer Schlüsselinformation

Method and system for writing an information key

Procédé et système pour inscrire une information de clé

(84) Benannte Vertragsstaaten:
DE FR GB

(30) Priorität: **22.08.1996 DE 19633802**

(43) Veröffentlichungstag der Anmeldung:
25.02.1998 Patentblatt 1998/09

(73) Patentinhaber:
- **Philips Intellectual Property & Standards GmbH**
  20099 Hamburg (DE)
  Benannte Vertragsstaaten:
  DE
- **Koninklijke Philips Electronics N.V.**
  5621 BA Eindhoven (NL)
  Benannte Vertragsstaaten:
  FR GB

(72) Erfinder:
- **Buhr, Wolfgang**
  Steindamm 94,
  20099 Hamburg/DE (DE)
- **Hörner, Helmut**
  Steindamm 94,
  20099 Hamburg (DE)

(74) Vertreter: **Peters, Carl Heinrich**
Philips Intellectual Property & Standards GmbH,
Postfach 50 04 42
52088 Aachen (DE)

(56) Entgegenhaltungen:
EP-A- 0 663 650
EP-A- 0 723 896
EP-B- 0 788 946
DE-A- 4 123 666
DE-A- 4 441 415
DE-C- 19 532 067

EP 0 825 316 B2

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren und ein System zum Einschreiben einer von einer zentralen Stelle gesichert zu einer entfernten Stelle übertragenen Schlüsselinformation in einen dort vorhandenen Datenträger. Bei einer bevorzugten Anwendung ist der Datenträger ein Schlüssel für ein Kraftfahrzeug, wobei der Schlüssel von einem Händler an den rechtmäßigen Besitzer des Kraftfahrzeugs ausgegeben werden soll, beispielsweise weil dieser einen Schlüssel zusätzlich benötigt oder einen ursprünglich beim Kauf des Kraftfahrzeugs empfangenen Schlüssel verloren hat. Es sei jedoch bemerkt, daß das erfindungsgemäße Verfahren bzw. System auch für andere Anwendungsfälle geeignet ist, beispielsweise für Schlüssel für Zugangskontrollen zu bestimmten Räumen oder Bereichen. Mit dem erfindungsgemäßen Verfahren bzw. System können ganz allgemein ausgewählte zugeordnete Informationen gesichert in einen Datenträger eingeschrieben werden.

[0002] In der EP 0 723 896 A2 wird ein Verfahren zur Diebstahlsicherung motorangetriebener Kraftfahrzeuge beschrieben, unter Verwendung eines Diebstahlsicherungssystems, mit einem die Wegfahrsperrenfunktion enthaltenden Steuergerät, mindestens einer weiteren diebstahlrelevanten Systemkomponente und Übertragungsstrecken zur bidirektionalen Kommunikation zwischen den diebstahlrelevanten Systemkomponenten, einer externen Zentralstelle, sowie einer Übertragungseinheit, zur Datenübertragung zwischen den diebstahlrelevanten Systemkomponenten und der Zentralstelle. Um eine sichere und zuverlässige Inbetriebnahme der diebstahlrelevanten Systemkomponenten zu gewährleisten, ist vorgesehen, daß alle diebstahlrelevanten Systemkomponenten des Diebstahlsicherungssystems vor ihrer erstmaligen Inbetriebnahme jeweils eine für die jeweilige Systemkomponente charakteristische Identifikationsnummer und eine von außerhalb der Systemkomponente nichtauslesbare, individuelle Geheimnummer in einem nichtflüchtigen Datenspeicher der Systemkomponente abgespeichert, versehen werden. Durch die Zentralstelle werden die Identifikationsnummern und die Geheimnummern der diebstahlrelevanten Systemkomponenten registriert. Die zur Identifizierung der jeweiligen diebstahlrelevanten Systemkomponente dienenden Identifikationsnummern werden innerhalb des Diebstahlsicherungssystems und zwischen dem Diebstahlsicherungssystem und der Zentralstelle im Klartext übertragen. Die nicht im Klartext übertragenen Geheimnummern der diebstahlrelevanten Systemkomponenten dienen als Kommunikationsschlüssel für layptologische Protokolle bei der Datenübertragung der diebstahlrelevanten Systemkomponenten innerhalb des Diebstahlsicherungssystems oder/und mit der Zentralstelle.

[0003] Wenn eine Schlüsselinformation, die an einer zentralen Stelle gespeichert ist, in einen Datenträger an einer entfernten Stelle eingeschrieben werden soll, muß bei üblichen Systemen verhindert werden, daß die Übertragung der Schlüsselinformation zur entfernten Stelle unberechtigt abgehört werden kann, da sonst ein Betrüger die unberechtigt abgehörte Schlüsselinformation in eigene Datenträger einschreiben kann und damit sich beispielsweise unberechtigt Zugang zu gesicherten Räumen oder Bereichen verschaffen kann. Die andere Möglichkeit, in der zentralen Stelle die Schlüsselinformation in den Datenträger einzuschreiben und diesen dann zu der entfernten Stelle zu versenden, ist auch ungünstig, da der Datenträger beim Transport gestohlen werden kann.

[0004] Aufgabe der Erfindung ist es, ein Verfahren zum sicheren Einschreiben einer Schlüsselinformation in einen Datenträger anzugeben, der an einer anderen Stelle als die Stelle, wo die Schlüsselinformation erzeugt wird bzw. gespeichert ist, ausgegeben wird.

[0005] Diese Aufgabe wird erfindungsgemäß dadurch gelöst, daß der Schlüssel eine Ident-Information gespeichert enthält, die von außerhalb nicht auslesbar und somit geheim ist, und daß die Schlüsselinformation in der zentralen Stelle mit dieser Ident-Information verschlüsselt und die verschlüsselte Information zum Datenträger an der Ausgabestelle übertragen wird. Im Datenträger wird diese verschlüsselte Schlüsselinformation wieder entschlüsselt und gespeichert.

