(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
16. August 2012 (16.08.2012)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2012/107275 A1

(51) Internationale Patentklassifikation:
H04L 29/06 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2012/051047

(22) Internationales Anmeldedatum:
24. Januar 2012 (24.01.2012)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
102011003784.5 8. Februar 2011 (08.02.2011) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **HEIDENREICH, Georg** [DE/DE]; Eifelweg 22, 91056 Erlangen (DE). **LEETZ, Wolfgang** [DE/DE]; Ringstraße 24, 91080 Uttenreuth (DE).

(74) Gemeinsamer Vertreter: **SIEMENS AKTIENGESELLSCHAFT**; Postfach 22 16 34, 80506 München (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, 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, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

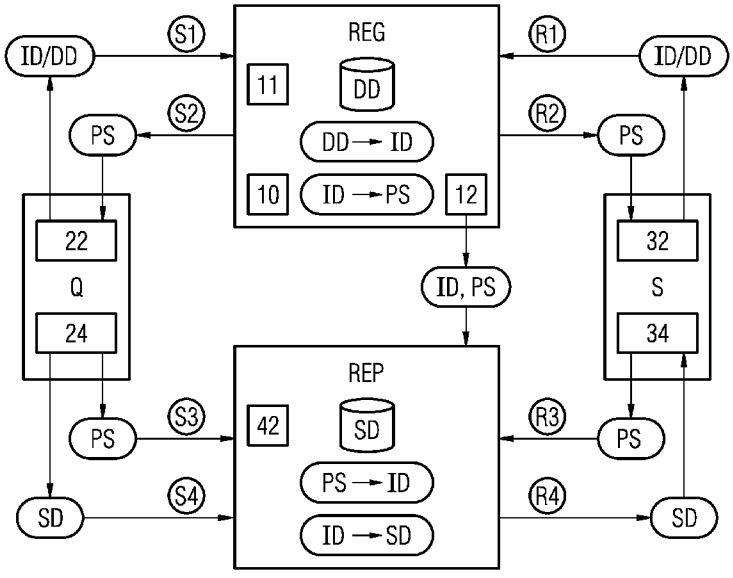
— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

[Fortsetzung auf der nächsten Seite]

(54) **Title**: SECURING ACCESS TO DISTRIBUTED DATA IN AN UNSECURE DATA NETWORK

(54) **Bezeichnung** : SICHERN VON ZUGRIFFEN AUF VERTEILTE DATEN IN EINEM UNSICHEREN DATENNETZ

FIG 1



(57) **Abstract**: The invention relates to a method and to a system, a registry, a repository and a computer program product for securely accessing sensitive medical data records stored in a repository (REP). Before accessing security-critical data (SD) in the repository (REP), a registration inquiry with a separate registry (REG) must be carried out in order to obtain a security token (PS) having limited temporary validity, for example in the form of a barcode. A data source (Q) and/or a data sink (S) can then use the security token (PS) to access the security-critical data (SD) in that an index module (42) indexes the data record inquired about on the repository (REG).

(57) **Zusammenfassung**: Die Erfindung betrifft ein Verfahren und ein System, eine Registry, ein Repository und ein Computerprogrammprodukt zum gesicherten Ausführen eines Zugriffs auf sensitive medizinische Datensätze, die in einem Repository (REP) gespeichert sind. Vor dem Zugriff auf sicherheitskritische Daten (SD) in dem Repository (REP) muss eine Registrierungsanfrage an eine separate Registry (REG) ausgeführt werden, um ein in seiner temporären Gültigkeit begrenztes Sicherheitstoken (PS), etwa in Form eines Barcodes, zu erhalten. Eine Datenquelle (Q) und/oder eine Datensenke (S) können dann mit dem Sicherheitstoken (PS) auf die sicherheitskritischen Daten (SD) zugreifen, indem ein Indexmodul (42) den angefragten Datensatz auf dem Repository (REG) indiziert.

WO 2012/107275 A1

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

Beschreibung

Sichern von Zugriffen auf verteilte Daten in einem unsicheren Datennetz

GEBIET DER ERFINDUNG

Die vorliegende Erfindung betrifft die Sicherheitstechnik und insbesondere die Zugriffssicherung von sicherheitskritischen Datensätzen in einem ungeschützten Netzwerk aus verteilten Datenbanken, wie zum Beispiel einem Cloudsystem. Des Weiteren betrifft die Erfindung das Gebiet der Medizintechnik, das sich insbesondere dadurch auszeichnet, dass sicherheitskritische Daten gespeichert und bereitgestellt werden müssen.

Gerade bei modernen Systemen ist es vorgesehen, die Datenhaltung möglichst flexibel zu gestalten, sodass die Daten von unterschiedlichen Systemen abrufbar und speicherbar sind und dabei insbesondere über das Internet kommunizieren.

HINTERGRUND DER ERFINDUNG - STAND DER TECHNIK

Insbesondere auf dem Gebiet der Medizintechnik ist es von daher eine notwendige Voraussetzung, die Zugriffe auf sicherheitskritische Daten vor unautorisierten Zugriffen zu schützen. Bei modernen Systemen, die einen Zugriff über das Internet zur Verfügung stellen, stellt dies eine hohe Gefahrenquelle dar. Unberechtigte Nutzer können Nachrichten illegal zwischen den einzelnen elektronischen Modulen abhören (Sender, Empfänger) - und dies in der Regel: ohne besonders hohen Aufwand betreiben zu müssen. Deshalb muss der Zugriff auf diese Daten einerseits hohen Sicherheitsanforderungen genügen. Andererseits ist es erforderlich, dass das System möglichst flexibel für einen Web-Einsatz und Zugriff z.B. von entfernten medizinischen Workstations ist und, dass jederzeit einzelne elektronische Instanzen hinzugeschaltet werden können. Des Weiteren ist der zu verwaltende Kreis von Usern, Applikationen und verteilten Datenbasen hoch. Auch das zu spei-

chernde hohe Datenvolumen muss bei der Auslegung von Sicherheitssystemen berücksichtigt werden.

Im Stand der Technik ist es bekannt, elektronische Datensätze vor einem unberechtigten Zugriff zu schützen. Dabei sind Verschlüsselungssysteme bekannt, die zum einen auf die Speicher (zum Beispiel auf die Festplatten der Computer) und zum anderen auf die Kommunikation zwischen den Netzwerkusern angewendet werden. Im Rahmen von Verschlüsselungssystemen, bei denen die Kommunikation (also die ausgetauschten Nachrichten) verschlüsselt werden, ist es im Stand der Technik bekannt, die Entschlüsslung jeweils auf Empfängerseite auszuführen. Dies stellt insofern ein Sicherheitsrisiko dar, als dass es grundsätzlich möglich ist, dass ein unberechtigter Nutzer die Nachricht - wenn auch in verschlüsselter Form - abfängt und diese in irgendeiner Form auf unberechtigte Weise verarbeitet, beschädigt oder unberechtigterweise weiterleitet. Darüber hinaus ist es im Stand der Technik bekannt, Indizes zur Suche bereitzustellen, um auf Datensätze in einem großen Datenbestand zugreifen zu können. Es sind jedoch keine Ansätze vorgesehen, um sicherheitskritische persönliche Daten zu sichern.

AUFGABE DER ERFINDUNG

Die vorliegende Erfindung hat sich deshalb zur Aufgabe gestellt, ein informationstechnologisches System bereitzustellen, das den Zugriff auf sicherheitskritische Daten, die in einem ungeschützten Netz kommuniziert werden, sichert und bei dem gleichzeitig eine Indexierung mit schneller Suchfunktion möglich ist. Des Weiteren soll der Datenzugriff auf sicherheitskritische Daten, insbesondere medizinische Datensätze eines Patienten, flexibler gestaltet werden unter Einhaltung von höchsten Sicherheitsanforderungen.

Auch soll eine informationstechnologische Infrastruktur bereitgestellt werden, mit der insofern Kosten gespart werden können, als dass der bisher notwendige lokale Schutz von

Festplatten in den einzelnen Systemen durch ein zentrales Schutzsystem ersetzt werden kann.

