(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
12. Mai 2016 (12.05.2016)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2016/070872 A1

(51) Internationale Patentklassifikation:
G06F 21/32 (2013.01) *H04W 12/08* (2009.01)
H04L 9/32 (2006.01) *H04W 4/00* (2009.01)
H04L 29/06 (2006.01) *H04W 4/02* (2009.01)

(21) Internationales Aktenzeichen: PCT/DE2015/100469

(22) Internationales Anmeldedatum:
5. November 2015 (05.11.2015)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2014 116 183.1
6. November 2014 (06.11.2014) DE

(71) Anmelder: **BUNDESDRUCKEREI GMBH** [DE/DE]; Kommandantenstraße 18, 10969 Berlin (DE).

(72) Erfinder: **WOLF, Andreas**; Lortzingweg 6, 07743 Jena (DE).

(74) Anwalt: **BOEHMERT & BOEHMERT**; Hollerallee 32, 28209 Bremen (DE).

(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).

[Fortsetzung auf der nächsten Seite]

(54) **Title**: METHOD FOR PROVIDING AN ACCESS CODE IN A PORTABLE DEVICE, AND PORTABLE DEVICE

(54) **Bezeichnung** : VERFAHREN ZUM BEREITSTELLEN EINES ZUGANGSCODES AUF EINEM PORTABLEN GERÄT UND PORTABLES GERÄT

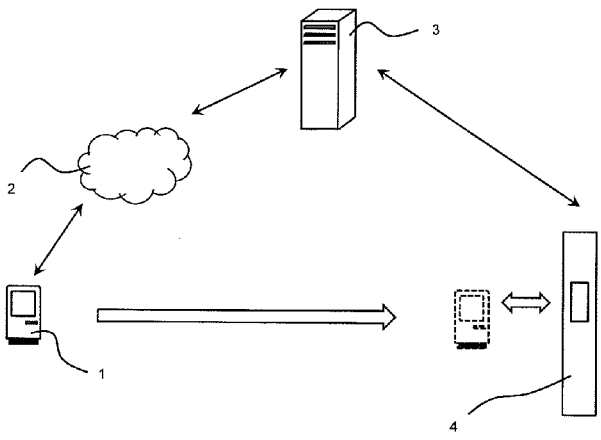

Fig. 1

(57) **Abstract**: The application relates to a method for providing an access code in a portable device (1) that has a user interface and is designed for wireless data communication. In said method, authentication reference data are stored in a central data processing device (3), said reference data comprising person-related data containing biometric reference data for a user of the portable device (1) as well as a device identification for the portable device (1), an authentication process in which the user is authenticated is carried out in reaction to a detected event, the reference data and authentication data, which comprise person-related authentication data for the user, including biometric authentication data, and an authenticating device identification for the portable device (1), being evaluated in the central data processing device (3) and/or in the portable device (1) in order for the user to be authenticated, and in reaction to a successful authentication process, an access code which can be evaluated by an access control device (4) in order to determine whether access is authorized for the user is provided in the portable device (1). The application further relates to a portable device (1) comprising a user interface and a communication module for wireless data communication.

(57) **Zusammenfassung**:

[Fortsetzung auf der nächsten Seite]

WO 2016/070872 A1

Veröffentlicht:

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

— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eingehen (Regel 48 Absatz 2 Buchstabe h)*

Die Anmeldung betrifft ein Verfahren zum Bereitstellen eines Zugangscodes auf einem portablen Gerät (1), welches eine Benutzerschnittstelle aufweist und eingerichtet ist für eine drahtlose Datenkommunikation, bei dem Referenzdaten für eine Authentifizierung in einer zentralen Datenverarbeitungseinrichtung (3) hinterlegt werden, wobei die Referenzdaten personenbezogene Daten, die biometrische Referenzdaten enthalten, für einen Nutzer des portablen Geräts (1) und eine Gerätekennung für das portable Gerät (1) umfassen, als Reaktion auf ein detektiertes Ereignis ein Authentifizierungsprozess ausgeführt wird, bei dem der Nutzer authentifiziert wird, wobei zum Authentifizieren des Nutzers in der zentralen Datenverarbeitungseinrichtung (3) und / oder im portablen Gerät (1) die Referenzdaten und Authentifizierungsdaten ausgewertet werden, welche personenbezogene Authentifizierungsdaten für den Nutzer, einschließlich biometrischer Authentifizierungsdaten, und eine Authentifizierungsgerätekennung für das portable Gerät (1) umfassen, und als Reaktion auf eine erfolgreiche Authentifizierung ein Zugangscode in dem portablen Gerät (1) bereitgestellt wird, welcher zum Bestimmen einer Zugangsberechtigung des Nutzers von einem Zugangskontrollgerät (4) auswertbar ist. Des Weiteren betrifft die Anmeldung ein portables Gerät (1) mit einer Benutzerschnittstelle und einem Kommunikationsmodul für eine drahtlose Datenkommunikation.

Verfahren zum Bereitstellen eines Zugangscodes auf einem portablen Gerät und portables Gerät

Die Erfindung betrifft ein Verfahren zum Bereitstellen eines Zugangscodes auf einem portablem Gerät und ein portables Gerät.

Hintergrund

In Verbindung mit verschiedensten Anwendungen besteht die Notwendigkeit für die Kontrolle des Zugangs von Personen zu einer bestimmten Örtlichkeit, sei es zum Beispiel ein Betriebs- oder Firmengelände oder auch ein Veranstaltungshalle. Bekannte Zugangskontrollsysteme arbeiten zum Beispiel kartenbasiert, was bedeutet, dass berechtigte Personen über eine Karte verfügen, zum Beispiel eine Chipkarte oder einer Karte mit einem Magnetstreifen oder einem aufgedruckten Barcode, die von einem Zugangskontrollgerät ausgewertet werden kann, um die Zugangsberechtigung des Kartennutzers zu prüfen. Auf diese Weise kann eine besitzbasierte Zugangskontrolle zum Beispiel mit einer wissensbasierten Zugangskontrolle kombiniert werden, zum Beispiel einer persönlichen Identifikationsnummer, die auf der Karte oder in einer Datenbank gespeichert ist und deren Eingabe vom Zugangskontrollgerät ausgewertet wird.

