



(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
31.01.2018 Patentblatt 2018/05

(51) Int Cl.:
B42D 25/305 (2014.01)

(21) Anmeldenummer: **17001285.0**

(22) Anmeldetag: **26.07.2017**

(84) Benannte Vertragsstaaten:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Benannte Erstreckungsstaaten:
BA ME
Benannte Validierungsstaaten:
MA MD

(71) Anmelder: **Giesecke+Devrient Mobile Security GmbH**
81677 München (DE)

(72) Erfinder:
• **Dörfler, Walter**
81373 München (DE)
• **Hönisch, Ulf**
85579 Neubiberg (DE)
• **Kruse, Georg**
85609 Aschheim (DE)

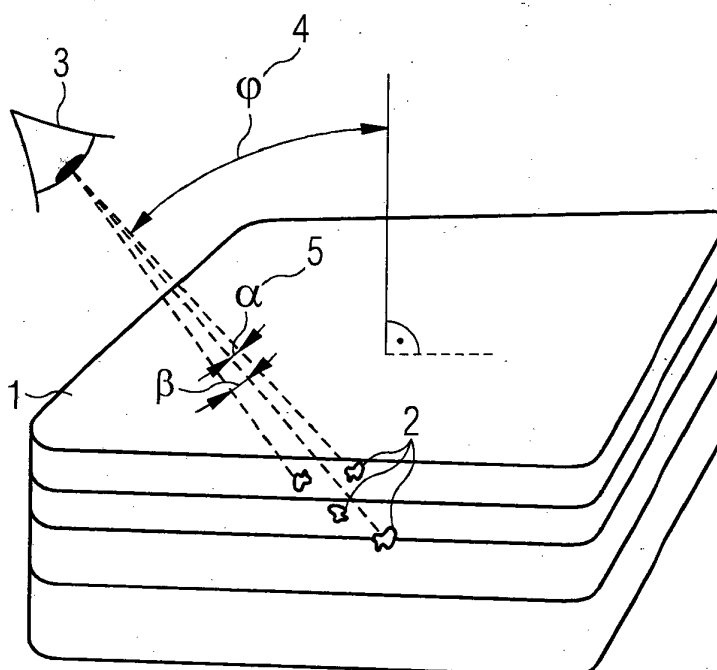
(30) Priorität: **29.07.2016 DE 102016009260**

(54) **FINGERABDRUCK EINES SICHERHEITSDOKUMENTS**

(57) Die vorliegende Erfindung ist gerichtet auf ein Verfahren zum Überprüfen eines Wertdokuments, derart, dass lediglich solche Sicherheitsmerkmale berücksichtigt werden, welche sich aus einem herkömmlichen Herstellungsprozess ergeben. Die Erfindung ist ferner gerichtet auf ein entsprechend ausgestaltetes Wertdo-

kument, sowie auf ein Prüfungsgerät und als Personalisierungsgerät bezüglich des Wertdokuments. Die Erfindung ist außerdem gerichtet auf ein Computerprogrammprodukt mit Steuerbefehlen, welche das vorgeschlagene Verfahren implementieren.

FIG 2



Beschreibung

[0001] Die vorliegende Erfindung ist gerichtet auf ein Verfahren zum Überprüfen eines Wertdokuments, derart, dass lediglich solche Sicherheitsmerkmale berücksichtigt werden, welche sich aus einem herkömmlichen Herstellungsprozess ergeben. Die Erfindung ist ferner gerichtet auf ein entsprechend ausgestaltetes Wertdokument, sowie auf ein Prüfungsgerät und ein Personalisierungsgerät bezüglich des Wertdokuments. Die Erfindung ist außerdem gerichtet auf ein Computerprogrammprodukt mit Steuerbefehlen, welche das vorgeschlagene Verfahren implementieren.

[0002] WO 2008/028476 A2 zeigt ein Sicherheitsdokument bzw. ein Wertdokument, enthaltend zumindest ein Sicherheitsmerkmal, welches in definierter räumlicher Position angeordnet ist. Das auf Echtheit zu prüfende Dokument wird mit der sogenannten "Service-Enhanced Raman Spektroskopie-Verfahren", auch SERS genannt, untersucht, wobei Zuschlagsstoffe vorgesehen sind. Der sogenannte Raman-Spektrometer operiert in einem Nanometerbereich und wird beispielsweise in einem forensischen Anwendungsszenario eingesetzt. Hierbei ist besonders nachteilig, dass keine handelsübliche Kamera zum Einsatz kommen kann. Auch ist das Wertdokument gemäß dieser Technologie entsprechend anzupassen, und es kann kein herkömmliches Wertdokument verwendet werden.

[0003] Ferner sind weitere Verfahren bekannt, welche Strukturmerkmale, wie z. B. eine Verteilung von Fasern in einem entfernt gelegenen Datenspeicher, also einer Datenbank, abspeichern. Ein solches Verfahren ist beispielsweise gezeigt in der US 2006/0294583 A1. Ferner sind weitere Systeme zur Verifikation bekannt, wie sie beispielsweise in der US 2007/0025619 A1 gezeigt sind.

[0004] Allgemein bekannt sind sogenannte Wertdokumente, also Banknoten, Ausweisdokumente bzw. Kreditkarten, welche typischerweise Sicherheitsmerkmale aufweisen und mehrschichtig aufgebaut sind. So werden beispielsweise sogenannte Smartcards mehrschichtig aufgebaut, elektronische Komponenten eingebracht und die Schichten in einem abschließenden Verfahren zusammenlaminiert. Typischerweise werden diese Wertdokumente in hohen Stückzahlen bereitgestellt, und erst nach einem Herstellungsprozess werden diese Wertdokumente personalisiert.

[0005] Ein Personalisieren eines Wertdokuments wird gemäß bekannter Verfahren derart durchgeführt, dass in einen fertigen Kreditkartenrohling personalisierte Daten, wie beispielsweise ein Lichtbild bzw. eine Beschichtung eingebracht werden. Sogenannte Smardcards weisen jedoch auch weitere Speicher auf, in die personalisierte Daten eingeschrieben werden können. Dies kann ein Kreditkarteninhaber oder ein Name einer Bank sein. Hierbei wird die Personalisierung jedoch typischerweise nicht aus dem Dokument ausgelesen, sondern vielmehr wird ein Name bereitgestellt, welcher dann in die Smartcard eingraviert wird.