ALLGEMEINE BESCHREIBUNG DER ERFINDUNG

Die vorstehende Aufgabe wird durch die beiliegenden nebengeordneten Patentansprüche gelöst, insbesondere durch ein Verfahren, ein System, eine Registry, ein Repository und ein Computerprogrammprodukt.

Im Folgenden wird die Erfindung anhand der verfahrensgemäßen Ausführung beschrieben. Hierbei erwähnte Vorteile, alternative Ausführungsformen oder vorteilhafte Weiterbildungen sind ebenso auch auf die anderen Anspruchsformen, insbesondere auf das System, auf die Registry und/oder auf das Repository bzw. auf das Computerprogrammprodukt zu übertragen und umgekehrt. Mit anderen Worten kann auch das System (oder die anderen beanspruchten Gegenstände) mit Merkmalen weitergebildet sein, die im Rahmen des Verfahrens beschrieben und/oder beansprucht worden sind. Gemäß einer bevorzugten Ausführungsform handelt es sich bei dem Verfahren um ein computerimplementiertes Verfahren. Alternativen sehen hier jedoch vor, zumindest teilweise auf eine Hardwarelösung zurückzugreifen, sodass die einzelnen Schritte des Verfahrens durch entsprechende Hardwaremodule mit der entsprechenden Funktionalität ausgeführt werden, z.B. als Bauteile eines Microcontrollers oder Microprozessors. Dabei ist es grundsätzlich möglich, dass nicht alle Schritte des Verfahrens auf derselben Computerinstanz ausgeführt werden, sondern das Verfahren kann für ein verteiltes System ausgelegt werden, sodass einzelne Schritte auf einer ersten Computerinstanz und die anderen Schritte auf weiteren Computerinstanzen ausgeführt werden.

Ein Aspekt der Erfindung bezieht sich somit auf ein computerimplementiertes oder microprozessor-implementiertes Verfahren zum gesicherten Zugriff auf Datensätze in einer unsicheren Netzwerkumgebung, wie zum Beispiel dem Internet. Dabei interagieren unterschiedliche Hardwareinstanzen miteinander, die

voneinander vollständig getrennt sind, also mit anderen Worten in physikalischer Hinsicht entkoppelt sind:

- eine zentrale Registry, die als Computerinstanz zur Zugriffsregistrierung ausgebildet ist,

- zumindest ein separat von der Registry bereitgestelltes Repository, das zur Datenhaltung von sicherheitskritischen Daten bestimmt ist,

- zumindest eine Datenquelle und zumindest eine Datensenke.

Die Datenquelle und die Datensenke führen Zugriffe auf die Datensätze der Registry und/oder des Repository's aus. Vorzugsweise ist es vorgesehen, dass sich die Datenquelle oder die Datensenke zum Ausführen eines Zugriffs einmalig bei der Registry registrieren muss.

Wie vorstehend bereits erwähnt, bezieht sich die bevorzugte Ausführungsform auf eine Anwendung im medizintechnischen Gebiet, sodass es sich bei den Datensätzen um sicherheitskritische (Patienten-)Daten handelt. Daneben umfassen die Datensätze auch demographische Daten, wie zum Beispiel den Patientennamen, das Patientengeburtsdatum, den Patientenort, Versicherungsdaten etc, die regelmäßig geringere Sicherheitsanforderungen für einen Zugriff aufweisen, als die sicherheitskritischen Daten (zum Beispiel Anamnesedaten, Befunddaten, medizinische Bilder).

Vereinfachend kann davon ausgegangen werden, dass der erfindungsgemäße Vorschlag vier separate Computerinstanzen umfasst: eine Registry, ein Repository, eine Datenquelle (zum Beispiel ein medizinisches Bildgebungssystem oder ein Bildspeichersystem) und eine Datensenke (zum Beispiel eine Befundungsworkstation). Selbstverständlich liegt es ebenso im Rahmen der Erfindung, hier mehrere der vorstehend erwähnten Instanzen bereitzustellen, sodass beispielsweise eine Vielzahl

von Repositories mit einer Vielzahl von Datenquellen und einer Vielzahl von Datensenken interagieren, die jeweils über ein Kommunikationsnetz kommunizieren. Zum Zwecke der leichteren Verständlichkeit wird im Folgenden meist nur eine der oben erwähnten Instanzen beschrieben, ohne die Erfindung hierauf zu beschränken.

Ein wesentlicher Aspekt der vorliegenden Erfindung ist darin zu sehen, dass sicherheitskritische Daten einer Person niemals in einer gemeinsamen Nachricht - oder allgemein: niemals zusammen - mit personenidentifizierenden Daten über das Netzwerk (zum Beispiel das Internet als unsichere Netzwerkumgebung) kommuniziert werden. Dieser Ansatz bringt den wesentlichen Vorteil mit sich, dass selbst dann, falls ein unberechtigter Anwender den Datenverkehr abhört und Daten ermittelt, nicht in der Lage ist, diese einer Person zuzuordnen. Eine Zuordnung zwischen Person und sicherheitskritischen Daten wird damit auch bei abgefangenen Nachrichten nicht möglich.

Erfindungsgemäß umfasst das Verfahren folgende Verfahrensschritte:

- getrenntes Bereitstellen der sicherheitskritischen Daten und der demographischen Daten, indem die demographischen Daten in der Registry und die sicherheitskritischen Daten in dem Repository gespeichert werden;

- Registrierungsanfrage seitens der Datenquelle und/oder seitens der Datensenke an die Registry, um für den Zugriff auf einen einer Person zugeordneten Datensatz eine Registrierung in Form einer Zuweisung eines Sicherheitstokens zu erhalten;

- auf diese Registrierungsanfrage wird seitens der Registry ein Sicherheitstoken an die anfragende Datenquelle und/oder Datensenke ausgegeben, das eindeutig

einem personenidentifizierenden Datensatz zugeordnet werden kann;

- Senden einer Nachricht von der Registry an das Repository, umfassend das ausgegebene Sicherheitstoken und den zugeordneten personenidentifizierenden Datensatz. Dabei kann diese Nachricht als Grundlage für eine Mappingvorschrift verwendet werden, die – möglicherweise zu einem späteren Zeitpunkt- auf dem Repository auszuführen ist;

- Senden einer Zugriffsnachricht mit dem Sicherheitstoken oder mit einer für die Anfrage eindeutigen Kennung von der Datenquelle und/oder der Datensenke an das Repository zum Zugriff auf in dem Repository gespeicherte sicherheitskritische Daten; wobei wahlweise das Sicherheitstoken oder eine eindeutige Kennung, die ihrerseits dem Sicherheitstoken eineindeutig zugeordnet ist, gesendet werden können;

- Anwenden der Mappingvorschrift auf dem Repository, mit dem Sicherheitstoken der Zugriffsnachricht den personenidentifizierenden Datensatz zu berechnen. Der personenidentifizierende Datensatz soll erfindungsgemäß dann als Index bei der Adressierung des mit dem Zugriff angeforderten Datensatzes von sicherheitskritischen Daten verwendet werden;

- Ausführen des Zugriffs auf den (angeforderten) Datensatz über den personenidentifizierenden Datensatz als Index.

Im Folgenden werden die im Rahmen dieser Patentanmeldung verwendeten Begrifflichkeiten erläutert.

Die Datensätze umfassen zumindest zwei Datenanteile: Einen Anteil mit „sicherheitskritischen Daten", die ein maximales Maß von Schutzmaßnamen (höchste Sicherheitsanforderungen) er-

fordern und einen Anteil mit demographischen Daten, die geringere Schutzmaßnahmen und damit ein geringeres Maß an Sensitivität erfordern. Die hauptsächliche Anwendung des erfindungsgemäßen Verfahrens liegt auf dem Gebiet der Medizintechnik. Sicherheitskritische Daten sind hier z.B. Gesundheitsdaten eines Patienten, wie Befunddaten, medizinische Bilddaten, Anamnesedaten, Berichtsdaten etc. In alternativen Ausführungsformen sind hier jedoch auch Finanzanwendungen oder Versicherungsanwendungen, sowie beliebige andere Anwendungen, die die Verarbeitung von sicherheitskritischen Daten erfordern, möglich. Die "demographischen Daten" werden in der Fachliteratur auch als "öffentliche Daten" bezeichnet, da diese ohnehin auf mobilen Datenträgern veröffentlicht werden (zum Beispiel in Form einer Versicherungskarte (oder der geplanten Gesundheitskarte): Geburtsname, Geburtsdatum, etc.). Der Begriff "unsichere Netzwerkumgebung" soll beliebige Cloudsysteme oder Netzwerksysteme kennzeichnen, bei denen die computerbasierten Instanzen Daten austauschen. Sobald ein Netzwerk für eine beliebige Anzahl von Teilnehmern zum Datenaustausch offen ist, ist es im Sinne der Erfindung "unsicher". Dies gilt nicht nur für das Internet, sondern auch für Wide Area Networks (WAN) oder Local Area Networks (LAN), z.B. Firmennetze oder Kliniknetze oder Netzverbunde, oder für andere digitale Netze.

