(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
30. Mai 2002 (30.05.2002)

PCT

(10) Internationale Veröffentlichungsnummer
WO 02/43012 A2

(51) Internationale Patentklassifikation[7]: G07D 7/00

(21) Internationales Aktenzeichen: PCT/DE01/04146

(22) Internationales Anmeldedatum:
7. November 2001 (07.11.2001)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
100 58 638.4 25. November 2000 (25.11.2000) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **ORGA KARTENSYSTEME GMBH** [DE/DE]; Am Hoppenhof 33, 33104 Paderborn (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **KAPPE, Frank** [DE/DE]; Kaiserforst 12, 33378 Rheda-Wiedenbrück (DE). **FISCHER, Dirk** [DE/DE]; Anemonenweg 3, 33106 Paderborn (DE). **RÜBBELKE, Hermann** [DE/DE]; Antoniustrasse 3, 33129 Delbrück (DE). **HENNEMEYER-SCHWENKER, Michael** [DE/DE]; Zur Imburg 4, 33165 Herbram (DE).

(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

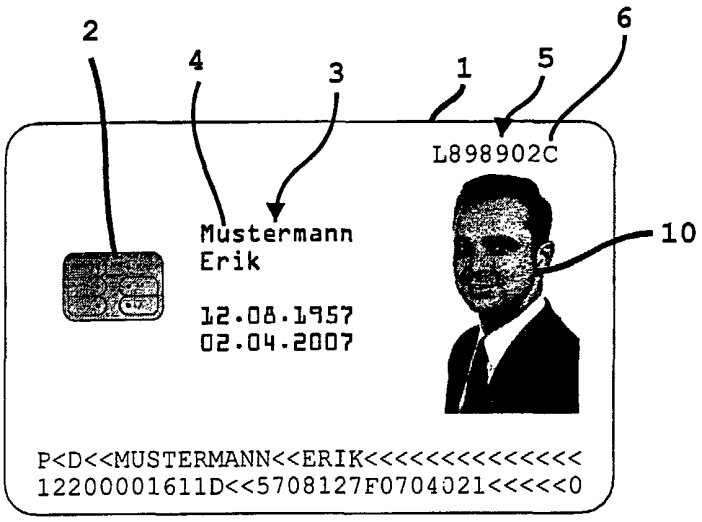
(84) Bestimmungsstaaten *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:
— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR PRODUCING A DATA CARRIER AND DATA CARRIER

(54) Bezeichnung: VERFAHREN ZUR HERSTELLUNG EINES DATENTRÄGERS SOWIE EIN DATENTRÄGER



(57) Abstract: The invention relates to a method for producing a data carrier such as an ID card or a credit card or a document of value or a security document. The data carrier comprises at least one first item of information (3) which is optically visible,especially readable, on the data carrier and is suitable for individualizing the data carrier in relation to other data carriers.The first item of information (3) is encrypted by means of an algorithm and the result of the encryption is stored on the data carrier in order to protect the data carrier against falsifications or manipulations.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zur Herstellung eines Datenträgers, wie eine Ausweis-, eine Kreditkarte oder dergleichen Wert- oder Sicherheitsdokument. Der Datenträger umfaßt mindestens eine erste Information (3), die visuell sichtbar, insbesondere lesbar auf dem Datenträger vorgesehen und geeignet ist, den Datenträger aus einer Reihe von Datenträgern zu individualisieren. Um den Datenträger gegen Fälschungen oder Manipulationen zu schützen, wird die erste Information (3) mittels eines Algorithmus verschlüsselt und das Ergebnis der Verschlüsselung wird auf dem Datenträger hinterlegt.

WO 02/43012 A2

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Verfahren zur Herstellung eines Datenträgers sowie ein Datenträger

Die Erfindung betrifft ein Verfahren zur Herstellung eines Datenträgers gemäß dem Oberbegriff von Anspruch 1 sowie einen insbesondere verfahrensgemäß hergestellten Datenträger nach dem Oberbegriff von Anspruch 11.

Bei den obigen Datenträgern handelt es sich um Wert- oder Sicherheitsdokumente, insbesondere um Ausweis- oder Kreditkarten, die neben allgemeinen Informationen individuelle Informationen, wie Benutzername, Benutzerporträt, Seriennummer oder dergleichen personen-, karten- oder dokumentspezifische Informationen aufweisen. Diese individuellen bzw. spezifischen Informationen sind bevorzugt Gegenstand von Fälschungen und Manipulationen und müssen entsprechend gesichert werden.

Aus der EP 0 906 834 A2 ist ein Datenträger mit wenigstens einer individuellen Information bekannt, wobei die individuelle Information eine Seriennummer umfaßt, die aus einem ersten Teil und einem zweiten Teil besteht. Der erste Teil und der zweite Teil der Seriennummer können eine unterschiedliche Farbe aufweisen und werden so auf dem Datenträger aufgebracht, daß die vollständige Seriennummer wiedergegeben wird. Durch die Teilung der Seriennummer und

durch das passergenaue Drucken der beiden Teile soll der Fälschungs- und Manipulationsschutz erhöht werden. Die Teilung der Seriennummer sowie die farbige Kennzeichnung der beiden Teile werden jedoch willkürlich festgelegt und bei einer Vielzahl von Datenträgern, wie Banknoten, in gleichbleibender Form und in gleichbleibender farbiger Gestaltung aufgebracht, so daß Fälschungen und Manipulationen nicht ausgeschlossen werden können.

Der Erfindung liegt daher die Aufgabe zugrunde, ein Verfahren zur Herstellung eines Datenträgers sowie einen Datenträger bereitzustellen, der einen verbesserten Fälschungs- oder Manipulationsschutz aufweist.

Diese Aufgabe wird durch die Merkmale der unabhängigen Ansprüche gelöst. Vorteilhafte Weiterbildungen sind in den Unteransprüchen beschrieben.

Ein Kerngedanke des erfindungsgemäßen Verfahrens besteht darin, daß eine erste Information, die eine individuelle Information darstellt, wie der Name des autorisierten Benutzers des Datenträgers, mittels eines Algorithmus verschlüsselt und das Ergebnis der Verschlüsselung auf dem Datenträger hinterlegt wird. Das Ergebnis der Verschlüsselung stellt eine zusätzliche Information dar, die von der Allgemeinheit nicht entschlüsselt werden kann. Nur autorisierte Personen, die über den Algorithmus verfügen, sind in der Lage, die zusätzliche Information zu entschlüsseln und anhand der zusätzlichen Information festzustellen, ob Fälschungen oder Manipulationen stattgefunden haben.