Auch ist bekannt, Biometrieverfahren (personenbasierte Kontrolle) einzusetzen. Auf diese Weise sind komplexe Prüfszenearien für die Zugangskontrolle mit Hilfe der Zugangskarte implementierbar.

Die Kontrolle erfolgt bei den verschiedenen Systemen unmittelbar am Zugangskontrollpunkt in geeigneter Form, indem auf der Zugangskarte gespeicherte Informationen ausgelesen werden, beispielsweise mittels Magnetstreifenleser, kontaktbehaftete oder kontaktlose Smartcard, Strichcodeleser oder dergleichen.

Bei den bekannten Zugangskontrollsystemen werden die mit der Zugangskontrolle unmittelbar verbundenen Handlungen durch den Nutzer der Zugangskarte direkt am Kontrollpunkt vollzogen.

Dies kann an Zugangssystemen zu Schlangen und hiermit verbundenen Wartezeiten für die den Zugang begehrenden Personen führen, zum Beispiel zu Stoßzeiten an einem Betriebseingang oder auch am Zugangstor eines Veranstaltungsortes wie einem Stadion oder einer Konzerthalle.

Das Dokument WO 2010/112586 A1 offenbart ein Verfahren zur Zugangskontrolle. Mit einem Mobiltelefon wird ein Identifikationscode an einen Zugangsknoten gesendet. Falls der Identifikationscode als gültig erkannt wird, wird von dem Zugangsknoten ein Zugangscode an das Mobiltelefon gesendet und auf einer Anzeige des Mobiltelefons dargestellt. Mit einer Kamera wird der Zugangscode erfasst und, falls der Zugangscode als gültig erkannt wird, der Zugang gewährt.

Das Dokument US 2013/0262873 A1 offenbart ein Verfahren und ein System zum Authentifizieren von Nutzern. Ein Codeschlüssel wird an ein Mobilgerät eines Nutzers übersandt. Mittels des Codeschlüssels wird eine Kommunikation zwischen dem Mobilgerät und einem Server verschlüsselt. Biometrische Daten des Nutzers werden an den Server übersandt. Der Server bestimmt ein biometrisches Modell des Nutzers zur späteren Authentifizierung. Ein verschlüsseltes biometrisches Modell wird in dem Mobilgerät gespeichert.

Zusammenfassung

Aufgabe der Erfindung ist es, ein Verfahren zum Bereitstellen eines Zugangscodes auf einem portablen Gerät sowie ein portables Gerät anzugeben, die bei Gewährleistung eines hohen Sicherheitsstandards eine einfache und zeitsparende sowie benutzerfreundliche Abwicklung der Zugangskontrolle ermöglichen.

Zur Lösung der Aufgabe ist ein Verfahren zum Bereitstellen eines Zugangscodes auf einem portablem Gerät nach dem unabhängigen Anspruch 1 geschaffen. Der nebengeordnete Anspruch 10 betrifft ein portables Gerät. Ausgestaltungen sind Gegenstand von abhängigen Unteransprüchen.

Nach einem Aspekt ist ein Verfahren zum Bereitstellen eines Zugangscodes auf einem portablen Gerät geschaffen, welches eine Benutzerschnittstelle aufweist und für eine drahtlose Datenkom-

munikation eingerichtet ist. Über die Benutzerschnittstelle ist des dem Nutzer des portablen Geräts insbesondere ermöglicht, Daten einzugeben. Die Benutzerschnittstelle kann eine Tastatur und / oder einen Touchscreen umfassen. Bei dem portablen Gerät kann es sich zum Beispiel um ein Mobilfunktelefon, einen Tabletcomputer oder einen portablen Personalcomputer handeln. Bei dem Verfahren zum Bereitstellen des Zugangscodes werden Referenzdaten für eine Authentifizierung in einer zentralen Datenverarbeitungseinrichtung hinterlegt. Eine Datenkommunikation zwischen dem portablen Gerät und der zentralen Datenverarbeitungseinrichtung ist unter Einbeziehung einer drahtlosen Datenkommunikation ermöglicht, zum Beispiel über ein Mobilfunknetz. Die in der zentralen Datenverarbeitungseinrichtung hinterlegten Referenzdaten umfassen personenbezogene Daten, die biometrische Referenzdaten enthalten, für einen Nutzer des portablen Geräts sowie eine Gerätekennung für das portable Gerät. Bei dem Verfahren wird als Reaktion auf ein detektiertes Ereignis ein Authentifizierungsprozess gestartet, bei dem der Nutzer authentifiziert wird. Hierbei werden zur Nutzerauthentifizierung in der zentralen Datenverarbeitungseinrichtung und / oder im portablen Gerät die Referenzdaten und Authentifizierungsdaten ausgewertet. Das Auswerten kann einen Vergleich von Referenzdaten und Authentifizierungsdaten umfassen. Die Authentifizierungsdaten enthalten personenbezogene Authentifizierungsdaten für den Nutzer, einschließlich biometrischer Authentifizierungsdaten, sowie eine Authentifzierungsgerätekennung für das portable Gerät. Als Reaktion auf die erfolgreiche Authentifizierung des Nutzers wird in dem portablen Gerät ein Zugangscode bereitgestellt, welcher zum Bestimmen einer Zugangsberechtigung des Nutzers von einem Zugangskontrollgerät auswertbar ist, wenn der Nutzer Zugang begehrt.

Nach einem weiteren Aspekt ist ein portables Gerät mit einer Benutzerschnittstelle und einem Kommunikationsmodul für eine drahtlose Datenkommunikation geschaffen, welches mittels einer auf dem portablen Gerät installierten Software-Applikation zur Verwendung bei dem Verfahren zum Bereitstellen des Zugangscodes eingerichtet ist.

