(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
11. Februar 2016 (11.02.2016)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2016/020202 A1

(51) Internationale Patentklassifikation:
G06F 19/00 (2011.01)

(21) Internationales Aktenzeichen: PCT/EP2015/066875

(22) Internationales Anmeldedatum:
23. Juli 2015 (23.07.2015)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2014 215 806.0
8. August 2014 (08.08.2014) DE

(72) Erfinder; und
(71) Anmelder : **LEMBERGER, Matthias** [DE/DE]; Schwarzhölzlstr. 1, 93474 Arrach (DE).

(74) Anwälte: **GASSNER, Wolfgang** et al.; Marie-Curie-Str. 1, 91052 Erlangen (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).

Veröffentlicht:

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

WO 2016/020202 A1

(54) Title: METHOD FOR UPLOADING AND RESPECTIVELY DOWNLOADING AT LEAST ONE FILE CONTAINING DATA REQUIRING PROTECTION CONCERNING THE STATE OF HEALTH OF A PATIENT WITHIN A NETWORKED COMPUTER SYSTEM

(54) Bezeichnung : VERFAHREN ZUM HOCHLADEN BZW. HERUNTERLADEN ZUMINDEST EINER SCHUTZBEDÜRFTIGE DATEN ZUM GESUNDHEITSZUSTAND EINES PATIENTEN ENTHALTENDEN DATEI INNERHALB EINES VERNETZTEN COMPUTERSYSTEMS

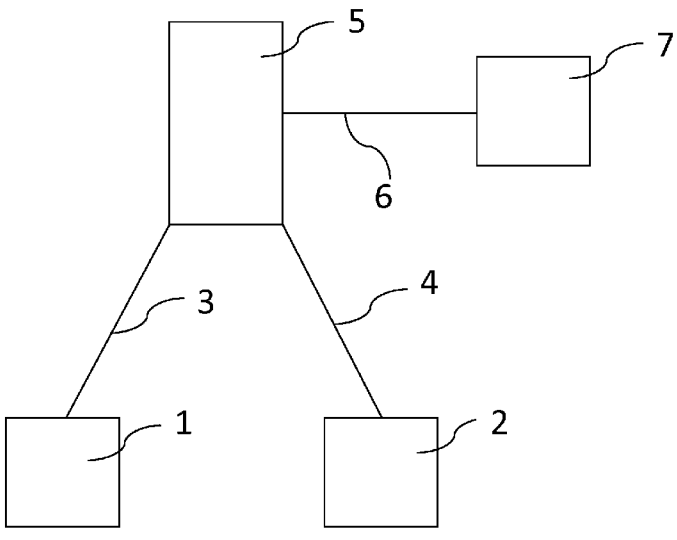

Fig. 1

(57) Abstract: The invention relates to a method for uploading and a method for downloading at least one file containing data requiring protection concerning the state of health of a patient within a networked computer system, comprising a mobile first computer (1), a second computer (2) and a central server system (5). The mobile first computer (1) is assigned to the patient and provided with an application for storing and managing patient-related data. The second computer (2) is assigned to a consultant consulted by the patient with regard to the latter's state of health. The central server system (5) provides a platform for communication via the Internet using a browser and comprises an encrypted cloud.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zum Hochladen sowie ein Verfahren zum Herunterladen zumindest einer schutzbedürftige Daten zum Gesundheitszustand

[Fortsetzung auf der nächsten Seite]

eines Patienten enthaltenden Datei innerhalb eines vernetzten Computersystems, umfassend einen mobilen ersten Computer (1), einen zweiten Computer (2) und ein zentrales Serversystem (5). Der mobile erste Computer (1) ist dem Patienten zugeordnet und mit einer Applikation zum Speichern und Verwalten patientenbezogener Daten versehen. Der zweite Computer (2) ist einer vom Patienten bezüglich dessen Gesundheitszustands konsultierten Konsultationsperson zugeordnet. Das zentrale Serversystem (5) stellt eine Plattform zur Kommunikation über das Internet unter Verwendung eines Browsers bereit und umfasst eine verschlüsselte Cloud.

Verfahren zum Hochladen bzw. Herunterladen zumindest einer schutzbedürftige Daten zum Gesundheitszustand eines Patienten enthaltenden Datei innerhalb eines vernetzten Computersystems

Die Erfindung betrifft ein Verfahren zum Hochladen zumindest einer schutzbedürftige Daten zum Gesundheitszustand eines Patienten enthaltenden Datei innerhalb eines vernetzten Computersystems. Weiterhin betrifft die Erfindung ein Verfahren zum Herunterladen zumindest einer schutzbedürftige Daten zum Gesundheitszustand eines Patienten enthaltenden Datei innerhalb eines vernetzten Computersystems.

Nach dem Stand der Technik sind allgemein Datenbanken zum Speichern und Verwalten von Dateien bekannt, welche schutzbedürftige Daten zum Gesundheitszustand von Patienten enthalten. Solche Datenbanken werden beispielsweise von Krankenhäusern betrieben. Bei einer Konsultation einer Gesundheitseinrichtung außerhalb des betreffenden Krankenhauses ist ein Zugriff auf diese Daten schwierig.

Aufgabe der Erfindung ist es, die Nachteile nach dem Stand der Technik zu beheben. Insbesondere soll ein Verfahren zum Hochladen und ein Verfahren zum Herunterladen von schutzbedürftige Patientendaten enthaltenden Dateien angegeben werden, wobei der jeweilige Patient die Kontrolle über die ihn betreffenden Dateien hat, eine hohe Datensicherheit gewährleistet ist, und wobei eine vom Patienten bezüglich dessen Gesundheitszustands konsultierte Konsultationsperson keine spezifische Software zum Hochladen bzw. zum Herunterladen solcher Dateien benötigt.

Diese Aufgabe wird durch die Merkmale der Ansprüche 1 und 3 gelöst. Zweckmäßige Ausgestaltungen ergeben sich aus den Merkmalen der Ansprüche 2 und 4 bis 10.

Nach Maßgabe der Erfindung ist vorgesehen, dass das vernetzte Computersystem einen mobilen ersten Computer, einen zweiten Computer und ein zentrales Serversystem umfasst.

Der mobile erste Computer ist vorzugsweise ein Mobiltelefon, Handy, Smartphone oder iPhone. Weiterhin kann es sich bei dem mobilen ersten Computer auch um einen tragbaren Computer handeln, wie beispielsweise ein Tablet, Netbook oder Laptop. Der mobile erste Computer weist vorzugsweise ein Betriebssystem wie Android, IOS oder Windows auf. Der zweite Computer ist vorzugsweise ein PC. Das zentrale Serversystem kann genau einen Rechner umfassen. In diesem Fall steht der Begriff "Serversystem" für einen Server. Das zentrale Serversystem kann aber auch beispielsweise einen Cluster von Rechnern umfassen. Zusätzlich zum zentralen Serversystem kann ein Spiegelserversystem bereitstehen. Im Spiegelserversystem kann eine fortlaufend aktualisierte Kopie der im zentralen Serversystem gespeicherten Daten vorgehalten werden. Bei einem Ausfall des zentralen Serversystem kann das Spiegelserversystem an dessen Stelle treten.

Der mobile erste Computer ist dem Patienten zugeordnet und mit einer Applikation zum Speichern und Verwalten patientenbezogener Daten versehen.

Der zweite Computer ist einer vom Patienten bezüglich dessen Gesundheitszustands konsultierten Konsultationsperson zugeordnet. Der zweite Computer kann jeder beliebige von der Konsultationsperson benutzte Computer sein.

Das zentrale Serversystem stellt eine Plattform zur Kommunikation über das Internet unter Verwendung eines Browsers bereit und umfasst eine verschlüsselte Cloud. Bei der Plattform zur Kommunikation über das Internet handelt es sich vorzugsweise um einen über das World Wide Web verfügbaren Internetauftritt. Unter der verschlüsselten Cloud wird eine Datenbank bzw. ein Datenbanksystem verstanden, deren bzw. dessen Daten verschlüsselt sind.

Nach Maßgabe der Erfindung ist vorgesehen, dass das Hochladen der zumindest einen Datei in die verschlüsselte Cloud seitens des Patienten gegenüber der Konsultationsperson durch die folgenden Schritte autorisiert wird:

Erzeugen eines Zugangscodes mittels der Applikation durch den Patienten,

Bekanntgeben des Zugangscodes durch den Patienten an die Konsultationsperson,

Herstellen einer Verbindung zum Datenaustausch zwischen dem zweiten Computer und dem zentralen Serversystem durch die Konsultationsperson,

Eingabe des Zugangscodes über die Plattform durch die Konsultationsperson,

Überprüfen des Zugangscodes und bei Gültigkeit des Zugangscodes:

Herstellen einer verschlüsselten Datenverbindung zwischen dem zweiten Computer und der verschlüsselten Cloud,

Hochladen der zumindest einen Datei durch die Konsultationsperson vom zweiten Computer in die verschlüsselte Cloud über die verschlüsselte Datenverbindung,

Speichern der zumindest einen Datei in der verschlüsselten Cloud.