Die Begriffe "Registry" und "Repository" sollen computerbasierte, physikalische Hardwareinstanzen kennzeichnen, die externe oder interne Festplatten (z.B. RAID Systeme) oder andere Mittel zur Datenhaltung umfassen und Schnittstellen zur Kommunikation mit den anderen Instanzen. Darüber hinaus sind sie zur Speicherung von Mappingvorschriften (oder Abbildungsvorschriften) bestimmt, um Datensätze, die in deren Speicher abgelegt sind, zu indizieren. Sowohl die in der Registry als auch die in dem Repository abgelegten Datensätze sind über einen Index adressierbar bzw. indizierbar.

Bei dem „Identifikator" handelt es sich vorzugsweise um einen personenidentifizierenden Datensatz. Für den Fall der medi-

zintechnischen Verwendung hat dies schlicht den Hintergrund, dass sowohl die demographischen Datensätze (eines Patienten) als auch die sicherheitskritischen Datensätze (eines Patienten) genau einem Patienten zugeordnet können werden müssen. Die Zuordnung zwischen Identifikator und Person (als Patient) muss auf eineindeutige Weise möglich sein. Das System sieht hierfür vorzugsweise eine bijektive Abbildung vor. Fehler treten dann auf, wenn ein Identifikator unterschiedlichen Personen zugeordnet ist oder, wenn unterschiedliche Identifikatoren einer Person zugeordnet sind. Letzteres ist im Stand der Technik als Dublettenproblem bekannt. Beide Fälle müssen vermieden werden. Der Identifikator wird gemäß der erfindungsgemäßen Lösung vorzugsweise vom System selbst generiert und kann nach eigenen Sicherheitsvorkehrungen gebildet sein. In der Regel wird hier eine Kombination aus demographischen Daten gegebenenfalls mit weiteren identifizierenden Hinweisen verwendet(optional noch angereichert mit Angabe einer elektronischen Adresse der beteiligten computerbasierten Instanzen, einem Zeitstempel oder einer Zufallszahl oder weiteren Parametern). Alternativ ist es jedoch auch möglich, dass die externen Systeme, die Datenquelle und/oder die Datensenke einen eigenen Identifikator bereitstellen und verwenden. Dieser muss nicht notwendigerweise mit dem Identifikator des Systems übereinstimmen. Dann wird eine Zuordnung zwischen Datenquellen/Datensenken-ID und interner ID vorgenommen. Diese Zuordnung kann evtl. auftretende Dubletten in der Registry zusammenführen.

In der Registry sind die demographischen Daten gespeichert. Darüber hinaus ist eine Zuordnung (vorzugsweise in Form einer Tabellen-Datenstruktur) gespeichert:

- Personenidentifizierender Identifikator - demographische Daten.

Da die Sicherheitstoken vorzugsweise nicht wiederholt verwendet werden, ist es erfindungsgemäß auch nicht vorgesehen, diese zu speichern, da dies mit einem Sicherheitsrisiko ver-

bunden wäre. Die Zuordnung „Sicherheitstoken – Identifikator" muss zwar verfügbar sein, aber nicht gespeichert werden.

In dem Repository sind die sicherheitskritischen Daten gespeichert. Darüber hinaus umfasst das Repository auch zwei Zuordnungen (vorzugsweise wieder in Form von Tabellen-Datenstrukturen):

1. Zuordnung zwischen personenidentifizierendem Identifikator - sicherheitskritischer Datensatz und

2. Zuordnung zwischen Sicherheitstoken - personenidentifizierender Identifikator.

Wie vorstehend bereits erwähnt, ist es erfindungsgemäß vorgesehen, dass der personenidentifizierende Identifikator vorzugsweise vom internen System generiert wird, das die Registry verwaltet. Dabei verwendet das Repository lediglich die von der Registry mit dem Sicherheitstoken versendeten Identifikatoren.

Der Begriff "Datenquelle" meint computerbasierte Instanzen, die Datensätze generieren und an das Repository zum Speichern versenden, um sie dort für andere Instanzen zugreifbar zu machen. Die Datenquellen können Computer, Computernetzwerke, Geräte, wie beispielsweise Laborgeräte, bildgebende medizinische Systeme etc. sein. Sie kommunizieren vorzugsweise über ein bestimmtes Protokoll, insbesondere das DICOM-Protokoll (DICOM: Digital Imaging and Communications in Medicine).

Die "Datensenke" bezieht sich ebenfalls auf computerbasierte Instanzen, die wie Clients fungieren und Daten von dem Repository abfragen. Dabei handelt es sich um Workstations, um mobile Geräte (PDA, Laptop, etc.) oder andere elektronische Module. Vorzugsweise umfasst das erfindungsgemäße Zugriffssystem eine zentrale Registry, eine Vielzahl von Repositories, eine Vielzahl von Datenquellen und eine Vielzahl von Datensenken. Alternativ sind hier auch andere Ausführungen

denkbar, sodass beispielsweise mehrere Registries vorgesehen sein können, die von einer übergeordneten Instanz verwaltet werden. Ebenso kann nur ein Repository, das dann als zentraler Speicher fungiert, vorgesehen sein. Wesentlich ist, dass alle beteiligten Instanzen räumlich bzw. physikalisch getrennte Einheiten sind und über ein offenes Netzwerk miteinander interagieren (zum Beispiel über das Internet).

Bei dem "Sicherheitstoken" handelt es sich vorzugsweise um ein digitales Pseudonym. Es existiert somit eine eindeutige Zuordnung zwischen einem personenidentifizierenden Datensatz und dem Pseudonym. Wesentlich für die Generierung des Pseudonyms ist es, dass von dem Pseudonym nicht auf personenbezogene Datensätze geschlussfolgert werden kann. Mit anderen Worten kann ein unberechtigter Nutzer, der das Pseudonym "abhört" keine Rückschlüsse auf die Person oder für die Person gespeicherte Datensätze (sicherheitskritische oder demographische Daten) ausführen. In einer alternativen Ausführungsform ist es auch möglich, das Sicherheitstoken als Hardwaremerkmal auszubilden und beispielsweise in der Form eines Sicherheitsmerkmals (Hardwarebauteil mit integriertem Sicherheitschip etc.) bereitzustellen.

Ein wesentlicher Vorteil der erfindungsgemäßen Lösung ist darin zu sehen, dass auch während des Betriebs des erfindungsgemäßen Verfahrens, das System flexibel auf weitere Anforderungen angepasst werden kann. So ist es beispielsweise möglich, dass auch während des Betriebs Repositories, Datenquellen und/oder Datensenken verändert werden können (zum Beispiel hinzugefügt oder gelöscht bzw. geändert). Damit kann das System an die jeweils aktuellen Anforderungen angepasst werden und ist damit skalierbar.

Gemäß einer bevorzugten Ausführungsform ist es vorgesehen, dass das Kommunikationsprotokoll zur Kommunikation zwischen den beteiligten Instanzen asynchron ist. Dies (ist in der Praxis sehr verbreitet und) hat den Vorteil, dass Nachrichten, die zwischen den beteiligten Instanzen ausgetauscht wer-

den, zu beliebigen Zeitpunkten beantwortet werden können. Es liegt jedoch ebenso im Rahmen der Erfindung ein synchrones Kommunikationsprotokoll oder eine Mischung von asynchronem und synchronem Protokoll zu verwenden.