[0006] Dieses Verfahren hat den Vorteil, daß die Datenträger frei versandt werden können, da sie keine Schlüsselinformation enthalten, so daß ein eventueller Dieb die Datenträger nicht benutzen kann. Das unberechtigte Abhören einer übertragenen verschlüsselten Schlüsselinformation ist für einen Betrüger ebenfalls nicht von Nutzen, wenn er nicht einen Datenträger mit der richtigen Ident-Information hat, in die er die verschlüsselte Schlüsselinformation einschreiben könnte.

[0007] Dabei ist es wichtig, daß jeder Datenträger eine weitere, offene Ident-Information enthält, die auslesbar ist. Damit ist es dann möglich, daß jeder Datenträger eine individuelle, von anderen Datenträgern unterschiedliche Ident-Information gespeichert enthält, indem die Zuordnung zwischen der weiteren, offenen Ident-Information und der geheimen Ident-Information an der zentralen Stelle gespeichert wird. Mit dieser Maßnahme kann eine verschlüsselte Schlüsselinformation ausschließlich nur von einem, dem richtigen Datenträger richtig entschlüsselt werden.

[0008] Um die Zuordnungen von geheimer Ident-Information und Schlüsselinformation sowie der weiteren, offenen Ident-Information leichter organisieren zu können, ist es zweckmäßig, wenn in den Datenträger an einer weiteren Stelle die Ident-Information und die offene Ident-Information eingeschrieben wird, bevor der Datenträger zur entfernten Stelle transportiert wird. Diese weitere Stelle muß dann über eine geschützte Informationsübertragungsverbindung mit der zentralen Stelle gekoppelt sein, damit dort die gleichen Informationen eingeschrieben werden können. Die weitere Stelle kann auch mit der zentralen Stelle identisch sein.

[0009] Die zum Datenträger zu übertragende Schlüs-

selinformation ist wenigstens einem individuellen Objekt, beispielsweise einem Kraftfahrzeug eindeutig zugeordnet. Wenn ein Datenträger einem solchen individuellen Objekt zugeordnet werden soll, muß die dieses Objekt kennzeichnende Objekt-Information zur zentralen Stelle übertragen werden. Um auch diesen Übertragungsweg zu sichern, ist es zweckmäßig, die Objekt-Information vor der Übertragung zur zentralen Stelle mit der weiteren, offenen Ident-Information zu verschlüsseln.

[0010] Für die Verschlüsselung von Daten sind eine Vielzahl verschiedener Verfahren bekannt. Bei dem erfindungsgemäßen Verfahren kann als besonders einfache Verschlüsselung und Entschlüsselung der Schlüsselinformation und der Objekt-Information eine Exclusiv-Oder-Verknüpfung mit der Ident-Information verwendet werden. Da die Ident-Information geheim ist, ist selbst bei Kenntnis des Verschlüsselungsverfahrens eine Entschlüsselung ohne Kenntnis der Schlüsselinformation nicht möglich.

[0011] Zusätzlich oder auch anstelle der Verschlüsselung mittels Exclusiv-Oder-Verknüpfung kann für die Verschlüsselung der Objekt-Information vor der Übertragung von der entfernten Stelle zur zentralen Stelle noch ein unsymmetrisches Verschlüsselungsverfahren eingesetzt werden, wobei für die Verschlüsselung der Objekt-Information bzw. der verschlüsselten Objekt-Information der offene Schlüssel verwendet wird, während in der zentralen Stelle die Entschlüsselung mit dem geheimen Schlüssel des unsymmetrischen Verschlüsselungsverfahrens durchgeführt wird.

[0012] Die Erfindung betrifft ferner ein System zum Einschreiben einer von einer zentralen Stelle gesichert zu einer entfernten Stelle übertragenen Schlüsselinformation in einen dort vorhandenen Datenträger sowie einen Datenträger und ein Terminal zur Verwendung in einem derartigen System.

[0013] Ein Ausführungsbeispiel der Erfindung wird nachfolgend anhand der Zeichnung näher erläutert. Darin enthält eine zentrale Stelle 20 zwei Speicher 21 und 25. Der Speicher 21 enthält zwei Gruppen 22 und 23 von Speicherplätzen, die jeweils paarweise einander zugeordnet sind. Durch Aufrufen eines Speicherplatzes der Gruppe 23 mit einer bestimmten Information, nämlich einer offenen Ident-Information eines bestimmten Datenträgers bei Datenträgern mit individuellen unterschiedlichen Ident-Informationen oder der Angabe einer Datenträgergruppe bei Datenträgern mit gruppenweise gleicher Ident-Information, wird diese zugehörige Ident-Information aus dem zugeordneten Speicherplatz der Gruppe 22 ausgelesen.

[0014] In entsprechender Weise umfaßt der Speicher 25 in diesem Beispiel drei Gruppen 26, 27 und 28 von Speicherplätzen. In den Speicherplätzen der Gruppe 26 sind Objekt-Informationen gespeichert, und jedem dieser Speicherplätze ist ein bestimmter Speicherplatz der Gruppe 27 zugeordnet, der eine diesem Objekt zugeordnete Schlüsselinformationen enthält. Ferner sind jedem Speicherplatz der Gruppe 26 vorzugsweise mehrere Speicherplätze der Gruppe 28 zugeordnet die eine Anzahl Identifiziernummern enthalten. Deren Bedeutung wird später etwas näher erläutert.