Zum Übertragen oder Austauschen von elektronischen Daten bei dem Verfahren kann zwischen dem mobilen Gerät und der zentralen Datenverarbeitungseinrichtung ein gesicherter Datenkanal für eine gewünschte Zeit ausgebildet werden. Ein solcher gesicherter Datenkanal kann in Abhän-

gigkeit von dem Sicherheitsstandard des Zugangskontrollsystems für eine sichere Datenkommunikation zwischen dem portablen Gerät und der zentralen Datenverarbeitungseinrichtung genutzt werden.

Handelt es sich bei dem portablen Gerät zum Beispiel um ein Mobilfunktelefon, ist als Gerätekennung beispielsweise die sogenannte IMEI-Nummer für das Verfahren nutzbar (IMEI - International Mobile Equipment Identity). Eine ein Gerät in einem Netzwerksystem individualisierende Gerätekennung kann im Netzwerk übergreifend oder auch nur lokal in einem Teil des Netzwerks gültig sein.

Zum Bereitstellen auf dem portablen Gerät kann der Zugangscode im portablen Gerät selbst und / oder in der zentralen Datenverarbeitungseinrichtung erzeugt werden. Im Fall des Erzeugens in der zentralen Datenverarbeitungseinrichtung wird der Zugangscode dann an das portable Gerät übertragen und dort in der übertragenen Form oder in geänderter Form bereitgestellt, zum Beispiel zum Ausgeben über ein Display.

Die Einbeziehung biometrischer Daten zur Personenidentifikation ermöglicht eine personalisierte Zugangskontrolle mit hohem Sicherheitsstandard.

Das Authentifizieren des Nutzers und das Bereitstellen des Zugangscodes auf dem portablen Gerät erfolgen, bevor der Nutzer den Ort des Zugangskontrollgeräts erreicht, so dass der Nutzer vorbereitet ist, beim Erreichen des Zugangskontrollortes den Zugangscode auf dem portablen Gerät unmittelbar und ohne zeitliche Verzögerung dem Zugangskontrollgerät zu präsentieren. Auf diese Weise können zum Beispiel Wartezeiten für Zugang begehrende Personen an einem Zugangskontrollgerät vermieden werden.

Der Authentifizierungsprozess kann mittels einer auf dem portablen Gerät laufenden Applikation gestartet werden, wenn mindestens ein Ereignis aus der folgenden Gruppe von Ereignissen detektiert wird: Erreichen eines vorbestimmten Orts und Erreichen einer Zeitvorgabe. Die auf dem portablen Gerät laufende Applikation kann als Softwaremodul ausgeführt sein, welches auf das

portable Gerät heruntergeladen und hier installiert wurde. Wird von der Applikation eines der auslösenden Ereignisse detektiert, kann der Authentifizierungsprozess gleich oder zeitlich versetzt zum Detektieren des Ereignisses gestartet werden. Es kann vorgesehen sein, dass die Applikation eine Bestätigung vom Nutzer des portablen Geräts erfasst und erst danach den Authentifizierungsprozess initiiert. Mit Hilfe der Applikation kann der Nutzer zum Beispiel eine Stadt oder ein Betriebsgelände als vorbestimmten Ort festlegen, so dass der Authentifizierungsprozess gestartet werden kann, wenn das portable Gerät die Stadt oder das Betriebsgelände erreicht oder in einen vorgegebenen Umkreis hierzu eintritt. Es kann vorgesehen sein, dass mit Hilfe des portablen Geräts Signale detektiert werden, die lediglich im Umkreis des Ortes, für den die Zugangskontrolle ausgeführt wird, zu empfangen sind. Eine solche Selektion von Signalen kann beispielsweise mittels Nutzung ausgewählter Frequenzbereiche und / oder beschränkter Reichweite der gesendeten Signale erreicht werden. In Verbindung mit dem Erreichen einer Zeitvorgabe kann es sich beispielsweise um einen Tag oder eine Tageszeit handeln, deren Erreichen mit einem Zeitmodul des portablen Geräts überprüft und detektiert wird. Die Applikation kann auch als Reaktion auf optische Sichtbarkeit von Signalen starten, zum Beispiel nach dem Aufnehmen eines bestimmten QR-Codes von einer Hauswand, beispielweise mittels der Kamera des Mobilfunktelefons. In diesem Fall kann der Authentifizierungsprozess als Reaktion auf eine Benutzeraktion am portablen Gerät starten.

Zum Bestimmen des Erreichens des vorbestimmten Orts können elektronische Informationen einer Lokalisierungseinrichtung des portablen Geräts ausgewertet werden. Zum Beispiel kann das portable Gerät ein GPS-Modul (GPS – Global Positioning System) aufweisen, so dass hiermit eine Bestimmung des momentanen Aufenthaltsorts des portablen Geräts ermöglicht ist. Diese elektronische Information kann dann von der auf dem portablen Gerät laufenden Applikation genutzt werden, um zu bestimmen, ob der Authentifizierungsprozess gestartet werden soll.

Die personenbezogenen Authentifizierungsdaten können für den Nutzer, einschließlich der biometrischen Authentifizierungsdaten, wenigstens teilweise mittels eines oder mehrerer Funktionsmodule des portablen Geräts erfasst werden. In den verschiedenen Ausgestaltungen können die biometrischen Referenzdaten wie auch die biometrischen Authentifizierungsdaten eine oder

mehreren Arten von biometrischen Daten und / oder hieraus abgeleiteten Informationen umfassen, zum Beispiel Fingerabdruck, Irisbild und / oder Gesichtsbild. Auch eine Unterschriftenerkennung und / oder ein Doodle-Malen kann einbezogen werden. Auch eine Sprachprobe kann alternativ oder ergänzend für die Authentifizierung herangezogen werden. Die biometrischen Daten können teilweise oder ausschließlich mittels des portablen Geräts erfasst werden, welches zu diesem Zweck über entsprechende Funktionsmodule verfügt, zum Beispiel einen Fingerabdrucksensor, eine Kamera und / oder ein berührungsempfindliches Display.