[0006] Zum Personalisieren von Wertdokumenten sind viele Techniken bekannt, wie beispielsweise das Lasern einer Oberfläche von Smardcards. Hierbei erfolgt jedoch typischerweise ein Personalisieren unabhängig von dem Herstellungsprozess bzw. Produktionsprozess, da sonst Smardcards nicht in großer Stückzahl mit wenigem technischem Aufwand bereitgestellt werden können. Somit erfolgt gemäß dem Stand der Technik ein Personalisieren typischerweise unabhängig von einem Herstellungsprozess eines Wertdokuments.

[0007] Ferner ist es bekannt, hergestellte Wertdokumente nach ihrer Personalisierung zu registrieren. Hierzu hält beispielsweise der Hersteller eine Datenbank vor, in der beispielsweise Seriennummern von Wertdokumenten eingeschrieben werden und bei einer späteren Überprüfung der Wertdokumente herangezogen werden. Hierbei ist es jedoch besonders nachteilig, dass zum Überprüfen dieser Datenbank eine Kommunikationsschnittstelle vorgehalten werden muss, die dem Auslesen der hinterlegten Daten dient.

[0008] Typischerweise erfolgt eine Personalisierung von Wertdokumenten, beispielsweise ID-Dokumenten, mittels Lasergravur- oder Farbdruk. Die Erkennung und die Positionsbestimmung sowie die Auswertung der Heligkeitsinformationen, Farbinformationen und Strukturinformationen von Mustern bzw. Druckmarken erfolgt hierbei mittels einer Kamera. Letzteres geschieht typischerweise innerhalb einer Personalisierungsanlage unmittelbar vor der Personalisierung des Datenträgers.

[0009] Hierbei ist es besonders nachteilig, dass der Stand der Technik Strukturinformation von Wertdokumenten nur innerhalb einer Fläche und nicht im Volumen abprüft. Diese Fläche liegt in der Regel offen vor, d. h. ist gegen Verfälschung bzw. Zerstörung oder Abnutzung nicht oder nur unzureichend geschützt. Wird die Fläche ganz oder teilweise zerstört, ist eine Verifikation nicht länger möglich. Als Prüfmittel wird ein spezielles Gerät benötigt, welches eine hohe Ortsauflösung, ggf. im Mikrometerbereich oder darunter, aufweisen muss. Zur Speicherung bzw. Verifikation ist die Verbindung zu einer Datenbank erforderlich.

[0010] Es ist somit eine Aufgabe der vorliegenden Erfindung, ein Verfahren zum Prüfen eines Wertdokuments bereitzustellen, welches sicher mit geringem technischem Aufwand durchgeführt werden kann, und dennoch nicht in den Herstellungsprozess des Wertdokuments eingreift. Es ist ferner eine Aufgabe der vorliegenden Erfindung, ein entsprechend eingerichtetes Wertdokument bereitzustellen sowie ein Prüfungsgerät und ein Personalisierungsgerät zum Betreiben zumindest von einzelnen Verfahrensschritten. Es ist ferner eine Aufgabe der vorliegenden Erfindung, ein Computerprogrammprodukt bereitzustellen, mit Steuerbefehlen, welche das vorgeschlagene Verfahren implementieren.

[0011] Die Aufgabe wird gelöst durch den Gegenstand des Patentanspruchs 1. Weitere vorteilhafte Ausgestaltungen sind in den Unteransprüchen angegeben.

[0012] Demgemäß wird ein Verfahren zum Überprüfen

eines Werdokuments vorgeschlagen durch eine Verifikation des Werdokuments mittels eines Vergleichens eines ausgelesenen und eines abgespeicherten optischen Sicherheitsmerkmals, wobei das Sicherheitsmerkmal auf dem Werdokument abgespeichert wird, und, dass das Sicherheitsmerkmal aus einem Toleranzbereich eines Herstellungsprozesses des Werdokuments resultiert.

[0013] Ein Werdokument ist hierbei jegliches sicherheitsrelevante Dokument, beispielsweise Ausweispaapire, Banknoten, Kreditkarten und/ oder Smartcards. Hierbei kann generell ein Werdokument einem Bezahlvorgang bzw. einem Authentisieren dienen. Beispielsweise liegt das Werdokument als ein Ausweisdokument vor, mit dem eine Identität nachgewiesen werden soll, oder es soll sich Zugang zu sensiblen Bereichen, seien dies örtliche Bereiche oder aber auch datentechnische Bereiche, verschafft werden. Beispielsweise ist das Werdokument eingerichtet, sensible Daten oder Dienste freizuschalten. Da ein solches Werdokument lediglich von autorisierten Stellen ausgegeben wird, ist es notwendig, die Echtheit des Werdokuments zu verifizieren. Dies wird vorliegend als ein Überprüfen des Werdokuments bezeichnet, wobei ein positives Überprüfen eines Werdokuments dessen Echtheit bestätigt.

[0014] Liegt ein gefälschtes Werdokument vor oder nicht das erwartete Werdokument, so erfolgt ein negatives Überprüfen des Werdokuments.

[0015] Auf dem erfindungsgemäßen Werdokument bzw. gemäß dem erfindungsgemäßen Verfahren liegen zwei optische Merkmale vor. Das eine optische Merkmal liegt tatsächlich auf dem Werdokument vor und entsteht aus einem Herstellungsprozess des Werdokuments an sich. Das andere Sicherheitsmerkmal, welches abgespeichert wird, spiegelt das auszulesende Sicherheitsmerkmal wieder. Das heißt also, dass das ausgelesene Sicherheitsmerkmal tatsächlich physisch auf dem Werdokument vorliegt, während es sich bei dem abgespeicherten optischen Sicherheitsmerkmal um eine Repräsentation des tatsächlich vorliegenden optischen Sicherheitsmerkmals handelt. Dies ist erfindungsgemäß deshalb besonders vorteilhaft, da nicht gleichzeitig das ausgelesene und das abgespeicherte Sicherheitsmerkmal in einem Arbeitsschritt eingebracht werden, sondern vielmehr erfolgt erst implizit ein Einbringen des optischen Merkmals, woraufhin dieses ausgelesen wird und als eine Repräsentation des optischen Sicherheitsmerkmals abgespeichert wird.