Vorzugsweise erfolgt das Erzeugen des Zugangscodes mittels der Applikation ohne die Notwendigkeit einer Datenverbindung zwischen dem mobilen ersten Computer und dem zentralen Serversystem. Der Zugangscode kann auch erst nach seinem Erzeugen und ggf. nach der Bekanntgabe an die Konsultationsperson an das zentrale Serversystem übermittelt werden. Die Übermittlung des Zugangscodes erfolgt vorzugsweise über eine verschlüsselte Datenverbindung zwischen dem mobilen ersten Computer und dem zentralen Serversystem. Die verschlüsselte Datenverbindung zwischen dem mobilen ersten Computer und dem zentralen

Serversystem kann bereits bestehen oder vor der Übermittlung hergestellt werden. Vorzugsweise wird der Zugangscode ohne weiteres Zutun des Patienten automatisch durch die Applikation vom mobilen ersten Computer an das zentrale Serversystem übermittelt.

Das Bekanntgeben des Zugangscodes durch den Patienten an die Konsultationsperson kann beispielsweise durch mündliche Mitteilung, auch am Telefon, durch handschriftliche Notiz, durch Versenden einer Kurznachricht bzw. E-Mail oder in einem Chat erfolgen.

Zweckmäßigerweise wird die Verbindung zum Datenaustausch zwischen dem zweiten Computer und dem zentralen Serversystem durch die Konsultationsperson herstellt, indem die Konsultationsperson eine ihr bekannte oder durch den Patienten bekanntgegebene URL, welche dem vom zentralen Serversystem bereitgestellten Internetauftritt zugeordnet ist, in einen auf dem zweiten Computer geöffneten Browser eingibt. Vorzugsweise ist die Verbindung zum Datenaustausch zwischen dem zweiten Computer und dem zentralen Serversystem verschlüsselt. Besonders bevorzugt ist eine Verschlüsselung nach dem https-Protokoll.

Die Eingabe des Zugangscodes erfolgt vorzugsweise über eine vom Internetauftritt umfasste Webseite. Dazu kann auf der Webseite ein Eingabefeld vorgesehen sein. Es ist möglich, dass der Patient dem Arzt einen Internetlink, z. B. per E-Mail, übermittelt, mit dem der Arzt unmittelbar zur Website gelangt.

Unter dem Herstellen einer verschlüsselten Datenverbindung zwischen dem zweiten Computer und der verschlüsselten Cloud wird eine verschlüsselte Datenverbindung zwischen dem zweiten Computer und dem zentralen Serversystem verstanden, die zum Übertragen von Daten in die verschlüsselte Cloud verwendet wird. Grundsätzlich kann die verschlüsselte Datenverbindung mit der Verbindung zum Datenaustausch identisch sein. In der Praxis wird beispielsweise beim https-Protokoll jedoch mit jeder Anfrage eine neue Datenverbindung hergestellt.

Vorzugsweise wird die zumindest eine Datei selbst nicht verschlüsselt, bevor sie über die verschlüsselte Datenverbindung hochgeladen wird. Vorzugsweise wird die zumindest eine Datei erst beim Speichern in der verschlüsselten Cloud verschlüsselt.

Das Speichern der zumindest einen Datei in der verschlüsselten Cloud erfolgt vorzugsweise in einem unveränderten Dateiformat. Alternativ oder zusätzlich kann die zumindest eine Datei auch in ein anderes Dateiformat konvertiert werden und in diesem Dateiformat gespeichert werden. Beispielsweise können Röntgenbilder, welche die Konsultationsperson im DICOM-Format hochlädt, in ein für Bilder gängiges Dateiformat, wie beispielsweise JPEG, konvertiert werden und in der verschlüsselten Cloud sowohl im DICOM-Format als auch im JPEG-Format gespeichert werden. Im DOC-Format gespeicherte Dokumente können beispielsweise ins PDF-Format konvertiert werden und in der verschlüsselten Cloud sowohl im DOC-Format als auch im PDF-Format gespeichert werden.

Durch das erfindungsgemäße Verfahren besitzt der Patient die Kontrolle über die in der Cloud gespeicherten Daten zu seinem Gesundheitszustand. Grundsätzlich kann nur der Patient schutzbedürftige Daten zu seinem Gesundheitszustand enthaltende Dateien mit dem mobilen ersten Computer oder mit einem anderen von ihm betriebenen Computer in die verschlüsselte Cloud hochladen. Der Patient kann gemäß dem erfindungsgemäßen Verfahren ausnahmsweise der Konsultationsperson das Hochladen zumindest einer schutzbedürftige Daten zu seinem Gesundheitszustand enthaltenden Datei ermöglichen. Aufgrund der Verschlüsselung sowohl der Daten in der Cloud als auch der Datenverbindungen kann eine hohe Datensicherheit gewährleistet werden. Die Konsultationsperson braucht weiterhin keine spezifische Software auf dem zweiten Computer zu installieren.

Nach einer vorteilhaften Ausgestaltung ist vorgesehen, dass der Zugangscode die Konsultationsperson zum einmaligen Hochladen zumindest einer schutzbedürftige Daten zum Gesundheitszustand des Patienten enthaltenden Datei autorisiert. Das

heißt, der Zugangscode ist genau einmal verwendbar. Dadurch besitzt der Patient eine besonders gute Kontrolle über die in der Cloud gespeicherten Daten zu seinem Gesundheitszustand. Er kann sichergehen, dass nach erfolgtem Hochladen der zumindest einen Datei durch die dazu autorisierte Konsultationsperson keine weiteren Dateien ohne seine Zustimmung hochgeladen werden.

Alternativ dazu kann auch vorgesehen sein, dass ein permanenter Zugangscode mittels der Applikation durch den Patienten erzeugt wird. Der permanenter Zugangscode autorisiert die Konsultationsperson zum mehrfachen Hochladen jeweils zumindest einer schutzbedürftige Daten zum Gesundheitszustand eines Patienten enthaltenden Datei. Das heißt, der permanente Zugangscode ist mehrmals verwendbar. Dadurch wird die Handhabung des Verfahrens insbesondere in solchen Fällen vereinfacht, in denen bei einer bestimmten Konsultationsperson regelmäßig Daten zu einem bestimmten Patienten anfallen, und in denen ein ausgeprägtes Vertrauensverhältnis zwischen Patient und Konsultationsperson besteht. Zweckmäßigerweise kann der permanente Zugangscode mittels der Applikation durch den Patienten zu einem späteren Zeitpunkt wieder deaktiviert werden. Dadurch kann der Patient wieder die vollständige Kontrolle über die in der Cloud gespeicherten Daten zu seinem Gesundheitszustand zurückerlangen. Weiterhin ist es für den Patienten zweckmäßigerweise jederzeit möglich, nach eigenem Belieben Dateien, welche Daten zu seinem Gesundheitszustand enthalten, aus der Cloud zu löschen.

Weiterhin kann vorgesehen sein, dass der einmal verwendbare bzw. der permanente Zugangscode mit einer durch den Patienten festgelegten Gültigkeitsdauer erzeugt wird, beispielsweise einer Anzahl von Stunden und/oder Tagen. Die Gültigkeitsdauer kann auch bis zu einer bestimmten Uhrzeit an einem bestimmten Datum bestimmt sein.

Nach Maßgabe der Erfindung ist weiterhin vorgesehen, dass das Herunterladen der zumindest einen Datei aus der verschlüsselten Cloud seitens des Patienten gegenüber der Konsultationsperson durch die folgenden Schritte autorisiert wird:

Herstellung einer Datenverbindung zwischen dem mobilen ersten Computer und dem zentralen Serversystem,

Auswahl der zumindest einen Datei durch den Patienten mittels der Applikation,

Erzeugen eines Zugriffslinks durch den Patienten mittels der Applikation, wobei der Zugriffslink zum Zugreifen auf die zumindest eine Datei bestimmt ist und eine vorbestimmte Gültigkeitsdauer hat,

Auswahl oder Eingabe einer E-Mail-Adresse der Konsultationsperson durch den Patienten mittels der Applikation,

Übermitteln des Zugriffslinks per E-Mail an die Konsultationsperson,

Ausführen des Zugriffslinks durch die Konsultationsperson vom zweiten Computer aus,

Herstellen einer verschlüsselten Datenverbindung zwischen dem zweiten Computer und der verschlüsselten Cloud, wenn der Zugriffslink als gültig erkannt worden ist,

Herunterladen der zumindest einen Datei auf den zweiten Computer über die verschlüsselte Datenverbindung zum Speichern und/oder Anzeigen auf dem zweiten Computer.