Der Zugangscode kann über eine Ausgabeeinrichtung des portablen Geräts ausgegeben werden. Es kann vorgesehen sein, dass der Zugangscode, zum Beispiel ein Strichcode oder ein QR- oder anderer 2D-Barcode, über eine Anzeigeeinrichtung des portablen Geräts ausgegeben wird. Auch kann der Zugangscode alternativ oder ergänzend auf einem Speicherbaustein des portablen Geräts gespeichert sein, derart, dass insbesondere ein kontaktloses Auslesen mit Hilfe eines zugeordneten Lesegeräts des Zugangskontrollsystems ermöglicht ist. Hierfür kann zum Beispiel die RFID-Technologie (RFID – Radio Frequency Identification) genutzt werden. Das Ausgeben ermöglicht allgemein eine Präsentation des nach erfolgreicher Authentifizierung bereitgestellten Zugangscodes gegenüber dem Zugangskontrollgerät.

Der Zugangscode kann dem Zugangskontrollgerät mittels NFC-Kommunikation (NFC – Near Field Communication) präsentiert werden.

Der Zugangscode kann als ein Zugangscode zeitlich begrenzter Gültigkeitsdauer bereitgestellt werden. Die zeitliche Begrenzung der Gültigkeitsdauer kann zum Beispiel darin bestehen, dass der in dem portablen Gerät bereitgestellte Zugangscode nach einem vorbestimmten Zeitraum ungültig wird. Auch kann vorgesehen sein, dass der Zugangscode erst zu einem Zeitpunkt gültig wird, der zeitlich beabstandet zur Bereitstellung in der Zukunft liegt. Es kann vorgesehen sein, dass nach Ablauf der Gültigkeitsdauer der Zugangscode durch die Applikation auf dem portablen Gerät automatisch gelöscht oder ungültig gemacht wird.

Der Zugangscode kann als ein örtlich begrenzter Zugangscode bereitgestellt werden, welcher seine Gültigkeit verliert, wenn festgestellt wird, insbesondere durch die Applikation auf dem portablen Gerät, dass das portable Gerät nach dem Bereitstellen des Zugangscodes einen vorgegebenen Ortsbereich verlässt. Verlässt beispielsweise das portable Gerät nach dem Bereitstellen des Zugangscodes einen vorgegebenen Ortsbereich, zum Beispiel eine Stadt, einen Stadtteil oder ein Betriebsgelände, so kann die Applikation eingerichtet sein, beim Feststellen dieses Ereignisses den bereitgestellten Zugangscode nachträglich zu löschen oder anders ungültig zu machen. Hierbei kann zum Beispiel die Ortsinformation eines GPS-Moduls des portablen Geräts ausgewertet werden.

Ein Teil der biometrischen Authentifizierungsdaten kann mittels einer Sensoreinrichtung vor Ort am Zugangskontrollgerät erfasst werden. Ein bereits vorher begonnener und noch nicht abgeschlossener Authentifizierungsprozess kann mittels derart erfasster biometrischer Daten vervollständigt und abgeschlossen werden. Auch bei dieser Ausführungsform wird der Authentifizierungsprozess gestartet, bevor das portable Gerät den Ort des Zugangskontrollgeräts erreicht. Im Fall erhöhter Sicherheitsbedürfnisse kann mit dieser Ausgestaltung eine erweiterte Datenerfassung und Auswertung vorgesehen sein.

Beschreibung von Ausführungsbeispielen

Nachfolgend werden weitere Ausführungsbeispiele unter Bezugnahme auf Figuren einer Zeichnung näher erläutert. Hierbei zeigen:

Fig. 1 eine schematische Darstellung zur Zugangskontrolle und

Fig. 2 ein Ablaufdiagramm zu einem Verfahren zum Bereitstellen eines Zugangscodes auf einem portablen Gerät.

Fig. 1 zeigt eine schematische Darstellung in Verbindung mit einer Zugangskontrolle. Einem Nutzer ist ein portables Gerät 1 zur Verfügung gestellt, welches über ein drahtloses Kommunikationsnetzwerk 2, zum Beispiel ein Mobilfunknetzwerk, elektronischen Daten mit einer zentralen Datenverarbeitungseinrichtung 3 austauschen kann, die zum Beispiel mit einem Server gebildet

ist. Die zentrale Datenverarbeitungseinrichtung 3 ist Teil eines Zugangskontrollsystems, zum Beispiel in Verbindung mit einem Betriebsgelände oder einer Sport- oder Veranstaltungsarena.

Auf dem portablen Gerät 1 wird dem Nutzer ein Zugangscode bereitgestellt, den der Nutzer dann gegenüber einem Zugangskontrollgerät 4 präsentieren kann, wenn der Nutzer mit dem portablen Gerät 1 an den Ort des Zugangskontrollgeräts 4 gelangt. Das Verfahren zum Bereitstellen des Zugangscodes wird bei dem gezeigten Ausführungsbeispiel an einem hiervon entfernten Ort schon gestartet, so dass der Zugangscode auf dem portablen Gerät 1 zur Verfügung steht, wenn der Nutzer mit dem portablen Gerät 1 an das Zugangskontrollgerät 4 gelangt.

Nachfolgend werden weitere Aspekte des Verfahrens zum Bereitstellen des Zugangscodes auf dem portablen Gerät 1 unter Bezugnahme auf das Ablaufdiagramm in Fig. 2 erläutert.