Vorzugsweise wird das Pseudonym bzw. das Sicherheitstoken vom System generiert. In einer bevorzugten Ausführungsform erfolgt dies direkt auf der Registry. Alternativ ist es auch möglich, das Pseudonym auf anderen computerbasierten Instanzen (zum Beispiel durch den Einsatz eines Zufallsgenerators) zu generieren und dann über eine Schnittstelle an die Registry zu übertragen. Wesentlich ist, dass die Datenquelle eine Anfrage zur Registrierung mit einem Identifikator an die Registry sendet. Dabei kann der Identifikator ein solcher sein, der von der Datenquelle generiert wurde und die Datensätze in der Datenquelle identifiziert. Alternativ kann der Identifikator auch ein systeminterner Identifikator sein, der die Datensätze in Registry/Repository identifiziert. Auf die Anfrage der Datenquelle mit dem Identifikator erzeugt die Registry das jeweilige Pseudonym (das Sicherheitstoken) und ordnet somit eindeutig einen Identifikator ein Pseudonym zu. Als Antwort auf die Anfrage sendet die Registry dann das Pseudonym an die anfragende Datenquelle.

Dasselbe Verfahren wird bei einer Anfrage der Datensenke angewendet. In diesem Fall sendet die Datensenke eine Registrierungsanfrage mit einem Identifikator an die Registry. Diese erzeugt auf den Identifikator das Sicherheitstoken und ordnet es dem Identifikator (systemintern) zu. Als Antwort auf die Anfrage sendet die Registry dann das Pseudonym (das Sicherheitstoken) an die anfragende Datensenke.

In beiden der vorstehend genannten Fälle (Registrierungsanfrage der Datenquelle und Registrierungsanfrage der Datensenke) ist es möglich, dass die Registry auf zwei unterschiedliche Arten antwortet:

1. Die Registry sendet jeweils nur das Sicherheitstoken als Antwort zurück. Die anfragende Instanz (Datenquelle/Datensenke) ordnet dann aufgrund der Sequenz der jeweiligen Nachrichten das erhaltene Sicherheitstoken dem jeweiligen Identifikator zu oder

2. die Registry sendet nicht nur das Sicherheitstoken als Antwort zurück, sondern zusätzlich zu dem Sicherheitstoken den dem Sicherheitstoken jeweils zugeordneten Identifikator (oder den der Anfrage jeweils zugeordneten Identifikator). Dabei ist die Zuordnung Identifikator – Sicherheitstoken eindeutig bzw. im mathematischen Sinne injektiv. Bei einer späteren, erneuten Anfrage wird erfindungsgemäß aus Sicherheitsgründen nicht das gleiche Token verwendet. Damit muss die anfragende Instanz (Datenquelle/Datensenke) keine Verwaltung der Nachrichten ausführen und kann unmittelbar die Zuordnung Identifikator und Sicherheitstoken aus der Antwort der Registry entnehmen.

Nachdem die Registry die Zuordnung zwischen Identifikator und Sicherheitstoken ausgeführt hat und die anfragende Instanz beantwortet hat, sendet die Registry eine Nachricht an das Repository, um auch das Repository über die Zuordnung zwischen Identifikator und Sicherheitstoken zu informieren.

In einer bevorzugten Ausführungsform ist es vorgesehen, dass das Sicherheitstoken nur eine temporäre Gültigkeit hat und somit nach einer konfigurierbaren Zeitspanne automatisch verfällt. Nach Ablauf dieser Zeitspanne wären Zugriffe auf Daten mit dem Sicherheitstoken nicht mehr möglich. Die Gültigkeit der Sicherheitstoken wird vom Repository verwaltet. Alternativ ist es auch möglich, die Sicherheitstokens von der Registry zu verwalten und entsprechende Nachrichten an das Repository zu übermitteln.

Nach Ausführung der vorstehend genannten Schritte sind sowohl die anfragende Instanz (Datenquelle oder Datensenke) und das Repository über das aktuell vergebene Sicherheitstoken informiert.

Daraufhin ist es möglich, dass die anfragende Instanz (Datenquelle, Datensenke) eine Zugriffsanfrage an das Repository sendet, da sie zum Zugriff registriert ist (nämlich durch den Besitz eines Sicherheitstokens). Die Datenquelle/Datensenke sendet eine Zugriffsnachricht, umfassend das Sicherheitstoken, an das Repository.

In einem nächsten Schritt kann das Repository aus dem empfangenen Sicherheitstoken und aus der Mappingvorschrift, die es von der Registry empfangen hat (Zuordnung zwischen Identifikator und Sicherheitstoken) auf eindeutige Weise auf den Identifikator schließen. Dies erfolgt vorzugsweise unter Zugriff auf eine Tabelle.

In einem weiteren Schritt kann dann auf eine weitere Tabelle in dem Repository zugegriffen werden. Dazu wird der im ersten Schritt berechnete Identifikator verwendet, um mit dem Identifikator auf den angeforderten Datensatz von sicherheitskritischen Daten zu schließen. Mit anderen Worten dient der berechnete Identifikator als Index für den Zugriff auf den angeforderten sicherheitskritischen Datensatz. Im nachfolgenden Schritt kann dann dieser Datensatz je nach Zugriffsform verändert werden.

Falls der Zugriff von der Datenquelle ausgeführt worden ist, ist ein Schreibzugriff vorgesehen, sodass die Datenquelle die "neuen" sicherheitskritischen Daten an das Repository sendet, um sie dort unter dem Identifikator zu speichern bzw. um den identifizierten sicherheitskritischen Datensatz entsprechend zu überschreiben oder zu modifizieren.

Falls die anfragende Instanz die Datensenke gewesen ist, soll ein Lesezugriff ausgeführt werden. Dann wird der indexierte

sicherheitskritische Datensatz des Repositories als Antwort auf die Zugriffsanfrage (Zugriffsnachricht) an die Datensenke gesendet. Erfindungsgemäß sind hierfür zwei Varianten vorgesehen:

1. Auf Anfrage eines Lesezugriffs der Datensenke kann das Repository antworten, indem es den indexierten Datensatz von sicherheitskritischen Daten an die Datensenke sendet. In diesem Fall erhält die Datensenke als Antwort auf ihre Leseanfrage lediglich den Datensatz. Die Verwaltung der empfangenen Nachrichten und insbesondere der Datensätze obliegt dabei der Datensenke. Die Datensenke muss aus der empfangenen Nachricht des Repositories mit den angeforderten sicherheitskritischen Daten eine Zuordnung zwischen dem Identifikator finden. Dies wird durch die Sequenz der ausgetauschten Nachrichten bzw. durch entsprechende Zeitstempel möglich.

2. Auf Anfrage der Datensenke für einen Lesezugriff auf sicherheitskritische Daten antwortet das Repository nicht nur mit dem Versenden einer Nachricht mit den angeforderten sicherheitskritischen Daten, sondern es wird eine Kombination(es kann auch ein anderweitiges Paket von möglicherweise unterschiedlichen Nachrichtenformaten: z.B. digital und per Post versendet werden), vorzugsweise jedoch in Form eines Tupels, versendet, umfassend: die angeforderten sicherheitskritischen Daten und zusätzlich das Sicherheitstoken, das diesen Daten zugeordnet ist (oder ein Identifikator, der der Anfrage zugeordnet ist). In diesem Fall muss die Datensenke keine weiteren Verwaltungsschritte ausführen, sondern sie kann aufgrund der empfangenen Antwortnachricht des Repositories direkt auf die Zuordnung zwischen Identifikator und sicherheitskritischen Daten schließen.

Vorteil der ersten Variante ist darin zu sehen, dass die Sicherheit noch weiter erhöht werden kann, da die sicherheitskritischen Daten von dem Repository an die Datensenke lediglich alleine und ohne weiteres Sicherheitstoken (was indirekt einen Schluss auf die Person ermöglicht) versendet wird.

Eine Alternative ist auch darin zu sehen, dass bei einem Lesezugriff der Datensenke das Repository als Antwort zwei Nachrichten sendet: zum Einen eine Nachricht mit den angeforderten sicherheitskritischen Daten und zum Anderen eine zweite Nachricht, die davor oder zeitlich danach liegen kann, das jeweils zugeordnete Sicherheitstoken. In dieser Ausführungsform entfällt der Verwaltungsaufwand auf der Datensenke. Dennoch kann die Sicherheitsstufe erhöht werden, da die sicherheitskritischen Daten ohne weiteren Zusatz verwendet.