[0015] An einer weiteren Stelle befindet sich ein Datenträger 10. In der Praxis sind selbstverständlich viele Datenträger vorhanden, die untereinander gleich aufgebaut sind und für die der hier angedeutete Datenträger 10 repräsentativ ist. Dieser Datenträger 10 enthält eine Verarbeitungseinheit 11 und vier Speicherplätze 12 bis 15. Der Speicherplatz 12 dient zum Speichern einer Ident-Information, die nur intern im Datenträger 10 verarbeitet werden kann und in keinem Fall nach außen abgegeben wird. Der Speicherplatz 13 enthält eine den individuellen Datenträger kennzeichnende weitere, offene Ident-Information, die nach außen ausgelesen werden kann. Diese beiden Informationen werden vorzugsweise von der zentralen Stelle 20 geliefert, wo diese beiden Informationen in zwei einander zugeordneten Speicherplätzen der Gruppen 22 und 23 des Speichers 21 eingeschrieben werden, und diese Informationen werden auch an der weiteren Stelle, an der sich der Datenträger 10 zunächst befindet, in die Speicherplätze 12 und 13 eingeschrieben. Die weitere Stelle kann mit der zentralen Station 20 identisch sein.

[0016] Dieses Einschreiben in Speicherplätze 12 und 13 erfolgt für eine Vielzahl von Datenträgern, und diese Datenträger werden dann über einen Transportweg 19 zu einer entfernten Stelle transportiert. Dieser Transportweg verläuft zumindest zum Teil über einen nicht geschützten Bereich, der durch die strichpunktierte Linie 39 angedeutet ist. Während dieses Teils des Transportwegs können die Datenträger möglicherweise gestohlen werden. Durch einen solchen Diebstahl kann jedoch kein wesentlicher Schaden entstehen, da die Datenträger noch keine Schlüsselinformation enthalten und somit an keinem Objekt benutzbar sind.

[0017] Wenn an der entfernten Stelle in einen Datenträger, nämlich in den in der Figur etwas ausführlicher dargestellten Datenträger 10', eine Schlüsselinformation für ein bestimmtes Objekt eingeschrieben werden soll, wird dieser Datenträger 10' mit einem Terminal 40 in Verbindung gebracht. Dadurch wird aus dem Speicherplatz 13' die darin enthaltene offene Ident-Information ausgelesen und über die Verbindung 43 dem Terminal 40 zugeführt. Ferner wird über einen Eingang 41, beispielsweise über eine Tastatur, eine Objekt-Information eingegeben. Diese beiden Informationen werden einer Verschlüsselungsvorrichtung zugeführt, die hier aus zwei Teilen 42 und 44 besteht.

[0018] Der Teil 42 der Verschlüsselungsvorrichtung ist hier als Exclusiv-Oder-Verknüpfung ausgeführt. Die verknüpfte Information, die also die mit der offenen Ident-Information verschlüsselte Objekt-Information darstellt, wird einem Teil 44 zugeführt, der eine unsymmetrische Verschlüsselung, beispielsweise nach dem RSA-Verfahren, mit einem festen Schlüssel durchführt, der hier als über einen Eingang 45 zugeführt angedeutet ist. Dieser Schlüssel braucht nicht geheim zu sein, da mit seiner

Hilfe eine Entschlüsselung nicht möglich ist.

[0019] Die zusätzliche Verschlüsselung mit der offenen Ident-Information bringt eine wesentliche Verbesserung der Sicherheit. Angenommen, die von einer Werkstatt übertragenen Daten, nämlich verschlüsselte Objekt-Information und offene Identinformation, wird von einem Betrüger abgehört, der selbst vorprogrammierte Schlüssel besitzt. Wenn dieser Betrüger die gleiche verschlüsselte Objekt-Information überträgt, aber mit der offenen Ident-Information seines Schlüssels, würde er ohne die Verschlüsselung mit der offenen Ident-Information die Schlüsselinformation für das Objekt erhalten, die mit der geheimen Ident-Information seines Schlüssels verschlüsselt ist und somit im Schlüssel richtig entschlüsselt wird, so daß ein gültiger Schlüssel für das Objekt widerrechtlich erhalten wird. Durch die zusätzliche Verschlüsselung mit der offenen Ident-Information wird die vom Betrüger übertragene verschlüsselte Objekt-Informationan der zentralen Stelleaber nicht richtig entschlüsselt, so daß die gewünschte Schlüsselinformation nicht aus dem Speicher 25 ausgelesen wird. Wenn der Betrüger aber die ebenfalls abgehörte offene Ident-Information mit überträgt, erhält er lediglich eine Schlüsselinformation, die nicht mit der in seinem Schlüssel gespeicherten geheimen Ident-Information verschlüsselt ist und die also nicht entschlüsselt werden kann. Es ist also nicht möglich, durch Belauschen einer berechtigten Übertragung für ein Objekt Daten zu erhalten,mit denen unbrechtigt ein Schlüssel für das gleiche Objekt erzeugt werden kann.

[0020] Die vom Teil 44 über die Leitung 47 abgegebene verschlüsselte Information wird nun ebenso wie die offene Ident-Information über die Leitung 43 der zentrale Stelle 20 zugeführt. Diese Übertragung kann über einen nicht gesicherten Weg erfolgen, da die verschlüsselte Information auf der Leitung 47 ohne Kenntnis des geheimen Schlüssels der unsymmetrischen Verschlüsselung nicht entschlüsselt werden kann und die offene Ident-Information keinen direkten Hinweis auf die im Datenträger benötigte Schlüsselinformation enthält.