Vorteilhafterweise wird mindestens ein Zeichen der ersten Information in Abhängigkeit des Ergebnisses der Verschlüsselung markiert. Besonders bevorzugte Markierungen sind farbige oder sonstige visuell sichtbare Kennzeichnungen der Zeichen der ersten Information, um die Überprüfbarkeit zu erleichtern. Zusätzlich oder alternativ kann die Markierung der ersten Information durch andere geeignete Kennzeichnungen bewirkt werden, wobei unter geeigneten Kennzeichnungen diejenigen Kennzeichnungen verstanden werden, die, sofern sie nicht visuell erkennbar sind, mit entsprechenden Hilfsmitteln, wie Detektoren oder dergleichen Geräte, erfaßbar sind. Beispielsweise können fluoreszierende oder magnetische Kennzeichnungen der Zeichen der ersten Information vorgesehen sein.

Der der Verschlüsselung zugrunde liegende Algorithmus kann so ausgelegt sein, daß lediglich eine einzige Information, beispielsweise die erste Information in den Algorithmus einbezogen wird und als Ergebnis eine markierte erste Information resultiert. Um eine komplexere Verschlüsselung zu erzielen, sind neben der ersten Information eine oder mehrere zweite Informationen, wie Seriennummern oder dergleichen Informationen vorgesehen, die zusätzlich zur ersten Information in den Algorithmus einbezogen werden können. Die zweiten Informationen brauchen nicht visuell sichtbar oder lesbar auf dem Datenträger vorgesehen sein. Sie können versteckt und/oder verschlüsselt im Bereich oder außerhalb des Bereichs des Datenträgers hinterlegt sein, was den Fälschungs- oder Manipulationsschutz erhöht. Zur Durchführung der Verschlüsselung, insbesondere bei der Überprüfung des Datenträgers, werden die derartig hinterlegten zweiten

Informationen in maschinenlesbare bzw. rechnerverarbeitbare Zeichen umgewandelt.

Der Algorithmus wird im wesentlichen anhand von Operatoren durchgeführt, wobei hierfür eine Vielzahl von Operatoren zur Verfügung steht. Bevorzugt werden Operatoren für Bit-Manipulationen, wie exklusive Oder-Operatoren, oder binäre arithmetische Operatoren, wie Additions-Operatoren oder Modulo-Operatoren, angewendet. Diese Operatoren benötigen in der Regel zwei Operanden bzw. Informationen, um eine Verknüpfung durchzuführen. Sie können jedoch auch auf einen einzelnen Operanden bzw. auf eine einzelne Information angewendet werden, wenn beispielsweise dem anderen Operanden ein konstanter (Zahlen-) Wert zugewiesen wird. Vor Anwendung der Operatoren auf die zur Verschlüsselung vorgesehene(n) Information(en) werden bzw. wird diese zweckmäßigerweise in numerische bzw. ganzzahlige Zahlenwerte umgewandelt, beispielsweise anhand des ASCII-Zeichensatzes.

Anhand dieser Operatoren ist die Verschlüsselung auf einfache Weise durchführbar, ohne daß ausgehend vom Ergebnis, d.h. ausgehend von der markierten ersten Information, Rückschlüsse auf die Durchführung der Markierung bzw. auf die konkrete Durchführung des Algorithmus oder auf die in den Algorithmus einbezogenen Informationen möglich sind.

Ein vorteilhafter Schritt des Algorithmus besteht darin, daß durch die Anwendung eines oder mehrerer geeigneter Operatoren auf die erste und/oder zweite(n) Information(en) eine Folge von Ziffern erhalten wird. Vorzugsweise weist die Folge von Ziffern eine begrenzte Anzahl von unterschiedlichen Ziffernwerten auf. Dies läßt sich bevorzugt mit Hilfe des

binären Modulo-Operators erreichen, der zusätzlich oder alternativ zu den oben erwähnten Operatoren eingesetzt werden kann. Die Folge von Ziffern weist zweckmäßigerweise wenigstens zwei unterschiedliche Ziffernwerte, wie „0" oder „1" auf, wobei den Ziffern bzw. den Ziffernwerten jeweils eine bestimmte Kennzeichnung, wie eine Farbe, zugeordnet wird. Die so markierten Ziffern werden den Zeichen der ersten Information zugeordnet, so daß die Zeichen der ersten Information eine der zugeordneten Ziffer entsprechende Kennzeichnung erhalten. Die auf diese Weise erzeugte Markierung der ersten Information ist einfach durchführbar und stellt eine effektive Maßnahme zum Schutz gegen Fälschungen oder Manipulationen dar.

Ein gefälschter oder manipulierter Datenträger kann durch eine Überprüfung auf einfache Weise erkannt werden. Im Rahmen der Überprüfung wird bzw. werden zunächst die für die Durchführung der Verschlüsselung maßgebliche(n) Information(en) erfaßt. Anschließend wird der Algorithmus auf die Information(en) angewendet. Durch einen Vergleich der anhand des Algorithmus erhaltenen Markierung der ersten Information mit der auf dem Datenträger hinterlegten Markierung der ersten Information können unerlaubte Eingriffe problemlos festgestellt werden.

Die Erfindung befaßt sich ferner mit einem Datenträger, wie eine Ausweis-, Kreditkarte oder dergleichen Wert- oder Sicherheitsdokument. Der erfindungsgemäße Datenträger ist insbesondere nach dem oben beschriebenen Verfahren hergestellt. Ein Kerngedanke des erfindungsgemäßten Datenträgers besteht darin, daß die erste Information derart verschlüsselt ist, daß sie zumindest teilweise markiert auf dem Datenträger hinterlegt ist. Die Markierung der ersten

Information stellt ein Echtheitsmerkmal dar. Es ist daher nicht möglich, die markierte erste Information oder Teile davon zu verändern, ohne daß dies bei einer Überprüfung erkannt wird.

Von den eingangs beschriebenen Markierungen der ersten Information sind insbesondere die visuell erkennbaren Kennzeichnungen, wie eine wechselnde farbige oder eine unterschiedliche schriftbildliche Gestaltung der Zeichen der ersten Information, besonders bevorzugt. Diese visuell erkennbaren Kennzeichnungen lasssen sich sehr vorteilhaft in den Beschriftungsprozeß integrieren, beispielsweise wenn der Datenträger mit einem Laser (farblich) beschriftet wird.

Weitere bevorzugte und nachstehend aufgeführte Ausführungsformen der Erfindung sehen vor, daß eine oder mehrere zweite Information(en), die zur Verschlüsselung der ersten Information dienen, für nicht autorisierte Personen unzugänglich hinterlegt sind.