[0016] Somit werden also das ausgelesene Sicherheitsmerkmal und das abgespeicherte Sicherheitsmerkmal derart getrennt voneinander erzeugt, dass das ausgelesene Sicherheitsmerkmal ohne einen gesonderten Personalisierungsschritt in das Werdokument eingebracht wird, in einem unabhängig davon ausgestalteten Verfahrensschritt das tatsächliche optische Sicherheitsmerkmal ausgelesen wird und dann abgespeichert wird. Durch das Trennen dieser beiden Schritte erfolgt eine höhere Sicherheit, da ein Angreifer nicht weiß, welches

Sicherheitsmerkmal genau auszulesen ist.

[0017] Da das Verfahren nicht offengelegt ist, welches Sicherheitsmerkmal ausgelesen und abgespeichert wird, hat der Angreifer keine Möglichkeit, das abgespeicherte optische Sicherheitsmerkmal selbst zu erstellen. Zwar mag der Angreifer diverse optische Sicherheitsmerkmale auf einem Werdokument erkennen, weiß aber nicht genau, welches Sicherheitsmerkmal ausgelesen wurde bzw. an welcher Stelle das Sicherheitsmerkmal ausgelesen wurde.

[0018] Zwar sind dem Fachmann diverse Möglichkeiten bekannt, ein optisches Merkmal auszulesen, dies kann jedoch derart willkürlich gewählt werden, dass jedes Sicherheitsmerkmal vorliegend Verwendung finden kann. Somit weiß der Fachmann generell, wie er das erfindungsgemäße Verfahren durchführen soll, der Angreifer weiß jedoch nicht, welches Sicherheitsmerkmal nunmehr genau gewählt wurde. So kann der Durchschnittsfachmann beispielsweise eine beliebige Stelle an der Oberfläche des Werdokuments auslesen und diese gesammelten Daten dann auf dem Werdokument abspeichern. Hierbei können beispielsweise bestimmte Strukturmerkmale des Werdokuments gemessen werden, oder aber es kann auch ein Schichtenmodell derart analysiert werden, dass transparente Schichten durchleuchtet werden, derart, dass lediglich opake Schichten ausgelesen werden. Auch wenn dies dem Fachmann im Allgemeinen bekannt ist, so weiß der Angreifer nicht, wie er nun das optische Sicherheitsmerkmal auf dem Werdokument abspeichern soll.

[0019] Ein Abspeichern des optischen Sicherheitsmerkmals kann derart ausgeführt werden, dass eine Repräsentation des optischen Sicherheitsmerkmals auf dem Werdokument aufgebracht, eingebracht bzw. abgespeichert wird. Ein Abspeichern kann generell dadurch erfolgen, dass beispielsweise eine textuelle Repräsentation des optischen Merkmals auf dem Werdokument angebracht wird. Hierzu kann jedoch auch ein Datenspeicher des Werdokuments Verwendung finden, in dem das optische Sicherheitsmerkmal abgelegt wird.

[0020] Beispielsweise sind in dem Werdokument zwei elektronische Komponenten verbaut. Diese sollen spezifikationsgemäß in einem bestimmten Winkel zueinander angeordnet sein. Da in einem Herstellungsprozess eine Vielzahl von Werdokumenten bereitgestellt werden muss, kann es vorkommen, dass einige Merkmale des Werdokuments von der tatsächlichen Spezifikation abweichen. Beispielsweise ist eine elektrische Komponente leicht verschoben in das Werdokument eingebracht. Nun wird gemäß dem vorgeschlagenen Verfahren das Sicherheitsmerkmal eines Winkels zwischen zwei Komponenten ausgelesen, welches optisch erkennbar ist, und wird auf dem Datenspeicher bzw. auf dem Werdokument an sich abgespeichert. Stehen zwei Komponenten nicht orthogonal aufeinander, so kann die Abweichung zwischen den beiden Komponenten von der Sollposition abgespeichert werden. Dies kann texturell auf dem Werdokument abgespeichert werden, kann aber

auch in den Speicher des Werdokuments eingeschrieben werden.

[0021] Ein solches Abspeichern des optischen Sicherheitsmerkmals kann mit irgendeiner Codierung derart erfolgen, dass die Codierung auf dem Werdokument aufgebracht wird. Der Fachmann kennt diverse Codierungen, beispielsweise eine Binärcodierung, anhand derer Sicherheitsmerkmale beschrieben werden können. Somit wird das optische Sicherheitsmerkmal abgespeichert, ohne dass dies darauf zwingendermaßen abstellt, dass das optische Merkmal an sich abgespeichert wird, sondern vielmehr können irgendwelche Formate bzw. irgendwelche Repräsentationen des optischen Sicherheitsmerkmals abgespeichert werden. Hierbei ist es vorteilhaft, die Codierung derart zu wählen, dass ein Angreifer diese nicht direkt entschlüsseln kann. Das heißt, dass ein Angreifer zum Entschlüsseln der abgespeicherten optischen Sicherheitsmerkmale erst Wissen über den Codierungsalgorithmus haben muss, bevor er es decodieren kann. Dies wiederum ist ein weiteres Sicherheitsmerkmal des vorgeschlagenen Verfahrens.

[0022] Ein Toleranzbereich eines Herstellungsprozesses des Werdokuments ist ein solcher Bereich, der nicht explizit vorgesehen ist, also nicht zur Personalisierung des Werdokuments dient, sondern vielmehr aufgrund unvermeidlicher Variationen der Herstellungsmaterialien bzw. Herstellungsgeräte entsteht. Dies ist also ein Bereich, der spezifikationsgemäß nicht bezüglich dem Werdokument vorgesehen ist, sondern der sich einfach aufgrund des Herstellungsprozesses ergibt und eben keinen gesonderten Personalisierungsschritt bzw. keinen gesonderten Sicherungsschritt verlangt.

[0023] So sind beispielsweise diverse Verfahren zur Personalisierung von Werdokumenten bekannt, wie das Einbringen von diffusen Partikeln in das Werdokument. Hierbei handelt es sich jedoch nicht um einen Toleranzbereich im Sinne der vorliegenden Erfindung, da diese Partikel wissentlich, also spezifikationsgemäß, eingebracht werden. Auch wenn die Partikel nicht berechenbar in diffuser Ausrichtung in dem Werdokument zu liegen kommen, so handelt es sich hierbei nicht um einen Toleranzbereich. Ein Toleranzbereich ist genau der Bereich, der eine Differenz zwischen einer Spezifikation eines Werdokuments und eines tatsächlich hergestellten Werdokuments beschreibt.