[0021] In der zentralen Stelle 20 wird die verschlüsselte Information auf der Leitung 47 einer Entschlüsselungsvorrichtung zugeführt, die die Teile 32 und 34 umfaßt. Im Teil 34 wird eine Entschlüsselung der über die Leitung 47 übertragenen Information durchgeführt, und zwar mit Hilfe eines geheimen Schlüssels, der hier über einen Eingang 35 zugeführt angedeutet ist. Am Ausgang 37 des Teils 34 der Entschlüsselungsvorrichtung liegt dann die gleiche Information vor wie am Ausgang der Exclusiv-Oder-Verknüpfung 42 im Terminal 40. Dies ist jedoch noch nicht die über den Eingang 41 des Terminals 40 zugeführte Objekt-Information. Daher führt die Leitung 37 auf eine Exclusiv-Oder-Verknüpfung 32, die an einem weiteren Eingang die offene Ident-Information über die Leitung 43 erhält. Am Ausgang 33 der Exclusiv-Oder-Verknüpfung 32 liegt nun die entschlüsselte Objekt-Information vor, mit der der Speicher 25 angesteuert wird. Dabei wird in der Gruppe 26 der Speicherplatz ausgewählt, der diese Objekt-Information enthält, und aus dem zugehörigen Speicherplatz der Gruppe 27 wird die Schlüsselinformation ausgelesen. Ferner wird mit Hilfe der offenen Ident-Information auf der Leitung 43 der Speicher 21 angesteuert, indem der Speicherplatz der Gruppe 23 aufgesucht wird, der diese Ident-Information enthält, und der zugehörige Speicherplatz der Gruppe 22, der die geheime Ident-Information enthält, wird ausgelesen.

[0022] Die aus dem Speicher 21 und dem Speicher 25 ausgelesene Information wird einer Verschlüsselungsanordnung 30 zugeführt, die hier ebenfalls als Exclusiv-Oder-Verknüpfung ausgeführt ist. Die an deren Ausgang 31 auftretende Information wird nun zur entfernten Stelle übertragen, wobei der Übertragungsweg nicht sicher sein muß, da die entschlüsselte Schlüsselinformation aus der Information auf der Leitung 31 nur mit Hilfe der richtigen geheimen Ident-Information zu gewinnen ist, die jedoch im Datenträger verborgen gespeichert ist und nicht direkt übertragen wird.

[0023] Im vorliegenden Beispiel wird aus dem Speicher 25 außerdem noch aus einem zugeordneten Speicherplatz der Gruppe 28 eine Identifiziernummer ausgelesen und über die Leitung 38 zur entfernten Stelle übertragen, wobei ebenfalls ein ungesicherter Weg verwendet werden kann.

[0024] In der entfernten Stelle werden die Informationen auf der Leitung 31 und der Leitung 38 über das Terminal 40 dem Datenträger 10' zugeführt. Die Identifiziernummer auf der Leitung 38 wird im Datenträger 10' direkt in den Speicherplatz 15' eingeschrieben, während die verschlüsselte Schlüsselinformation auf der Leitung 31 einer Entschlüsselungsvorrichtung 17 zugeführt wird, die an einem weiteren Eingang die geheime Ident-Information aus dem Speicherplatz 12' erhält. Diese Entschlüsselungsvorrichtung ist wieder als Exclusiv-Oder-Verknüpfung ausgeführt und gibt somit am Ausgang die entschlüsselte Schlüsselinformation ab, die in den Speicherplatz 14' eingeschrieben wird. Damit enthält der Datenträger 10' nun alle für seine Benutzung bei einem bestimmten Objekt, beispielsweise bei einem Kraftfahrzeug, notwendigen Informationen, ohne daß die entscheidend wichtige Schlüsselinformation bei der Übertragung auf unberechtigte Weise ermittelt werden kann.

[0025] Die Identifiziernummer im Speicherplatz 15' ist für das beschriebene Verfahren nicht unbedingt notwendig und dient, wenn der Datenträger ein Schlüssel für ein Kraftfahrzeug ist, dazu, daß im Kraftfahrzeug zunächst über diese Identifiziernummer geprüft wird, ob es sich um einen zulässigen Schlüssel handelt, bevor mit Hilfe der Schlüsselinformation geprüft wird, ob es sich um einen berechtigten Schlüssel handelt. Wenn nämlich mit einem nicht berechtigten Schlüssel, d.h. mit einer falschen Schlüsselinformation, eine Anzahl Startversuche durchgeführt worden sind, werden alle Funktionen des Kraftfahrzeugs dauerhaft blockiert, wobei die Blockierung nur mit einer bestimmten, geheimen Prozedur auf-

gehoben werden kann. Durch die Identifiziernummer wird also verhindert, daß mit einem falschen Schlüssel, der z.B. zu einem anderen Kraftfahrzeug gehört und somit selbstverständlich eine andere Schlüsselinformation enthält, als gültig erkannte Fehlversuche durchgeführt werden können.

[0026] Zweckmäßig enthält jeder für ein Kraftfahrzeug berechtigte Schlüssel eine andere Identifiziernummer, und dafür sind im Speicher 25 zu jeder Objekt-Information und ebenso in dem zugehörigen Objekt eine Anzahl Identifiziernummern gespeichert.

[0027] Es ist klar, daß die Verschlüsselung im Terminal 40 mit Hilfe der Teile 42 und 44 und die entsprechende Entschlüsselung in der zentralen Stelle auch auf andere Weise als beschrieben durchgeführt werden kann. Wichtig ist, daß die Information auf der Leitung 47 in einer Weise verschlüsselt ist, die eine Entschlüsselung nur durch übertragene Informationen nicht möglich macht.