Die zwischen dem mobilen ersten Computer und dem zentralen Serversystem hergestellte Datenverbindung ist vorzugsweise verschlüsselt.

Die Auswahl der zumindest einen Datei durch den Patienten mittels der Applikation erfolgt vorzugsweise aus den in der verschlüsselten Cloud gespeicherten Dateien, welche Daten zum Gesundheitszustand des Patienten enthalten. Es ist aber

auch möglich, dass der Patient eine Datei oder mehrere Dateien auswählt, welche noch nicht in der verschlüsselten Cloud gespeichert sind. Diese Datei bzw. diese Dateien können auf dem mobilen ersten Computer gespeichert sein oder in anderer Weise vom mobilen ersten Computer aus verfügbar sein. Diese Datei bzw. diese Dateien werden in diesem Fall in einem weiteren Schritt vom mobilen ersten Computer in die verschlüsselte Cloud hochgeladen. Insbesondere ist es möglich, dass sowohl zumindest eine in der verschlüsselten Cloud gespeicherte Datei als auch zumindest eine noch nicht in der verschlüsselten Cloud gespeicherte Datei auswählt werden. Die zumindest eine noch nicht in der verschlüsselten Cloud gespeicherte Datei wird dann vorzugsweise in dem weiteren Schritt vom mobilen ersten Computer in die verschlüsselte Cloud hochgeladen. Vorzugsweise wird sie dort verschlüsselt gespeichert.

Insbesondere für den Fall, dass zumindest zwei Dateien ausgewählt werden, wird in der verschlüsselten Cloud vorzugsweise ein die zumindest zwei Dateien umfassendes Archiv erstellt. Die zumindest zwei Dateien können daraufhin in Form des Archivs auf den zweiten Computer heruntergeladen werden. Vorzugsweise werden die zumindest zwei Dateien entschlüsselt, bevor sie in das Archiv aufgenommen werden. Das Archiv ist vorzugsweise verschlüsselt. Dazu kann vorgesehen sein, dass der Patient in einem weiteren Schritt ein Entpack-Passwort bestimmt und dieses Entpack-Passwort der Konsultationsperson bekanntgibt. Das Bekanntgeben des Entpack-Passworts kann beispielsweise durch mündliche Mitteilung, auch am Telefon, durch handschriftliche Notiz, durch Versenden einer Kurznachricht bzw. E-Mail oder in einem Chat erfolgen. Die Konsultationsperson kann das Archiv nach dem Herunterladen mit dem Entpack-Passwort entschlüsseln und entpacken. Vorzugsweise werden die zumindest zwei Dateien in unverschlüsselter Form in das verschlüsselte Archiv aufgenommen. Bei dem Archiv kann es sich um eine Containerdatei handeln. Die Containerdatei kann zusätzlich komprimiert sein. Vorzugsweise hat das Archiv ein gängiges Dateiformat, wie beispielsweise ZIP oder RAR. Aus einem solchen Archiv können auf dem zweiten Computer leicht wieder die zumindest zwei Dateien extrahiert werden. Die gleiche Vorge-

hensweise über ein Archiv mit den gleichen Ausgestaltungsvarianten ist selbstverständlich auch möglich, wenn genau eine Datei ausgewählt wird.

Andererseits ist es selbstverständlich auch in dem Fall, dass zumindest zwei Dateien ausgewählt werden, möglich, dass diese Dateien als einzelne Dateien bereitgestellt werden, ohne diese in ein Archiv aufzunehmen. Dabei kann der Zugriffslink auf ein Verzeichnis gerichtet sein, aus dem die Dateien einzeln vom zentralen Serversystem heruntergeladen werden können. Weiterhin kann auch ein Erzeugen mehrerer Zugriffslinks vorgesehen sein.

Der Zugriffslink umfasst vorzugsweise einen Hashcode, besonders bevorzugt einen Hashcode mit Salt. Weiterhin umfasst der Zugriffslink vorzugsweise eine URL unter Verwendung des https-Protokolls. Die vorbestimmte Gültigkeitsdauer beträgt vorzugsweise eine Anzahl von Stunden und/oder Tagen, besonders bevorzugt genau einen Tag. Die vorbestimmte Gültigkeitsdauer kann auch bis zu einer bestimmten Uhrzeit an einem bestimmten Datum bestimmt sein.

Vorzugsweise wird dem Patienten zur Auswahl der E-Mail-Adresse der Konsultationsperson durch die Applikation eine Liste von Konsultationspersonen angezeigt. Die Liste kann unabhängig vom jeweiligen Patienten alle bekannten Konsultationspersonen umfassen. Alternativ kann die Liste alle Konsultationspersonen umfassen, welche mit einer Krankenkasse zusammenarbeiten, in der der Patient Mitglied ist. Weiterhin alternativ dazu kann die Liste nur diejenigen Konsultationspersonen umfassen, die der betreffende Patient bereits konsultiert hat. Dabei ist es auch möglich, dass sich die durch die Applikation angezeigte Liste aus verschiedenen Teillisten zusammensetzt. Die Liste bzw. die Teillisten können vom zentralen Serversystem und/oder vom mobilen ersten Computer bereitgestellt werden. Die Liste bzw. die Teillisten können von einer Krankenkasse, von einem Betreiber des zentralen Serversystems und/oder vom Patienten selbst erstellt werden. Abgesehen von der Auswahl über eine Liste kann die E-Mail-Adresse der Konsultationsperson aber auch vom Patienten direkt in ein in der Applikation vorgesehenes Eingabefeld eingegeben werden.

Vorzugsweise wird die E-Mail zur Übermittelung des Zugriffslinks an die Konsultationsperson vom zentralen Serversystem aus versendet.

Das Ausführen des Zugriffslinks kann beispielsweise dadurch erfolgen, dass die Konsultationsperson am zweiten Computer den Zugriffslink in der geöffneten E-Mail anklickt oder den Zugrifflink durch Eingabe in einem Browser aufruft.

Die verschlüsselte Datenverbindung zwischen dem zweiten Computer und der verschlüsselten Cloud wird vorzugsweise unter Verwendung des https-Protokolls hergestellt.

Vorzugsweise wird die zumindest eine Datei entschlüsselt, bevor sie über die verschlüsselte Datenverbindung von der verschlüsselten Cloud auf den zweiten Computer heruntergeladen wird.

Durch das erfindungsgemäße Verfahren besitzt der Patient die Kontrolle über die in der Cloud gespeicherten Daten zu seinem Gesundheitszustand. Grundsätzlich kann nur der Patient schutzbedürftige Daten zu seinem Gesundheitszustand enthaltende Dateien mit dem mobilen ersten Computer oder mit einem anderen von ihm betriebenen Computer aus der verschlüsselten Cloud herunterladen. Der Patient kann gemäß dem erfindungsgemäßen Verfahren ausnahmsweise der Konsultationsperson das Herunterladen zumindest einer schutzbedürftige Daten zu seinem Gesundheitszustand enthaltenden Datei ermöglichen. Aufgrund der Verschlüsselung sowohl der Daten in der Cloud als auch der Datenverbindungen kann eine hohe Datensicherheit gewährleistet werden. Die Konsultationsperson braucht keine spezifische Software auf dem zweiten Computer zu installieren.

Vorzugsweise ist die zumindest eine Datei aus der folgenden Gruppe ausgewählt: Arztbrief, Krankenhausbericht, Behandlungsbericht, Gutachten, Röntgen-, CT- und/oder MRT-Bild. Die zumindest eine Datei kann auch ein aus einem beliebigen bildgebenden Verfahren resultierendes digitales Bild sein. Die Dokumente bzw.

Bilder sind vorzugsweise bereits ursprünglich in digitaler Form geschaffen worden. Alternativ können sie aber auch beispielsweise durch Einscannen nachträglich digitalisiert worden sein.

Das Röntgen-, CT- und/oder MRT-Bild ist vorzugsweise im DICOM-Format gespeichert. Das DICOM-Format ist auf Bilder aus bildgebenden Verfahren der Medizin optimiert und kann Zusatzinformationen enthalten. Zur Anzeige solcher Bilder ist jedoch eine spezielle Software erforderlich. Zweckmäßigerweise werden daher zu im DICOM-Format hochgeladenen Bildern zusätzlich in ein gängiges Bildformat konvertierte Bilder in der verschlüsselten Cloud gespeichert. Dadurch hat der Patient die Möglichkeit, diese Bilder im gängigen Format von der Cloud herunterzuladen und sich auf dem mobilen ersten Computer anzeigen zu lassen, ohne dass dabei er eine Software zur Anzeige des DICOM-Formats benötigt.

Die Konsultationsperson ist vorzugsweise ein Arzt, ein Therapeut, ein Radiologe, ein Heilpraktiker, ein Sanitäter oder eine mit einem aus diesen zusammenarbeitende Person.

