(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
17. März 2016 (17.03.2016)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2016/037295 A1

(51) Internationale Patentklassifikation:
G06K 19/14 (2006.01) *G06K 17/00* (2006.01)
G06Q 10/08 (2012.01)

(21) Internationales Aktenzeichen: PCT/CH2015/000131

(22) Internationales Anmeldedatum:
9. September 2015 (09.09.2015)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
01362/14 9. September 2014 (09.09.2014) CH

(71) Anmelder: **KABA AG** [—/CH]; Mühlebühlstrasse 23, 8620 Wetzikon (CH).

(72) Erfinder: **KUSTER, Christian**; Höhenstrasse 21, 8342 Wernetshausen (CH). **SCHACHER, Edgar**; Bachstrasse 3, 8604 Volketswil (CH).

(74) Anwalt: **FREI PATENTANWALTSBÜRO AG**; Postfach 1771, 8032 Zürich (CH).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

(54) **Title**: IDENTIFICATION SYSTEM, METHOD AND USER MEDIUM

(54) **Bezeichnung** : IDENTIFIZIERUNGSSYSTEM, VERFAHREN UND BENUTZERMEDIUM

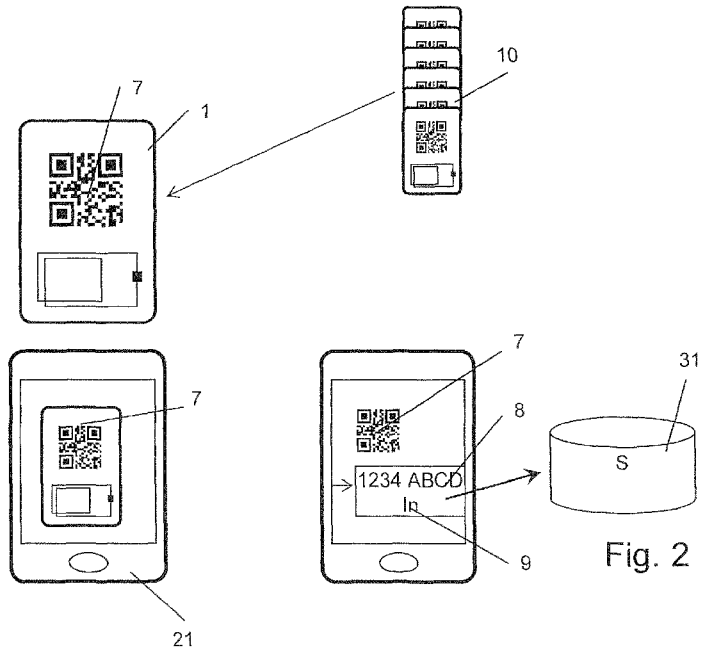


Fig. 2

(57) **Abstract**: An identification system is described that has: a plurality of user media (1), each of which has an integrated circuit (2) having memory means and an identification code (8) stored in the memory means; at least one reading device; wherein the reading device (41) is capable of contactlessly reading data for an authentication process from the integrated circuit (2) via radio waves; and wherein the identification system additionally has a user management device (31) and is capable of initiating or not initiating a process on the basis of whether the read user medium is recorded as authorised in the user management device. The system is distinguished in that each user medium additionally has an optically readable code (7) that contains an identification information item individually identifying the user medium in question, wherein the identification system is capable of recording a user medium recognised via the optically readable code in the user management device.

(57) **Zusammenfassung**: Ein Identifizierungssystem wird beschrieben, welches aufweist: Eine Mehrzahl von Benutzemiedien (1), von denen jedes eine integrierte Schaltung (2) mit Speichermitteln und einen in den Speichermitteln abgespeicherten

[Fortsetzung auf der nächsten Seite]

WO 2016/037295 A1

Identifikationscode (8) aufweist; mindestens eine Leseeinrichtung; wobei die Leseeinrichtung (41) befähigt ist, für einen Authentifizierungsprozess über Radiowellen berührungslos aus der integrierten Schaltung (2) Daten auszulesen; und wobei das Identifizierungssystem ferner eine Benutzerverwaltungseinrichtung (31) aufweist und befähigt ist, einen Vorgang abhängig davon, ob in der Benutzerverwaltungseinrichtung das ausgelesene Benutzermedium als berechtigt vermerkt ist, auszulösen oder nicht auszulösen. Das System zeichnet sich dadurch aus, dass jedes Benutzermedium ferner einen optisch auslesbaren Code (7) aufweist welcher eine das betreffende Benutzermedium individuell identifizierende Identifikationsinformation beinhaltet, wobei das Identifizierungssystem befähigt ist, ein über den optisch auslesbaren Code erkanntes Benutzermedium in der Benutzerverwaltungseinrichtung zu vermerken.

IDENTIFIZIERUNGSSYSTEM, VERFAHREN UND BENUTZERMEDIUM

Die Erfindung betrifft das Gebiet Identifizierungstechnologie, wie sie beispielsweise für Sicherheits- und Datenträgersysteme zur Anwendung kommt. Sie betrifft insbesondere ein Identifizierungssystem, ein Verfahren und ein Benutzermedium.

Identifizierungssysteme (oft auch als Identifikationssysteme bezeichnet, oft wäre der Begriff „Authentifizierungssystem" korrekter) kommen zum Einsatz bei unterschiedlichen Anwendungen wie der Zugangskontrolle (in sogenannten ‚online-Identifizierungssystemen, bei denen ein Objekt, zu dem der Zugang kontrolliert wird, in Kontakt mit einer zentralen Einheit steht, und in ‚offline'-Systemen bei denen das nicht der Fall ist), Wertkartensystemen, Datenerfassungssystemen etc.

Meist weisen die Identifizierungssysteme Benutzermedien – beispielsweise „Smart Cards" oder auch mit einem entsprechenden Datenträger versehene physische Schlüssel – auf, die mit einem Datenspeicher versehen sind, auf dem ein geeigneter Identifikationscode abgespeichert ist. In der Anwendung findet – meist berührungslos – ein Datenaustausch mit einer Leseeinrichtung statt, wobei anhand des Identifikationscodes ein Authentifizierungsprozess ausgeführt wird und die gewünschte Aktion – bspw. die Freigabe eines Objektes, der Bezug einer Ware oder Dienstleistung, das Schreiben einer Information auf das Benutzermedium, etc. – nur erfolgreich durchgeführt wird, wenn in der Leseeinrichtung oder eventuell im

BESTÄTIGUNGSKOPIE

Benutzermedium die Berechtigung des mit dem Identifikationscode versehenen Benutzermediums festgestellt wird oder das Resultat einer Rechenoperation auf Basis dieses einen gewünschten Wert ergibt.

Ein praktisches Problem stellt sich oft bei grösseren Identifizierungssystemen, in welchen die Anzahl und Identität der Nutzer nicht von Anfang an, beim Einrichten des Identifizierungssystems, bekannt sein kann. In solchen Identifizierungssystemen muss es möglich sein, auch lange nach dem Einführen des Identifizierungssystems neue funktionsfähige Benutzermedien zu verteilen, beispielsweise an neu eintretende Mitarbeiter oder neue Kunden. In der Praxis wird das oft so gehandhabt, dass dem Systembetreiber eine grössere Anzahl von bereits mit einem Identifikationscode versehenen Benutzermedien zur Verfügung gestellt wird und/oder dass solche Benutzermedien beim Hersteller nachbestellt werden können. Zur Initialisierung wird ein dem neuen Benutzer auszuhändigendes Benutzermedium zunächst von einem Lesegerät erfasst, welches in einer zentralen Einheit vorhanden ist. Dort werden dann die Berechtigungen dieses Benutzers definiert, und anschliessend kann das Benutzermedium dem Benutzer ausgehändigt werden.