Diese Ausführungen bestehen auch für den Schreibzugriff der Datenquelle auf das Repository:

1. Die Datenquelle sendet, z.B. zeitlich versetzt oder in unterschiedlichen Datenformaten, zwei unterschiedliche Nachrichten an das Repository. In einer ersten Nachricht sendet sie das Sicherheitstoken, das vom Repository zur Indizierung des jeweiligen Datensatzes verwendet wird. In einer zweiten Nachricht sendet sie die jeweiligen sicherheitskritischen Daten für den Schreibzugriff. Das Repository indiziert die so empfangenen Daten mit dem zuvor empfangenen Identifikator, der aus dem Sicherheitstoken abgeleitet wird.

2. In einer zweiten Variante sendet die Datenquelle nicht zwei getrennte Nachrichten, sondern lediglich eine Nachricht, die sowohl das Sicherheitstoken und zusätzlich die sicherheitskritischen Daten umfasst. Das Repository verwendet das Sicherheitstoken wiederum dazu, die sicherheitskritischen Daten zu indizieren.

Vorzugsweise werden die sicherheitskritischen Daten direkt auf dem Repository gespeichert. Alternativ ist es vorgesehen, dass das Repository lediglich Verweise (Links) auf die sicherheitskritischen Daten umfasst, die auf einer anderen Instanz abgelegt sind. Dabei stehen das Repository und die weitere Instanz in Datenaustausch.

Aufgrund des asynchronen Protokolls ist es möglich, dass eine Datenquelle einen Schreibzugriff auf das Repository ausführt, während die Datensenke gleichzeitig einen Lesezugriff auf einen anderen Datensatz des Repositories beantragt bzw. ausführt. Des Weiteren ist es möglich, dass die Verfahrensschritte zur Registrierung der anfragenden Instanz (Datenquelle, Datensenke) zeitlich unabhängig von dem jeweiligen Datenzugriff der anfragenden Instanz auf das Repository ausgeführt werden können. Dabei ist lediglich die zeitliche Gültigkeitsdauer des Sicherheitstokens zu berücksichtigen. Bis auf das Einhalten dieser Gültigkeitsdauer kann der Registrierungsvorgang zu einem beliebigen Zeitpunkt vor dem Ausführen des Zugriffs ausgeführt werden. Damit kann das Verfahren noch flexibler gestaltet werden.

Ein wesentlicher Vorteil der erfindungsgemäßen Lösung ist darin zu sehen, dass der Zugriff auf die sicherheitskritischen Daten in dem Repository wesentlich schneller ausgeführt werden kann, da eine direkte Indizierung mit dem eindeutigen Identifikator möglich ist. Damit können die im Repository gespeicherten Datensätze gezielt adressiert werden und zwar nicht nur innerhalb des Repository‘s, sondern auch von den anfragenden Instanzen, nämlich der Datenquelle und der Datensenke.

Des Weiteren wird die Sicherheit des Zugriffssystems deutlich erhöht, da, wie vorstehend erwähnt, lediglich Nachrichten von unterschiedlichen Instanzen ausgetauscht werden, wobei niemals in einer Nachricht gemeinsam personenbezogenen Datensät-

ze mit sicherheitskritischen Daten verwendet werden. Mit anderen Worten, werden die beteiligten physikalischen Instanzen (Datenquelle, Datensenke, Registry und Repository) so weit voneinander getrennt, dass auch ein ungesichertes Netzwerk, wie das Internet, für den Datenaustausch von sicherheitskritischen Daten verwendet werden kann, und wobei zudem die Daten auf maximale Weise vor unberechtigtem Zugriff geschützt sind, selbst dann, wenn die Nachrichten abgehört werden.

Ein wichtiger Vorteil ist auch darin zu sehen, dass der Zugriff deutlich beschleunigt werden kann, da die einzelne Festplatten des Repository's nicht, wie bisher notwendig, in dem gleichen Maße zugriffsgeschützt werden müssen, was den Zugriff grundsätzlich beschleunigt, da die sicherheitskritischen Daten erfindungsgemäß nicht mit personenidentifizierenden Hinweisen kommuniziert werden.

Ein wesentlicher Aspekt der Erfindung ist auch darin zu sehen, dass zwei unterschiedliche Identifikationsmerkmale verwendet werden: zum Einen der personenidentifizierende Identifikator, der für eine Person gilt und dies lebenslang und zum anderen das Sicherheitstoken, das vom System generiert wird und nur temporäre Gültigkeit hat. Ein Dritter darf nicht von dem Identifikator auf das Sicherheitstoken schließen können. Ebenso wenig darf ein Dritter umgekehrt von dem Sicherheitstoken auf den Identifikator schließen können. Grundsätzlich sollte ein Identifikator eine Person eineindeutig identifizieren. Mit anderen Worten ist eine bijektive Abbildung zwischen realer Person und Identifikator vorgesehen. In gängigen IT-Gesundheitssystemen werden aus Sicherheitsgründen sogenannte Dubletten jedoch geduldet. Damit kann eine Person prinzipiell auch unterschiedliche Identifikatoren haben. Das Repository kann erfindungsgemäß anhand externer demographischer Merkmale diese Dubletten stets auflösen und dazu den oben beschriebenen Vorgang der Versendung von Sicherheitstoken entsprechend mehrfach ausführen. Diese Auflösung kann als Verfahren in der Registry jederzeit eingeführt, modifiziert

oder unterbunden werden, ohne dauerhafte Datenbestände zu verändern.

Üblicherweise wird der Identifikator von der Registry generiert. Dazu können unterschiedliche Mechanismen vorgesehen sein. Üblicherweise wird eine Hash-Funktion auf eine Kombination von unterschiedlichen Parametern ausgeführt, umfassend alle oder ausgewählte der folgenden Daten: Demographische Daten, eine lokale Zeitangabe, gegebenenfalls ein Regionalkennung, die eindeutig für das Netzwerk ist und gegebenenfalls noch weitere Parameter. Alternativ ist es möglich, den Identifikator nicht von der Registry erzeugen zu lassen, sondern von einer anderen Instanz, beispielsweise von der anfragenden Instanz (Datenquelle, Datensenke) oder anderen Instanzen und diese an die Registry weiterzuleiten. Auf jeden Fall muss sichergestellt sein, dass ein Dritter nicht aus dem Wissen eines Sicherheitstokens auf ein anderes Sicherheitstoken schließen kann.

In diesem Zusammenhang ist darauf hinzuweisen, dass die Mechanismen zum Generieren des Sicherheitstokens den Gegenstand der vorliegenden Erfindung nicht beschränken. Mit anderen Worten sind auch unterschiedliche Methoden zur Tokengenerierung möglich. So ist beispielsweise das Anwenden einer Hash-Funktion auf folgende Parameter möglich: einen GUID (globally unique identifier), der von der Betriebssystemplattform auf Anfrage gebildet wird, die lokale Uhrzeit, eine Zufallszahl und/oder die Ablaufzeit der Gültigkeit des neuen Sicherheitstokens.

Eine weitere Lösung der vorstehend genannten Aufgabe besteht in einem System zum gesicherten Zugriff auf Datensätze gemäß dem beiliegenden Anspruch. Das System umfasst in physikalischer Hinsicht voneinander getrennte Hardwareinstanzen: vorzugsweise eine zentrale Registry, zumindest ein Repository und eine Vielzahl von Datenquellen und eine Vielzahl von Datensenken.

Die Registry ist erfindungsgemäß durch ein Benachrichtigungsmodul erweitert, das dazu ausgebildet ist, eine Nachricht von der Registry an das Repository zu senden, um das Repository über die aktuell ausgegebenen Sicherheitstoken zu den jeweils zugeordneten Identifikatoren zu informieren.

Die Datenquelle ist erfindungsgemäß mit einem Registriermodul ausgebildet, das dazu bestimmt ist, eine Registrierungsanfrage an die Registry zu senden und deren Ergebnis (mit dem Sicherheitstoken) zu empfangen. Darüber hinaus ist die Datenquelle mit einem Zugriffsmodul ausgebildet, um einen Schreibzugriff mit sicherheitskritischen Daten und mit dem Sicherheitstoken auf das Repository auszuführen.