Nach einer vorteilhaften Ausgestaltung ist vorgesehen, dass das Verfahren die folgenden zusätzlichen Schritte umfasst:

Einloggen in der Applikation auf dem mobilen ersten Computer durch den Patienten.

Das Einloggen erfolgt vorzugsweise unter Verwendung eines Einlogg-Passworts, besonders bevorzugt zusammen mit einem Benutzernamen. Vorzugsweise hat der Patient dazu den Benutzernamen und das Einlogg-Passwort in dazu durch die Applikation vorgesehene Eingabefelder einzugeben. Der Benutzernamen kann auch bereits in der Applikation vermerkt sein. Das Einlogg-Passwort ist vorzugsweise im zentralen Serversystem gespeichert, vorzugsweise als Hashcode mit Salt. Zur Überprüfung, ob das eingegebene Einlogg-Passwort mit dem im zentralen Serversystem zum betreffenden Patienten gespeicherten Einlogg-Passwort

übereinstimmt, wird vorzugsweise eine verschlüsselte Datenverbindung zwischen dem mobilen ersten Computer und dem zentralen Serversystem hergestellt. Nach dem Einloggen stehen dem Patienten vorzugsweise der vollständige von einem Endbenutzer benutzbare Funktionsumfang der Applikation sowie ein Zugriff auf die in der verschlüsselten Cloud gespeicherten Dateien, welche Daten zu seinem Gesundheitszustand enthalten, zur Verfügung. Zusätzlich kann durch das zentrale Serversystem überprüft werden, ob für den Patienten bestimmte Vertragskonditionen, beispielsweise das Vorhandensein eines kostenpflichtigen Abonnements vorliegen. Abhängig davon kann dem Patienten der vollständige oder nur ein eingeschränkter Funktionsumfang der Applikation zur Verfügung gestellt werden.

Nach einer weiteren vorteilhaften Ausgestaltung ist vorgesehen, dass das Verfahren die folgenden zusätzlichen Schritte umfasst:

Erfassen zumindest eines biometrischen Merkmals einer die Applikation verwendenden Person mittels des mobilen ersten Computers,

Identifizieren der die Applikation verwendenden Person als den für die Verwendung der Applikation autorisierten Patienten.

Die zusätzlichen Schritte können Teil des Einloggen in der Applikation auf dem mobilen ersten Computer durch den Patienten sein. Die zusätzlichen Schritte können aber auch zusätzlich zu einem Einloggen unter Verwendung eines Einlogg-Passworts vorgesehen sein. Bei dem erfassten zumindest einem biometrischen Merkmal kann es sich um einen Fingerabdruck handeln. Zum Erfassen des Fingerabdrucks sieht der mobile erste Computer zweckmäßigerweise einen Fingerabdruckscanner vor. Zum Überprüfen des zumindest einen biometrischen Merkmals können biometrische Daten des Patienten auf dem mobilen ersten Computer und/oder im zentralen Serversystem gespeichert sein, vorzugsweise in verschlüsselter Form. Gegebenenfalls ist zur Identifizierung des Patienten also eine Datenverbindung zwischen dem mobilen ersten Computer und dem zentralen Serversystem herzustellen. Durch die zusätzlichen Schritte wird ein Missbrauch der Ap-

plikation und damit verbunden der schutzbedürftigen Patientendaten durch einen Dritten verhindert, der Zugang zum mobilen ersten Computer erlangt hat.

Zweckmäßigerweise ermöglicht die Applikation eine Anzeige von Notfalldaten ohne Einloggen, ohne das Identifizieren des Patienten anhand biometrischer Merkmale bzw. ohne sonstige Zugangshindernisse. Solche Notfalldaten umfassen beispielsweise Informationen zur Blutgruppe, zu einzunehmenden Medikamenten, zu Allergien, zu Krankheiten und/oder Besonderheiten des Patienten, wie das Vorhandensein von Implantaten.

Vorzugsweise erfolgen sowohl die Datenverbindungen zwischen dem mobilen ersten Computer und dem zentralen Serversystem als auch die Datenverbindungen zwischen dem zweiten Computer und dem zentralen Serversystem über das Internet.

Nach einer weiteren vorteilhaften Ausgestaltung ist vorgesehen, dass die Datenverbindung zwischen dem mobilen ersten Computer und dem zentralen Serversystem und/oder die Datenverbindung zwischen dem zweiten Computer und dem zentralen Serversystem nach einem SSL-Standard verschlüsselt hergestellt wird. Insbesondere kann vorgesehen sein, dass jede Datenverbindung zwischen dem mobilen ersten Computer und dem zentralen Serversystem und/oder jede Datenverbindung zwischen dem zweiten Computer und dem zentralen Serversystem nach einem SSL-Standard verschlüsselt hergestellt wird. Unter SSL-Standard wird ein Verschlüsselungsprotokoll verstanden, welches auf das SSL-Protokoll zurückgeht. Insbesondere sind davon Weiterentwicklungen unter der Bezeichnung TLS (Transport Layer Security) umfasst.

Die Datenverbindungen zwischen dem mobilen ersten Computer und dem zentralen Serversystem bzw. zwischen dem zweiten Computer und dem zentralen Serversystem können insbesondere nach dem https-Protokoll erfolgen.

Nach einer weiteren vorteilhaften Ausgestaltung ist vorgesehen, dass

die schutzbedürftigen Daten zum Gesundheitszustand des Patienten in der verschlüsselten Cloud und/oder auf dem mobilen ersten Computer nach dem Advanced-Encryption-Standard verschlüsselt gespeichert werden. Der Advanced-Encryption-Standard wird üblicherweise mit AES abgekürzt. Besonders bevorzugt wird eine AES-256-Verschlüsselung.

Vorzugsweise erfolgt die AES-256-Verschlüsselung der schutzbedürftigen Daten zum Gesundheitszustand des Patienten auf dem mobilen ersten Computer unter Verwendung eines Verschlüsselungspassworts. Entsprechend können die Daten unter Verwendung des Verschlüsselungspassworts wieder entschlüsselt werden. Das Verschlüsselungspasswort wird vorzugsweise beim Installieren der Applikation durch den Patienten bestimmt. Vorzugsweise wird dabei ein SHA-256-Hashcode des Verschlüsselungspassworts auf dem mobilen ersten Computer gespeichert, beispielweise in SharedPreferences bei einem mit Android betriebenen mobilen ersten Computer oder in NSUserdefaults bei einem mit IOS betriebenen mobilen ersten Computer.

Vorzugsweise erfolgt die AES-256-Verschlüsselung der schutzbedürftigen Daten zum Gesundheitszustand des Patienten in der verschlüsselten Cloud unter Verwendung des Einlogg-Passworts. Das Einlogg-Passwort ist vorzugsweise im zentralen Serversystem gespeichert, vorzugsweise als Hashcode mit Salt. Die Daten können unter Verwendung des Einlogg-Passworts wieder entschlüsselt werden. Vorzugsweise wird die zumindest eine Datei entschlüsselt, bevor sie über die verschlüsselte Datenverbindung von der verschlüsselten Cloud auf den zweiten Computer heruntergeladen wird. Im Fall des Erstellens eines Archivs wird die zumindest eine Datei vorzugsweise entschlüsselt, bevor sie in das Archiv aufgenommen wird. Das Archiv wird vorzugsweise unter der Verwendung eines vom Patienten bestimmten Entpack-Passworts verschlüsselt und in dieser verschlüsselten Form über die verschlüsselte Datenverbindung auf den zweiten Computer heruntergeladen.

Weiterhin wird ein zum Verfahren zum Herunterladen der zumindest einen schutzbedürftige Daten zum Gesundheitszustand des Patienten enthaltenden Datei alternatives Verfahren vorgestellt.

Beim alternativen Verfahren wird ebenfalls die zumindest eine schutzbedürftige Daten zum Gesundheitszustand des Patienten enthaltende Datei durch den Patienten mittels der Applikation ausgewählt und eine E-Mail-Adresse der Konsultationsperson durch den Patienten mittels der Applikation ausgewählt oder eingegeben. Sind eine oder mehrere der ausgewählten Dateien noch nicht auf dem mobilen ersten Computer gespeichert, werden diese Datei oder Dateien von der verschlüsselten Cloud auf den mobilen ersten Computer über eine verschlüsselte Datenverbindung heruntergeladen. Aus der zumindest einen Datei wird auf dem mobilen ersten Computer vorzugsweise eine verschlüsselte ZIP-Datei erstellt. Vorzugsweise enthält die verschlüsselte ZIP-Datei die zumindest eine Datei in unverschlüsselter Form. Vorzugsweise bestimmt der Patient ein Entpack-Passwort, mit welchem die verschlüsselte ZIP-Datei durch die Konsultationsperson entschlüsselt und entpackt werden kann, und gibt der Konsultationsperson dieses Entpack-Passwort bekannt. Das Bekanntgeben des Entpack-Passworts kann beispielsweise durch mündliche Mitteilung, auch am Telefon, durch handschriftliche Notiz, durch Versenden einer Kurznachricht bzw. E-Mail oder in einem Chat erfolgen. Die zumindest eine Datei bzw. die verschlüsselte ZIP-Datei wird per E-Mail vom mobilen ersten Computer aus an die Konsultationsperson übermittelt. Dabei kann vorgesehen sein, dass textlich darstellbare Daten direkt im Text der E-Mail vorgesehen werden. In diesem Fall kann auf eine zusätzliche Übermittlung der die Textdaten enthaltenden Dateien in der E-Mail verzichtet werden. Das alternative Verfahren kann eine eigenständige Erfindungen bilden.