Patentansprüche

1. Verfahren zum Einschreiben einer von einer zentralen Stelle gesichert zu einer entfernten Stelle übertragenen Schlüsselinformation in einen dort vorhandenen Datenträger, der nach dem Einschreiben einem ausgewählten von mehreren Objekten über die Schlüsselinformation eindeutig zugeordnet ist und der eine nach außen nicht abgebbare Ident-Information sowie eine weitere, offene Ident-Information, die auslesbar ist, gespeichert enthält, die einander zugeordnet auch in der zentralen Stelle gespeichert sind, wobei zunächst eine das individuelle Objekt kennzeichnende Objekt-Information sowie die weitere, offene Ident-Information zur zentralen Stelle übertragen werden, dort die zur Objekt-Information gespeicherte Schlüsselinformation ausgelesen und mit der zur übertragenen weiteren, offenen Ident-Information gespeicherten Ident-Information verschlüsselt und die verschlüsselte Schlüsselinformation zum Datenträger übertragen und im Datenträger mit der darin gespeicherten Ident-Information entschlüsselt und die entschlüsselte Schlüsselinformation gespeichert wird,
   wobei in den Datenträger an einer weiteren Stelle, die über eine geschützte Informationsübertragungsverbindung mit der zentralen Stelle gekoppelt ist, die Ident-Information und die weitere, offene Ident-Information vor dem Transport des Datenträgers zur entfernten Stelle eingeschrieben wird und diese Ident-Information auch an der zentralen Stelle gespeichert wird,
   und wobei die Objekt-Information vor der Übertragung zur zentralen Stelle mit der offenen Ident-Information verschlüsselt wird.

2. Verfahren nach Anspruch 1, wobei die Verschlüsselung und Entschlüsselung der Schlüsselinformation und der Objekt-Information durch eine Exclusiv-Oder-Verknüpfung mit der weiteren, offenen Ident-Information erfolgt.

3. Verfahren nach Anspruch 1, wobei die verschlüsselte Objekt-Information vor der Übertragung durch ein unsymmetrisches Verschlüsselungsverfahren mit den diesem zugeordneten öffentlichen Schlüssel zusätzlich verschlüsselt wird und in der zentralen Stelle mit dem geheimen Schlüssel des Verschlüsselungsverfahrens entschlüsselt wird.

4. System zum Einschreiben einer von einer zentralen Stelle gesichert zu einer entfernten Stelle übertragenen Schlüsselinformation in einen dort vorhandenen Datenträger, der nach dem Einschreiben einem ausgewählten von mehreren Objekten über die Schlüsselinformation eindeutig zugeordnet ist, wobei die zentrale Stelle einen ersten Speicher, der wenigstens eine Ident-Information und eine zugeordnete weitere Ident-Information sowie für jedes der mehreren Objekte eine das Objekt kennzeichnende Objekt-Information und die dem Objekt zugeordnete Schlüsselinformation enthält, und eine Verschlüsselungsanordnung zum Verschlüsseln einer aus dem ersten Speicher ausgelesenen Schlüsselinformation mit der Ident-Information sowie eine Übertragungsanordnung zum Übertragen der verschlüsselten Schlüsselinformation an die entfernte Stelle umfaßt, und wobei der Datenträger einen zweiten Speicher, der einen ersten Speicherplatz für eine Ident-Information, einen zweiten Speicherplatz für eine Schlüsselinformation und einen dritten Speicherplatz für eine den Datenträger kennzeichnende weitere Ident-Information enthält, sowie eine Entschlüsselungsvorrichtung umfaßt, die mit einem Informationseingang des Datenträgers und mit dem ersten Speicherplatz verbunden ist zum Abgeben einer entschlüsselten Schlüsselinformation nach Empfang einer verschlüsselten Schlüsselinformation und zum Einschreiben der entschlüsselten Schlüsselinformation in den zweiten Speicherplatz.
   wobei an der entfernten Stelle ein Terminal vorgesehen ist, mit dem der Datenträger koppelbar ist, um das Auslesen der weiteren Ident-Information auszulösen und diese weitere Ident-Information an die zentrale Stelle zu übertragen und die danach von der zentralen Stelle übertragene verschlüsselte Schlüsselinformation zu empfangen und an den Datenträger zu übertragen, und
   wobei das Terminal eine Verschlüsselungsvorrichtung enthält, um eine eingegebene Objekt-Information mit der weiteren Ident-Information zu verschlüsseln und an die zentrale Stelle zu übertragen, und die zentrale Stelle eine Entschlüsselungsvorrichtung enthält, um die empfangene verschlüsselte Objekt-Information mittels der ebenfalls übertragenen weiteren Ident-Information zu entschlüsseln und mit

der entschlüsselten Objekt-Information den ersten Speicher anzusteuern und die zugeordnete Schlüsselinformation auszulesen.

5. System nach Anspruch 4, wobei die Verschlüsselungsvorrichtung in der zentralen Stelle und die Entschlüsselungsvorrichtung im Datenträger als Exclusiv-Oder-Verknüpfungselement aufgebaut sind.

6. System nach Anspruch 4 oder 5, wobei die Verschlüsselungsvorrichtung im Terminal eingerichtet ist, die verschlüsselte Objekt-Information zusätzlich mit dem öffentlichen Schlüssel einer unsymmetrischen Verschlüsselung zusätzlich zu verschlüsseln und an die zentrale Stelle zu übertragen und die Entschlüsselungsvorrichtung in der zentralen Stelle eingerichtet ist, um die empfangene zusätzlich verschlüsselte Objekt-Information mit dem geheimen Schlüssel der unsymmetrischen Verschlüsselung und mit der ebenfalls empfangenen weiteren Ident-Information zu entschlüsseln und die entschlüsselte Objekt-Information an den ersten Speicher abzugeben.