Nachteilig an dieser Lösung ist, dass dieser Vorgang die physische Anwesenheit des Benutzermediums am Ort der zentralen Einheit bedingt. Folglich kann ein neu in das Identifizierungssystem einzuführendes Benutzermedium nur an einem einzigen Ort initialisiert werden. Das ist insbesondere bei Identifizierungssystemen mit dezentralen Elementen durchaus nachteilig. Ausserdem bedingt das das Vorhandensein einer solchen zentralen Einheit mit einer eigenen Leseeinrichtung und mit einer Kommunikationsmöglichkeit mit den Leseeinrichtungen, was nicht zwangslos in jede Systemorganisation passt.

Als Alternative kommt bei einigen Standards die dezentrale Programmierung der Leseeinrichtungen über RFID in Frage, was jedoch nicht von allen Standards unterstützt wird.

Aus der WO 2005/081174 ist ein System für den Versand und das Nachverfolgen von Stückgut bekannt. Dieses System sieht vor, dass die Güter mit einem elektronischen Etikett in Form eines RFID-‚tags' und zusätzlich mit einem Strichcode versehen sind. Beim Versenden werden die Strichcodes der einer Verpackungseinheit zugeordneten Güter erfasst und an einen Datenserver gesendet. Dieser generiert einen elektronischen Produktcode (EPC), welcher auf das elektronisch Etikett geschrieben wird. Das ermöglicht beim Empfänger eine fälschungssicherere Authentifizierung als wenn das Gut bloss einen Strichcode aufwiese. Für die hier geschilderte Anwendung ist das für Stückgut entwickelte Verfahren nur schon deshalb keine Lösung, weil auch dieses die physische Anwesenheit des elektronischen Etiketts am Ort eines RFID-Schreibgeräts bedingt.

Die US 2004/0201479 betrifft ein Gegenstands-Nachverfolgungssystem bspw. für Bibliotheken. Es wird vorgeschlagen, aus Performancegründen existierende strichcodebasierte System durch ein auf RFID basierendes System zu ersetzen, wobei Bücher (oder andere Medien) auch beides – sowohl einen Strichcode als auch einen RFID-Tag aufweisen können. Es wird weiterhin vorgeschlagen, dass das Lesegerät auch RFID-Tags erzeugen kann, für Medien, die bis dann erst mit einem Strichcode versehen sind. Auch dieses Vorgehen bringt aus denselben Gründen wie beim System nach WO 2005/081174 für die hier geschilderte Anwendung keine weiteren Vorteile.

Es ist folglich eine Aufgabe der vorliegenden Erfindung, ein Identifizierungssystem und ein entsprechendes Verfahren zur Verfügung zu stellen, welche Nachteile des

Standes der Technik überwinden und welche insbesondere ein einfaches Hinzufügen von neuen Benutzermedien zum System ermöglichen, ohne die Sicherheit zu kompromittieren.

Diese Aufgabe wird gelöst durch die Erfindung, wie sie in den Patentansprüchen definiert ist.

Gemäss einem Aspekt der Erfindung weist das Identifizierungssystem wie an sich bekannt eine Mehrzahl von Benutzermedien auf, von denen jedes eine integrierte Schaltung mit Speichermitteln und einem in den Speichermitteln abgespeicherten Identifikationscode aufweist, wobei die integrierte Schaltung befähigt ist, für einen Authentifizierungsprozess über Radiowellen (über RFID) berührungslos an eine Leseeinrichtung Daten zu übermitteln. Die Benutzermedien sind weiterhin mit einem optisch auslesbaren Code versehen, welcher eine eindeutige individuelle Identifikation des Benutzermediums beinhaltet. Der optisch auslesbare Code kann insbesondere den Identifikationscode beinhalten, beispielsweise gar mit ihm identisch sein. Alternativ ist auch möglich, dass die Identifikationsinformation den Identifikationscode zwar nicht beinhaltet, aber für mindestens in einer Gruppe von Benutzermedien (bspw. den für ein bestimmtes Land oder einem bestimmten Anwendersegment zur Verfügung stehenden) eine eindeutige Zuordnung zum Identifikationscode ermöglicht.

Wie erwähnt weisen dabei die Benutzermedien den Identifikationscode schon auf. Sämtliche für den Authentifizerungsprozess nötigen Angaben sind in den Speichermitteln bereits vorhanden. Es braucht daher im Unterschied zum vorstehend diskutierten Stand der Technik keinen Schreibvorgang und keine andere Modifikation am Benutzermedium um dieses zum System hinzuzufügen und es für Vorgänge zu berechtigen. Vielmehr erfordert das Hinzufügen ausschliesslich den

entsprechenden Vermerk auf Seiten der Benutzerverwaltungseinrichtung, weshalb ausreichend ist, dass optisch auslesbare Daten und/oder optisch ausgelesene Daten an dieses übermittelt werden.

Die Benutzerverwaltungseinrichtung kommuniziert mit der Leseeinrichtung, welche den Authentifizierungsprozess anhand des Datenaustauschs über Radiowellen durchführt, und das Resultat des Authentifizierungsprozesses ist abhängig davon, ob das Benutzermedium in der Benutzerverwaltungseinrichtung vermerkt ist oder nicht. Diese Kommunikation zwischen der Benutzerverwaltungseinrichtung und der Leseeinrichtung kann online, im Moment der Authentifizierung, oder offline, als Aufdatierung eines Datenspeichers der Leseeinrichtung, geschehen.

Mit anderen Worten bildet der Identifikationscode einen Identifikationsdatensatz oder einen Teil eines solchen Identifikationsdatensatzes, welcher in der integrierten Schaltung von Anfang an vorhanden ist und alle für den Authentifizierungsprozess notwendigen Daten aufweist. Für die Berechtigung zum genannten Vorgang braucht es also nur noch den Vermerk in der Benutzerverwaltungseinrichtung als ‚berechtigt' der nach dem optischen Auslesen gemacht wird.

Besonders bevorzugt kann sein, wenn jeder Identifikationscode weltweit nur für ein einziges Benutzermedium vergeben wird und die Identifikationsinformation entweder den Identifikationscode vollständig umfasst, mindestens wesentliche Teile des Identifikationscodes umfasst (bspw. wenn mögliche Redundanzen für Redundanztests, bspw. Prüfbits, zum Identifikationscode gerechnet werden, allenfalls ohne diese Redundanzen) vollständig umfasst, oder diesem mindestens eindeutig zuordenbar ist.

In Ausführungsformen kann das Benutzermedium so eingerichtet sein, dass der Identifikationscode einen dem Hersteller eindeutig zugeordneten elektronischen Herstellerschlüssel („Stamp") enthält. Während des Authentifizierungsprozesses oder vorgängig zu diesem kann dann eine Leseeinrichtung die Identität dieses Teils des Identifikationscodes mit dem von ihr selbst abgespeicherten Herstellerschlüssel prüfen, was als zusätzliche Massnahme gegen Manipulationen dient.

Der optisch auslesbare Code kann insbesondere ein 2D-Code sein. Die Verwendung von Codes der an sich bekannten Art, bspw. von QR-Codes ist möglich.

Das Identifizierungssystem weist auch mindestens eine Leseeinrichtung auf, die zum erwähnten Datenaustausch mit den Benutzermedien zwecks Authentifizierungsprozess befähigt ist. Abhängig vom Resultat des Authentifizierungsprozesses wird das Identifizierungssystem einen Vorgang auslösen oder nicht, bspw. das Aufschliessen einer Türe, das Abbuchen eines Geldbetrags oder den Zugang zu einem EDV-System etc..

Das Identifizierungssystem weist ausserdem eine Benutzerverwaltungseinrichtung auf. Diese kann im der Leseeinrichtung integriert oder von dieser separat sein (und bspw. im letzteren Fall mit mehreren der Leseeinrichtungen zusammenwirken). Die Freigabe des Vorgangs erfolgt abhängig davon ob in der Benutzerverwaltungseinrichtung das am Datenaustausch beteiligte Benutzermedium als berechtigt vermerkt ist oder nicht.