Als ein weiteres Verfahren zum Hochladen von schutzbedürftige Daten zum Gesundheitszustand eines Patienten enthaltenden Dateien kann eine Datenübernahme aus einer von einer Gesundheitseinrichtung betriebenen Datenbank erfolgen. Bei der Gesundheitseinrichtung kann es sich um eine Arztpraxis oder um ein Krankenhaus handeln. Die übernommenen Daten können in der verschlüsselten

Cloud und/oder auf dem mobilen ersten Computer gespeichert werden. Das weitere Verfahren kann eine eigenständige Erfindungen bilden.

Nachfolgend werden bevorzugte Ausführungsbeispiele der Erfindung anhand von Zeichnungen näher erläutert. Es zeigen:

Fig. 1 schematische Darstellung von an den erfindungsgemäßen Verfahren beteiligten Hardwarekomponenten,

Fig. 2 Flussdiagramm zu einem ersten Ausführungsbeispiel des Verfahrens zum Hochladen der zumindest einen schutzbedürftige Daten zum Gesundheitszustand eines Patienten enthaltenden Datei,

Fig. 3 Flussdiagramm zu einem zweiten Ausführungsbeispiel des Verfahrens zum Hochladen der zumindest einen schutzbedürftige Daten zum Gesundheitszustand eines Patienten enthaltenden Datei, und

Fig. 4 Flussdiagramm zu einem Ausführungsbeispiel des Verfahrens zum Herunterladen der zumindest einen schutzbedürftige Daten zum Gesundheitszustand eines Patienten enthaltenden Datei.

Fig. 1 zeigt eine schematische Darstellung von an den erfindungsgemäßen Verfahren beteiligten Hardwarekomponenten. Ein mobiler erster Computer 1 und ein zweiter Computer 2 sind über eine erste Datenverbindung 3 bzw. eine zweite Datenverbindung 4 mit einem zentralen Serversystem 5 verbunden. Der mobile erste Computer 1 ist einem Patienten zugeordnet und mit einer Applikation zum Speichern und Verwalten patientenbezogener Daten versehen. Der zweite Computer 2 ist einer vom Patienten bezüglich dessen Gesundheitszustands konsultierten Konsultationsperson zugeordnet. Bei der Konsultationsperson handelt es sich beispielsweise um einen den Patienten behandelten Arzt. Die erste 3 und die zweite Datenverbindung 4 erfolgen jeweils über das Internet und sind jeweils nach einem SSL-Standard verschlüsselt. Das zentrale Serversystem 5 umfasst eine Cloud.

Sowohl in der Cloud als auch auf dem mobilen ersten Computer 1 sind Dateien gespeichert, welche schutzbedürftige Daten zum Gesundheitszustand des Patienten enthalten. Diese Daten sind jeweils mit AES-256 verschlüsselt. Weiterhin ist das zentrale Serversystem 5 über eine dritte Datenverbindung 6 mit einem Spiegelserversystem 7 verbunden. Für den Fall, dass das zentrale Serversystem 5 und das Spiegelserversystem 7 lokal getrennt sind, ist die dritte Datenverbindung 6 nach einem SSL-Standard verschlüsselt.

Fig. 2 zeigt ein Flussdiagramm zu einem ersten Ausführungsbeispiel des Verfahrens zum Hochladen der zumindest einen schutzbedürftige Daten zum Gesundheitszustand des Patienten enthaltenden Datei. Beim Schritt S1 wird ein einmalig verwendbarer Zugangscode erzeugt. Dazu betätigt der Patient in der Applikation eine dafür vorgesehene Auswahlfläche. Daraufhin wird der erzeugte Zugangscode dem Patienten durch die Applikation auf dem mobilen ersten Computer 1 angezeigt. Beim Schritt S2 gibt der Patient seinem Arzt den Zugangscode bekannt. Dies kann mündlich bei einer Konsultation des Arztes erfolgen. In einem nicht dargestellten Schritt wird der Zugangscode vom mobilen ersten Computer 1 an das zentrale Serversystem 5 über eine nach einem SSL-Standard verschlüsselte erste Datenverbindung 3 übermittelt. Der nicht dargestellte Schritt kann zwischen dem Schritt S1 und dem Schritt S5 erfolgen. Für das Erzeugen und Anzeigen des Zugangscodes alleine wird keine erste Datenverbindung 3 zum zentralen Serversystem 5 benötigt. Durch die Schritte S1, S2 und den nicht dargestellten Schritt wird der Arzt zum einmaligen Hochladen der zumindest einen Datei autorisiert. Beim Schritt S3 ruft der Arzt vom zweiten Computer 2 aus über einen Browser eine ihm bekannte oder durch den Patienten, z. B. durch Übermittlung eines entsprechenden Internetlinks an den Arzt, bekanntgegebene URL auf, welche einem durch das zentrale Serversystem 5 bereitgestellten Internetauftritt zugeordnet ist, und stellt dadurch eine nach dem SSL-Standard verschlüsselte zweite Datenverbindung 4 zwischen dem zweiten Computer 2 und dem zentralen Serversystem 5 her. Die zweite Datenverbindung 4 erfolgt insbesondere nach dem https-Protokoll. Beim Schritt S4 gibt der Arzt den Zugangscode über ein Eingabefeld ein, welches durch eine dem Internetauftritt angehörende Webseite bereitgestellt wird. Beim Schritt

S5 überprüft das zentrale Serversystem 5 den Zugangscode auf seine Gültigkeit. Bei Gültigkeit des Zugangscodes wird im Schritt S6 erneut eine nach dem SSL-Standard verschlüsselte zweite Datenverbindung 4 zwischen dem zweiten Computer 2 und dem zentralen Serversystem 5 hergestellt. Beim Schritt S7 wird die zumindest eine Datei durch den Arzt vom zweiten Computer 2 in die verschlüsselte Cloud über die verschlüsselte zweite Datenverbindung 4 hochgeladen. Bei der zumindest einen Datei handelt es sich beispielsweise um einen Arztbrief im DOC-Format und um ein digitales Röntgenbild im DICOM-Format. Beim Schritt S8 werden der Arztbrief im DOC-Format und das digitale Röntgenbild im DICOM-Format gespeichert. Beim optionalen Schritt S9 wird der Arztbrief ins PDF-Format konvertiert und das digitale Röntgenbild ins JPEG-Format konvertiert. Beim optionalen Schritt S10 werden zusätzlich der Arztbrief im PDF-Format und das digitale Röntgenbild im JPEG-Format gespeichert. Das Speichern erfolgt jeweils mit einer AES-256-Verschlüsselung.

Fig. 3 zeigt ein Flussdiagramm zu einem zweiten Ausführungsbeispiel des Verfahrens zum Hochladen der zumindest einen schutzbedürftige Daten zum Gesundheitszustand des Patienten enthaltenden Datei. Beim Schritt S1' wird ein permanenter Zugangscode erzeugt, indem der Patient in der Applikation eine weitere Auswahlfläche betätigt. Wie beim ersten Ausführungsbeispiel wird der erzeugte Zugangscode dem Patienten durch die Applikation auf dem ersten mobilen Computer 1 angezeigt. Der Patient gibt wiederum beim Schritt S2 seinem Arzt den Zugangscode bekannt. Der Zugangscode wird wiederum in einem nicht dargestellten Schritt, welcher zwischen dem Schritt S1' und dem Schritt S5 erfolgen kann, vom mobilen ersten Computer 1 an das zentrale Serversystem 5 über eine verschlüsselte erste Datenverbindung 3 übermittelt. Durch die Schritte S1', S2 und den nicht dargestellten Schritt wird der Arzt zum mehrmaligen Hochladen jeweils zumindest einer Datei autorisiert. Während beim ersten Ausführungsbeispiel das Verfahren nach einmaligem Durchlaufen der Schritte S3 bis S8 bzw. S3 bis S10 beendet ist, können beim zweiten Ausführungsbeispiel die Schritte S3 bis S8 und/oder die Schritte S3 bis S10 mehrmals durchlaufen werden. Sofern der Patient aber in der Zwischenzeit den Zugangscode über die Applikation deaktiviert,

wird der Zugangscode bei einem weiteren Durchlaufen der Schritte beim Schritt S5 nicht mehr als gültig erkannt. Dadurch wird das Verfahren auch beim zweiten Ausführungsbeispiel beendet.