7. Datenträger zur Verwendung in einem System nach einem der Ansprüche 4 bis 6, mit einer Entschlüsselungsvorrichtung und einem Speicher mit einem ersten Speicherplatz zum Speichern einer Ident-Information und einem zweiten Speicherplatz zum Aufnehmen einer Schlüsselinformation, wobei die Entschlüsselungsvorrichtung mit dem ersten Speicherplatz gekoppelt ist, um eine empfangene verschlüsselte Schlüsselinformation mittels der aus dem ersten Speicherplatz ausgelesenen Ident-Information zu entschlüsseln und die entschlüsselte Schlüsselinformation in den zweiten Speicherplatz einzuschreiben, und wobei das Ausgeben der Ident-Information aus dem Datenträger gesperrt ist, wobei die Entschlüsselungsvorrichtung als Exclusiv-Oder-Verknüpfungselement ausgebildet ist.

8. Datenträger nach Anspruch 7, wobei der Speicher einen dritten Speicherplatz zum Aufnehmen einer weiteren Ident-Information aufweist, und der Speicher von außerhalb des Datenträgers ansteuerbar ist, um die weitere Ident-Information aus dem Speicher nach außen abzugeben.

9. Terminal zur Verwendung in einem System nach einem der Ansprüche 4 bis 6, mit einer Koppelvorrichtung für einen Datenträger, einer Übertragungsvorrichtung für Informationen, einer Eingabevorrichtung zum Eingeben von Informationen und einer Verschlüsselungsvorrichtung mit zwei Eingängen, die mit der Eingabevorrichtung und der Koppelvorrichtung verbunden sind, und einem Ausgang, der mit der Übertragungsvorrichtung verbunden ist, um eine über die Eingabevorrichtung eingegebene Objekt-Information mit einer über die Koppelvorrichtung zugeführte Ident-Information zu verschlüsseln und die verschlüsselte Objekt-Information an die Übertragungsvorrichtung abzugeben.

10. Terminal nach Anspruch 9, wobei die Verschlüsselungsvorrichtung dazu eingerichtet ist, die verschlüsselte Objekt-Information zusätzlich mit dem öffentlichen Schlüssel einer unsymmetrischen Verschlüsselung zu verschlüsseln und nur die zusätzlich verschlüsselte Objekt-Information an die Übertragungsvorrichtung abzugeben.

Claims

1. A method of writing key information transmitted securely from a central station to a remote station into a data carrier available at said remote station, which after being written into is unambiguously assigned to a selected one of a plurality of objects through the key information and which stores identification information that is not externally readable, as well as further public identification information that is readable, which types of identification information are stored, assigned to one another, also in the central station, wherein first object information characteristic of the individual object as well as the further public identification information is transmitted to the central station,
where the key information which has been stored for the object information is read out and encrypted with the identification information stored for the transmitted further public identification information and the encrypted key information is transmitted to the data carrier and is decrypted there with the identification information stored thereon and the decrypted key information is stored,
where at a further data carrier location, which is coupled to the central station via a secure information transmission link, the identification information and the further, public identification information is written prior to the transport from the data carrier to the remote station and this identification information is also stored at the central station,
and where the object information is encrypted with the further public identification information prior to the transmission to the central station.

2. A method as claimed in claim 1, wherein the encryption and decryption of the key information and of the object information is effected by means of an Exclusive-Or combination with the further open identification information.

3. A method as claimed in claim 1, wherein prior to transmission the encrypted object information is additionally encrypted with the public key associated

with an asymmetrical encryption method and is decrypted in the central station by means of the secret key of the encryption method.

4. A system for writing key information transmitted securely from a central station to a remote station into a data carrier available at said remote station, which key information after being written is unambiguously assigned to a selected one of a plurality of objects, wherein the central station comprises a first memory which stores at least identification information of one type and associated identification information of a further type, as well as object information characteristic of the object for each of the plurality of objects and stores the key information associated with the object, and an encryption device for encrypting key information read from the first memory with the identification information and a transmission device for transmitting the encrypted key information to the remote station, and wherein the data carrier comprises a second memory which contains a first storage area for identification information of one type, a second storage area for key information and a third storage area for identification information of a further type characteristic of the data carrier, and a decryption device which is connected to an information input of the data carrier and to the first storage area in order to supply decrypted key information upon reception of encrypted key information and to write the decrypted key information into the second storage area, wherein the remote station includes a terminal adapted to be coupled to the data carrier to initiate the read-out of the further identification information and to transmit this further identification information to the central station and to receive the encrypted key information subsequently transmitted from the central station and transmit it to the data carrier, and wherein the terminal includes an encryption device for encrypting written object information with the further identification information and transmit it to the central station, and the central station includes a decryption device for decrypting the received encrypted object information by means of the equally transmitted further identification information and for controlling the first memory and reading out the associated key information by means of the decrypted object information.

5. A system as claimed in claim 4, wherein the encryption device in the central station and the decryption device in the data carrier are constructed as Exclusive-Or logic elements.

6. A system as claimed in claim 4 or 5, wherein the encryption device in the terminal is adapted to encrypt the encrypted object information additionally with the public key of an asymmetrical encryption and to transmit it to the central station, and the decryption device in the central station is adapted to decrypt the received, additionally encrypted object information with the secret key of the asymmetrical encryption and with the likewise received further identification information and to supply the decrypted object information to the first memory.

7. A data carrier for use in a system as claimed in any one of the claims 4 to 6, comprising a decryption device and a memory having a first storage area for storing identification information and a second storage area for storing key information, the decryption device being coupled to the first storage area to decrypt received encrypted key information by means of the identification information read from the first storage area and to write the decrypted key information into the second storage area while read-out of the identification information from the data carrier is inhibited, wherein the decryption device is constructed as an Exclusive-Or logic element.