[0024] Genau dies ist ein Vorteil der vorliegenden Erfindung, da eben kein weiterer Personalisierungsschritt vorzusehen ist, sondern vielmehr, dass dieser eingespart werden kann. Erfindungsgemäß wurde somit erkannt, dass keinerlei Sicherheitsmerkmale explizit eingebracht werden müssen, sondern, dass diese bereits implizit aufgrund Abweichungen im Herstellungsprozess vorliegen. Somit ist auch bei einem genormten Werdokument, welches in großer Stückzahl hergestellt wird, stets ein individueller Toleranzbereich erkennbar, der ein erstes Werdokument von einem zweiten Werdokument unterscheidet, obwohl diese aus der gleichen Serie stammen. Somit lässt sich das vorgeschlagene Verfahren be-

sonders effizient implementieren.

[0025] Gemäß einem Aspekt der vorliegenden Erfindung wird das Sicherheitsmerkmal auf dem Werdokument abgespeichert. Dies hat den Vorteil, dass das Sicherheitsmerkmal äußerlich auf dem Werdokument angebracht werden kann. Dies kann beispielsweise mittels einer Lasergravur oder einer Reliefbildung erfolgen. Somit weist das Werdokument das implizit vorhandene Sicherheitsmerkmal auf, sowie das Sicherheitsmerkmal, welches auf dem Werdokument angebracht bzw. eingebracht ist. Hierbei soll das Abspeichern des Sicherheitsmerkmals keinesfalls einschränkend verstanden werden, sondern vielmehr ist jedes Hinterlegen des optischen Sicherheitsmerkmals in irgendeiner Codierung als ein Abspeichern zu verstehen.

[0026] Gemäß einem weiteren Aspekt der vorliegenden Erfindung wird das Sicherheitsmerkmal derart abgespeichert, dass es optisch auf dem Werdokument auslesbar ist. Dies hat den Vorteil, dass die Repräsentation des Sicherheitsmerkmals derart auf dem Werdokument vorhanden ist, dass es beispielsweise mittels einer herkömmlichen Kamera oder einfach nach einer menschlichen Prüfung erkennbar ist. Beispielsweise kann eine Prüfsumme des Sicherheitsmerkmals gebildet werden, und hierdurch kann das optische Sicherheitsmerkmal anhand einer Prüfsumme derart auf dem Werdokument angebracht werden, dass die Prüfsumme für einen menschlichen Prüfer bzw. ein Lesegerät erkennbar ist.

[0027] Gemäß einem weiteren Aspekt der vorliegenden Erfindung wird das Sicherheitsmerkmal derart abgespeichert, dass es in einem Speicher des Werdokuments eingeschrieben wird. Dies hat den Vorteil, dass zumindest eine Repräsentation des optisch tatsächlich vorhandenen Sicherheitsmerkmals auf einem Datenspeicher, der in dem Werdokument verbaut ist, abgelegt wird. Somit ist es möglich, mittels eines Prüfgeräts das abgespeicherte Sicherheitsmerkmal auszulesen und dies mit dem tatsächlich vorhandenen Sicherheitsmerkmal zu vergleichen. Hierbei ist es ebenfalls besonders vorteilhaft, dass das abgespeicherte Sicherheitsmerkmal nicht sofort von einem Angreifer erkennbar ist. Vielmehr ist ein Lesegerät erforderlich, welches das Sicherheitsmerkmal aus dem Speicher des Werdokuments ausliest.

[0028] Gemäß einem weiteren Aspekt der vorliegenden Erfindung erfolgt eine positive Verifikation, falls das ausgelesene und das abgespeicherte Sicherheitsmerkmal im Wesentlichen übereinstimmen. Dies hat den Vorteil, dass auch optische Varianzen berücksichtigt werden können, die typischerweise entstehen, falls ein optisches Merkmal mittels einer Kamera ausgelesen wird. Somit muss das tatsächlich vorhandene Sicherheitsmerkmal und das abgespeicherte Sicherheitsmerkmal nicht gänzlich übereinstimmen, sondern vielmehr reicht ein Schwellwert, welcher erfüllt werden muss, um eine positive Verifikation durchzuführen. So kann beispielsweise spezifiziert werden, dass ein im Wesentlichen Überein-

stimmen dann gegeben ist, falls das abgespeicherte Sicherheitsmerkmal zu einem gewissen Prozentsatz mit dem ausgelesenen Sicherheitsmerkmal übereinstimmt. Somit kann beispielsweise berücksichtigt werden, dass das optische Sicherheitsmerkmal leicht schief ausgelesen wird bzw. unter ungünstigen Lichtverhältnissen ausgelesen wird. Stimmen das ausgelesene Sicherheitsmerkmal und das abgespeicherte Sicherheitsmerkmal auch nicht im Wesentlichen überein, so folgt eine negative Verifikation des Sicherheitsdokuments, und es wird als ein gefälschtes Sicherheitsdokument bzw. Wertdokument erkannt oder zumindest als ein Wertdokument, das so nicht erwartet wurde. Somit können Authentifizierungsprozesse bei einer negativen Verifikation abgebrochen werden.

[0029] Gemäß einem weiteren Aspekt der vorliegenden Erfindung bezieht sich ein Toleranzbereich auf eine Schichtung, ein Strukturmerkmal, eine Schichtdicke, eine Farbgebung, eine Schwärzung, ein Spaltenmaß, eine Position einer Komponente, einem Winkel zwischen zwei Komponenten und/ oder eine Anordnung von mindestens einer Komponente. Dies hat den Vorteil, dass sich diverse Strukturmerkmale eines Wertdokuments dafür erfindungsgemäß eignen, dass diese als ein Sicherheitsmerkmal verwendet werden können. Beispielsweise kann eine Varianz in einer Dicke einer Schicht derart verwendet werden, dass transparente und opake Schichten ein gewisses Muster erzeugen, welches als ein Sicherheitsmerkmal dienen kann. Beispielsweise weisen einzelne Schichten sowohl transparente als auch opake Stellen auf, die in einem Durchlicht ein bestimmtes charakteristisches Merkmal ergeben. Hierbei muss das charakteristische Merkmal nicht absichtlich in das Wertdokument eingebracht werden, wie es bekannt wäre, sondern vielmehr eignen sich Varianzen im Herstellungsprozess, die das Wertdokument eindeutig charakterisieren. Beispielsweise kann es auch bei einer Farbgebung zu Toleranzen kommen, da beispielsweise bei einer Drucktechnik Farbverläufe verwischen bzw. die einzelnen Muster farblich nicht klar abgegrenzt sind. Auch ist es möglich, dass aufgrund der hohen Stückzahl von Wertdokumenten Spaltenmaße variieren, da sich die Herstellungsmaschinen nicht exakt justieren lassen. Gleiches gilt für die Position von Komponenten bzw. von Winkel zwischen den Komponenten als auch für den Abstand zwischen Komponenten, da diese nicht immer exakt gemäß der Spezifikation vorliegen, sondern dass vielmehr charakteristische Toleranzbereiche gegeben sind. Hierbei ist es besonders vorteilhaft, eine Auswahl der Toleranzbereiche zu kombinieren, um zu einem Sicherheitsmerkmal zu gelangen. Beispielsweise kann sowohl eine Schichtdicke als auch ein Spaltenmaß gemeinsam als ein Sicherheitsmerkmal dienen. Somit ist es dem Durchschnittsfachmann bewusst, dass der die aufgeführten Toleranzbereiche derart kombinieren kann, dass er zu einem optischen Sicherheitsmerkmal gelangt. Beispielsweise ist es auch möglich, einzelne Schichten mittels eines Lasers zu schwärzen und hierbei diese Schwärzung