Der Authentifizierungsprozess selbst kann wie an sich bekannt und mit den Standards/Merkmalen von an sich bekannten Identifizierungssystemen (bspw. Mifare, Legic, etc.) stattfinden.

Weiter ist das Identifizierungssystem befähigt, einem über den optisch auslesbaren Code erkannten Benutzermedium eine Berechtigung zu verleihen, indem dieses in der Benutzerverwaltungseinrichtung entsprechend vermerkt wird.

Zu diesem Zweck kann das Identifizierungssystem eine Programmierungseinheit aufweisen, die befähigt ist, die Benutzerverwaltungseinrichtung entsprechend zu programmieren.

Die Programmierungseinheit kann gemäss einer ersten Option eine Software aufweisen, welche auf einem Gerät läuft, welches einerseits ein Mittel zum Erfassen des optisch auslesbaren Codes aufweist und andererseits ein Mittel zum Austauschen von Daten mit der Leseeinrichtung. Dieses Mittel zum Austauschen von Daten mit der Leseeinrichtung kann bspw. ein Kommunikationsmittel zum Herstellen einer bspw. drahtlosen Punkt-zu-Punkt-Verbindung über einen Kommunikationsstandard, bspw. NFC, Bluetooth, Infrarot, gepulste Informationsübertragung („UWB"), Induktion, etc. sein. Dabei kann insbesondere bevorzugt sein, wenn dieser Kommunikationsstandard verschieden vom Standard ist, welcher für die Authentifizierung (RFID) benutzt wird, was ein Sicherheitsmerkmal darstellt. Ein solches Gerät kann beispielsweise ein Smartphone sein, welches den Datenaustausch über Nahfeldkommunikation (NFC) und/oder Bluetooth bzw. einen anderen geeigneten Kommunikationsstandard unterstützt; auch andere Kommunikationsstandards wie WLAN etc. sind möglich.

Gemäss einer weiteren Option kann die Programmierungseinheit auch als Teil einer zentralen Einheit ausgebildet sein, welche mit den Leseeinrichtungen des Identifizierungssystems in Kommunikationsverbindung steht oder in Kommunikationsverbindung bringbar ist. In diesem Fall kann die Erfassung des optisch auslesbaren Codes ebenfalls über ein Smartphone oder dergleichen erfolgen

und an die zentrale Einheit übermittelt werden. Eine solche zentrale Einheit kann auch die Benutzerverwaltungseinrichtung umfassen; alternativ kann sie dezentrale Benutzerverwaltungseinrichtungen – bspw. in jeder Leseeinheit – entsprechend ansteuern.

Nebst dem Erkennen der Identifikationsinformation über den optisch auslesbaren Code kann das Verleihen einer Berechtigung in der Praxis noch an weitere Bedingungen geknüpft sein, welche von der Programmierungseinheit vorgegeben werden, bspw. die Eingabe eines alphanumerischen Codes durch den Benutzer, die Erkennung eines Sicherheitsmerkmals etc.; die Programmierungseinheit kann ausserdem so ausgebildet sein, dass sie je nachdem unterschiedliche Berechtigungen vergeben kann und/oder zur Vergabe von Berechtigungen zunächst in Kommunikationsverbindung mit einer anderen Einheit stehen muss und sich von dort nötige Daten geben lassen muss.

Ausser der – beispielsweise das Benutzermedium individuell und eindeutig identifizierenden – Identifikationsinformation kann der optisch auslesbare Code auch weitere Informationen beinhalten, bspw.

- Informationen über die physische Ausgestaltung des Benutzermediums, und/oder
- Informationen über eine Version des Benutzermediums, und/oder
- Informationen über einen anzuwendenden Funktechnologie-Standard, und/oder
- Informationen über die Grösse eines für Anwendungen und/oder Anweisungen in den Speichermitteln zur Verfügung stehenden Datenspeichers.

Zusammen mit dem optisch auslesbaren Code können weitere Informationen an die Benutzerverwaltungseinrichtung übermittelt werden. Insbesondere können diese Informationen dazu dienen, das zum optisch auslesbaren Code gehörende Benutzermedium einem Benutzer oder einer Gruppe von Benutzern zuzuordnen. Beispielsweise kann es sich dabei um eine Gruppe von Benutzern handeln, welche auf Grund Ihrer Funktion über dieselben Berechtigungen verfügen. Bei den weiteren Informationen kann es sich beispielsweise um eine Personalnummer, eine alphabetische und/oder numerische Kennung, ein Passwort und/oder einen Namen des Benutzers handeln. Eine solche Personalisierung des Benutzermediums ermöglicht eine auf einen Benutzer oder eine Benutzergruppe spezifisch abgestimmte Freigabe von Berechtigungen.

Aufgrund der Ausgestaltung der Benutzermedien kann ein neuer Benutzer, welcher ein Benutzermedium erhalten hat, oder eine mit ihm zusammenarbeitende Person (eine betriebsinterne Verwalterin der elektronischen Schlüssel zum Beispiel) die ihm zustehende Berechtigung erlangen, ohne dass er selbst oder das Benutzermedium sich an einem bestimmten Ort befinden oder einfinden muss. Ferner kann das Identifizierungssystem so ausgelegt sein, dass der Benutzer nicht auf ein Gerät zurückgreifen muss, welches ein integraler Bestandteil des Identifizierungssystems ist. Beispielsweise kann es sich dabei um ein persönliches Gerät des Benutzers, beispielsweise sein Mobiltelefon, oder um ein Gerät des Arbeitgebers, beispielsweise eine Kamera oder einen Scanner, handeln.

Ferner kann das Vermerken eines Benutzermediums und gegebenenfalls des dem Benutzermedium zugeordnete Benutzer durch den Benutzer selbst, initiiert werden, indem der Benutzer den optisch auslesbaren Code und gegebenenfalls weitere Informationen an die Programmierungseinheit aktiv übermittelt. Das heisst auch, dass in derart ausgestalteten Ausführungsformen kein Benutzermedium ohne eine Aufnahmeanfrage von Benutzerseite her in der Benutzerverwaltung vermerkt wird.

Ein passives, d.h. ohne Mitwirken des Trägers des Benutzermediums, Vermerken eines Benutzermediums ist ausgeschlossen. Ferner kann eine erfolgreiche Aufnahmeanfrage eine oder mehrere Zustimmungen des Benutzers, beispielsweise die Zustimmung zu Verhaltensregeln oder zu einem Pflichtenheft beinhalten.

Neben dem Benutzer selbst, können auch weitere Personen die Benutzerseite repräsentieren, beispielsweise Vorgesetzte oder zentrale Organe eines Unternehmens.

Ein Verfahren zum Hinzufügen eines Benutzermediums zu einem Identifizierungssystem (insbesondere der vorstehend definierten Art) aufweisend eine Mehrzahl von Benutzermedien mit je einer integrierten Schaltung mit Speichermitteln und einen in den Speichermitteln abgespeicherten Identifikationscode und aufweisend mindestens eine Leseeinrichtung sowie eine Benutzerverwaltungseinrichtung , umfasst die Schritte

- Zur Verfügung-Stellen des Benutzermediums mit dem in den Speichermitteln abgespeicherten Identifikationscode sowie mit einem optisch auslesbaren Code, welcher eine das Benutzermedium individuell identifizierende Identifikationsinformation beinhaltet,
- Optisches Auslesen des optisch auslesbaren Codes,
- Auswerten des ausgelesenen optisch auslesbaren Codes mit Extraktion der Identifikationsinformation,
- Vermerken des Benutzermediums durch die Benutzerverwaltungseinrichtung.

Neben der Extraktion der Identifikationsinformation ist auch eine Verifikation und/oder eine Plausibilitätsprüfung der Identifikationsinformation denkbar.