Gemäß einer vorteilhaften Ausführungsform ist bzw. sind die zweite(n) Information(en) in einem auf dem Datenträger vorgesehenen Speicher- oder Zusatzelement, wie ein integrierter Schaltkreis, Magnetstreifen oder dergleichen enthalten. Zusätzlich oder alternativ kann bzw. können die zweite(n) Information(en) außerhalb des Bereichs des Datenträgers vorgesehen sein, wobei die zweite(n) Information(en) vorzugsweise in einem externen Speicher, beispielsweise in einer zentralen Datenbank oder dergleichen Speichereinrichtung, gespeichert ist bzw. sind. Durch diese konstruktive Maßnahme wird die Überprüfung durch autorisierte Personen erleichtert, da die zweite(n) Information(en) auf

einfache Weise erfaßbar sind, indem sie aus den oben erwähnten Speichern ausgelesen wird bzw. werden. Darüberhinaus kann bei einer derart gesicherten Hinterlegung der zweiten Information(en) eine für alle Datenträger einheitliche zweite Information vorgesehen sein.

Eine weitere vereinfachte Überprüfungsmöglichkeit des erfindungsgemäßen Datenträgers ergibt sich gemäß einer weiteren bevorzugten Ausführungsform dadurch, daß die zur Verschlüsselung vorgesehene(n) Information(en) sowie der Algorithmus selbst in dem integrierten Schaltkreis des Datenträgers gespeichert sind. Zu diesem Zweck umfaßt der integrierte Schaltkreis vorzugsweise einen Mikroprozessorchip. Mikroprozessorchips sind äußerst schwierig zu manipulieren und ermöglichen daher eine für unautorisierte Personen unzugängliche Speicherung der obigen Daten. Besonders vorteilhaft ist bei dieser Ausführungsform die Möglichkeit, das Ergebnis der Verschlüsselung zwecks Überprüfung direkt vom Datenträger bzw. vom integrierten Schaltkreis abzurufen.

Gemäß einer weiteren vorteilhaften Ausführungsform ist bzw. sind die zweite(n) Information(en) in einer auf dem Datenträger vorgesehenen bildhaften Darstellung enthalten, wobei die zweite(n) Informationen vorzugsweise verschlüsselt und/oder versteckt in der bildhaften Darstellung hinterlegt ist bzw. sind. Diese konstruktive Maßnahme eignet sich insbesondere für Ausweiskarten oder -dokumente, auf denen eine bildhafte Darstellung in Form eines Benutzerporträts aufgebracht ist. Das Benutzerporträt stellt eine personenindividuelle Information dar, die häufig Fälschungen oder Manipulationen unterzogen wird, indem beispielsweise das ursprüngliche Benutzerporträt durch ein neues Benutzerporträt

ersetzt wird. Durch die Hinterlegung von verschlüsselten und/oder versteckten Informationen in der bildhaften Darstellung werden diese bei derartigen Manipulationen ebenfalls entfernt oder zumindest derart verändert, so daß ein solcher Eingriff festgestellt werden kann.

Die Erfindung wird nachstehend, auch hinsichtlich weiterer Merkmale und Vorteile, anhand der Beschreibung von Ausführungsbeispielen und unter Bezugnahme auf die beiliegenden Zeichnungen näher erläutert. Es zeigt:

Fig. 1 einen erfindungsgemäßen Datenträger in Draufsicht,

Fig. 2 und 3 Tabellen zur Verdeutlichung der Durchführung einer Verschlüsselung, und

Fig. 4 eine schematisch dargestellte Anordnung zur Überprüfung des erfindungsgemäßen Datenträgers.

In Fig. 1 ist eine Ausführungsform eines Datenträger 1 gezeigt, der eine Ausweiskarte darstellt. Auf dem Datenträger 1 sind individuelle Informationen, insbesondere personen- oder kartenspezifische Informationen, wie Benutzername 3, Seriennummer 5, Benutzerporträt 10, Geburtsdaten des Benutzers und dergleichen Informationen lesbar bzw. visuell sichtbar aufgebracht. Diese individuellen Informationen können durch mehrere maschinenlesbare Zeichen bzw. Zeilen, die im konkreten Ausführungsbeispiel im unteren Bereich des Datenträgers 1 vorgesehen sind, ergänzt werden. Der Datenträger 1 kann einen integrierten Schaltkreis 2 aufweisen, der zweckmäßigerweise

einen Mikroprozessorchip umfaßt. Alternativ oder zusätzlich kann ein Magnetstreifen (nicht gezeigt) vorgesehen sein.

Der Benutzername 3 stellt eine erste Information dar und umfaßt eine definierte Anzahl von Zeichen 4, die derart markiert auf dem Datenträger 1 aufgebracht sind, daß jedes Zeichen 4 eine bestimmte Farbe aufweist. Anstelle der verschieden farbigen bzw. wechselnden farbigen Gestaltung der Zeichen 4 können andere geeignete visuell sichtbare Kennzeichnungen vorgesehen sein. Beispielsweise können sich die Zeichen 4 hinsichtlich ihres Schriftbildes unterscheiden, indem die Zeichen 4 wechselweise in Normal-, Kursiv- oder Fettschrift auf dem Datenträger 1 aufgebracht werden. Derartige Kennzeichnungen lassen sich vorteilhaft in den Beschriftungsprozeß integrieren, wobei der markierte Benutzername 3 oder eine sonstige markierte erste Information vorzugsweise mittels Laserdruck, Laserstrahlung, Farbsublimationsdruck, Thermotransferdruck oder Tintenstrahldruck auf dem Datenträger 1 aufgebracht wird. Eine andere Möglichkeit der Kennzeichnung umfaßt beispielsweise die Verwendung von fluoreszierenden Stoffen oder magnetischen Materialien, die mittels geeigneter Verfahren auf bzw. in den Datenträger 1 auf- bzw. eingebracht werden können.

Um eine durchschaubare Beziehung zwischen den Zeichen 4 des Benutzernamens 3 und ihren jeweiligen Farben zu vermeiden, wird der zu markierende Benutzername 3 auf der Basis eines Algorithmus verschlüsselt. Die Verschlüsselung des Benutzernamens 3 wird nachfolgend anhand der Fig. 2 und 3 im Detail beschrieben.

In Fig. 2 ist eine Tabelle zur Verdeutlichung der Verschlüsselung gezeigt. Der Benutzername 3, bestehend aus Nachname und Vorname ist in Zeile 11 der Tabelle zeichenweise angeordnet. Der Benutzername 3 wird mit der Seriennummer 5, die eine zweite, zur Verschlüsselung bestimmte Information darstellt, verschlüsselt. Die Seriennummer 5 weist eine definierte Anzahl Zeichen 6 auf und ist in Zeile 13 der Tabelle zeichenweise angeordnet.