Fig. 4 zeigt ein Flussdiagramm zu einem Ausführungsbeispiel des Verfahrens zum Herunterladen der zumindest einen schutzbedürftige Daten zum Gesundheitszustand des Patienten enthaltenden Datei. Beim Schritt S21 loggt sich der Patient auf dem mobilen ersten Computer in der Applikation ein. Dazu wird eine verschlüsselte zweite Datenverbindung 4 zwischen dem mobilen ersten Computer 1 und dem zentralen Serversystem 5 hergestellt. Der Patient gibt einen Benutzernamen und ein Einlogg-Passwort ein. Das zentrale Serversystem 5 überprüft die Korrektheit des Einlogg-Passworts. Ist das Einlogg-Passwort korrekt, erlangt der Patient Zugriff auf den vollständigen Bedienungsumfang der Applikation sowie auf die in der verschlüsselten Cloud gespeicherten Dateien, welche Daten zu seinem Gesundheitszustand enthalten. Beim Schritt S22 ruft der Patient in der Applikation einen Menüpunkt zur Bereitstellung von Dateien an eine Konsultationsperson, insbesondere einen den Patienten behandelnden Arzt, auf. Beim Schritt S23 kann der Patient mittels der Applikation die zumindest eine bereitzustellende Datei auswählen. Eine solche Datei kann in der verschlüsselten Cloud gespeichert sein und/oder vom mobilen ersten Computer 1 aus verfügbar sein. Beispielsweise wählt der Patient ein in der verschlüsselten Cloud gespeichertes digitales Röntgenbild im DICOM-Format und einen auf dem mobilen ersten Computer 1 gespeicherten Arztbrief im PDF-Format aus. Der Arztbrief ist dabei noch nicht in der verschlüsselten Cloud gespeichert. Im Schritt S24 wird der Arztbrief als PDF-Datei über eine verschlüsselte erste Datenverbindung 3 vom mobilen ersten Computer 1 an das zentrale Serversystem 5 übertragen und verschlüsselt in der Cloud gespeichert. Der Schritt S24 entfällt, sofern keine noch nicht in der verschlüsselten Cloud gespeicherte Datei ausgewählt wurde. Beim Schritt S25 wird durch das zentrale Serversystem 5 ein verschlüsseltes ZIP-Archiv aus dem digitalen Röntgenbild im DICOM-Format und dem Arztbrief im PDF-Format erstellt. Der Patient hat dazu ein Entpack-Passwort festzulegen. Der Patient gibt das Entpack-Passwort daraufhin seinem Arzt bekannt. Dies kann mündlich bei einer Konsultation des Arztes

erfolgen. Der Schritt S25 kann beispielsweise entfallen, wenn genau eine Datei ausgewählt wurde. In einem alternativen Ausführungsbeispiel kann Schritt S25 weggelassen werden, und stattdessen können ggf. mehrere einzelne Dateien zum Herunterladen bereitgestellt werden. Beim Schritt S26 wird ein Zugriffslink auf die verschlüsselte ZIP-Datei mit einer vorbestimmte Gültigkeitsdauer erzeugt. Diese Gültigkeitsdauer bestimmt der Patient mittels der Applikation. Der Patient bestimmt beispielsweise als Gültigkeitsdauer einen Tag. Beim Schritt S27 wählt der Patient den Arzt aus einer durch die Applikation angezeigten Liste aus. Die Liste umfasst alle Konsultationspersonen, welche der Patient bereits konsultiert hat. Alternativ dazu kann der Patient in ein durch die Applikation vorgesehenes Eingabefeld eine E-Mail-Adresse des Arztes eingegeben. Im Schritt S28 übermittelt das zentrale Serversystem 5 den Zugriffslink per E-Mail an den Arzt. Beim Schritt S29 führt der Arzt den Zugriffslink vom zweiten Computer 2 aus aus. Dies kann beispielsweise durch ein Anklicken des Zugriffslinks in der geöffneten E-Mail geschehen. Im Schritt S30 wird eine verschlüsselte zweite Datenverbindung 4 zwischen dem zweiten Computer 2 und dem zentralen Serversystem 5 hergestellt. Beim Schritt S31 wird überprüft, ob der Zugriffslink gültig ist. Ist dies der Fall, wird beim Schritt S32 die verschlüsselte ZIP-Datei von der Cloud über die verschlüsselte zweite Datenverbindung 4 auf den zweiten Computer 2 heruntergeladen und dort gespeichert bzw. ohne Speichern ausgeführt. Beim Schritt S33 entschlüsselt und entpackt der Arzt die verschlüsselte ZIP-Datei mit Hilfe des Entpack-Passworts. Damit stehen dem Arzt das digitale Röntgenbild im DICOM-Format und der Arztbrief im PDF-Format in unverschlüsselter Form auf dem zweiten Computer 2 zum Speichern und/oder zur Anzeige zur Verfügung.

Bezugszeichenliste

1	mobiler erster Computer
2	zweiter Computer
3	erste Datenverbindung
4	zweite Datenverbindung
5	zentrales Serversystem
6	dritte Datenverbindung
7	Spiegelserversystem

Patentansprüche

1. Verfahren zum Hochladen zumindest einer schutzbedürftige Daten zum Gesundheitszustand eines Patienten enthaltenden Datei innerhalb eines vernetzten Computersystems, umfassend einen mobilen ersten Computer (1), einen zweiten Computer (2) und ein zentrales Serversystem (5),

wobei der mobile erste Computer (1) dem Patienten zugeordnet ist und mit einer Applikation zum Speichern und Verwalten patientenbezogener Daten versehen ist,

wobei der zweite Computer (2) einer vom Patienten bezüglich dessen Gesundheitszustands konsultierten Konsultationsperson zugeordnet ist,

wobei das zentrale Serversystem (5) eine Plattform zur Kommunikation über das Internet unter Verwendung eines Browsers bereitstellt und eine verschlüsselte Cloud umfasst,

wobei das Hochladen der zumindest einen Datei in die verschlüsselte Cloud seitens des Patienten gegenüber der Konsultationsperson durch die folgenden Schritte autorisiert wird:

Erzeugen eines Zugangscodes mittels der Applikation durch den Patienten,

Bekanntgeben des Zugangscodes durch den Patienten an die Konsultationsperson,

Herstellen einer Verbindung zum Datenaustausch zwischen dem zweiten Computer (2) und dem zentralen Serversystem (5) durch die Konsultationsperson,

Eingabe des Zugangscodes über die Plattform durch die Konsultationsperson,

Überprüfen des Zugangscodes und bei Gültigkeit des Zugangscodes:

Herstellen einer verschlüsselten Datenverbindung zwischen dem zweiten Computer (2) und der verschlüsselten Cloud,

Hochladen der zumindest einen Datei durch die Konsultationsperson vom zweiten Computer (2) in die verschlüsselte Cloud über die verschlüsselte Datenverbindung,

Speichern der zumindest einen Datei in der verschlüsselten Cloud.

2. Verfahren nach Patentanspruch 1, wobei der Zugangscode die Konsultationsperson zum einmaligen Hochladen zumindest einer schutzbedürftige Daten zum Gesundheitszustand des Patienten enthaltenden Datei autorisiert.

3. Verfahren zum Herunterladen zumindest einer schutzbedürftige Daten zum Gesundheitszustand eines Patienten enthaltenden Datei innerhalb eines vernetzten Computersystems, umfassend einen mobilen ersten Computer (1), einen zweiten Computer (2) und ein zentrales Serversystem (5) mit einer verschlüsselten Cloud,

wobei der mobile erste Computer (1) dem Patienten zugeordnet ist und mit einer Applikation zum Speichern und Verwalten patientenbezogener Daten versehen ist,

wobei der zweite Computer (2) einer vom Patienten bezüglich dessen Gesundheitszustands konsultierten Konsultationsperson zugeordnet ist,

wobei das Herunterladen der zumindest einen Datei aus der verschlüsselten Cloud seitens des Patienten gegenüber der Konsultationsperson durch die folgenden Schritte autorisiert wird:

Herstellung einer Datenverbindung zwischen dem mobilen ersten Computer (1) und dem zentralen Serversystem,

Auswahl der zumindest einen Datei durch den Patienten mittels der Applikation,

Erzeugen eines Zugriffslinks durch den Patienten mittels der Applikation, wobei der Zugriffslink zum Zugreifen auf die zumindest eine Datei bestimmt ist und eine vorbestimmte Gültigkeitsdauer hat,

Auswahl oder Eingabe einer E-Mail-Adresse der Konsultationsperson durch den Patienten mittels der Applikation,

Übermitteln des Zugriffslinks per E-Mail an die Konsultationsperson,

Ausführen des Zugriffslinks durch die Konsultationsperson vom zweiten Computer (2) aus,

Herstellen einer verschlüsselten Datenverbindung zwischen dem zweiten Computer (2) und der verschlüsselten Cloud, wenn der Zugriffslink als gültig erkannt worden ist,

Herunterladen der zumindest einen Datei auf den zweiten Computer (2) über die verschlüsselte Datenverbindung zum Speichern und/oder Anzeigen auf dem zweiten Computer (2).