Das optische Auslesen kann bspw. das Aufnehmen eines Bildes mindestens des optisch auslesbaren Codes mit einer Digitalkamera umfassen.

Das Benutzermedium kann zur Verfügung gestellt werden, indem es als beliebiges Benutzermedium einer gewünschten physischen Ausgestaltung genommen wird, gegebenenfalls mit dem richtigen Herstellerschlüssel, bspw. aus einem vorhandenen Vorrat von Benutzermedien.

Nebst dem Identifizierungssystem und dem Verfahren ist auch ein Benutzermedium für ein solches System und/oder ein solches Verfahren Gegenstand des vorliegenden Schutzrechts.

Nachfolgend werden Eigenschaften und Ausführungsbeispiele der Erfindung anhand von schematischen Figuren diskutiert. In den Figuren zeigen:

- Fig. 1 ein Benutzermedium;
- Fig. 2 den Ablauf bei der Registrierung eines Benutzermediums;
- Fig. 3 einen Authentifizierungsprozess; und
- Fig. 4 ein Ablauf bei der Durchführung des Authentifizierungsprozesses.

Das Benutzermedium 1 gemäss **Figur 1** ist bspw. als Karte, als Schlüssel oder als in ein anderes Medium (bspw. eine Uhr oder ein Mobiltelefon) integrierte Vorrichtung ausgebildet. Es weist wie an sich bekannt einen RFID-Chip 2 und eine RFID-Antenne 3 auf. In der gezeichneten Ausführungsform ist der RFID-Chip 2 ein rein passiver Chip der über keinen eigenen Batterie- oder Netzanschluss verfügt, so dass die für den Lese- und allenfalls einen Schreibprozess benötigte Energie allein von der Leseeinrichtung stammt.

Der RFID-Transponder (mit dem RFID-Chip 2 und der RFID-Antenne 3) kann in an sich bekannter Art ausgeführt sein.

Der RFID-Chip kann insbesondere als Chip einer bekannten Transponder-Technologie entsprechen, bspw. der Mifare-Chipkartentechnik oder der Legic-Technologie.

Der Chip enthält einen Datenspeicher mit unter anderem einem eindeutigen Identifikationscode 4, anhand dessen während eines Authentifizierungsprozesses die Berechtigung des Benutzermedium-Inhabers für einen bestimmten Vorgang geprüft wird.

Nebst dem eindeutigen Identifikationscode kann der Datenspeicher optional noch andere Informationen beinhalten. Daneben kann der RFID-Chip auch Speicherbereiche aufweisen, die für bestimmte Applikationen beschreibbar sein können. In diesen Ausführungsformen wird das Identifizierungssystem auch mindestens ein Lesegerät aufweisen, welches nicht nur Lesen, sondern auch schreiben kann.

Beispielsweise kann der RFID-Chip drei Segmente beinhalten. Das erste Segment enthält die Card-ID. Das zweite Segment ist für die Anwendung „Schrankschloss" („Garderobenschlüssel") reserviert, bei denen das Benutzermedium temporär einem anfänglich frei wählbaren Lesegerät zugeordnet wird und so bspw. ein temporär reserviertes Schloss wieder öffnen kann. Das dritte Segment dient für Anweisungen, welche auf das Benutzermedium geschrieben werden können, bspw. Berechtigung zufügen, Berechtigung wegnehmen, Berechtigung auswechseln.

Nebst dem RFID-Transponder weist das Benutzermedium auch einen optisch auslesbaren Code 7 auf. Dieser kann als 2-dimensionaler Code, bspw. als QR-Code, oder als eindimensionaler Code, bspw. als Strichcode ausgebildet sein und irgend eine Form aufweisen, die das optoelektronische Auslesen ermöglicht. Auch eine Darstellung in Buchstaben und/oder Zahlen ist möglich und ein optisch auslesbarer Code im Sinne der vorliegenden Erfindung. Oft besonders bevorzugt sind aufgrund ihrer Leistungsfähigkeit und der Möglichkeit zur Fehlerkorrektur jedoch binäre und/oder zweidimensionale Codes.

Der optisch auslesbare Code 7 enthält folgende Informationen:

- Informationen, welche die Bestimmung der Identität des Benutzermediums, d.h. eine individuelle Identifikation ermöglichen. Diese Informationen können insbesondere aus dem Identifikationscode bestehen oder diesen ganz oder zum Teil beinhalten. Es ist aber im Prinzip auch möglich, dass diese Identifikations-Informationen vom Identifikationscode verschieden sind und – bspw. anhand einer Tabelle oder durch geeignete Rechenoperationen – eine Zuordnung zu diesem ermöglichen. Wichtig ist, dass diese Informationen für das Benutzermedium individuell sind, d.h. ein Benutzermedium von einem anderen unterscheiden. Insbesondere können sie so sein, dass jede Identifikations-

Information weltweit nur einmal vergeben wird. Es ist aber auch nicht ausgeschlossen, dass sie mehrmals vergeben werden, bspw. für verschiedene Länder oder verschiedene Abnehmersegmente, wobei innerhalb eines solchen Segments jede Identifikationsinformation bevorzugt nur einmal vergeben wird.

- Optional Informationen darüber, was die physische Ausgestaltung des Benutzermediums ist (Schlüssel, Karte, aktiver Transponder, etc.)

- Optional Informationen über die Version,

- Optional Informationen über die anzuwendende Funktechnologie (den anzuwendenden Standard);

- Optional Informationen über die Grösse des für Anwendungen und/oder Anweisungen im RFID-Chip zur Verfügung stehenden Speichers. Wenn dieser wie vorstehend diskutiert segmentiert ist, können diese Informationen die Grösse des dritten Segments beinhalten.

Diese optional im optisch auslesbaren Code enthaltenen Informationen können je einzeln oder in beliebigen Kombinationen vorhanden sein; insbesondere kann der optisch auslesbare Code auch alle diese Informationen kombiniert enthalten.

Figur 2 illustriert den Vorgang bei der Initialisierung eines Benutzermediums, d.h. der Registrierung durch die Benutzerverwaltungseinrichtung. Benutzermedien 1 werden im Allgemeinen in genügender Menge vorproduziert und stehen den Betreibern in einem Vorrat 10 zur Verfügung. Für die Initialisierung nimmt der

Betreiber ein beliebiges Benutzermedium 1 der gewünschten physischen Ausgestaltung vom Stapel. Der Benutzer oder eine ihn unterstützende Person erfasst dann den optisch auslesbaren Code. Das kann bspw. einfach durch Abfotografieren, hier mit einem Smartphone 21 geschehen. Das Identifizierungssystem weist geeignete Auslesesoftware auf, um die Informationen aus dem optisch auslesbaren Code 7 auszulesen.

Eine solche Auslesesoftware kann bspw. als App gleich auf dem Smartphone 21 vorhanden sein. Alternativ kann vom Smartphone (oder einem anderen Gerät mit Digitalkamerafunktion) auch das ganze aufgenommene Bild weitergeleitet und die Auslesesoftware entsprechend beim Empfänger vorhanden sein.

Die ausgelesene, im optisch auslesbaren Code enthaltene Information, beinhaltend den Identifikationscode 8 und gegebenenfalls die weiteren Informationen 9 werden der Benutzerverwaltungseinrichtung 31 weitergegeben. Diese registriert das Benutzermedium und gibt ihm die der Anwendung entsprechende Berechtigung.