Das protable Gerät 1 kann ein netzfähiges IT-Gerät sein, das ein Benutzer aus anderem Grund schon besitzt (BYOD - Bring Your Own Device), zum Beispiel ein Mobilfunktelefon, insbesondere ein sogenantes Smartphone. Auf dem portablen Gerät 1 läuft eine Anwendung (Software-Applikation), die drahtlos über das Kommunikationsnetzwerk 2 mit der zentralen Datenverarbeitungseinrichtung 3 Kontakt aufnehmen und mit dieser Daten austauschen kann. Diese Anwendung wird vorab verteilt, sie kann etwa im Internet oder zum Download zur Verfügung stehen. Außerdem ist ein Smartphone regelmäßig personengebunden, und sein Besitz kann bereits als ein Authentifizierungsfaktor verwendet werden.

Nach Installation der Anwendung auf dem portablen Gerät 1 registriert sich der Benutzer bei der zentralen Datenverarbeitungseinrichtung 3 (Schritt 10 in Fig. 1). Hierbei können elektronische Schlüssel zur Absicherung der Kommunikation ausgetauscht, benötigte Personendaten und die IMEI des IT-Geräts registriert werden. Abhängig vom gewünschten Sicherheitsniveau werden die für das verwendete Authentifizierungsverfahren erforderlichen Referenzdaten über das portable Gerät 1 oder auch in der zentralen Datenverarbeitungseinrichtung 3 erfasst. So können zum Beispiel Gesichtsbilddaten für eine Gesichtserkennung etwa durch den Benutzer live erfasst und dann qualitätsgesichert abgespeichert werden. Diese Daten können beispielweise auch vom

Reisepass des Nutzers erfasst werden, oder elektronische Bilder sind in einer Mitarbeiter-Datenbank schon vorhanden.

Begehrt jemand Zugang zu einer durch ein Zugangskontrollsystem gesicherten Umgebung, oder ist bekannt / steht zu vermuten, dass er dieses in Kürze tun will, wird ein Authentifizierungsprozess durch die Anwendung auf dem portablen Gerät 1 gestartet. Vor dem Auslösen des Authentifizierungsprozesses wird ein Ereignis erfasst oder detektiert (Schritt 20).

Beim Authentifizierungsprozess wird eine sogenannte Challenge angefordert oder unaufgefordert auf das portable Gerät 1 geschickt (Schritt 30). So könnte ein Betriebsmitarbeiter eine derartige Challenge jeden Morgen auf sein portables Gerät 1 gesendet bekommen. Alternativ könnte die Challenge (etwa bei Besuchern) in einer Besucherzentrale übergeben werden, beispielsweise per 3D-Barcode.

Die Challenge kann personen- und / oder zeitgebunden sein, also nur für einen bestimmten Benutzer und nur für einen bestimmten Zeitraum gültig sein. Wird der Personenbezug weggelassen, was zu einer Einschränkung der Sicherheitsfunktion führen wird, aber für manche Anwendungen tolerierbar ist, kann die Challenge zeitabhängig (und nicht personenabhängig) im Vorfeld des Zugangskontrollpunktes verfügbar sein und durch das portable Gerät 1 automatisch bestimmt werden. Hierbei können zum Beispiel elektronische Signale eines GPS-Sensors im portablen Gerät 1 und / oder Zeitinfomationen ausgewertet werden. Auch könnte der Nutzer des portablen Geräts 1 durch die hierauf laufende Anwendung veranlasst werden, einen Barcode (QR, Datamatrix, Aztec, etc.) zu scannen.

Die Challenge liegt bereits vor dem Eintreffen des Benutzers am Zugangskontrollgerät 4 auf dem portablen Gerät 1 vor. Ein QR-Code kann etwa bereits vor dem Erreichen des Kontrollpunktes gescannt werden, wenn er groß genug an irgendeiner Wand oder auf anmutig im Gelände verteilten Displays angezeigt wird.

Liegt die Challenge vor, bittet die Anwendung auf dem portablen Gerät 1 den Benutzer um Durchführen der Authentifizierung. Zu diesem Zweck bringt der Benutzer Authentifizierungsdaten bei (Schritt 40). Der Benutzer erfasst zum Beispiel ein Bild seines Gesichtes, einen Fingerabdruck, eine Sprachprobe und / oder andere biometrische Daten wie Unterschrift oder Doodle-Malen. Oder er gibt ein Geheimnis ein, etwa eine Passphrase. Oder er legt eine NFC-Karte an das portable Gerät 1. Möglich sind auch Kombinationen dieser Faktoren. Das portable Gerät 1 stellt einen sicheren Übertragungskanal zur zentralen Datenverarbeitungseinrichtung 3 her (Schritt 50) und übermittelt an diese eine anhand der Challenge und charakteristischer Daten des portablen Geräts 1 wie etwa der IMEI des portablen Geräts 1 ermittelte Antwort (Response, Schritt 60). Außerdem übermittelt das protbale Gerät 1 die vorher für die Authentifikation erhobenen Authentifizierungsdaten, im Falle biometrischer Verfahren zum Beipiel auch hieraus extrahierten Merkmalsdaten.

Es ist möglich, die Verifikation auf dem portabelen Gerät 1 und / oder in der zentralen Datenverarbeitungseinrichtung 3 durchzuführen, insbesondere abhängig vom zu erreichenden Sicherheitsniveau. Bei Scheitern einer biometrischen Verifikation kann diese wiederholt werden.

Nach erfolgreicher Prüfung der Antwort und der übertragenen Authentifizierungsdaten versendet die zentralen Datenverarbeitungseinrichtung 3 an das portable Gerät 1 einen Zugangscode (Schritt 70), der vorzugsweise eine bestimmte Zeit gültig ist, zum Beispiel einen Tag.

Am Kontrollpunkt ist nur noch die Prüfung dieses Zugangscodes durch das Zugangskontrollgerät 4 erforderlich, die etwa durch Präsentation eines 2D-Barcodes gegenüber dem Zugangskontrollgerät 4 erfolgt. Auch Präsentation per NFC ist möglich.