Ebenso ist die Datensenke mit einem Registriermodul ausgebildet, um die Registrierungsanfrage an die Registry zu senden und deren Ergebnis (Sicherheitstoken) zu empfangen. Darüber hinaus ist die Datensenke mit einem Zugriffsmodul ausgebildet, um den Lesezugriff der Datensenke auf Datensätze des Repositories auszuführen. Es dient dazu, einen Lesezugriff mit dem Sicherheitstoken an das Repository zu senden und die Antwort des Repository‘s, umfassend die angefragten sicherheitskritischen Daten, die dem Sicherheitstoken zugeordnet sind, zu empfangen.

Das Repository ist erfindungsgemäß weitergebildet mit einem Indexmodul, das zum Zugriff auf zwei Tabellen ausgebildet ist, um aus dem Sicherheitstoken der anfragenden Instanz einen Identifikator abzuleiten und um - in einem zweiten Schritt - aus dem abgeleiteten Identifikator den angefragten sicherheitskritischen Datensatz zu indizieren und für den Zugriff vorzubereiten.

Die vorstehend im Zusammenhang mit dem Verfahren erwähnten alternativen Ausbildungsformen der Erfindung sind ebenso auch auf das System mit den Modulen anzuwenden.

Eine weitere Lösung besteht in einer Registry und in einem Repository gemäß den beiliegenden Ansprüchen, sowie in einem Computerprogrammprodukt. Das Computerprogrammprodukt kann ein Computerprogramm umfassen, das auf einem Speichermedium (zum Beispiel auf einem mobilen Datenträger oder auf einem internen Speicher eines Computers) gespeichert sein kann. Ebenso ist es möglich, das Computerprogramm als verteiltes System bereitzustellen, sodass einzelne Module, die durch die einzelnen Funktionen der Verfahrensschritte definiert sind auf den unterschiedlichen Instanzen des Systems ausgeführt werden. Dabei ist es möglich, dass einzelne Teile des Computerprogramms zum Download bereitgestellt werden.

FIGURENBESCHREIBUNG

In der nachfolgenden, detaillierten Figurenbeschreibung werden nicht einschränkend zu verstehende Ausführungsbeispiele mit deren Merkmalen und weiteren Vorteilen anhand der Zeichnung beschrieben. In dieser zeigen:

Figur 1 zeigt eine schematische, übersichtsartige Darstellung eines erfindungsgemäßen Systems gemäß einer bevorzugten Ausführungsform und dabei ausgetauschten Nachrichten in zeitlicher Reihenfolge und

Figur 2 eine schematische Darstellung von beteiligten physikalischen Instanzen in einer Gesamtdarstellung und

Figur 3 eine schematische Darstellung von zwischen den einzelnen Instanzen ausgetauschten Nachrichten und physikalischen Merkmalen und

Figur 4 eine schematische Darstellung von ausgetauschten Nachrichten zwischen einer Registry und einer Datenquelle/Datensenke zum Zwecke der Registrierung.

Im Folgenden wird die Erfindung im Zusammenhang mit einem Ausführungsbeispiel unter Bezugnahme auf Figur 1 näher erläutert.

Die Erfindung betrifft ein System und ein Verfahren zum gesicherten Zugriff auf Datensätze in einer unsicheren Netzwerkumgebung, wie zum Beispiel im Internet. Dabei stehen die beteiligten Hardwareinstanzen über das Internet in Datenaustausch, wie Speicherinstanzen, umfassend eine Vielzahl von Festplatten, eine Vielzahl von Datenquellen Q, die Daten zur Verfügung stellen (diese haben je nach Applikation unterschiedlichen Inhalt), eine Vielzahl von Datensenken S, die Daten anfordern .

Wie in Figur 2 schematisch dargestellt ist in einer bevorzugten Ausführungsform der Erfindung eine zentrale Registry REG vorgesehen, die über das Internet mit weiteren Hardwareinstanzen kommuniziert: mit einer Vielzahl von Datenquellen Q_1, Q_2, einer Vielzahl von Repositories REP_1, REP_2, REP_3, einer Vielzahl von Datensenken S_1, S_2, etc. Alternativ ist es auch möglich, dass nicht nur eine zentrale Registry REG vorgesehen ist, sondern auch hier mehrere Registry-Instanzen bereitgestellt werden, die von einer übergeordneten Instanz verwaltet werden. Beim Datenaustausch muss dann die jeweils angesprochene Registry adressiert werden. Die anderen Instanzen Datenquelle Q, Repository REP und Datensenke S stehen über das Internet in Datenaustausch.

In Figur 1 ist der Übersichtlichkeit und Einfachheit halber nur eine Datenquelle Q, ein Repository REP und eine Datensenke S dargestellt, um den Datenaustausch zwischen diesen Instanzen zu erläutern. Wie vorstehend erwähnt, werden in der Realität eine Vielzahl von Datenquellen Q, Repositories REP und Datensenken S bereitgestellt werden.

In einer hauptsächlichen Ausführungsform der Erfindung betrifft das Verfahren ein Bereitstellen zum gesicherten

Zugriff auf medizinische oder gesundheitsbezogene Datensätze über das Internet. Die Datenquellen Q sind medizinische Bildgebungssysteme, Archivierungssysteme, wie zum Beispiel PACS-Systeme (Picture Archiving and Communication Systems), die selbst üblicherweise als Netzwerk implementiert sind und auf eine Cloud von Repositories REP zugreifen. Selbstverständlich können die Datenquellen Q auch über einen lokalen Speicher verfügen. Grundsätzlich können die Datenquellen Q von unterschiedlichen Hardware- oder Computer-basierten Instanzen ausgebildet sein, die in der jeweiligen Anwendung in der Rolle als Bereitsteller von Daten (Supplier) oder Sender dienen. Die Datensenken S können beispielsweise beliebige Clients sein, die an Workstations arbeiten, um beispielsweise medizinische Befunde zu sichten oder Patientendaten anderweitig zu verarbeiten. Je nach Anwendung können die Datensenken aus unterschiedlichen Computer-basierten Bauteilen gebildet sein, die in der Rolle sicherheitskritische Daten anfordern.

Die vorliegende Erfindung entstammt der grundsätzlichen Problemstellung, wie sicherheitskritische Daten (zum Beispiel medizinische Patientendaten oder andere zu sichernde finanzielle Daten eines Users) in einem Netzwerk schnell und sicher übertragen werden können, und wobei gleichzeitig ein möglichst flexibler Zugriff von allen beteiligten Instanzen auf die jeweiligen sicherheitskritischen Daten möglich ist. Das höchste Maß an Flexibilität kann bei heutigen Anwendungen über die Zugriffsmöglichkeit über das Internet bereitgestellt werden. Der Datenaustausch über das Internet ist aber höchst unsicher, da er von unberechtigten Dritten abgehört werden kann, sodass die abgefangenen Daten missbraucht werden können. Somit sind die beiden vorstehend genannten Zielsetzungen eigentlich widersprüchlich und dichotom bzw. komplementär. Ein Fachmann denkt bei der Problemstellung, den Datenaustausch sicherer zu machen, grundsätzlich nicht daran, das ungeschützte Internet zu verwenden. Die erfindungsgemäße Lösung legt dennoch ein System vor, bei dem das Internet verwendet werden kann, bei dem aber der Datenaustausch zwischen den beteiligten Instanzen über das Internet insofern höchsten Si-

cherheitsanforderungen genügt, weil niemals Nachrichten ausgetauscht werden, die personenidentifizierende Daten gemeinsam mit sicherheitskritischen Daten kommunizieren.

Grundsätzlich bezieht sich das vorgeschlagene System bzw. Verfahren zum Zugriff auf sensitive Daten bzw. Daten mit unterschiedlichen Sicherheitsstufen. Je nach Anwendung kann es sich hier beispielsweise um Gesundheitsdaten eines Patienten handeln oder um finanzielle Daten eines Anwenders handeln. Dabei ist es vorgesehen, dass diese Datensätze in zwei unterschiedliche Kategorien aufgeteilt werden:

1. in demographische Daten DD und
2. in sicherheitskritische Daten SD.