mit einer Schichtdicke als ein Sicherheitsmerkmal zu kombinieren. Variiert eine Schichtdicke, so ist es auch möglich, dass eine Schwärzung durch einen Laser derart variiert, dass das eindeutige Sicherheitsmerkmal entsteht. Hierbei ist es erfindungsgemäß vorteilhaft, dass die tatsächliche Ausgestaltung eines jeden Wertdokuments im Wesentlichen gemäß einer Spezifikation erfolgt, wobei lediglich die Toleranzbereiche als ein möglicher Raum für ein Sicherheitsmerkmal dienen. Somit ist es also nicht notwendig, das Wertdokument extra zu personalisieren, sondern vielmehr werden Toleranzbereiche eines Herstellungsprozesses verwendet, um ein Sicherheitsmerkmal zu definieren.

[0030] Gemäß einem weiteren Aspekt der vorliegenden Erfindung stellt das optische Sicherheitsmerkmal ein dreidimensionales Sicherheitsmerkmal dar. Dies hat den Vorteil, dass nicht lediglich ein Auslesen der Oberfläche des Wertdokuments erfindungsgemäß durchgeführt wird, sondern vielmehr wird das Wertdokument auch in seiner Tiefe ausgelesen und somit implizit ein Sicherheitsmerkmal ausgelesen. Das dreidimensionale Sicherheitsmerkmal kann hierbei auf eine Oberflächenstruktur des Wertdokuments abstellen, kann aber auch transparente Schichten derart berücksichtigen, dass ein Winkel eines optisch variablen Sicherheitsmerkmals berücksichtigt wird. Ferner können auch gewisse Abstände oder Farbgebungen berücksichtigt werden, die durch eine transparente Schicht des Wertdokuments sichtbar werden.

[0031] Somit ist es auch möglich, diverse transparente Schichten derart vorzusehen, dass sich ein dreidimensionales Sicherheitsmerkmal ergibt.

[0032] Gemäß einem weiteren Aspekt der vorliegenden Erfindung liegt das ausgelesene optische Merkmal im Inneren des Wertdokuments vor. Dies hat den Vorteil, dass das optische Merkmal in einer inneren Schicht des Wertdokuments geschützt werden kann, so dass es vor Abrieb bzw. Abnutzung gesichert ist. Somit ist über dem optischen Merkmal eine transparente Schicht vorzusehen, welche es ermöglicht, das optische Merkmal des Wertdokuments von außen auszulesen.

[0033] Gemäß einem weiteren Aspekt der vorliegenden Erfindung wird das abgespeicherte optische Sicherheitsmerkmal in Form einer Prüfsumme abgespeichert. Dies hat den Vorteil, dass eine weitere Codierung verwendet wird, die es ermöglicht, nicht das optische Sicherheitsmerkmal an sich abzuspeichern, sondern vielmehr wird das optische Sicherheitsmerkmal durch eine Prüfsumme abgespeichert, derart, dass ein Angreifer nicht direkt ohne technische Hilfsmittel Rückschlüsse auf das optische Merkmal ziehen kann.

[0034] Gemäß einem weiteren Aspekt der vorliegenden Erfindung wird das ausgelesene optische Sicherheitsmerkmal in eine Repräsentation übergeführt und als Sicherheitsmerkmal abgespeichert. Dies hat den Vorteil, dass zwar das optische Sicherheitsmerkmal an sich in seiner physischen Form direkt erkennbar ist, nicht jedoch das abgespeicherte Sicherheitsmerkmal. Zwar ent-

spricht typischerweise das abgespeicherte Sicherheitsmerkmal dem tatsächlich vorliegenden optischen Sicherheitsmerkmal, wobei jedoch eine andere Repräsentation gewählt wird. Die Wahl der Repräsentation ist zwar dem Durchschnittsfachmann geläufig, der Angreifer weiß jedoch wiederum nicht, welche Repräsentation genau gewählt wurde, und kann somit von dem abgespeicherten Sicherheitselement nicht auf das tatsächliche Sicherheitselement rückschließen. Dies ist insbesondere deshalb vorteilhaft, da das abgespeicherte optische Sicherheitselement komplett verschlüsselt werden kann.

[0035] Gemäß einem weiteren Aspekt der vorliegenden Erfindung werden mehrere optische Sicherheitsmerkmale ausgelesen und jeweils auf dem Werdokument zusätzlich hinterlegt. Dies hat den Vorteil, dass die mehreren optischen Sicherheitselemente sowohl physisch auf dem Werdokument an sich vorliegen, als auch deren Repräsentation, beispielsweise in Form einer Beschriftung des Werdokuments oder mittels einer Ablage der mehreren optischen Sicherheitsmerkmale in einem Speicher des Werdokuments. Somit lassen sich auch diverse optische Sicherheitsmerkmale beliebig kombinieren.

[0036] Die Aufgabe wird auch gelöst durch ein Werdokument aufweisend ein abgespeichertes Sicherheitsmerkmal, welches einem optischen Sicherheitsmerkmal des Werdokuments entspricht, wobei das optische Sicherheitsmerkmal aus einem Toleranzbereich eines Herstellungsprozesses des Werdokuments resultiert.

[0037] Die Aufgabe wird auch gelöst durch ein Prüfungsgerät, welches eingerichtet ist zum Prüfen des Werdokuments.

[0038] Ferner wird die Aufgabe gelöst durch ein Personalisierungsgerät zum Personalisieren des Werdokuments mittels eines Abspeicherns des Sicherheitsmerkmals.