Die Sicherheitseigenschaften eines derartigen Prozesses und seiner Implementierung lassen sich entsprechend den anwendungsbezogenen Erfordernissen skalieren. Die eigentliche Prüfung am Kontrollpunkt ist nur noch das Auswerten des Zugangscodes, etwa eines Bar- oder Strichcodes. Auch bei Ergänzung des Systems durch weitere Authentifikationsverfahren sind am Kontrollpunkt keine Hardware-Änderungen erforderlich.

Ist das System anfänglich nur an das portabele Gerät 1, insbesondere ein Mobiltelefon, bzw. den Besitz desselben gebunden, kann in einer Ausführung der zugangsberechtigende Code, beispielsweise ein Strichcode, übermittelt werden, sobald die Challenge vom richtigen portabelen Gerät 1 beantwortet wird. Dieser Code wird am Zugangskontrollpunkt präsentiert. Später entschließt man sich, zusätzlich Gesichtserkennung einzusetzen. Jetzt gehört zur Beantwortung der Challenge auch noch die Übermittlung von Biometriedaten (Bild oder Merkmalsvektor). Am Zugangskontrollpunkt selbst ist nach wie vor nur die Präsentation des Codes erforderlich. Später nachgerüstete weitere Sensorik und / oder Hardwaretoken (etwa eine NFC-Karte oder ähnlich) erfordern also am Zugangskontrollpunkt selbst keine Änderungen mehr.

Ist ein Bereich mit spezifischen Sicherheitsanforderungen abzusichern, für die die Sensorik nicht sinnvoll in einem mobilen Gerät integriert werden kann oder dies aus Sicherheitserwägungen (Manipulationsschutz) nicht geraten erscheint, können an der Zugangskontrollstelle zusätzliche Geräte installiert werden, zum Beispiel ein Iris- oder ein Handvenensensor. Für die auf diesen Geräten durchzuführenden Authentifikationsschemata liefert der Zutrittscode zumindest eine behauptete Idendität („claimed ID“) des Benutzers, so dass auch hier keine spezifischen Token ausgegeben werden müssen und das System trotzdem im Verifikationsmodus läuft (1:1-Suche in der Datenbank anhand der behaupteten Identität) und keine Identifikation (1:N-Suche) erforderlich ist.

Der zeitintensive interaktive Teil eines Kontrollvorganges, bei dem es am Zugangskontrollgerät 4 zur Schlangenbildung kommen kann, wird auf ein Minimum reduziert oder ganz ausgeschlossen. Damit ist ein hoher Durchsatz mit wenigen Kontrollpunkten bei Beibehaltung des geforderten Sicherheitsniveaus möglich. Der Kontrollprozess wird entzerrt, große Teile können vom Benutzer bereits vorab erledigt werden. Es ist nicht erforderlich, ein physisches Credential auszugeben, was verloren gehen kann. Optional kann eine Personenbindung erfolgen, etwa per Gesichtserkennung, ohne dass dafür am Kontrollpunkt zusätzliche Kameras oder andere Hardware erforderlich wären. Generell ist das erreichbare Sicherheitsniveau weitgehend skalierbar.

Die in der vorstehenden Beschreibung, den Ansprüchen sowie der Zeichnung offenbarten Merkmale können sowohl einzeln als auch in beliebiger Kombination für die Verwirklichung der verschiedenen Ausführungen von Bedeutung sein.

Ansprüche

1. Verfahren zum Bereitstellen eines Zugangscodes auf einem portablen Gerät (1), welches eine Benutzerschnittstelle aufweist und eingerichtet ist für eine drahtlose Datenkommunikation, bei dem
   - Referenzdaten für eine Authentifizierung in einer zentralen Datenverarbeitungseinrichtung (3) hinterlegt werden, wobei die Referenzdaten personenbezogene Daten, die biometrische Referenzdaten enthalten, für einen Nutzer des portablen Geräts (1) und eine Gerätekennung für das portable Gerät (1) umfassen,
   - als Reaktion auf ein detektiertes Ereignis ein Authentifizierungsprozess ausgeführt wird, bei dem der Nutzer authentifiziert wird, wobei zum Authentifizieren des Nutzers in der zentralen Datenverarbeitungseinrichtung (3) und / oder im portablen Gerät (1) die Referenzdaten und Authentifizierungsdaten ausgewertet werden, welche personenbezogene Authentifizierungsdaten für den Nutzer, einschließlich biometrischer Authentifizierungsdaten, und eine Authentifizierungsgerätekennung für das portable Gerät (1) umfassen, und
   - als Reaktion auf eine erfolgreiche Authentifizierung ein Zugangscode in dem portablen Gerät (1) bereitgestellt wird, welcher zum Bestimmen einer Zugangsberechtigung des Nutzers von einem Zugangskontrollgerät (4) auswertbar ist.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Authentifizierungsprozess mittels einer auf dem portablen Gerät (1) laufenden Applikation gestartet wird, wenn mindestens eine Ereignis aus der folgenden Gruppe von Ereignissen detektiert wird: Erreichen eines vorbestimmten Orts und Erreichen einer Zeitvorgabe.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass zum Bestimmen des Erreichens des vorbestimmten Orts elektronische Informationen einer Lokalisierungseinrichtung des portablen Geräts (1) ausgewertet werden.

4. Verfahren nach mindestens einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass die personenbezogenen Authentifizierungsdaten für den Nutzer, ein-

schließlich die biometrischen Authentifizierungsdaten, wenigstens teilweise mittels eines oder mehrerer Funktionsmodule des portablen Geräts (1) erfasst werden.

5. Verfahren nach mindestens einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass der Zugangscode über eine Ausgabeeinrichtung des portablen Gerätes (1) ausgegeben wird.

6. Verfahren nach mindestens einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass der Zugangscode dem Zugangskontrollgerät (4) mittels NFC-Kommunikation präsentiert wird.