4. Verfahren nach einem der vorhergehenden Patentansprüche, wobei die zumindest eine Datei aus der folgenden Gruppe ausgewählt ist: Arztbrief, Krankenhausbericht, Behandlungsbericht, Gutachten, Impfpass, Allergiepass, Organspendeausweis, Röntgen-, CT- und/oder MRT-Bild.

5. Verfahren nach Patentanspruch 4, wobei das Röntgen-, CT- und/oder MRT-Bild im DICOM -Format gespeichert ist.

6. Verfahren nach einem der vorhergehenden Patentansprüche, wobei die Konsultationsperson ein Arzt, ein Therapeut, ein Radiologe, ein Heilpraktiker, ein Sanitäter oder eine mit einem aus diesen zusammenarbeitende Person ist.

7. Verfahren nach einem der vorhergehenden Patentansprüche, wobei das Verfahren den folgenden zusätzlichen Schritt umfasst:

Einloggen in der Applikation auf dem mobilen ersten Computer durch den Patienten.

8. Verfahren nach einem der vorhergehenden Patentansprüche, wobei das Verfahren die folgenden zusätzlichen Schritte umfasst:

Erfassen zumindest eines biometrischen Merkmals einer die Applikation verwendenden Person mittels des mobilen ersten Computers (1),

Identifizieren der die Applikation verwendenden Person als den für die Verwendung der Applikation autorisierten Patienten.

9. Verfahren nach einem der vorhergehenden Patentansprüche, wobei

die Datenverbindung zwischen dem mobilen ersten Computer (1) und dem zentralen Serversystem (5) und/oder die Datenverbindung zwischen dem zweiten Computer (2) und dem zentralen Serversystem (5) nach einem SSL-Standard verschlüsselt hergestellt wird.

10. Verfahren nach einem der vorhergehenden Patentansprüche, wobei die schutzbedürftigen Daten zum Gesundheitszustand des Patienten in der verschlüsselten Cloud und/oder auf dem mobilen ersten Computer (1) nach dem Advanced-Encryption-Standard verschlüsselt gespeichert sind.