In einem Authentifizierungsprozess, wie in **Figur 3** dargestellt, wird eine Leseeinrichtung 41 den Identifkationscode 8 über RFID aus dem RFID-Chip 2 auslesen und an die Benutzerverwaltungseinrichtung 31 weitergeben, welche den Identifikationscode mit den registrierten Daten abgleicht und, sofern vorher der Initialisierungsprozess stattgefunden hat und das Benutzermedium als registriert erkannt wird, die entsprechende Freigabe erzeugt. Es kann auch vorgesehen sein, dass der Authentifizierungsprozess nicht ein Auslesen des ganzen Identifikationscode als solchen beinhaltet, sondern einen anders gearteten, die Authentifizierung des Benutzers durch die Leseeinrichtung und zugeordnete Benutzerverwaltungseinrichtung ermöglichenden Datenaustausch – insbesondere wenn die Benutzerverwaltungseinrichtung in der Leseeinrichtung integriert ist.

Figur 4 zeigt schematisch einen möglichen während der Authentifizierung ablaufenden Prozess zur Plausibilitätsprüfung. Wenn beim Ausleseprozess in einem ersten Schritt 101 das Segment mit dem Identifikationscode gefunden wird, wird anschliessend dieses Segment ausgelesen 102. Dann werden in einem weiteren Schritt 103 gewisse Vorgaben für den Medientyp untersucht und anschliessend wird eine Redundanzprüfung 104 durchgeführt, um eventuelle Lesefehler auszuschliessen. Schliesslich wird ein Abgleich 105 eines dedizierten Teils des Identifikationscodes mit dem Herstellerschlüssel (‚Stamp') durchgeführt. Nur wenn alle Tests 103-105 erfolgreich waren, wird der ausgelesene Identifkationscode für die Berechtigungsprüfung 106 verwendet. Ansonsten wird er als ungültig verworfen 107 und das Verfahren wird beendet.

Die optionale Identität eines Teils des Identifkationscodes mit dem sogenannten Stamp ist ein Sicherheitsmerkmal, welches beispielsweise durch das Legic-System ermöglicht wird. Der Stamp ist ein pro Hersteller individueller elektronischer Schlüssel. Indem dieser optional zum Teil des Identifikationscodes gemacht und obiger Abgleich 105 mit diesem durchgeführt wird, ergibt sich eine zusätzliche Sicherheit; bspw. kann so ausgeschlossen werden, dass jemand durch Manipulation systemfremden Benutzermedien funktionierende Berechtigungen verleiht.

Die Benutzerverwaltungseinrichtung 31 kann in die jeweilige Leseeinrichtung integriert oder von dieser separat, bspw. in einem Systemserver, eingerichtet sein.

Das Registrieren eines neuen Benutzermediums gemäss Figur 2 kann als Programmierung der Benutzerverwaltungseinrichtung 31 aufgefasst werden. Die Programmierung erfolgt durch eine Instanz, welche die entsprechende Berechtigung hat und vor welcher sich ein die für die Programmierung verantwortliche Person

beispielweise auf geeignete Art identifizieren muss. Dafür gibt es beispielswese folgende Möglichkeiten:

- Die Programmierungseinheit wird durch eine Software gebildet, welche auf dem Smartphone (oder anderen Endgerät) läuft, mit welchem auch die Erfassung und Auswertung des optisch auslesbaren Codes erfolgt. Die Programmierung erfolgt dann einen geeigneten Kommunikationskanal, beispielsweise über Nahfeldkommunikation (NFC) oder Bluetooth oder einen anderen drahtlosen direkten Punkt-zu-Punkt Kommunikationskanal direkt an die in der Leseeinrichtung vorhandene Benutzerverwaltungseinrichtung.

- Die Programmierungseinheit wird durch eine Software gebildet, welche ebenfalls auf dem Smartphone (oder anderen Endgerät) läuft, die Übertragung an die Benutzerverwaltungseinrichtung erfolgt jedoch über das Internet (Cloud-Lösung), wodurch eine Mehrzahl von dezentralen Benutzerverwaltungseinrichtungen gleichzeitig erreicht werden kann, wobei dafür vorausgesetzt ist, dass diese über eine Datenverbindung ins Internet – bspw. über ein integriertes Mobilfunk-Endgerät oder ein integriertes Modem oder eine drahtbehaftete oder drahtlose Verbindung zu einem Computer – verfügen.

- Die Programmierungseinheit ist als Teil einer zentralen Einheit ausgebildet, welche mit den Leseeinrichtungen des Identifizierungssystems in Kommunikationsverbindung steht oder in Kommunikationsverbindung bringbar ist, beispielsweise ebenfalls drahtbehaftet oder über einen Mobilfunkstandard, oder über einen für Kurzstrecken konzipierten Standard wie ZigBee oder WLAN. Diese Möglichkeit lässt sich auch besonders gut mit der Option kombinieren, die Benutzerverwaltungseinrichtung ebenfalls zentral, bspw. in derselben zentralen Einheit und unter Umständen mit der Programmierungseinheit integriert

vorzusehen. Beim Vorgehen gemäss dieser Option kann die Software zum Auslesen des optisch auslesbaren Codes dezentral im Smartphone (oder anderen Endgerät) oder alternativ in der zentralen Einheit vorgesehen sein, wobei im letzteren Fall das Smartphone (oder andere Endgerät) lediglich die unverarbeiteten Bilddaten oder interpretierte Bilddaten (jeweils verschlüsselt oder unverschlüsselt) an die zentrale Einheit übertragen muss.

PATENTANSPRÜCHE

1. Identifizierungssystem, aufweisend

   - Eine Mehrzahl von Benutzermedien (1), von denen jedes eine integrierte Schaltung (2) mit Speichermitteln und einen in den Speichermitteln abgespeicherten Identifikationscode (8) aufweist;

   - mindestens eine Leseeinrichtung (41);

   - wobei die Leseeinrichtung (41) befähigt ist, für einen Authentifizierungsprozess über Radiowellen berührungslos aus der integrierten Schaltung (2) Daten auszulesen;

   - und wobei das Identifizierungssystem ferner eine Benutzerverwaltungseinrichtung (31) aufweist und befähigt ist, einen Vorgang abhängig davon, ob in der Benutzerverwaltungseinrichtung das über die Radiowellen ausgelesene Benutzermedium als berechtigt vermerkt ist, auszulösen oder nicht auszulösen;

   - **dadurch gekennzeichnet**, dass jedes Benutzermedium ferner einen optisch auslesbaren Code (7) aufweist welcher eine das betreffende Benutzermedium individuell identifizierende Identifikationsinformation beinhaltet, wobei das Identifizierungssystem befähigt ist, ein über den optisch auslesbaren Code erkanntes Benutzermedium in der Benutzerverwaltungseinrichtung zu vermerken.

2. Identifizierungssystem gemäss Anspruch 1, wobei mindestens innerhalb einer Gruppe von Benutzermedien eine eindeutige Zuordnung zwischen dem Identifikationscode und der Identifikationsinformation besteht.

3. Identifizierungssystem nach Anspruch 2, wobei die Identifikationsinformation den Identifikationscode (8) aufweist.

4. Identifizierungssystem nach einem der vorangehenden Ansprüche, ferner aufweisend ein Mittel zum Auswerten des durch eine Kamera erfassten optisch auslesbaren Codes und eine Programmierungseinheit zum Vermerken des erkannten Benutzermediums in der Benutzerverwaltungseinrichtung.

5. Identifizierungssystem nach Anspruch 4, wobei das Mittel zum Auswerten als auf einem Mobiltelefon (21) mit Digitalkamera ausführbares Programm oder Programmteil vorhanden ist.

6. Identifizierungssystem nach Anspruch 4 oder 5, wobei die Programmierungseinheit als auf einem Mobiltelefon (21) mit Digitalkamera ausführbares Programm oder Programmteil vorhanden ist.

7. Identifizierungssystem nach Anspruch 6, wobei die Benutzerverwaltungseinrichtung (31) in der Leseeinrichtung (41) integriert ist und die Programmierungseinheit befähigt ist, über eine drahtlose Punkt-zu-Punkt-Verbindung mit der Leseeinrichtung Daten auszutauschen, wobei diese drahtlose Punkt-zu-Punkt-Verbindung über eine anderen Datenübertragungsstandard erfolgt als das Auslesen des Benutzermediums.