7. Verfahren nach mindestens einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass der Zugangscode als ein Zugangscode zeitlich begrenzter Gültigkeitsdauer bereitgestellt wird.

8. Verfahren nach mindestens einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass der Zugangscode als ein örtlich begrenzter Zugangscode bereitgestellt wird, welcher seine Gültigkeit verliert, wenn festgestellt wird, dass das portable Geräte (1) nach dem Bereitstellen des Zugangscodes einen vorgegebenen Ortsbereich verlässt.

9. Verfahren nach mindestens einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass ein Teil der biometrischen Authentifizierungsdaten mittels einer Sensoreinrichtung vor Ort am Zugangskontrollgerät (4) erfasst wird.

10. Portables Gerät (1) mit einer Benutzerschnittstelle und einem Kommunikationsmodul für eine drahtlose Datenkommunikation, welches mittels einer installierten Applikation eingerichtet ist zur Verwendung in einem Verfahren nach mindestens einem der vorangehenden Ansprüche.

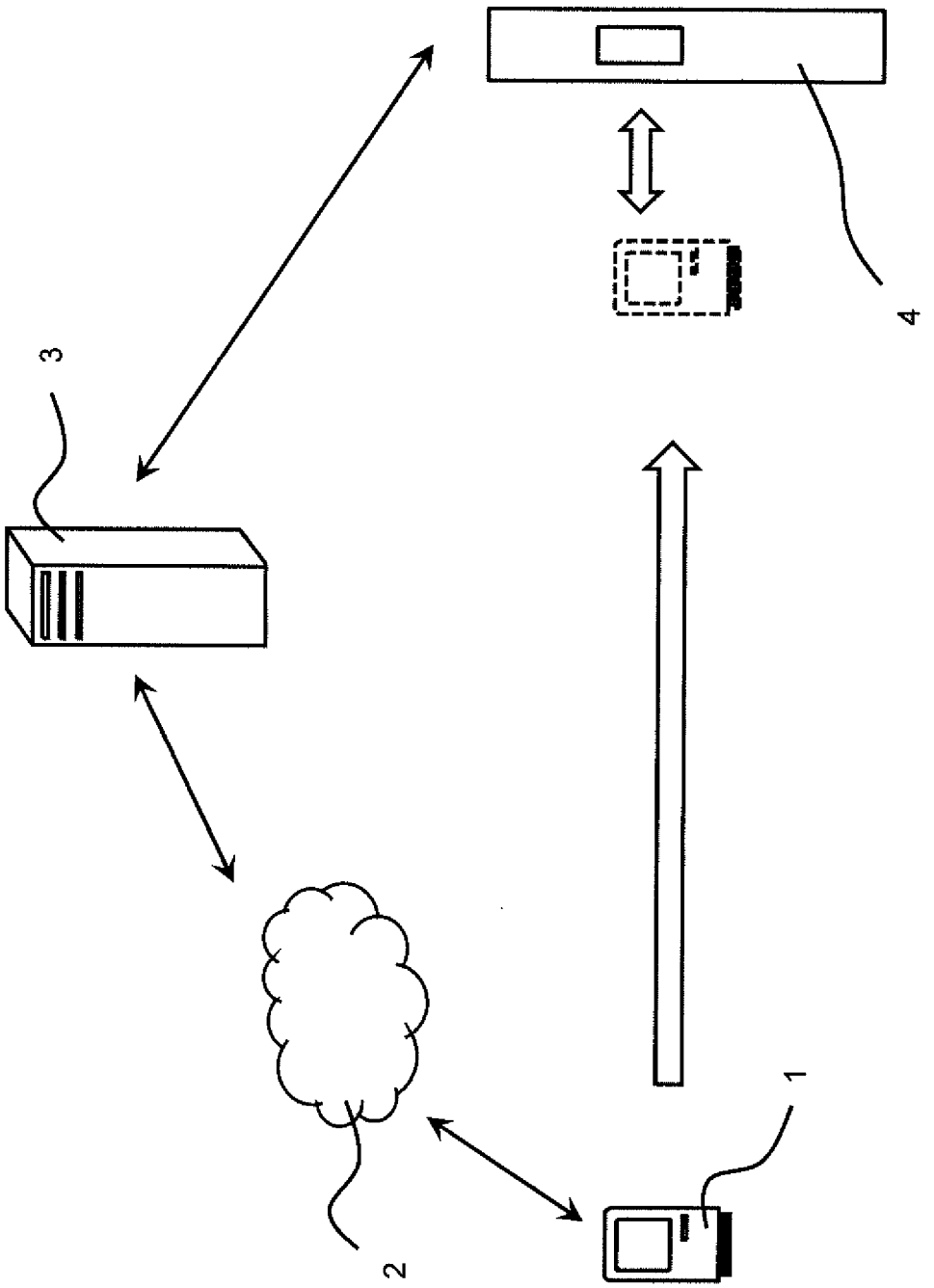

Fig. 1

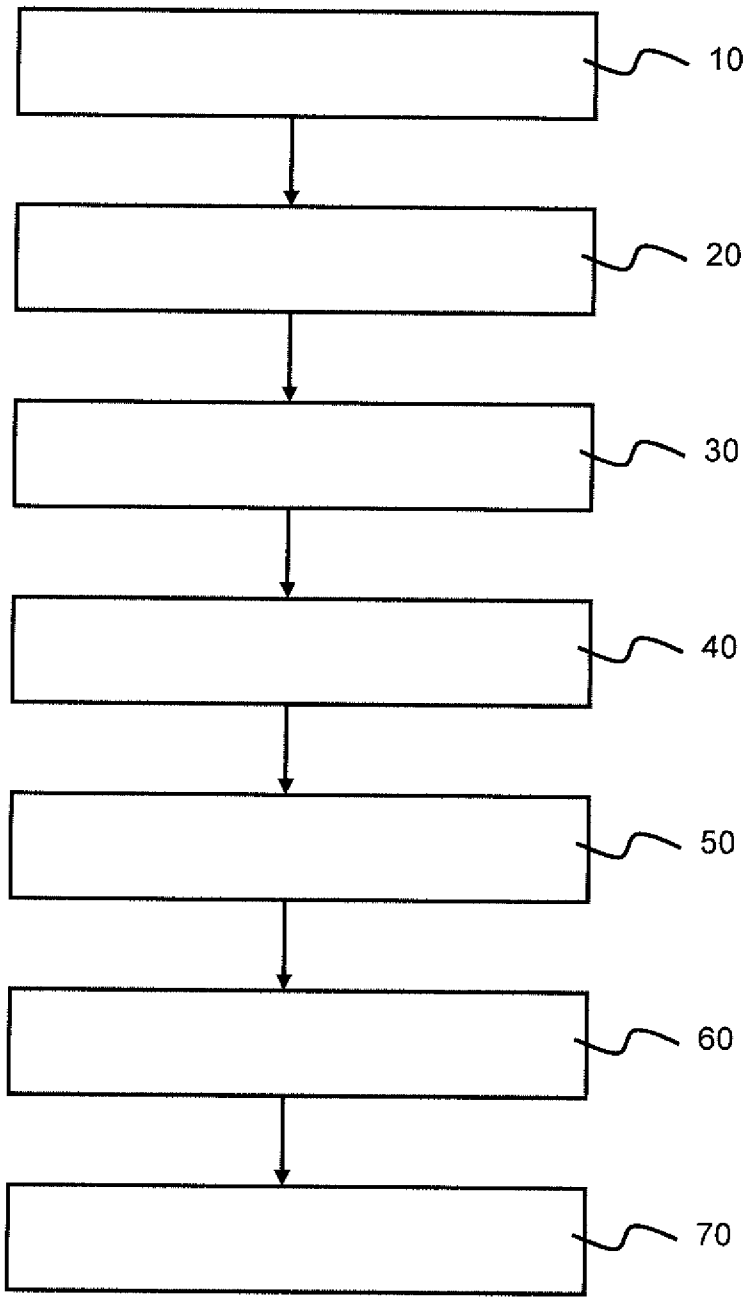

Fig. 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/DE2015/100469

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/32 H04L9/32 H04L29/06 H04W12/08 H04W4/00 H04W4/02
ADD.
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)
G06F H04L H04W

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, COMPENDEX, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2012/169461 A1 (DUBOIS JR RICHARD L [US]) 5 July 2012 (2012-07-05) abstract; figures 2,4,5 paragraph [0030] - paragraph [0042] paragraph [0045] - paragraph [0051] -----	1-10
X	US 2011/205016 A1 (AL-AZEM SAMER [US] ET AL) 25 August 2011 (2011-08-25) abstract paragraph [0009] - paragraph [0013] paragraph [0022] - paragraph [0028] paragraph [0031] - paragraph [0052] -----	1-10

-/--

[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
17 March 2016	29/03/2016

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	Kraska, Nora

1

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

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GB 2 417 858 A (BAJWA ANWAR SHARIF [GB]; SALEH ROBERT NAIM [GB]) 8 March 2006 (2006-03-08) abstract paragraph [0008] - paragraph [0016] paragraph [0021] -----	1-10