Bei den demographischen Daten handelt es sich ebenfalls um sicherheitskritische Daten, die jedoch eine etwas geringere Sensitivität aufweisen als die sicherheitskritischen Daten SD. Demographische Daten DD sind beispielsweise der Name, der Geburtsort, das Geburtsdatum, der Versicherungsträger, der Arbeitgeber der jeweiligen Person oder Identitäten, die von einer externen (nicht der Registry REG und nicht dem Repository REP zugeordnet) Instanz ausgegeben werden. Bei den „externen Identitäten" kann es sich beispielsweise um einen externen Identifikator, z.B. einen Index handeln, der von der Datenquelle und/oder von der Datensenke verwendet wird, um die Datensätze auf Datenquelle/Datensenke zu adressieren. Dieser Identifikator muss nicht zwangsläufig mit dem Identifikator übereinstimmen, der vom Registry/Repository-System verwendet wird. Erfindungsgemäß ist hier ein Mapping vorgesehen.

Grundsätzlich hebt die Erfindung darauf ab, dass die demographischen Daten DD und die sicherheitskritischen Daten SD in zwei unterschiedlichen Hardwareinstanzen (zum Beispiel Speicher-Servern) und in physikalischer Hinsicht getrennt voneinander bereitgestellt werden. Die demographischen Daten DD

werden in der Registry REG und die sicherheitskritischen Daten SD werden in dem Repository REP bereitgestellt.

Falls von irgendeiner Stelle ein Zugriff auf die sicherheitskritischen Daten SD im Repository REP angefordert wird, so ist dies nur möglich, wenn zunächst in einem ersten Schritt eine Registrierung von der Registry REG erfolgreich angefordert und der jeweils anfragenden Instanz bereitgestellt werden konnte.

Sowohl in der Registry REG als auch in dem Repository REP sind sensitive Daten gespeichert. Diese Datensätze müssen für einen Zugriff adressierbar sein.

Erfindungsgemäß ist es nun vorgesehen, dass zur Adressierung der jeweiligen Datensätze zwei unterschiedliche Identifikationssysteme verwendet werden.

1. Ein personenidentifizierender Identifikator ID und

2. ein Sicherheitstoken, das auch in der Form eines Pseudonyms PS ausgebildet sein kann.

Der (interne) Identifikator ID dient zum eineindeutigen Identifizieren einer Person und damit auch eines Datensatzes, der dieser Person zugeordnet ist. Beispielsweise können über den Identifikator ID alle Befunddateien, alle Bilddaten des Patienten, sowie auch seine demographischen Daten DD angesprochen werden. Der Identifikator ID indiziert die personenbezogenen Datensätze im System der Registry REG und des Repositories REP. Dabei ist darauf hinzuweisen, dass sowohl die Datenquelle Q, als auch die Datensenke S andere Identifikatoren haben können.

Zum Zwecke der Sicherheit ist es vorgesehen, dass der Identifikator ID nur intern verwendet wird und mit keiner Nachricht an Datenquelle Q und Datensenke S (und somit nicht nach außen) gegeben wird (lediglich die Registry REG versendet eine

Nachricht mit dem Identifikator ID an das Repository REP). Vorzugsweise wird die Kommunikation zwischen diesen beiden Instanzen einer erhöhten Überwachung unterzogen (z.B. Verschlüsselung etc.). Das Sicherheitstoken oder das Pseudonym PS können nach außen kommuniziert werden.

Das Sicherheitstoken PS kann in zwei unterschiedlichen Ausprägungen bereitgestellt werden:

1. Als digitaler Code, in Form eines Pseudonyms PS oder

2. als Hardwarebauteil, etwa in Form eines USB-Sticks mit entsprechendem Chip zur Identifikation oder in Form einer Sicherheitskarte mit dem Code, der entweder als Magnetstreifen oder auf dem Chip implementiert sein kann, darüber sind auch andere Datenträger bzw. Schlüssel möglich.

Vorzugsweise ist es vorgesehen, dass der Identifikator ID in der Registry REG erzeugt wird. Alternativ kann dies auch von einer separaten Instanz ausgeführt werden, die über entsprechende Schnittstellen mit der Registry REG verbunden ist.

Gemäß einem Aspekt ist es vorgesehen, dass auch das Sicherheitstoken oder Pseudonym PS von der Registry REG generiert werden. Dabei wird ein Mapping bereitgestellt, das von dem personenbezogenen Identifikator ID auf das jeweilige Pseudonym PS und umgekehrt verweist. Ebenso ist ein Mapping vorgesehen zwischen dem Identifikator ID und den in der Registry REG gespeicherten demographischen Daten DD. Mit anderen Worten kann der Identifikator ID dazu verwendet werden, gezielt einen Datensatz von demographischen Daten DD in der Registry REG anzusprechen bzw. zu adressieren.

Wie in Figur 1 dargestellt und oben erwähnt, umfasst die Registry REG in der bevorzugten Ausführungsform einen Sicherheitstoken-Generator 10 und einen Identifikator-Generator 11.

Im Folgenden wird der erfindungsgemäße Ablauf des Verfahrens zum Ausführen eines gesicherten Zugriffs auf die sicherheitskritischen Datensätze in Zusammenhang mit Figur 1 näher beschrieben.

In Figur 1 sind die ausgetauschten Nachrichten mit den Bezeichnungen "S1", "S2", "S3" und "S4" gekennzeichnet. Dabei soll die Ziffer die Reihenfolge der Schritte in einer bevorzugten Ausführungsform kennzeichnen.
Die mit "S" gekennzeichneten Schritte bezeichnen die Nachrichten, die zwischen Datenquelle und Registry/Repository ausgetauscht werden. Bei dem Zugriff, der von der Datenquelle Q auf das Repository REP ausgeführt wird, handelt es sich um einen STORE- bzw. Schreibzugriff (deshalb sind die Nachrichten, die im Zusammenhang mit der Datenquelle Q ausgetauscht werden als S (für STORE) bezeichnet).

Im Unterschied dazu ist die Datensenke S dazu ausgebildet, Daten von dem Repository (oder von der Registry) anzulesen; es handelt sich somit um einen RETRIEVE-Befehl. Entsprechend sind die Nachrichten, die im Zusammenhang mit der Datensenke S ausgetauscht werden mit einem "R" gekennzeichnet, wie "R1", "R2", "R3" und "R4" (siehe Figur 1). Wie beim STORE-Befehl soll die Ziffer die Reihenfolge der Schritte in einer bevorzugten Ausführungsform kennzeichnen.

Für die Ausführung eines Schreibzugriffes gilt vorzugsweise folgender Ablauf.
In einem ersten Schritt S1 greift die Datenquelle Q mit einem Registriermodul 22 unter Angabe eines Identifikators ID auf die Registry REG zu. Bei dem Identifikator ID kann es sich um einen solchen handeln, der die Daten innerhalb der Datenquelle Q eindeutig kennzeichnet. Der Identifikator ID muss nicht zwangsläufig auch ein Identifikator für die Datensätze in Registry REG und/oder Repository REP sein, da ein Mapping auf dem internen Identifikator (intern für Registry und Repository) vorgesehen ist. Bei dem Identifikator ID, der von Daten-

quelle Q an Registry REG gesendet wird kann es sich um eine Auswahl von demographischen Daten DD handeln, wie beispielsweise einen Patientennamen, Patientengeburtsdatum oder andere patientenbezogene Datensätze.

Der Identifikator wird dann von der Registry empfangen und verarbeitet. Falls der Identifikator bereits ein interner Identifikator ist sind keine weiteren Mappingfunktionen auf den internen Identifikator notwendig. Andernfalls, falls also der Identifikator ID, der von der Datenquelle Q an das Registry REG gesendet wird, nur ein Teil von demographischen Daten ist und somit nicht dazu ausgebildet ist, personenspezifische Daten eindeutig zu identifizieren (zum Beispiel nur Patientenname) ist ein Mapping vorgesehen, um aus dem empfangenen Teil der demographischen Daten DD einen systeminternen Identifikator ID zu generieren. Dies wird von dem Identifikator-Generator 11 der Registry REG ausgeführt. Mit dem so ermittelten Identifikator ID ist es möglich, ein Pseudonym PS zu generieren. Dies wird durch den Sicherheitstoken-Generator 10 der Registry REG ausgeführt. Dabei ist es vorteilhafterweise vorgesehen, dass hier eine bijektive Abbildung zwischen Identifikator ID und Pseudonym PS vorgesehen ist. Damit kann genau einem Identifikator genau ein Pseudonym zugeordnet werden.