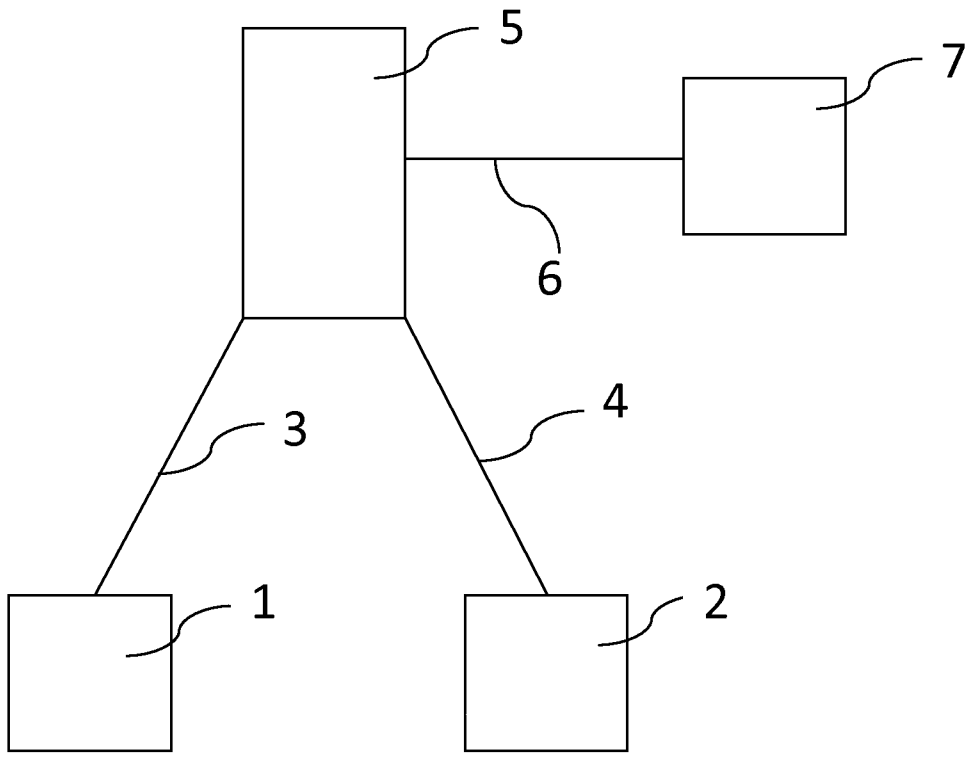

Fig. 1

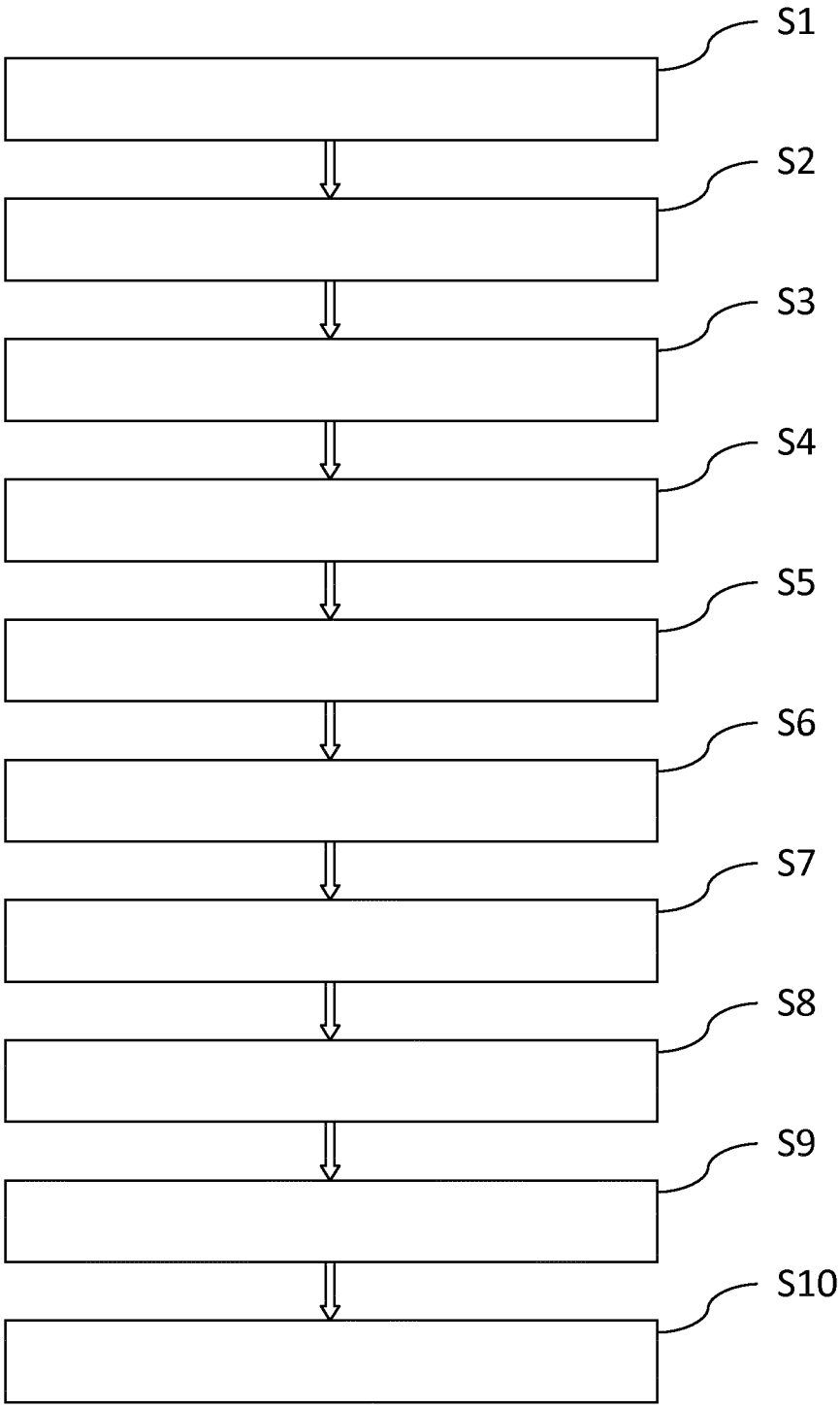

Fig. 2

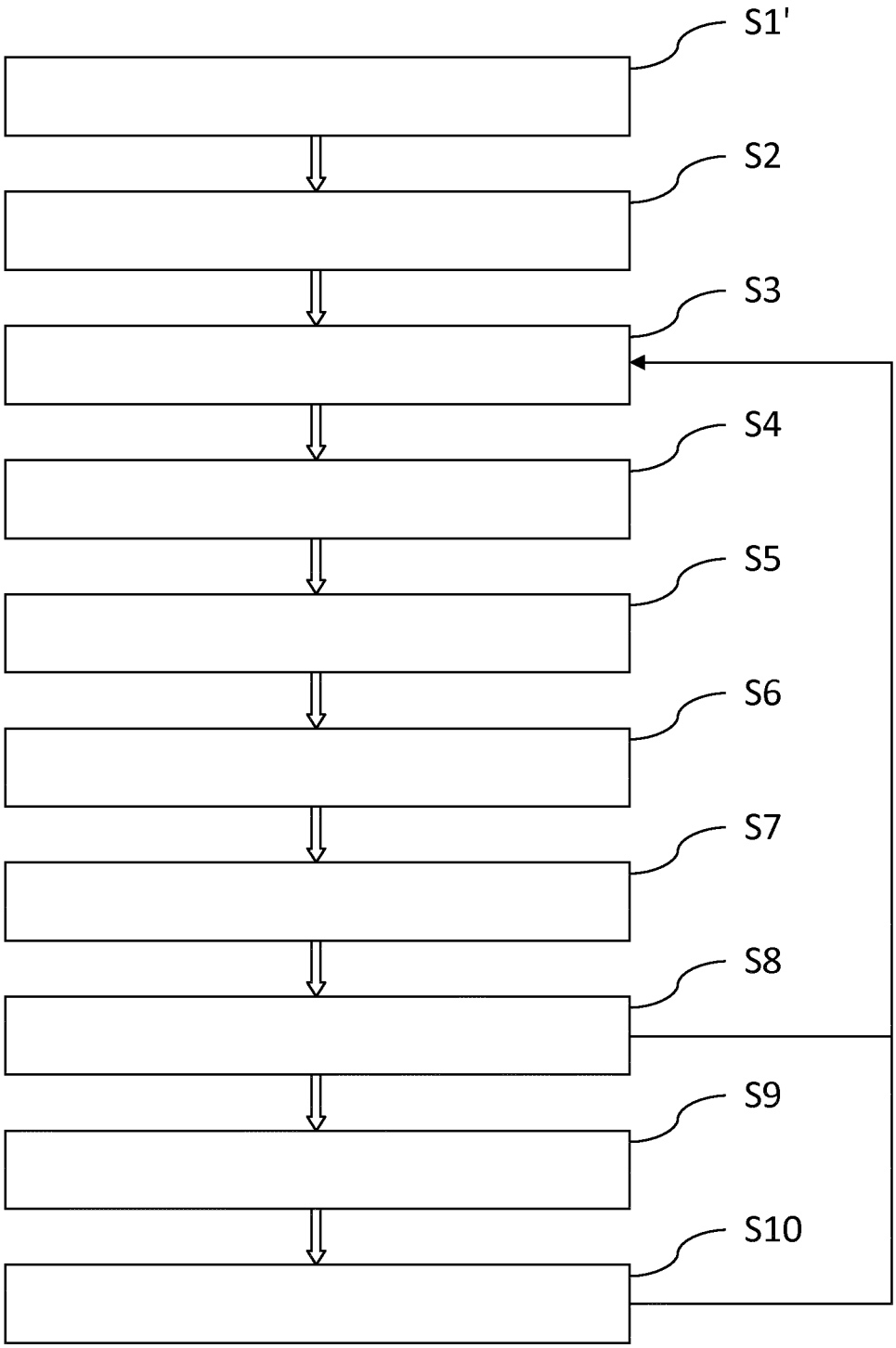

Fig. 3

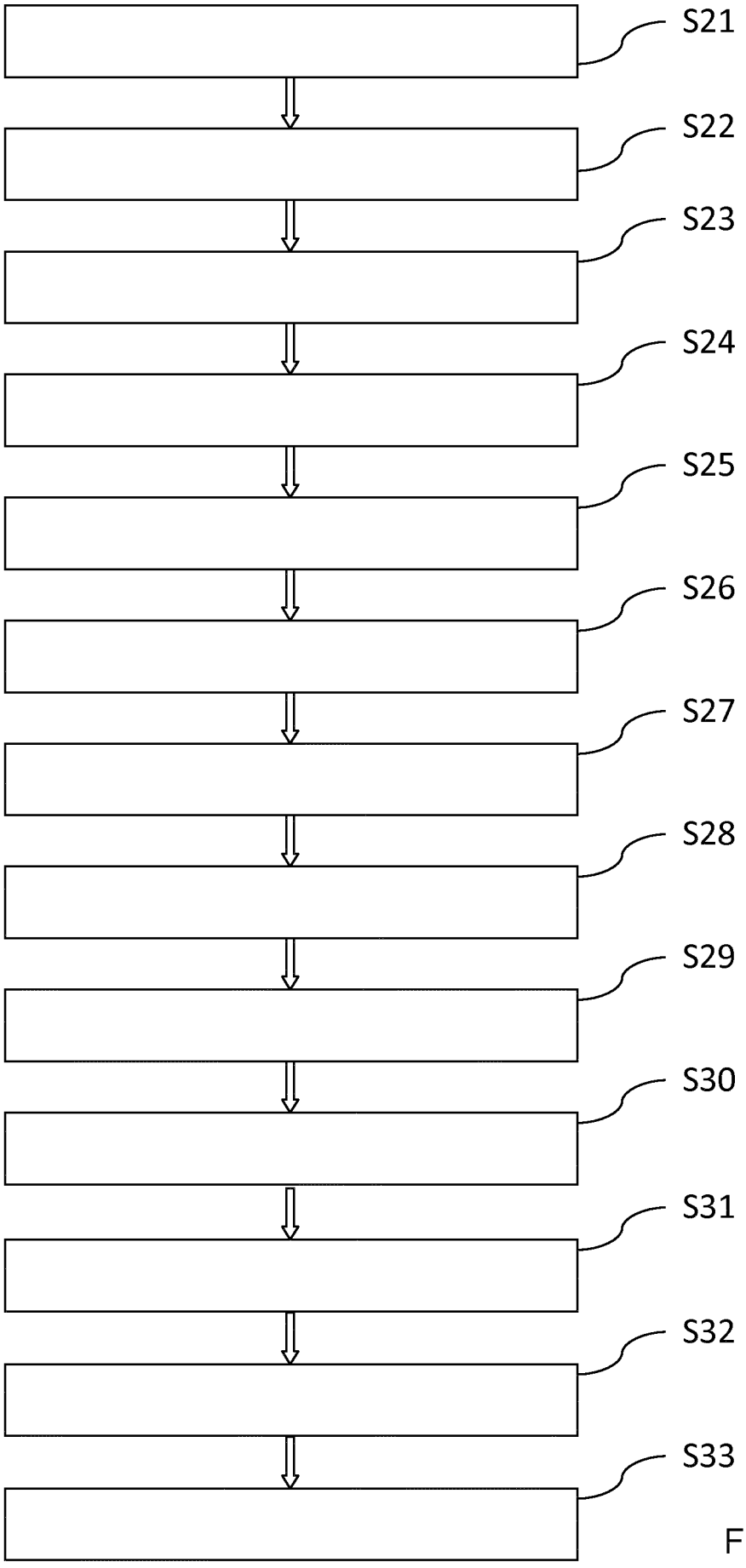

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/066875

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F19/00
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

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	US 2005/165627 A1 (FOTSCH EDWARD J [US] ET AL) 28 July 2005 (2005-07-28) abstract; figure 10 paragraphs [0076], [0078], [0108], [0107] paragraph [0093]; claim 23 -----	1-10

☐ Further documents are listed in the continuation of Box C.

☒ 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
24 September 2015	09/11/2015

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	Samulowitz, Michael

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2015/066875

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005165627 A1	28-07-2005	US 2005165627 A1	28-07-2005
		WO 2006102206 A2	28-09-2006

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2015/066875

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G06F19/00
ADD.

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G06F

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	US 2005/165627 A1 (FOTSCH EDWARD J [US] ET AL) 28. Juli 2005 (2005-07-28) Zusammenfassung; Abbildung 10 Absätze [0076], [0078], [0108], [0107] Absatz [0093]; Anspruch 23 -----	1-10

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ 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
24. September 2015	09/11/2015

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	Samulowitz, Michael

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2015/066875

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2005165627 A1	28-07-2005	US 2005165627 A1	28-07-2005
		WO 2006102206 A2	28-09-2006