A	DE 10 2005 059001 A1 (ARENDT HANS-HENNING [DE]; PHENG LEE KONG [MY]) 14 June 2007 (2007-06-14) paragraph [0013] - paragraph [0022] paragraph [0079] - paragraph [0088] -----	1-10

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/DE2015/100469

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2012169461 A1	05-07-2012	CN 103404121 A	20-11-2013
		EP 2659661 A1	06-11-2013
		US 2012169461 A1	05-07-2012
		WO 2012091888 A1	05-07-2012
US 2011205016 A1	25-08-2011	NONE	
GB 2417858 A	08-03-2006	NONE	
DE 102005059001 A1	14-06-2007	DE 102005059001 A1	14-06-2007
		WO 2007065809 A2	14-06-2007

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE2015/100469

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G06F21/32 H04L9/32 H04L29/06 H04W12/08 H04W4/00
H04W4/02
ADD.
Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G06F H04L H04W

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, COMPENDEX, INSPEC, IBM-TDB

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2012/169461 A1 (DUBOIS JR RICHARD L [US]) 5. Juli 2012 (2012-07-05) Zusammenfassung; Abbildungen 2,4,5 Absatz [0030] - Absatz [0042] Absatz [0045] - Absatz [0051] -----	1-10
X	US 2011/205016 A1 (AL-AZEM SAMER [US] ET AL) 25. August 2011 (2011-08-25) Zusammenfassung Absatz [0009] - Absatz [0013] Absatz [0022] - Absatz [0028] Absatz [0031] - Absatz [0052] ----- -/--	1-10

[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
17. März 2016	29/03/2016

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	Kraska, Nora

1

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	GB 2 417 858 A (BAJWA ANWAR SHARIF [GB]; SALEH ROBERT NAIM [GB]) 8. März 2006 (2006-03-08) Zusammenfassung Absatz [0008] - Absatz [0016] Absatz [0021] -----	1-10
A	DE 10 2005 059001 A1 (ARENDT HANS-HENNING [DE]; PHENG LEE KONG [MY]) 14. Juni 2007 (2007-06-14) Absatz [0013] - Absatz [0022] Absatz [0079] - Absatz [0088] -----	1-10

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/DE2015/100469

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2012169461 A1	05-07-2012	CN 103404121 A	20-11-2013
		EP 2659661 A1	06-11-2013
		US 2012169461 A1	05-07-2012
		WO 2012091888 A1	05-07-2012
US 2011205016 A1	25-08-2011	KEINE	
GB 2417858 A	08-03-2006	KEINE	
DE 102005059001 A1	14-06-2007	DE 102005059001 A1	14-06-2007
		WO 2007065809 A2	14-06-2007