[0039] Ferner wird die Aufgabe gelöst durch ein Computerprogrammprodukt mit Steuerbefehlen, welche das vorgeschlagene Verfahren implementieren bzw. die vorgeschlagenen Endgeräte betreiben.

[0040] Hierbei ist es besonders vorteilhaft, dass die Verfahrensmerkmale, wie sie gemäß dem Verfahren vorgeschlagen werden, auch als strukturelle Merkmale bezüglich dem vorgeschlagenen Werdokument vorliegen können. Somit kann jeder Verfahrensschritt auf ein strukturelles Merkmal des Werdokuments abgebildet werden. Ferner können die strukturellen Merkmale des Werdokuments auch mittels Verfahrensschritten nachvollzogen werden. Ferner eignet sich das vorgeschlagene Verfahren zum zumindest teilweise Betreiben des Prüfungsgeräts bzw. des Personalisierungsgeräts. Das Computerprogrammprodukt ist ferner eingerichtet, das vorgeschlagene Verfahren zu implementieren bzw. die vorgeschlagenen Endgeräte zu betreiben.

[0041] Weitere vorteilhafte Ausgestaltungen werden im Folgenden anhand der beigelegten Figuren erläutert. Es zeigt:

Fig. 1: eine Prüfungsanordnung eines Werdokuments gemäß einem Aspekt der vorliegenden Erfindung,

Fig. 2: das Werdokument gemäß einem Aspekt der vorgeschlagenen Erfindung; und

Fig. 3: das Werdokument gemäß einem weiteren Aspekt der vorliegenden Erfindung.

[0042] Fig. 1 zeigt eine Systemanordnung, aufweisend eine Halterung 12 für einen Datenträger 14, der mittels einer Drehachse 16 rotiert werden kann. Hierzu ist ein Motor 18 vorgesehen. Eine Kamera 112 überprüft hier ein Werdokument, welches den Datenträger 14 aufweist, welcher mittels der Beleuchtung 110 beleuchtet wird. Die vorliegende Prüfungsanordnung wird mittels einer Steuerung 114 angesteuert. Das vorgeschlagene Verfahren ist wesentlich einfacher und somit auch für die Realisierung eines entsprechenden Prüfgerätes zur Verwendung z. B. durch einen Grenzbeamten möglich, verglichen mit dem Stand der Technik. Außerdem kann das vorgeschlagene Verfahren bereits bei der Personalisierung des Sicherheitsdokuments eingesetzt werden, um mit einem ggf. kundenspezifischen Algorithmus, beispielsweise unter Verwendung einer Prüfziffer, die dann für eine spätere Prüfung im Feld z. B. im Klartext mit auf das Sicherheitsdokument aufgebracht oder auch in den Chip der Karte eingeschrieben werden kann. Dieses Einschreiben kann beispielsweise verschlüsselt erfolgen.

[0043] Hierzu werden die Ist-Positionen verschiedener Merkmale vermessen, und diese werden mittels einer Prüfziffer zum späteren Abgleich bzw. zur Echtheitsprüfung hinterlegt.

[0044] Somit wird statt der Fläche eines Papiers bzw. Werdokuments das Volumen z. B. eines aus transparenten Schichten und ggf. einer oder mehreren opaken Schichten aufgebauten ID-Dokuments bzw. Datenträgers genutzt, und eine Mehrzahl an Varianten, ggf. auch statistisch verteilten Merkmalen bzw. Strukturelemente des Datenträgers, werden zur Ermittlung einer Echtheitswahrscheinlichkeit des Datenträgers verwendet.

[0045] Zu überprüfende Merkmale können bereits im Kartenrohling vorhanden sein bzw. alternativ oder zusätzlich im Rahmen der Personalisierung des Datenträgers aufgebracht werden.

[0046] Die Strukturmerkmale bzw. Sicherheitsmerkmale werden dabei aus einem inneren, gegen Schädigung gut geschützten Bereich der Karte gelesen und ausgewertet. Als Strukturmerkmale können dabei auch quasi zufällig verteilte, ggf. dreidimensional erfasste Strukturen wie Differenzpositionen und Differenzwinkel von Einzelstrukturen wie z. B. Schwärzungen von Teilbereichen innerer Schichten durch Lasereinwirkung verwendet werden. Die Auswertung der Strukturmerkmale kann ggf. auch unter schieferm Winkel erfolgen, um z. B. dreidimensionale Merkmale oder Relativpositionen vorteilhaft erfassen zu können.

[0047] Die ausgelesenen Informationen können dann entweder komplett, in Teilen oder über Bildung einer

Prüfsumme in Klartext, eventuell auch verschlüsselt, gelasert, gedruckt oder in dem Chip der Karte eingeschrieben und ggf. zusätzlich noch in einer Datenbank erfasst werden. Eine Übertragung der Informationen auf den Datenträger setzt allerdings voraus, dass die Merkmalsauswertung unmittelbar nach erfolgter Personalisierung des auszuwertenden Bereichs oder auch vor der Chip-Personalisierung erfolgt, solange der Datenträger im Zugriff der entsprechenden Personalisierungsanlage ist. Eine Offenlegung der Art und Weise der Merkmalsauswertung ist nicht erforderlich und kann innerhalb eines entsprechend ausgestatteten Prüfgerätes erfolgen. Ein Reverse-Engineering wird dadurch erschwert, was die Qualität der Absicherung des Datenträgers gegen Fälschung erhöht.

[0048] Durch die Überprüfung von dreidimensional angeordneten Strukturmerkmalen kann identifiziert werden, ob ein Ausweisdokument durch den Austausch einzelner Schichten verfälscht worden ist.

[0049] Durch Überprüfung vieler Strukturmerkmale lässt sich die Sicherheit der Verifikation erhöhen. In diesem Fall bleibt ein Datenträger auch bei Ausfall eines oder mehrerer Strukturmerkmale mit hinreichender Sicherheit verifizierbar. Eine Überprüfung der Daten- bzw. Dokumentenintegrität im Feld kann zumindest für einige der Ausführungsformen sehr einfach, z. B. mittels konventionellen Dokumentscannern erfolgen, die um einen entsprechenden Prüfalgorithmus ergänzt sind. Hierbei kann es sich um Flächen- oder Zeilenkameras handeln. Dieser Algorithmus kann ggf. kundenspezifisch angepasst werden. Eine Datenbankverbindung ist aber zumindest für einige der Ausführungsformen nicht erforderlich.