In einem ersten Schritt der Verschlüsselung werden die Zeichen 4 des Benutzernamens sowie die Zeichen 6 der Seriennummer 5 anhand des ASCII- Zeichensatzes in numerische bzw. ganzzahlige Zahlenwerte 7 und 8 umgewandelt, wie in den Zeilen 12 und 14 der Tabelle dargestellt ist. In einem weiteren Schritt werden die Zahlenwerte 7 des Benutzernamens 3 und die Zahlenwerte 8 der Seriennummer 5 anhand eines exklusiven Oder-Operators XOR zahlenweise bzw. bitweise miteinander verknüpft. Das Ergebnis dieser Verknüpfung ist in Zeile 15 der Tabelle aufgeführt. Anstelle des exklusiven Oder-Operators XOR können andere geeignete Operatoren für Bit-Manipulationen oder binäre arithmetische Operatoren, wie Additions-Operatoren + , auf die Zahlenwerte 7 und 8 angewendet werden. In einem weiteren Schritt wird ein Modulo-Operator %, der zu den binären arithmetischen Operatoren zählt, auf das Ergebnis der obigen Verknüpfung angewendet. Anhand des Modulo-Operators % wird eine Folge von Ziffern 9 erhalten, die in Zeile 16 der Tabelle aufgelistet ist. Die Ziffern 9 umfassen eine definierte Anzahl von unterschiedlichen Ziffernwerten, wobei die Anzahl der unterschiedlichen Ziffernwerte durch die Wahl eines Teilers T des Modulo-Operators % bestimmt wird. Wird dem Teiler T des Modulo-Operators % der Wert „2" zugeordnet, so erhält man zwei unterschiedliche Ziffernwerte „0" und „1", wie in Zeile 16 der

Tabelle dargestellt ist. Den Ziffern 9 bzw. den unterschiedlichen Ziffernwerten in Zeile 16 der Tabelle werden in einem weiteren Schritt jeweils eine bestimmte Farbe oder sonstige Kennzeichnung zugeordnet, so daß jede Ziffer 9 eine bestimmte Farbe repräsentiert. Beispielsweise wird den Ziffern 9 mit dem Ziffernwert „0" die Farbe blau zugeordnet, wobei die Farbe blau durch das Symbol o verdeutlicht wird . Den Ziffern 9 mit dem Ziffernwert „1" wird die Farbe rot zugeordnet, wobei die Farbe rot durch das Symbol * gekennzeichnet ist. Die derart farbig markierten Ziffern 9 werden in einem weiteren Schritt den Zeichen 4 des Benutzernamens 3 zugeordnet, wie in Zeile 17 der Tabelle gezeigt ist, so daß die Zeichen 4 eine der zugeordneten Ziffer 9 entsprechende Farbe erhalten.

Die Wahl des Teilers T des Modulo-Operators % hängt im wesentlichen davon ab, wieviele Farben oder sonstige Kennzeichnungen verwendet werden sollen. Möchte man den Benutzernamen 3 beispielsweise mit 3 unterschiedlichen Farben markieren, so wird der Teiler T auf den Wert „3" gesetzt, wie in Zeile 18 der Tabelle gezeigt ist. Hierduch werden insgesamt drei unterschiedliche Ziffernwerte „0", „1" und „2" erhalten, denen eine bestimmte Farbe zugeordnet wird. Dem neu hinzugekommenen Ziffernwert „2" wird eine weitere Farbe, beispielsweise die Farbe grün zugeordnet, wobei die Farbe grün durch das Symbol Δ gekennzeichnet ist. Die farbig markierten Ziffern 9 werden in einem weiteren Schritt den Zeichen 4 des Benutzernamens 3 zugeordnet, so daß hieraus ein dreifarbig markierter Benutzername 3 resultiert, wie in Zeile 19 der Tabelle verdeutlicht ist.

Ein weiteres Ausführungsbeispiel zur Verschlüsselung des Benutzernamens 3 ist in Fig. 3 anhand einer zweiten Tabelle

verdeutlicht. Als zweite, zur Verschlüsselung bestimmte Information ist der Benutzername 3 in abgewandelter Form vorgesehen. Der abgewandelte Benutzername 3a umfaßt Zeichen 4a und ist in Zeile 13a der Tabelle angeordnet. Der abgewandelte Benutzername 3a wird dadurch erhalten, indem der in Zeile 11a angeordnete Benutzername 3 beispielsweise um eine Zeichenposition nach rechts verschoben wird und das am rechten Zeilenende befindliche Zeichen „k" an den Zeilenanfang gesetzt wird. Alternativ kann der Benutzername 3 um mehrere Zeichenpositionen verschoben oder auf sonstige Weise verändert werden, so daß eine abgewandelte Form des Benutzernamens 3 erhalten wird. Analog zu dem vorhergehenden Beispiel gemäß Fig. 2 werden die Zeichen 4 des Benutzernamens 3 und die Zeichen 4a des abgewandelten Benutzernamens 3a anhand des ASCII-Zeichensatzes in numerische bzw. ganzzahlige Zahlenwerte 7 und 7a umgewandelt, die in den Zeilen 12a und 14a dargestellt sind. Auf die Zahlenwerte 7 und 7a wird der exklusive Oder-Operator XOR angewendet und das in Zeile 15a gezeigte Ergebnis der Verknüpfung erhalten. Anschließend wird der Modulo-Operator % mit dem Teiler T gleich „2" (siehe Zeile 16a) oder alternativ der Modulo-Operator % mit dem Teiler T gleich „3" (siehe Zeile 18a) auf das in Zeile 15a aufgeführte Ergebnis angewendet, um eine Folge von Ziffern 9 zu erhalten. Die Ziffern 9 weisen, wie oben bereits erwähnt, je nach Wahl bzw. Wert des Teilers T eine definierte Anzahl von unterschiedlichen Ziffernwerten auf. Die Zuordnung von definierten bzw. unterschiedlichen Farben erfolgt analog zu dem oben beschriebenen Beispiel gemäß Fig. 2. Man kann deutlich erkennen, daß durch die Verwendung lediglich einer unterschiedlichen zweiten Information, nämlich durch die Verwendung des abgewandelten Benutzernamens 3a anstelle der Seriennummer 5, eine völlig unterschiedliche Markierung des

Benutzernamens 3 resultiert, wie in Zeile 17a bzw. 19a der Tabelle dargestellt.

Anstelle des exklusiven Oder-Operators XOR kann beispielsweise der Additions-Operator + oder dergleichen Operatoren auf die Zahlenwerte 7 des Benutzernamens 3 und auf die Zahlenwerte 8 bzw. 7a der Seriennummer 5 bzw. des abgewandelten Benutzernamens 3a angewendet werden. Um eine komplexere Verschlüsselung zu erzielen, können auch mehrere Operatoren auf die obigen Zahlenwerte 7, 8 und 7a angewendet werden.