8. A data carrier as claimed in claim 7, wherein the memory comprises a third storage area for storing further identification information, and the memory is controllable from outside the data carrier in order to issue the further identification information from the memory.

9. A terminal for use in a system as claimed in any one of the claims 4 to 6, comprising a coupling device for a data carrier, a transmission device for information, an input device for the entry of information, and an encryption device having two inputs which are connected to the input device and the coupling device, and an output connected to the transmission device, for encrypting object information, which has been entered via the input device, with identification information applied via the coupling device, and for supplying the encrypted object information to the transmission device.

10. A terminal as claimed in claim 9, wherein the encryption device is adapted to encrypt the encrypted object information additionally with the public key of an asymmetrical encryption and to supply only the additionally encrypted object information to the transmission device.

Revendications

1. Procédé d'enregistrement d'une information de clé transmise de manière sécurisée d'un site central vers un site éloigné dans un support de données présent dans celui-ci qui, après enregistrement, est affecté de manière univoque à un objet sélectionné parmi plusieurs sur l'information de clé et qui contient une information d'identification enregistrée à ne pas

délivrer vers l'extérieur ainsi qu'une information d'identification ouverte supplémentaire qui peut être lue, lesquelles sont respectivement enregistrées après avoir été affectées l'une à l'autre dans le site central, une information d'objet caractérisant l'objet individuel ainsi que l'autre information d'identification ouverte étant d'abord transmises vers le site central, l'information de clé enregistrée à propos de l'information d'objet y étant lue et codée avec l'information d'identification supplémentaire à transmettre enregistrée avec l'information d'identification ouverte et l'information de clé codée étant transmise vers le support de données et décodée dans le support de données avec l'information d'identification qui y est enregistrée et l'information de clé décodée y étant enregistrée,
l'information d'identification et l'information d'identification supplémentaire ouverte étant enregistrées avant le transport du support de données vers le site éloigné dans le support de données à un autre endroit qui est couplé par l'intermédiaire d'une liaison protégée de transmission d'information avec le site central et cette information d'identification est également enregistrée dans le site central,
et l'information d'objet étant codée avant la transmission vers le site central avec l'information d'identification ouverte.

2. Procédé selon la revendication 1, le codage et le décodage de l'information de clé et de l'information d'objet étant assurés par une fonction OU exclusif avec l'information d'identification ouverte supplémentaire.

3. Procédé selon la revendication 1, dans lequel l'information d'objet codée est codée en supplément avant la transmission par un procédé de codage asymétrique avec la clé publique affectée à celui-ci, et décodée dans le site central avec la clé secrète du procédé de codage.

4. Système d'enregistrement d'une information de clé transmise de manière sécurisée d'un site central vers un site éloigné dans un support de données présent dans celui-ci qui, après enregistrement, est affecté de manière univoque à un objet sélectionné parmi plusieurs sur l'information de clé, le site central contenant une première mémoire qui contient au moins une information d'identification ainsi qu'une information d'identification supplémentaire affectée ainsi que, pour chacun des plusieurs objets, une information d'objet caractérisant l'objet et l'information de clé affectée à l'objet, et un dispositif de codage pour le codage d'une information de clé lue de la première mémoire avec l'information d'identification ainsi qu'un dispositif de transmission pour la transmission de l'information de clé codée au site central, le support de données contenant une deuxième mémoire qui comprend un premier emplacement de mémoire pour une information d'identification, un deuxième emplacement de mémoire pour une information de clé et un troisième emplacement de mémoire pour une information d'identification supplémentaire caractérisant le support de données ainsi qu'un dispositif de décodage qui est relié à une entrée d'information du support de données et au premier emplacement de mémoire en vue de la délivrance d'une information de clé décodée après réception d'une information de clé codée, et de l'enregistrement de l'information de clé décodée dans le deuxième emplacement de mémoire,
un terminal avec lequel le support de données peut être couplé étant prévu sur le site éloigné pour déclencher la lecture de l'information d'identification supplémentaire et transmettre cette information d'identification supplémentaire au site central et recevoir l'information de clé codée transmise ensuite par le site central et la transmettre au support de données, et
le terminal contenant un dispositif de codage afin de coder une information d'objet introduite avec l'information d'identification supplémentaire et la transmettre au point central et le point central contenant un dispositif de décodage afin de décoder l'information d'objet codée reçue à l'aide de l'information d'identification supplémentaire également transmise et de commander la première mémoire avec l'information d'objet décodée et de lire l'information de clé affectée.

5. Système selon la revendication 4, le dispositif de codage étant conçu dans le site central et le dispositif de décodage dans le support de données comme un élément de fonction OU exclusif.

6. Système selon la revendication 4 ou 5, le dispositif de codage étant prévu dans le terminal pour coder l'information d'objet codée en plus de la clé publique à l'aide d'un codage asymétrique et les transmettre au site central et le dispositif de décodage dans le site central est organisé pour pouvoir décoder l'information d'objet codée supplémentaire reçue avec la clé secrète du codage asymétrique et avec l'information d'identification supplémentaire également reçue et délivrer l'information d'objet décodée à la première mémoire.