8. Identifizierungssystem nach Anspruch 7, wobei die drahtlose Punkt-zu-Punkt-Verbindung eine Verbindung über den Nahfeldkommunikationsstandard oder über den Bluetooth-Standard ist.

9. Identifizierungssystem nach einem der vorangehenden Ansprüche, wobei die Programmierungseinheit Teil einer zentralen Einheit ist, die mit mindestens einigen Leseeinrichtungen (41) des Identifizierungssystems in Kommunikationsverbindung steht oder in Kommunikationsverbindung bringbar ist.

10. Identifizierungssystem nach einem der vorangehenden Ansprüche, wobei die Benutzerverwaltungseinrichtung (31) Teil einer zentralen Einheit ist, die mit mindestens einigen Leseeinrichtungen (41) des Identifizierungssystems in Kommunikationsverbindung steht oder in Kommunikationsverbindung bringbar ist.

11. Identifizierungssystem nach einem der vorangehenden Ansprüche, wobei der optisch auslesbare Code (7) ein binärer zweidimensionaler Code ist.

12. Identifizierungssystem nach einem der vorangehenden Ansprüche, wobei der optisch auslesbare Code nebst der Identifikationsinformation weitere Informationen (9) beinhaltet, wobei diese weiteren Informationen mindestens eines der folgenden Dinge beinhalten:

- Informationen über die physische Ausgestaltung des Benutzermediums;
- Informationen über eine Version des Benutzermediums;
- Informationen über einen anzuwendenden Funktechnologie-Standard;
- Informationen über die Grösse eines für Anwendungen und/oder Anweisungen in den Speichermitteln zur Verfügung stehenden Datenspeichers.

13. Identifizierungssystem nach einem der vorangehenden Ansprüche, wobei der Identifikationscode einen einem Hersteller des Identifizierungssystems eindeutig zugeordneten Herstellerschlüssel aufweist, wobei in der Leseeinrichtung und/oder der Benutzerverwaltungseinrichtung der Herstellerschlüssel abgespeichert ist, und wobei während des Authentifizierungsprozesses oder vorgängig der betreffende Teil des Identifikationscodes mit dem Herstellerschlüssel abgeglichen wird.

14. Verfahren zum Hinzufügen eines Benutzermediums zu einem Identifizierungssystem mit einer Mehrzahl von Benutzermedien, die je eine integrierte Schaltung (2) mit Speichermitteln und einen in den Speichermitteln abgespeicherten Identifikationscode (8) aufweisen, und mit mindestens einer Leseeinrichtung sowie einer Benutzerverwaltungseinrichtung (21), umfassend die Schritte:

- Zur Verfügung-Stellen des Benutzermediums mit dem in den Speichermitteln (2) abgespeicherten Identifikationscode (8) sowie mit einem optisch auslesbaren Code (7), welcher eine das Benutzermedium individuell identifizierende Identifikationsinformation beinhaltet,
- Optisches Auslesen des optisch auslesbaren Codes,
- Auswerten des ausgelesenen optisch auslesbaren Codes mit Extraktion der Identifikationsinformation,
- Vermerken des Benutzermediums durch die Benutzerverwaltungseinrichtung.

15. Verfahren nach Anspruch 14, wobei das Auswerten des ausgelesenen optisch auslesbaren Codes auch eine Verifikation und/oder Plausibilitätsprüfung der Identifikationsinformation beinhaltet.

16. Benutzermedium für ein Identifizierungssystem nach einem der Ansprüche 1 bis 13, aufweisend eine integrierte Schaltung (2) mit Speichermitteln und einen in den Speichermitteln abgespeicherten Identifikationscode (8), wobei die integrierte Schaltung (2) befähigt ist, für einen Authentifizierungsprozess über Radiowellen berührungslos an eine Leseeinrichtung Daten zu übermitteln, **gekennzeichnet durch** einen optisch auslesbaren Code (7) welcher eine Benutzermedium individuell identifizierende Identifikationsinformation beinhaltet.