Erfindungsgemäß kann jede auf dem Datenträger 1 vorgesehene visuell sichtbare, individuelle bzw. erste Information auf der Basis des oben beschriebenen Algorithmus markiert werden. Es ist nicht erforderlich, daß stets der Benutzername 3 oder eine sonstige zu markierende erste Information mit der Seriennummer 5, dem abgewandelten Benutzernamen 3a oder einer sonstigen zweiten Information verknüpft wird. Beispielsweise kann die Seriennummer 5 mit dem abgewandelten Benutzernamen 3a verknüpft werden, um eine Folge von Ziffern 9 zu erhalten. Wesentlich ist, daß als Ergebnis der Verschlüsselung den Zeichen 4 des Benutzernamens 3 eine definierte Farbe oder eine andere zur Unterscheidung der Zeichen 4 geeignete Kennzeichnung zugeordnet wird, wie in den Zeilen 17 und 19 der Tabelle von Fig. 2 und in den Zeilen 17a und 19a der Tabelle gemäß Fig. 3 gezeigt ist.
Gemäß einer weiteren Ausführungsform ist die Seriennummer 5, der abgewandelte Benutzername 3a oder dergleichen zweite Information in dem integrierten Schaltkreis 2 des Datenträgers 1 enthalten. Alternativ können diese Informationen auf einem Magnetstreifen (nicht gezeigt) des Datenträgers 1 hinterlegt sein. Eine weitere Möglichkeit zur Erhöhung des Schutzes gegen

Fälschungen und Manipulationen besteht darin, daß beispielsweise die Seriennummer 5 und/oder der abgewandelte Benutzername 3a gemäß einer weiteren Ausführungsform außerhalb des Bereichs des Datenträgers 1 vorgesehen sind und vorzugweise in einem externen Speicher 23 (vgl. Fig. 4) gespeichert sind. Als externer Speicher 23 dient eine gegen unautorisierte Zugriffe gesicherte zentrale Datenbank. Bei einer derart gesicherten Speicherung kann beispielsweise eine für alle Datenträger 1 einheitliche zweite Information zur Verschlüsselung des jeweiligen Benutzernamens 3 oder dergleichen ersten Information vorgesehen sein.

Der Datenträger 1 weist neben den personen- und kartenindividuellen Bezeichnungen und Beschriftungen ein Benutzerportät 10 oder eine sonstige bildhafte Darstellung auf. Gemäß einer weiteren vorteilhaften Ausführungsform ist beispielsweise die Seriennummer 5 und/oder der abgewandelte Benutzername 3a in dem Benutzerporträt 10 hinterlegt (nicht gezeigt). Die Seriennummer 5 und/oder der abgewandelte Benutzername 3a können verschlüsselt, beispielsweise als Barcode vorliegen, wobei eine derartige Hinterlegung bzw. Speicherung von Informationen vorzugsweise mit einem steganographischen Verfahren durchgeführt wird.

Zusätzlich oder alternativ kann die Seriennummer 5 und/oder der abgewandelte Benutzername 3a versteckt im Benutzerporträt 10 hinterlegt sein. Die versteckte Anordnung der Seriennummer 5 und/oder des abgewandelten Benutzernamens 3a erfolgt in Form eines sekundären Bildes, beispielsweise in Form des oben erwähnten Barcodes, wobei das sekundäre Bild in dem Benutzerporträt 10, das ein Primärbild darstellt, derart

verborgen ist, daß es lediglich mittels eines Dekoders oder dergleichen Hilfsmittel erkennbar wird.

In Fig. 4 ist eine Anordung zur Überprüfung des Datenträgers 1 schematisch dargestellt.

Zur Überprüfung des Datenträgers 1 wird der markiert vorliegende Benutzername 3 oder eine andere markierte erste Information sowie die zur Verschlüsselung bestimmte Seriennummer 5 oder eine sonstige zur Verschlüsselung bestimmte zweite Information von einer Kamera 20 oder einem optischen Scanner erfaßt und digitalisiert. In einem nachgeschalteten Mikroprozessor 21 werden die aufgenommenen Bilddaten des Benutzernamens 3 und der Seriennummer 5 ausgewertet und mittels optischer Zeichenerkennung (OCR) zu rechnerverarbeitbaren Zeichen 4 und 6 umgewandelt. Die rechnerverarbeitbaren Zeichen 4 und 6 des Benutzernamens 3 und der Seriennummer 5 werden einer Verifikationseinheit 22 zugeführt. In dieser Verifikationseinheit 22 wird der oben beschriebene Algorithmus auf die Zeichen 4 des Benutzernamens 3 und auf die Zeichen 6 der Seriennummer 5 angewendet und die Markierung des Benutzernamens 3 erneut ermittelt. Ist die ermittelte Markierung des Benutzernamens 3 identisch mit der auf dem Datenträger hinterlegten Markierung des Benutzernamens 3, gilt der Datenträger 1 als echt.

Sofern der Benutzername 3, die Seriennummer 5 oder sonstige zur Verschlüsselung bestimmten ersten und/oder zweiten Informationen in dem integrierten Schaltkreis 2 oder Magnetstreifen gespeichert sind, werden diese Informationen über einen Kartenleser 24 ausgelesen und der Verifikationseinheit 22 zugeleitet. Sind diese Informationen

außerhalb des Bereichs des Datenträgers 1 in einem externen Speicher 23 gespeichert, können sie aus dem externen Speicher 23 abgerufen und der Verifikationseinheit 22 zugeführt werden.

Gemäß einer weiteren Ausführungsform sind der Benutzername 3, die Seriennummer 5 oder sonstige zur Verschlüsselung vorgesehene Informationen sowie der Algorithmus in dem integrierten Schaltkreis 2 gespeichert, wobei der integrierte Schaltkreis 2 zweckmäßigerweise einen Mikroprozessorchip umfaßt. Die Überprüfung des Datenträgers 1 kann bei dieser Ausführungsform unmittelbar mittels des Mikroprozessorchips erfolgen.

Insgesamt zeichnet sich das erfindungsgemäße Verfahren sowie der erfindungsgemäße Datenträger durch einen effizienten Schutz gegen Fälschungen und Manipulationen sowie durch eine kostengünstige Herstellung aus. Die oben beschriebene Verschlüsselung kann aufgrund der Vielzahl der zur Verfügung stehenden Operatoren beliebig komplex gestaltet werden. Darüberhinaus kann anhand der Verschlüsselung eine definierte Markierung von einer oder mehreren Informationen auf dem Datenträger bewirkt werden, deren Kodierung nur autorisierten Personen zugänglich ist.