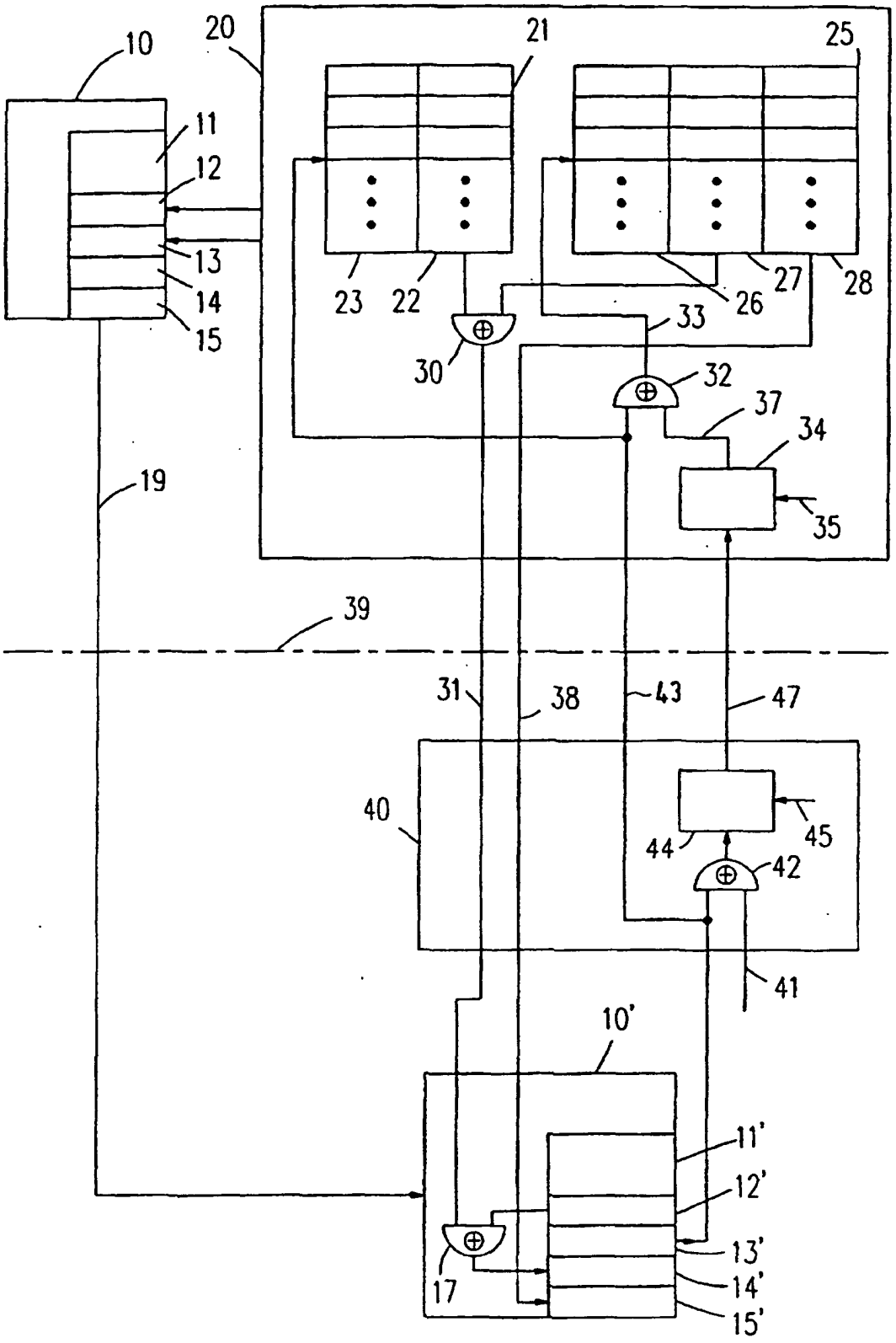
7. Support de données pour la mise en oeuvre dans un système selon l'une des revendications 4 à 6, avec un dispositif de décodage et une mémoire avec un premier emplacement de mémoire pour l'enregistrement d'une information d'identification et un deuxième emplacement de mémoire pour l'enregistrement d'une information de clé, le dispositif de décodage étant couplé avec le premier emplacement de mémoire afin de décoder une information de clé

codée reçue à l'aide de l'information d'identification lue à partir du premier emplacement de mémoire et d'enregistrer l'information de clé décodée dans le deuxième emplacement de mémoire et la délivrance de l'information d'identification hors du support de données étant bloquée, le dispositif de décodage étant conçu comme un élément de fonction OU exclusif.

8. Support de données selon la revendication 7, la mémoire présentant un troisième emplacement de mémoire pour l'enregistrement d'une information d'identification supplémentaire et la mémoire pouvant être commandée de l'extérieur du support de données afin de délivrer vers l'extérieur l'information de modification supplémentaire à partir de la mémoire.

9. Terminal pour la mise en oeuvre dans un système selon l'une des revendications 4 à 6, avec un dispositif de couplage pour un support de données, un dispositif de transmission pour les informations, un dispositif d'introduction pour l'introduction d'informations et un dispositif de codage avec deux entrées qui sont reliées au dispositif d'introduction et au dispositif de couplage et une sortie qui est reliée au dispositif de transmission afin de coder une information d'objet introduite par l'intermédiaire du dispositif d'introduction avec une information d'identification amenée par l'intermédiaire du dispositif de couplage et délivrer l'information d'objet codée au dispositif de transmission.

10. Terminal selon la revendication 9, le dispositif de codage étant conçu pour coder l'information d'objet codée en supplément avec la clé ouverte d'un codage asymétrique et délivrer seulement l'information d'objet codée en supplément au dispositif de transmission.


10
20
21
25
11
12
13
14
15
23
22
26
27
28
33
30
32
37
34
35
19
39
31
38
43
47
40
44
45
42
41
10'
11'
12'
13'
14'
15'
17

IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

Diese Liste der vom Anmelder aufgeführten Dokumente wurde ausschließlich zur Information des Lesers aufgenommen und ist nicht Bestandteil des europäischen Patentdokumentes. Sie wurde mit größter Sorgfalt zusammengestellt; das EPA übernimmt jedoch keinerlei Haftung für etwaige Fehler oder Auslassungen.

In der Beschreibung aufgeführte Patentdokumente

- EP 0723896 A2 **[0002]**