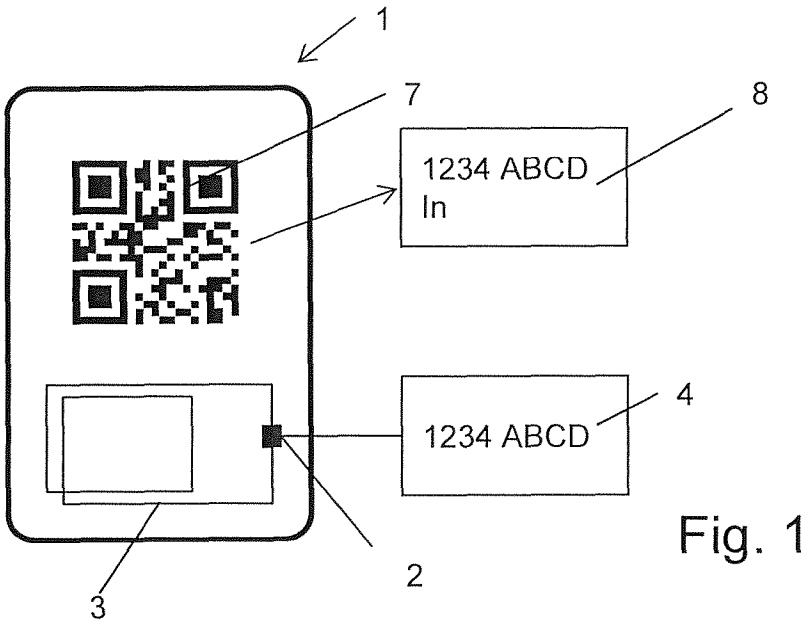


Fig. 1

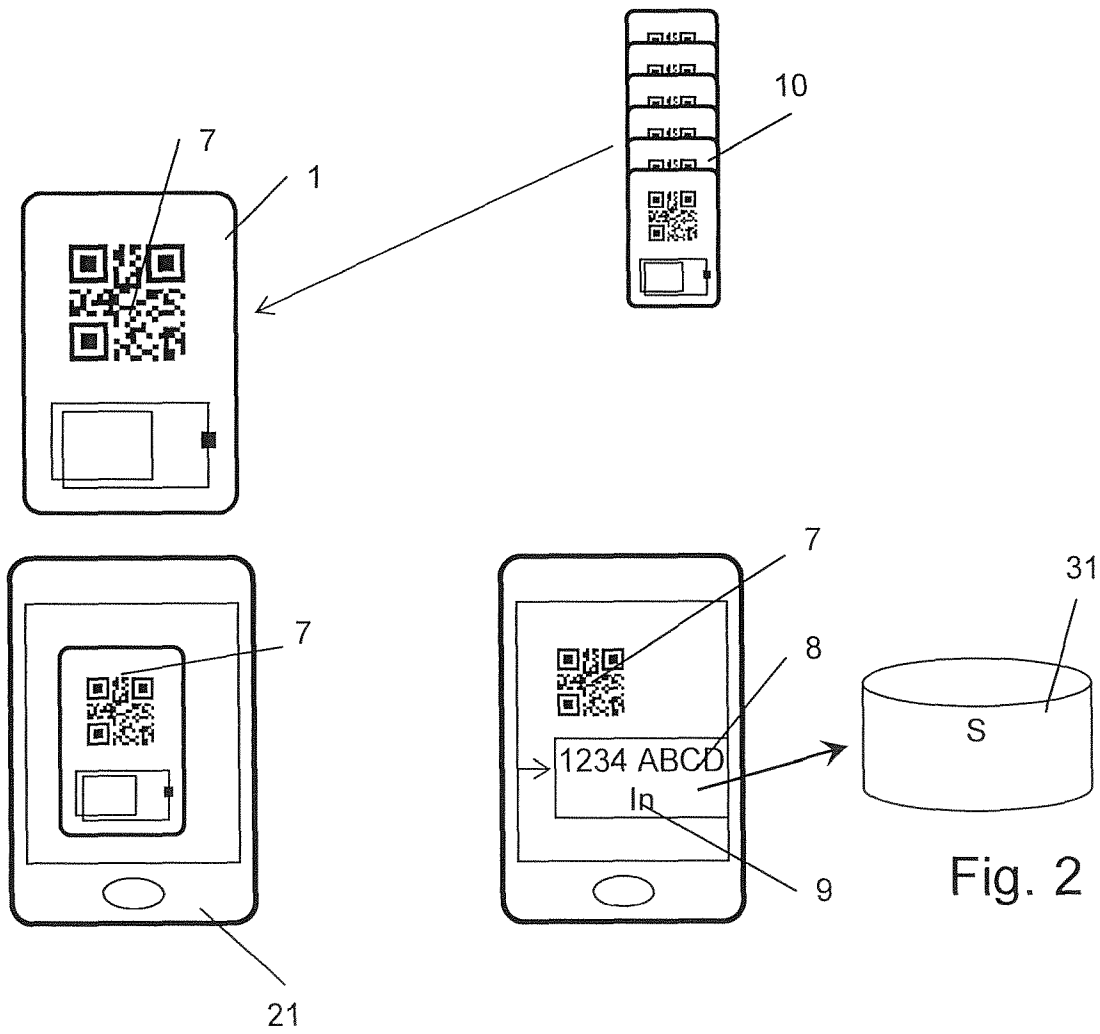


Fig. 2

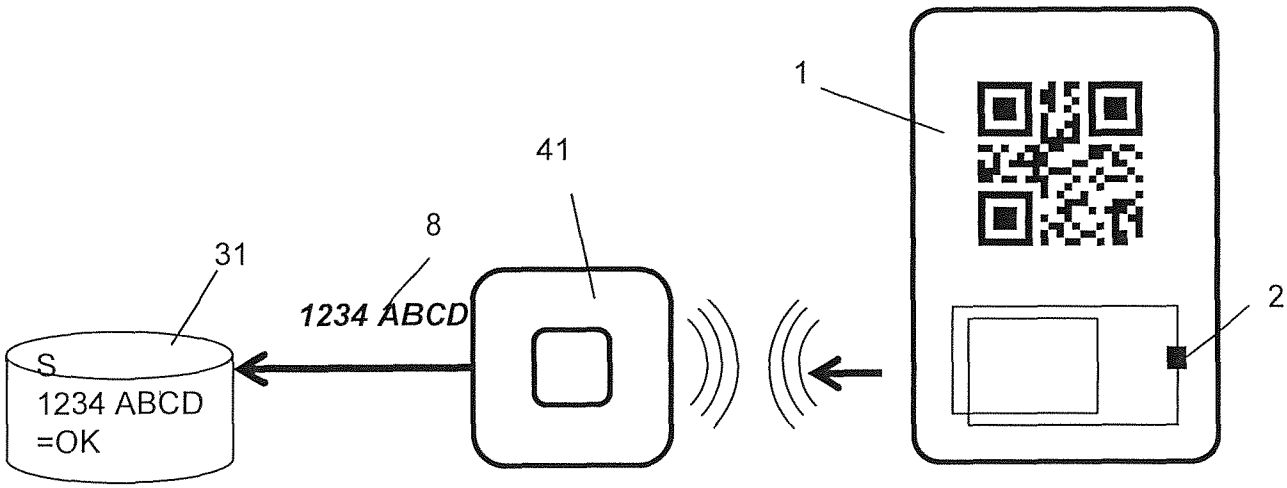

1
41
8
31
1234 ABCD
S
1234 ABCD
=OK
2

Fig. 3

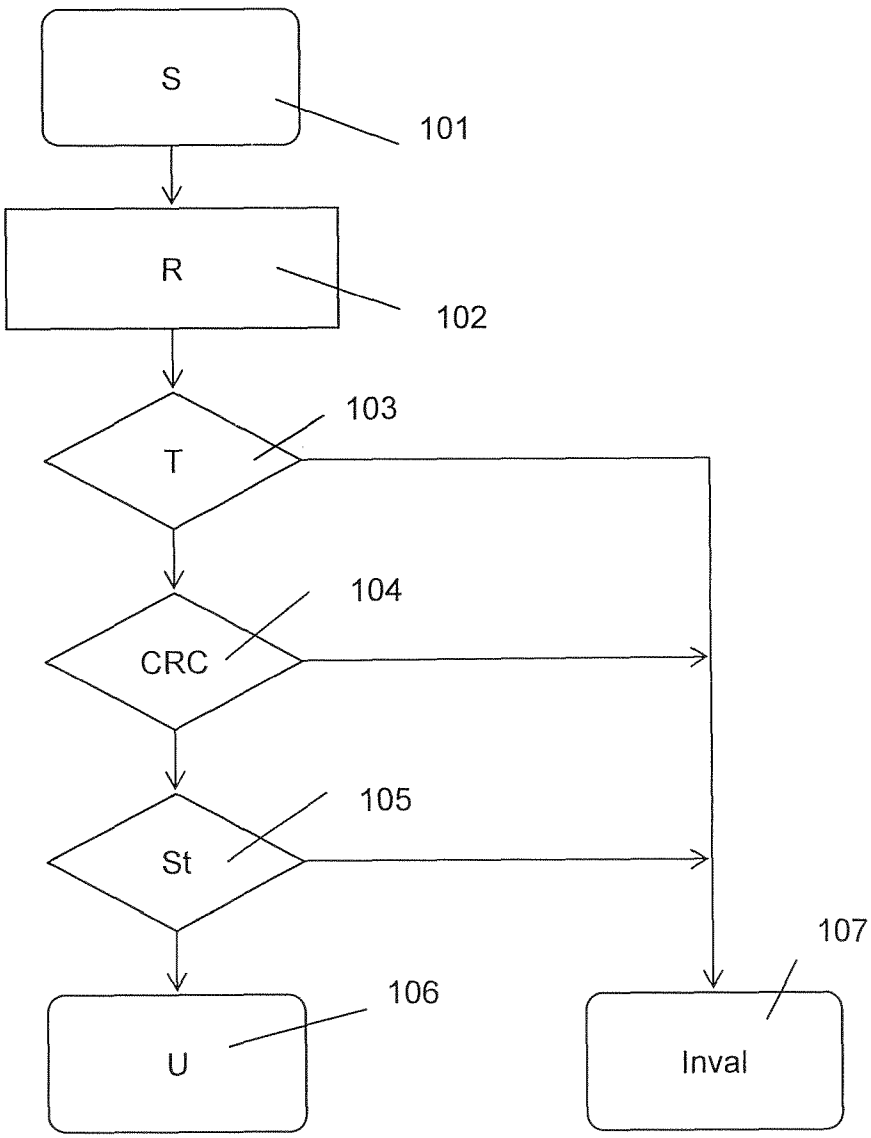

S
101
R
102
T
103
CRC
104
St
105
U
106
Inval
107

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/CH2015/000131

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06K19/14 G06Q10/08
ADD. G06K17/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06K G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2005/081174 A1 (MEADWESTVACO CORP [US]; CAMPERO RICHARD J [US]; PATEL KEYUR P [US]) 1 September 2005 (2005-09-01) cited in the application abstract paragraph [0026] - paragraph [0032] figures 2,3	1-16
X	US 2004/201479 A1 (GARBER SHARON R [US] ET AL) 14 October 2004 (2004-10-14) cited in the application abstract paragraph [0039] paragraph [0063] - paragraph [0065] paragraph [0080] figures 9-15	1-16