Bezugszeichenliste:

1	Datenträger
2	integrierter Schaltkreis
3	Benutzername
3a	abgewandelter Benutzername
4	Zeichen (Benutzername)
4a	Zeichen (abgewandelter Benutzername)
5	Seriennummer
6	Zeichen (Seriennummer)
7	Zahlenwert (Benutzername)
7a	Zahlenwert (abgewandelter Benutzername)
8	Zahlenwert (Seriennummer)
9	Ziffern
10	Benutzerporträt
11 - 19	Tabellenzeilen
11a-19a	Tabellenzeilen
20	Kamera
21	Mikroprozessor
22	Verifikationseinheit
23	Speicher
24	Kartenleser

XOR	exklusive Oder-Operator
%	Modulo-Operator
+	Additions-Operator
T	Teiler
*	rote Farbe
o	blaue Farbe
Δ	grüne Farbe

Verfahren zur Herstellung eines Datenträgers sowie ein Datenträger

---

Patentansprüche

1. Verfahren zur Herstellung eines Datenträgers, wie eine Ausweis-, eine Kreditkarte oder dergleichen Wert- oder Sicherheitsdokument, umfassend mindestens eine erste Information (3), die visuell sichtbar, insbesondere lesbar auf dem Datenträger vorgesehen und geeignet ist, den Datenträger aus einer Reihe von Datenträgern zu individualisieren, dadurch gekennzeichnet, daß die erste Information (3) mittels eines Algorithmus verschlüsselt und das Ergebnis der Verschlüsselung auf dem Datenträger hinterlegt wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die erste Information (3) eine definierte Anzahl von Zeichen (4) umfaßt, und daß das Ergebnis der Verschlüsselung derart auf dem Datenträger hinterlegt wird, daß mindestens ein Zeichen (4) der ersten Information (3) markiert wird.

3. Verfahren nach Anspruch 1 oder 2,

dadurch gekennzeichnet,
daß die Markierung der Zeichen (4) der ersten Information (3) durch eine unterschiedliche, insbesondere visuell sichtbare Kennzeichnung der Zeichen (4), wie eine unterschiedliche farbige oder schriftbildliche Gestaltung der Zeichen (4), bewirkt wird.

4. Verfahren nach einem der Ansprüche 1 bis 3,
dadurch gekennzeichnet,
daß mindestens eine zweite Information (3a, 5) vorgesehen ist, die zur Verschlüsselung der ersten Information (3) bestimmt ist.

5. Verfahren nach einem der Ansprüche 1 bis 4,
dadurch gekennzeichnet,
daß die mindestens eine zweite Information (3a, 5) zur Verschlüsselung Zeichen (4a, 6), insbesondere maschinenlesbare bzw. rechnerverarbeitbare Zeichen (4a, 6) umfaßt oder zu maschinenlesbaren bzw. rechnerverarbeitbaren Zeichen umgewandelt wird.

6. Verfahren nach einem der Ansprüche 1 bis 5,
dadurch gekennzeichnet,
daß der der Verschlüsselung zugrundeliegende Algorithmus folgende Schritte umfaßt:

1) Umwandeln der Zeichen (4) der ersten Information (3) und/oder der Zeichen (4a, 6) der zweiten Information(en) (3a, 5) in numerische bzw. ganzzahlige Zahlenwerte (7; 7a, 8), beispielsweise anhand des ASCII-Zeichensatzes, und

2) Anwenden mindestens eines Operators auf die Zahlenwerte (7) der ersten Information (3) und/oder auf die Zahlenwerte (7a, 8) der zweiten Information(en) (3a, 5), derart, daß hieraus eine Folge von Ziffern (9) resultiert, und

3) Markieren der Ziffern (9), derart, daß wenigstens eine Ziffer (9) eine bestimmte Kennzeichnung, wie eine bestimmte Farbe, aufweist, und

4) Zuordnen der Kennzeichnungen aufweisenden Ziffern (9) zu den Zeichen der ersten Information (3), derart, daß mindestens ein Zeichen (4) der ersten Information (3) eine der zugeordneten Ziffer (9) entsprechende Kennzeichnung erhält.

7. Verfahren nach Anspruch 6,
dadurch gekennzeichnet,
daß der mindestens eine Operator aus einer Gruppe von Operatoren ausgewählt wird, wobei die Gruppe von Operatoren vorzugsweise Operatoren für Bit-Manipulationen, wie exklusive Oder-Operatoren (XOR), und binäre arithmetische Operatoren, wie Additions-Operatoren (+), Modulo-Operatoren (%) oder dergleichen Operatoren, umfaßt.

8. Verfahren nach Anspruch 6 oder 7,
dadurch gekennzeichnet,
daß die erhaltene Folge von Ziffern (9) eine definierte Anzahl von unterschiedlichen Ziffernwerten aufweist, wobei die Anzahl der unterschiedlichen Ziffernwerte durch die Wahl eines Teilers des binären Modulo-Operators (%) vorgegeben wird.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, daß der Datenträger im Hinblick auf Fälschungen oder Manipulationen überprüfbar ist, wobei zur Überprüfung des Datenträgers der der Verschlüsselung zugrunde liegende Algorithmus angewendet wird.

10. Verfahren nach Anspruch 9, dadurch gekennzeichnet, daß die Überprüfung des Datenträgers folgende Schritte umfaßt:

5) Ermitteln bzw. Erfassen der für die Durchführung der Verschlüssselung bestimmten ersten Information (3) und/oder zweiten Information(en) (3a, 5),

6) Anwenden des Algorithmus auf die erste Information (3) und/oder auf die zweite(n) Informationen (3a, 5), und

7) Vergleich der aus dem Ergebnis des Algorithmus erhaltenen Markierung der ersten Information (3) mit der auf dem Datenträger hinterlegten Markierung der ersten Information (3).

11. Datenträger, wie Ausweis-, Kreditkarte oder dergleichen Wert- oder Sicherheitsdokument, insbesondere nach einem der Ansprüche 1 bis 10, mit mindestens einer ersten Information (3), die visuell sichtbar, insbesondere lesbar auf dem Datenträger vorgesehen ist und geeignet ist, den Datenträger aus einer Reihe von Datenträgern zu individualisieren, dadurch gekennzeichnet,

daß die erste Information (3) derart verschlüsselt ist, daß sie zumindest teilweise markiert auf dem Datenträger hinterlegt ist.

12. Datenträger nach Anspruch 11,
dadurch gekennzeichnet,
daß die erste Information (3) eine definierte Anzahl von Zeichen (4) umfaßt, wobei die Zeichen (4) derart markiert sind, daß sie sich hinsichtlich ihrer Farbe oder durch sonstige erfaßbare Kennzeichnungen, wie schriftbildliche Gestaltung, unterscheiden.

13. Datenträger nach Anspruch 11 oder 12,
dadurch gekennzeichnet,
daß mindestens eine zweite Information (3a, 5) vorgesehen ist, die zur Verschlüsselung der ersten Information (3) dient.

14. Datenträger nach einem der Ansprüche 11 bis 13,
dadurch gekennzeichnet,
daß die erste Information (3) und/oder die zweite(n) Information(en) (3a, 5) personen-, karten- oder dokumentspezifische Bezeichnungen bzw. Beschriftungen, wie ein Benutzername (3), eine Seriennummer (5) oder dergleichen individuelle Informationen umfassen, die insbesondere auf dem Datenträger vorgesehen sind.