[0050] Es lassen sich außerdem einfach aufgebaute Prüfgeräte herstellen, die im Wesentlichen aus einer Kamera, einem ggf. dreh- oder kippbaren Dokumentenhalter und einer Lichtquelle bestehen. Letztere Prüfgeräte lassen sich weitgehend der Prüfaufgabe anpassen und können eine größere Bandbreite an Prüfungen durchführen, z. B. auch mit Lichtquellen und Sensoren, die im nicht sichtbaren Wellenbereich arbeiten. Eine solche Anordnung ist in Fig. 1 gezeigt.

[0051] Fig. 2 zeigt ein Wertdokument 1 bzw. ein ID-Dokument. Dieses weist Strukturmerkmale 2 auf, die von einem Prüfgerät 3 unter einem bestimmten Betrachtungswinkel 4 ausgelesen werden. Hierdurch ergibt sich ein Differenzwinkel 5, da einzelne Strukturmerkmale herstellungstechnisch versetzt in dem Wertdokument 1 angeordnet sind.

[0052] Zur Überprüfung der Echtheit eines Sicherheitsdokuments werden Positionen, Winkel oder Abstände von im Inneren des Dokuments 1 dreidimensional angeordnete Merkmale erfasst, um eine Fälschung durch Austausch einzelner Schichten zu erkennen. Durch eine große Auswahl von Merkmalen ist selbst bei Ausfall einiger Merkmale eine sichere Überprüfung der Echtheit möglich. Die Merkmale können bereits in einer Folien-schicht vorhanden sein, z. B. Materialveränderung in ei-

ner Folie, oder bei der Personalisierung erzeugt werden, z. B. Schwärzungen mittels Laser. Die Positionen, Winkel oder Abstände der Merkmale werden auf dem Dokument und ggf. in einem Server gespeichert, während das Dokument personalisiert wird. Zur Prüfung der Echtheit werden die Positionen, Winkel und Abstände der Merkmale ermittelt und mit dem Gespeicherten verglichen.

[0053] Fig. 3 zeigt das erfindungsgemäße Wertdokument 1 mitsamt den Strukturmerkmalen 2. Ferner ist in dem vorliegenden Wertdokument, welches beispielsweise als eine Smartcard vorliegt, eine Toleranzkennzahl 3 bzw. ein Prüfraster 3 vorgesehen. Mittels dieses Prüfrasters lässt sich definieren, wie groß die Abweichungen des Wertdokuments von der Spezifikation sind. Hier wird eine Toleranzkennzahl proportional codiert, welche ein optisches Sicherheitsmerkmal beschreibt.

Patentansprüche

1. Verfahren zum Überprüfen eines Wertdokuments (1) durch eine Verifikation des Wertdokuments (1) mittels eines Vergleichens eines ausgelesenen und eines abgespeicherten optischen Sicherheitsmerkmals (2), **dadurch gekennzeichnet, dass** das Sicherheitsmerkmal (2) auf dem Wertdokument (1) abgespeichert wird, und, dass das Sicherheitsmerkmal (2) aus einem Toleranzbereich eines Herstellungsprozesses des Wertdokuments (1) resultiert.
2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** das Sicherheitsmerkmal (2) auf dem Wertdokument (1) abgespeichert wird.
3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass** das Sicherheitsmerkmal (2) derart abgespeichert wird, dass es optisch auf dem Wertdokument (1) auslesbar ist.
4. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das Sicherheitsmerkmal (2) derart abgespeichert wird, dass es in einen Speicher des Wertdokuments (1) eingeschrieben wird.
5. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** eine positive Verifikation erfolgt, falls das ausgelesene und das abgespeicherte Sicherheitsmerkmal (2) im Wesentlichen übereinstimmen.
6. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** sich der Toleranzbereich auf eine Schichtung, ein Strukturmerkmal, eine Schichtdicke, eine Farbgebung, eine Schwärzung, ein Spaltenmaß, eine Position einer Komponente, einen Winkel zwischen zwei Komponenten und/ oder eine Anordnung von mindestens

einer Komponente bezieht.

7. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das optische Sicherheitsmerkmal (2) ein dreidimensionales Sicherheitsmerkmal (2) darstellt. 5
8. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das ausgelesene optische Merkmal im Inneren des Werdokuments (1) vorliegt. 10
9. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das abgespeicherte optische Sicherheitsmerkmal (2) in Form einer Prüfsumme abgespeichert wird. 15
10. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** das ausgelesene optische Sicherheitsmerkmal (2) in eine Repräsentation übergeführt wird und als Sicherheitsmerkmal (2) abgespeichert wird. 20
11. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** mehrere optische Sicherheitsmerkmale ausgelesen und jeweils auf dem Werdokument (1) zusätzlich hinterlegt werden. 25
12. Werdokument (1) aufweisend ein abgespeichertes Sicherheitsmerkmal, welches einem optischen Sicherheitsmerkmal (2) des Werdokuments (1) entspricht, **dadurch gekennzeichnet, dass** das optische Sicherheitsmerkmal (2) aus einem Toleranzbereich eines Herstellungsprozesses des Werdokuments (1) resultiert. 30
35
13. Prüfungsgerät (4), **dadurch gekennzeichnet, dass** das Prüfungsgerät eingerichtet ist zum Prüfen des Werdokuments (1) nach Anspruch 12. 40
14. Personalisierungsgerät zum Personalisieren eines Werdokuments (1) nach Anspruch 12 mittels eines Abspeicherns des Sicherheitsmerkmals (2). 45
15. Computerprogrammprodukt mit Steuerbefehlen, welche das Verfahren gemäß einem der Ansprüche 1 bis 11 implementieren. 50