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 November 2015	25/11/2015

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Berger, Christian

2

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/CH2015/000131

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2004/090800 A2 (GIESECKE & DEVRIENT GMBH [DE]; GRAF HANS [DE]; FINKENZELLER KLAUS [DE]) 21 October 2004 (2004-10-21) abstract page 3, line 1 - line 2 page 6, last paragraph page 7, last paragraph - page 8, line 1 figures page 12, line 7 - line 9 -----	16

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/CH2015/000131

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2005081174 A1	01-09-2005	NONE	
US 2004201479 A1	14-10-2004	AT 352829 T	15-02-2007
		AT 376232 T	15-11-2007
		AT 400862 T	15-07-2008
		AT 445196 T	15-10-2009
		AT 464614 T	15-04-2010
		AT 466349 T	15-05-2010
		AT 483219 T	15-10-2010
		AU 762475 B2	26-06-2003
		BR 9913024 A	08-05-2001
		CA 2338601 A1	24-02-2000
		CA 2649129 A1	24-02-2000
		CN 1312933 A	12-09-2001
		CN 1516054 A	28-07-2004
		DE 1105855 T1	18-04-2002
		DE 69935017 T2	15-11-2007
		DE 69937373 T2	17-07-2008
		EP 1105855 A1	13-06-2001
		EP 1326219 A2	09-07-2003
		EP 1339032 A2	27-08-2003
		EP 1770591 A2	04-04-2007
		EP 1770592 A2	04-04-2007
		EP 1770593 A1	04-04-2007
		EP 1862981 A1	05-12-2007
		EP 1862982 A1	05-12-2007
		EP 1901251 A2	19-03-2008
		EP 2259239 A2	08-12-2010
		ES 2159502 T1	16-10-2001
		ES 2294212 T3	01-04-2008
		ES 2333897 T3	02-03-2010
		ES 2344741 T3	06-09-2010
		ES 2399594 T3	02-04-2013
		ES 2529584 T3	23-02-2015
		ES 2533350 T3	09-04-2015
		HK 1037048 A1	09-04-2009
		JP 5276144 B2	28-08-2013
		JP 5735608 B2	17-06-2015
		JP 5739382 B2	24-06-2015
		JP 2002522857 A	23-07-2002
		JP 2011175679 A	08-09-2011
		JP 2012195013 A	11-10-2012
		JP 2014006939 A	16-01-2014
		SG 106668 A1	29-10-2004
		SG 106669 A1	29-10-2004
		SG 107635 A1	29-12-2004
		SG 122782 A1	29-06-2006
		SG 128467 A1	30-01-2007
		US 6232870 B1	15-05-2001
		US 6486780 B1	26-11-2002
		US 2002008623 A1	24-01-2002
		US 2002167406 A1	14-11-2002
		US 2004201479 A1	14-10-2004
		US 2006145854 A1	06-07-2006
		US 2007011893 A1	18-01-2007
		US 2009102609 A1	23-04-2009
		US 2010176936 A1	15-07-2010
		WO 0010144 A1	24-02-2000

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/CH2015/000131

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2004090800 A2	21-10-2004	AT 428152 T	15-04-2009
		CN 1799058 A	05-07-2006
		DE 10317257 A1	04-11-2004
		EP 1616291 A2	18-01-2006
		EP 2081135 A2	22-07-2009
		ES 2444650 T3	26-02-2014
		JP 4759505 B2	31-08-2011
		JP 2006524851 A	02-11-2006
		PT 1616291 E	14-07-2009
		US 2007063055 A1	22-03-2007
		WO 2004090800 A2	21-10-2004

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/CH2015/000131

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G06K19/14 G06Q10/08
ADD. G06K17/00

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G06K G06Q

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 2005/081174 A1 (MEADWESTVACO CORP [US]; CAMPERO RICHARD J [US]; PATEL KEYUR P [US]) 1. September 2005 (2005-09-01) in der Anmeldung erwähnt Zusammenfassung Absatz [0026] - Absatz [0032] Abbildungen 2,3 -----	1-16
X	US 2004/201479 A1 (GARBER SHARON R [US] ET AL) 14. Oktober 2004 (2004-10-14) in der Anmeldung erwähnt Zusammenfassung Absatz [0039] Absatz [0063] - Absatz [0065] Absatz [0080] Abbildungen 9-15 ----- -/--	1-16

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
13. November 2015	25/11/2015

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Berger, Christian

2

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/CH2015/000131

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 2004/090800 A2 (GIESECKE & DEVRIENT GMBH [DE]; GRAF HANS [DE]; FINKENZELLER KLAUS [DE]) 21. Oktober 2004 (2004-10-21) Zusammenfassung Seite 3, Zeile 1 - Zeile 2 Seite 6, letzter Absatz Seite 7, letzter Absatz - Seite 8, Zeile 1 Abbildungen Seite 12, Zeile 7 - Zeile 9 -----	16

2

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/CH2015/000131

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 2005081174 A1	01-09-2005	KEINE	
US 2004201479 A1	14-10-2004	AT 352829 T	15-02-2007
		AT 376232 T	15-11-2007
		AT 400862 T	15-07-2008
		AT 445196 T	15-10-2009
		AT 464614 T	15-04-2010
		AT 466349 T	15-05-2010
		AT 483219 T	15-10-2010
		AU 762475 B2	26-06-2003
		BR 9913024 A	08-05-2001
		CA 2338601 A1	24-02-2000
		CA 2649129 A1	24-02-2000
		CN 1312933 A	12-09-2001
		CN 1516054 A	28-07-2004
		DE 1105855 T1	18-04-2002
		DE 69935017 T2	15-11-2007
		DE 69937373 T2	17-07-2008
		EP 1105855 A1	13-06-2001
		EP 1326219 A2	09-07-2003
		EP 1339032 A2	27-08-2003
		EP 1770591 A2	04-04-2007
		EP 1770592 A2	04-04-2007
		EP 1770593 A1	04-04-2007
		EP 1862981 A1	05-12-2007
		EP 1862982 A1	05-12-2007
		EP 1901251 A2	19-03-2008
		EP 2259239 A2	08-12-2010
		ES 2159502 T1	16-10-2001
		ES 2294212 T3	01-04-2008
		ES 2333897 T3	02-03-2010
		ES 2344741 T3	06-09-2010
		ES 2399594 T3	02-04-2013
		ES 2529584 T3	23-02-2015
		ES 2533350 T3	09-04-2015
		HK 1037048 A1	09-04-2009
		JP 5276144 B2	28-08-2013
		JP 5735608 B2	17-06-2015
		JP 5739382 B2	24-06-2015
		JP 2002522857 A	23-07-2002
		JP 2011175679 A	08-09-2011
		JP 2012195013 A	11-10-2012
		JP 2014006939 A	16-01-2014
		SG 106668 A1	29-10-2004
		SG 106669 A1	29-10-2004
		SG 107635 A1	29-12-2004
		SG 122782 A1	29-06-2006
		SG 128467 A1	30-01-2007
		US 6232870 B1	15-05-2001
		US 6486780 B1	26-11-2002
		US 2002008623 A1	24-01-2002
		US 2002167406 A1	14-11-2002
		US 2004201479 A1	14-10-2004
		US 2006145854 A1	06-07-2006
		US 2007011893 A1	18-01-2007
		US 2009102609 A1	23-04-2009
		US 2010176936 A1	15-07-2010
		WO 0010144 A1	24-02-2000

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/CH2015/000131

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 2004090800 A2	21-10-2004	AT 428152 T	15-04-2009
		CN 1799058 A	05-07-2006
		DE 10317257 A1	04-11-2004
		EP 1616291 A2	18-01-2006
		EP 2081135 A2	22-07-2009
		ES 2444650 T3	26-02-2014
		JP 4759505 B2	31-08-2011
		JP 2006524851 A	02-11-2006
		PT 1616291 E	14-07-2009
		US 2007063055 A1	22-03-2007
		WO 2004090800 A2	21-10-2004