15. Datenträger nach Anspruch 14,
dadurch gekennzeichnet,
daß die mindestens eine zweite Information (3a) zumindest teilweise inhaltsgleich zu der ersten Information (3) ist.

16. Datenträger nach einem der Ansprüche 11 bis 15,

dadurch gekennzeichnet,
daß die zweite(n) Information(en) (3a, 5) in einem auf dem Datenträger vorgesehenen Speicher- oder Zusatzelement, wie ein integrierter Schaltkreis (2), ein Magnetstreifen oder dergleichen enthalten ist bzw. sind, und/oder außerhalb des Bereichs des Datenträgers vorgesehen ist bzw. sind, wobei die zweite(n) Information(en) (3a, 5) vorzugsweise in einem externen Speicher (23), beispielsweise in einer zentralen Datenbank oder dergleichen Speichereinrichtung, gespeichert ist bzw. sind.

17. Datenträger nach einem der Ansprüche 11 bis 16,
dadurch gekennzeichnet,
daß die Verschlüsselung auf einem Algorithmus basiert, der zusätzlich zu der ersten Information (3) und/oder zu der bzw. den zweiten Information(en) (3a, 5) in dem integrierten Schaltkreis (2) des Datenträgers gespeichert ist, wobei der integrierte Schaltkreis (2) vorzugsweise einen Mikroprozessorchip umfaßt.

18. Datenträger nach einem der Ansprüche 11 bis 17,
dadurch gekennzeichnet,
daß die zweite(n) Information(en) (3a, 5) in einer auf dem Datenträger vorgesehenen bildhaften Darstellung (10) enthalten ist bzw. sind, wobei die zweite(n) Information(en) (3a, 5) vorzugweise verschlüsselt und/oder versteckt in der bildhaften Darstellung (10) hinterlegt ist bzw. sind.

19. Datenträger nach einem der Ansprüche 11 bis 18,
dadurch gekennzeichnet,
daß die insbesondere farbig markierte erste Information (3) mittels Laserdruck, Laserstrahlung, Farbsublimationsdruck,

Thermotransferdruck, Tintenstrahldruck oder dergleichen Druckverfahren auf dem Datenträger aufgebracht ist.

20. Vorrichtung zur Herstellung und/oder Überprüfung eines Datenträgers,
dadurch gekennzeichnet,
daß die Vorrichtung zur Herstellung und/oder Überprüfung eines Datenträgers nach einem der obigen Ansprüche modifiziert worden ist.

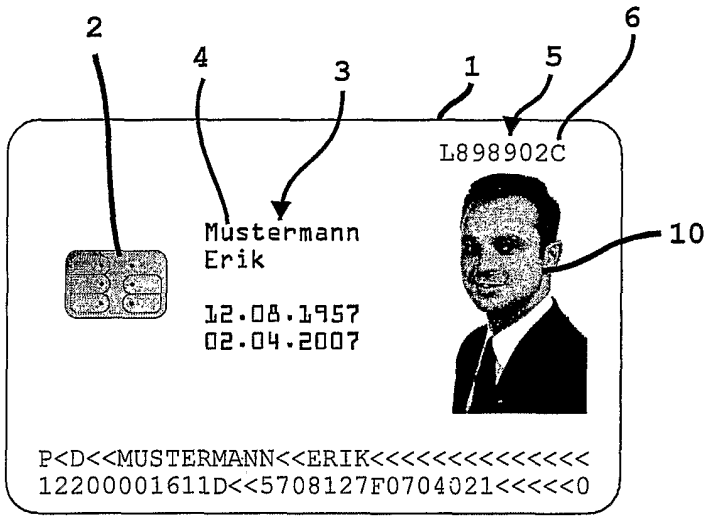

2
4
3
1
5
6
L898902C
Mustermann
Erik
12.08.1957
02.04.2007
10
P<D<<MUSTERMANN<<ERIK<<<<<<<<<<<<<<
12200001611D<<5708127F0704021<<<<<<0