50

55

FIG 1

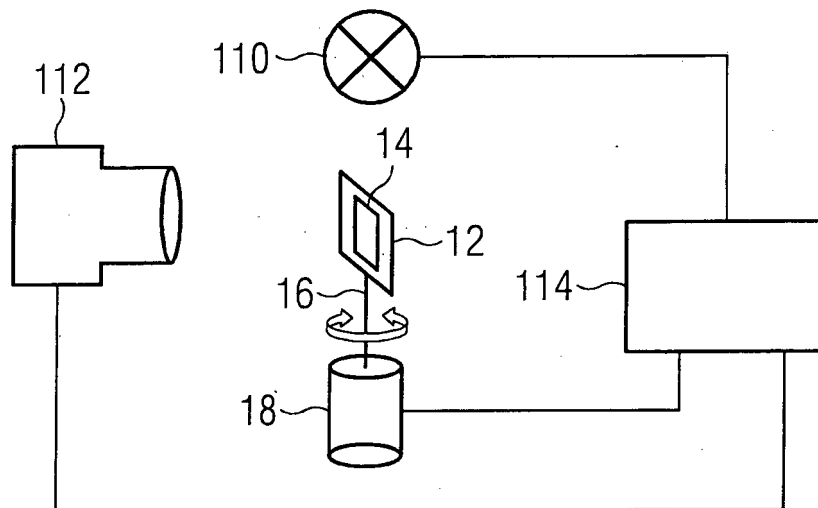


FIG 2

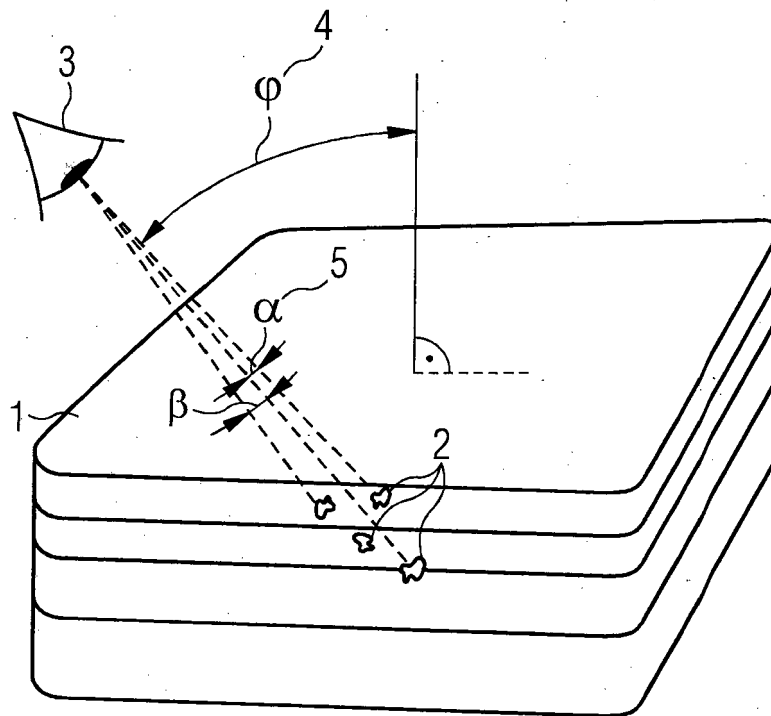
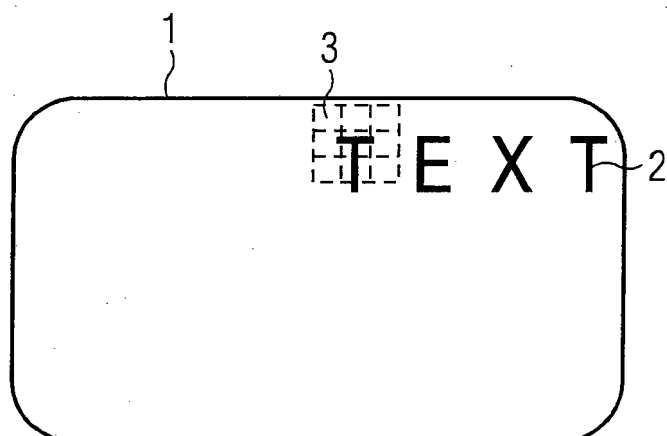


FIG 3





EUROPÄISCHER RECHERCHENBERICHT

 Nummer der Anmeldung
EP 17 00 1285

5

10

15

20

25

30

35

40

45

50

55

EINSCHLÄGIGE DOKUMENTE			
Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
X	WO 2007/087498 A2 (DIGIMARC CORP [US]; RHOADS GEOFFREY B [US]; RODRIGUEZ TONY F [US]; BRA) 2. August 2007 (2007-08-02) * Ansprüche 21,23 *	1-15	INV. B42D25/305
X	WO 2006/053023 A2 (DIGIMARC CORP [US]; RODRIGUEZ TONY F [US]; RHOADS GEOFFREY B [US]; SHA) 18. Mai 2006 (2006-05-18) * Anspruch 21 *	1	
			RECHERCHIERTE SACHGEBIETE (IPC)
			B42D
Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt			
Recherchenort München		Abschlußdatum der Recherche 18. September 2017	Prüfer Langbroek, Arjen
KATEGORIE DER GENANNTEN DOKUMENTE X : von besonderer Bedeutung allein betrachtet Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie A : technologischer Hintergrund O : mündliche Offenbarung P : Zwischenliteratur		T : der Erfindung zugrunde liegende Theorien oder Grundsätze E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist D : in der Anmeldung angeführtes Dokument L : aus anderen Gründen angeführtes Dokument & : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument	

EPO FORM 1503 03.92 (P04C03)

**ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT
 ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR.**

EP 17 00 1285

5 In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
 Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
 Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

18-09-2017

	Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
10	WO 2007087498 A2	02-08-2007	CN 101523408 A	02-09-2009
			EP 1977370 A2	08-10-2008
			EP 2293222 A1	09-03-2011
15			JP 5394071 B2	22-01-2014
			JP 2009524119 A	25-06-2009
			US 2007187505 A1	16-08-2007
			US 2007211920 A1	13-09-2007
			US 2007214406 A1	13-09-2007
20			US 2011311096 A1	22-12-2011
			US 2012074222 A1	29-03-2012
			US 2012163666 A1	28-06-2012
			US 2013290379 A1	31-10-2013
			WO 2007087498 A2	02-08-2007
25	WO 2006053023 A2	18-05-2006	EP 1825419 A2	29-08-2007
			US 2006115110 A1	01-06-2006
			US 2007201720 A1	30-08-2007
			US 2011102143 A1	05-05-2011
			US 2011142280 A1	16-06-2011
30			US 2012074220 A1	29-03-2012
			US 2012126017 A1	24-05-2012
			US 2013172048 A1	04-07-2013
			US 2016189326 A1	30-06-2016
			US 2017103493 A1	13-04-2017
35			WO 2006053023 A2	18-05-2006
40				
45				
50				
55				

EPO FORM P0461

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82

IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

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

In der Beschreibung aufgeführte Patentdokumente

- WO 2008028476 A2 [0002]
- US 20060294583 A1 [0003]
- US 20070025619 A1 [0003]