FIG. 1

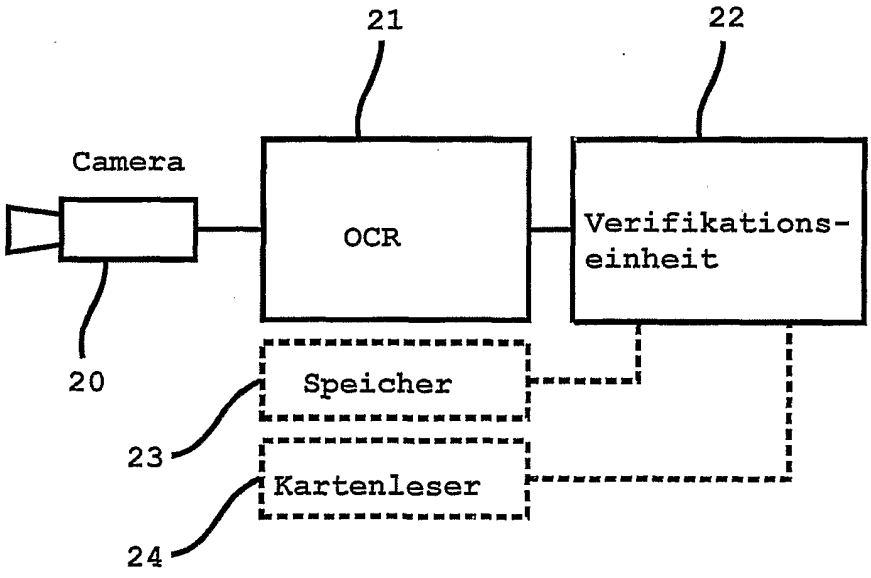

21
22
Camera
OCR
Verifikations-
einheit
20
Speicher
23
Kartenleser
24

FIG. 4

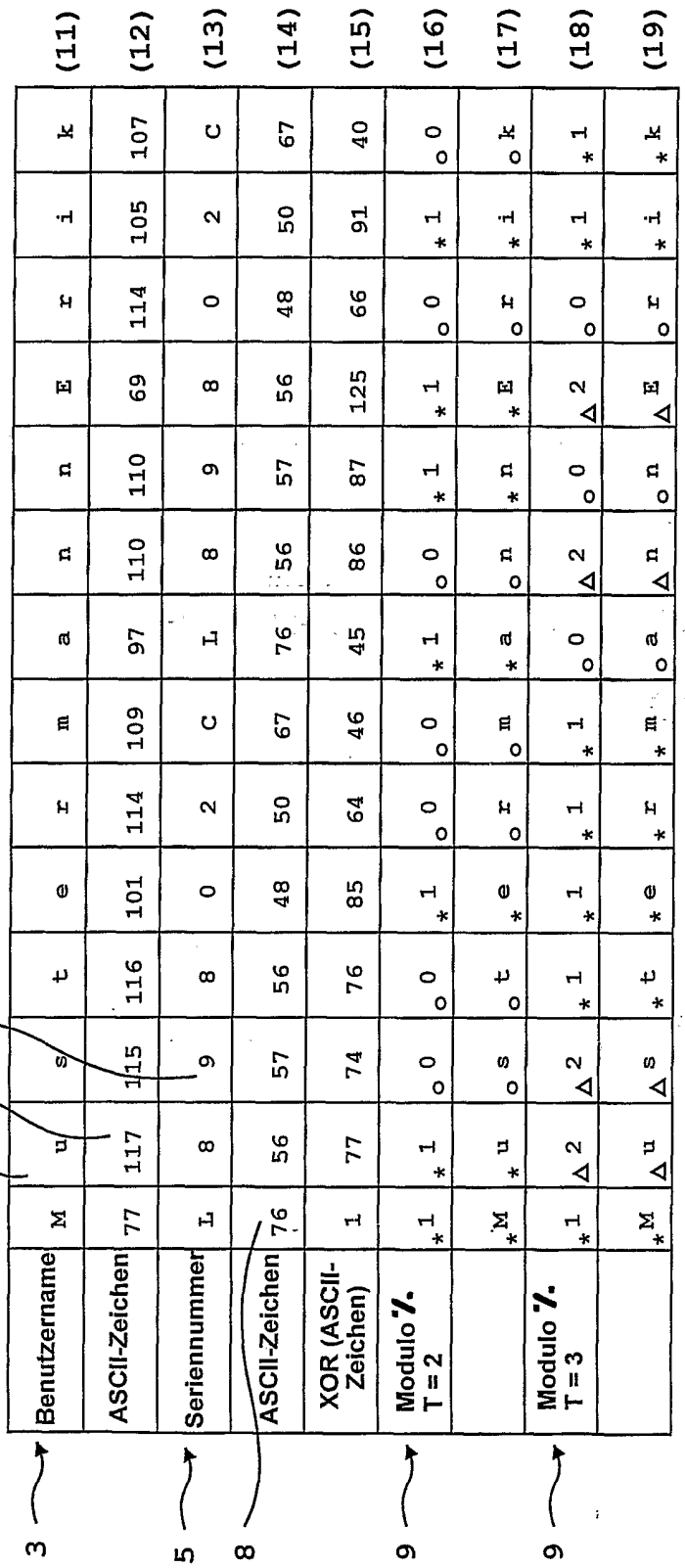

(11)
(12)
(13)
(14)
(15)
(16)
(17)
(18)
(19)
3
4
5
6
7
8
9
9
Benutzername
ASCII-Zeichen
Seriennummer
ASCII-Zeichen
XOR (ASCII-Zeichen)
Modulo %. T = 2
Modulo %. T = 3

FIG. 2

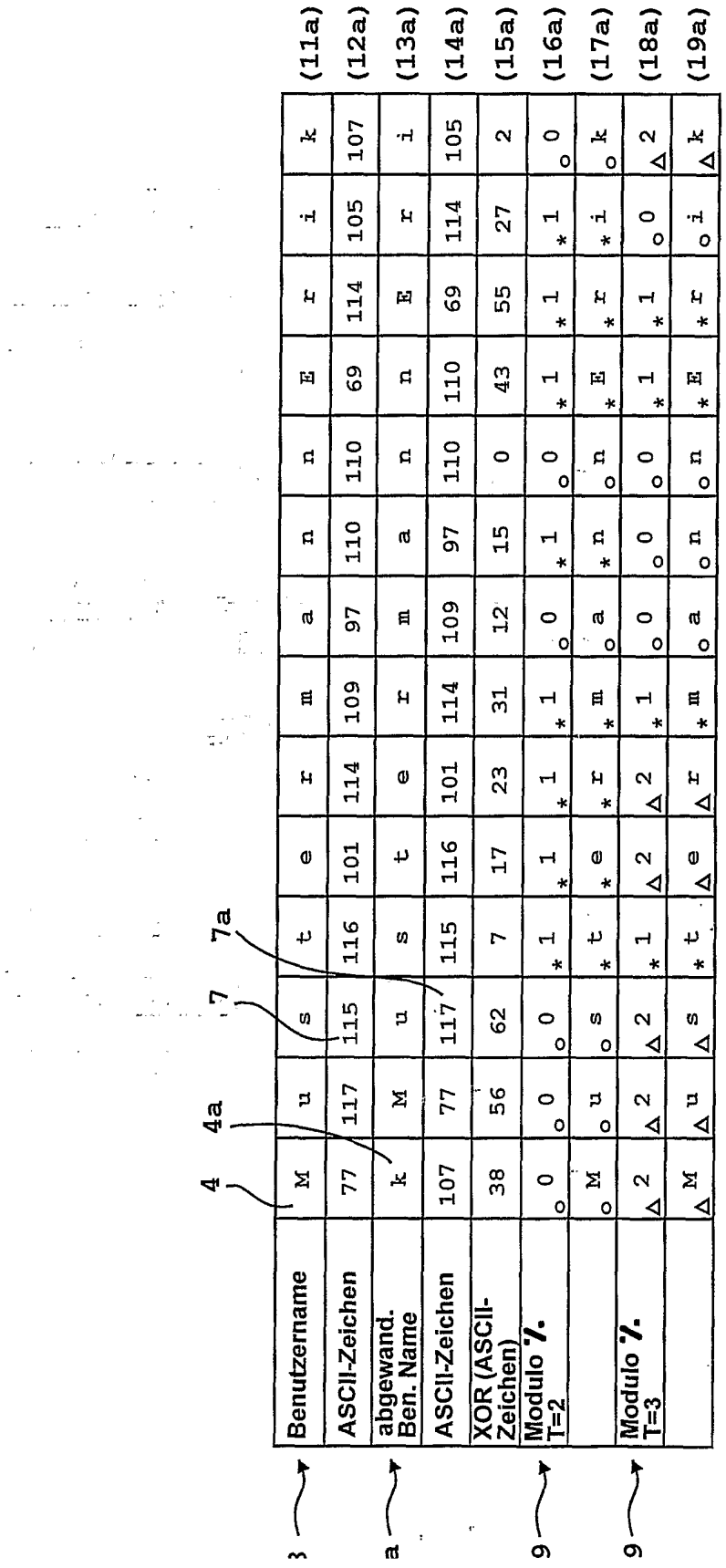

4
4a
7
7a
3
a
9
9
(11a)
(12a)
(13a)
(14a)
(15a)
(16a)
(17a)
(18a)
(19a)
Benutzername
ASCII-Zeichen
abgewand. Ben. Name
ASCII-Zeichen
XOR (ASCII-Zeichen)
Modulo %. T=2
Modulo %. T=3

FIG. 3