Anschließend werden die beiden folgenden Schritte ausgeführt, deren Reihenfolge variabel ist.

Es wird eine Nachricht von der Registry REG an das Repository REP gesendet, umfassend das ausgegebene Sicherheitstoken PS und den zugeordneten personenidentifizierenden Identifikator ID an das Repository REP, sodass bei späteren Zugriffen das Repository REP diese empfangenen Daten als Mappingvorschrift verwenden kann.

Vor, nach oder zeitgleich mit diesem Schritt wird im Schritt S2 das ermittelte Pseudonym PS an das Registriermodul 22 der Datenquelle Q gesendet. Wichtig ist dabei, dass das Pseudonym

PS nur temporäre Gültigkeit hat und nach einer konfigurierbaren Zeitspanne abläuft. Damit wird ein Datenzugriff auf das Repository REP nur innerhalb der Gültigkeitsdauer möglich.

In einem dritten Schritt S3 wird von einem Zugriffsmodul 24 der Datenquelle Q ein Zugriff auf das Repository REP ausgeführt, bei dem das zugewiesene Pseudonym PS an das Repository mitgeteilt wird.

In dieser Nachricht, zeitgleich mit dieser Nachricht oder in einer zusätzlichen weiteren Nachricht (gegebenenfalls in einem anderen Format und/oder auch über einen anderes Kommunikationsprotokoll, z.B. per Post oder per Mobilfunk) können dann sicherheitskritische Daten SD von dem Zugriffsmodul 24 der Datenquelle Q im Schritt S4 an das Repository REP gesendet werden. Das Repository REP ist damit mit allen Informationen ausgestattet, um den Zugriff auf dem Repository REP zu indizieren. Dazu verwendet das Repository REP die Zuordnung aus der Mappingvorschrift, die sie von der Registry REG erhalten hat. Aus dieser Mappingvorschrift kann sie das im Schritt S3 empfangene Pseudonym PS eindeutig einem internen personenidentifizierenden Identifikator ID zuordnen. Mit dem zugeordneten Identifikator ID ist die Indizierung der zugegriffenen sicherheitskritischen Daten SD möglich.

Im Folgenden wird der RETRIEVE-Befehl in Zusammenhang mit Figur 1 beschrieben.

In einem ersten Schritt R1 wird eine Registrieranfrage als Nachricht von dem Registriermodul 32 der Datensenke S an die Registry REG gesendet. Die Registrieranfrage enthält vorzugsweise einen Identifikator zur Identifikation des Datensatzes. Dabei kann es sich um einen Identifikator handeln, der auf der Datensenke S verwendet wird. Er muss nicht zwangsläufig auch als Identifikator in der Registry REG und/oder im Repository REP verwendet werden, da erfindungsgemäß eine Mappingvorschrift vorgesehen ist. Dieser Sachverhalt gilt auch für die Nachricht, die von der Datenquelle Q an die Registry REG

gesendet wird und ist in Figur 1 insofern gekennzeichnet, als die Nachricht von Datenquelle/Datensenke an Registry REG jeweils eine Alternative umfasst, nämlich "ID/DD". Dies soll kennzeichnen, dass der übersandte Identifikator nicht zwangsläufig vom System vergeben sein muss. Er kann durch die Mappingvorschrift auf einen systeminternen Identifikator ID „gemappt" werden.

Nach Erhalt der Nachricht R1 kann die Registry REG das Sicherheitstoken PS zu dem übersandten Identifikator vergeben. Wie oben in Zusammenhang mit dem STORE-Befehl erklärt, wird anschließend in wahlweiser Reihenfolge von der Registry REG eine Nachricht an das Repository REP gesendet, mit der das Repository über die Zuordnung "ID-PS" informiert wird.

Zusätzlich wird in Schritt R2 das zugeordnete Pseudonym PS (der Begriff Pseudonym wird im Rahmen dieser Beschreibung als Synonym zum Begriff Sicherheitstoken verwendet) an das Registriermodul 32 der Datensenke gesendet.

Die Datensenke S kann dann in einer späteren Zugriffsphase mit dem Zugriffsmodul 34 das erhaltene Pseudonym PS in Schritt R3 an das Repository REP senden.

Das Repository REP ist in der Lage aus dem empfangenen Pseudonym PS mittels der Mappingvorschrift "ID-PS" (empfangen von der Registry REG) auf den systeminternen Identifikator ID zu schließen. Mit dem Identifikator ID kann der sicherheitskritische Datensatz SD indiziert werden. Der Datensatz SD wird in Schritt R4 an das Zugriffsmodul 34 der Datensenke gesendet.

Wie in Figur 1 dargestellt, enthält keine der ausgetauschten Nachrichten sensitive Daten (sicherheitskritische Daten oder demographische Daten) in Kombination mit einem personenidentifizierenden Identifikator (zum Beispiel Patientenname etc.). Das bedeutet, dass selbst dann, wenn eine der Nachrichten abgefangen wird, entweder nur die sicherheitskriti-

schen Daten, wie Patientenbilder, Befunde etc. übermittelt werden oder nur die patientenidentifizierenden Daten oder Teile davon, wie zum Beispiel Patientenname, Patientengeburtsdatum, etc. Eine Zuordnung, welche medizinischen Gesundheitsdaten welchen Patienten zuzuordnen sind, ist auch beim Abfangen einer Nachricht nicht möglich.

Das Repository REP ist mit einem Indexmodul 42 ausgebildet, das zur Indizierung der jeweiligen sicherheitskritischen Daten für den Zugriff bestimmt ist.

Wie vorstehend bereits erwähnt, kann es sich bei dem Sicherheitstoken um ein digitales codiertes Signal in Form eines Pseudonyms PS handeln oder um ein Hardwarebauteil. Im Folgenden wird im Zusammenhang mit Figur 3 eine Ausführung der Erfindung erläutert, bei dem das Sicherheitstoken ein zugewiesener Schlüssel ist, der auf einem physikalischen Medium geträgert ist, wie beispielsweise auf einer Chipkarte oder einem Chip oder einem optischen Signal beispielsweise in Form eines Barcodes, z.B. eines eindimensionalen Barcodes oder vorzugweise eines 2D-Barcodes nach der Datamatrix-Norm (z.B. ISO/IEC 16022:2000 und ISO/IEC TR 24720:2008).

In dieser Ausführungsform ist es vorgesehen, dass der Kommunikationskanal zum Übersenden des Sicherheitstokens PS ein anderer ist als der Kommunikationskanal zum Austausch der Nachrichten mit Identifikator ID, demographischen Daten DD, sicherheitskritischen Daten SD. Die demographischen Daten DD, die sicherheitskritischen Daten SD und der Identifikator ID werden vorzugsweise über ein Computernetzwerk, zum Beispiel das Internet, ausgetauscht, während in dieser Ausführungsform das Sicherheitstoken PS als stofflich verkörpertes Sicherheitsmerkmal, zum Beispiel in Form einer Chipkarte oder dergleichen, auf anderem Wege, zum Beispiel auf dem Postwege, übersandt wird. Das Sicherheitstoken PS trägt in diesem Fall eine registrierende Prägung, die erforderlich ist, um einen Zugriff auf das Repository REP auszuführen. Diese Prägung wird dann vom Repository REP verglichen mit der Referenzprä-

gung, die es in einer separaten Nacht von der Registry REG erhalten hat. Dabei kann die Nachricht, die von der Registry REG an das Repository REP gesendet wird auch auf unterschiedlichen Kommunikationsprotokollen bzw. Netzwerken übertragen werden, wie per Post oder auch über das Internet als digitale Nachricht. Falls Registry REG das zugewiesene Sicherheitstoken PS als analoge Nachricht, zum Beispiel per Post an Datenquelle Q oder Repository REP sendet, sind die empfangenden Instanzen mit einem Wandlermodul ausgestattet, um das empfangene Signal automatisch in ein digitales Signal zu transformieren, was dann auf den Instanzen weiter verarbeitet werden kann.

In Zusammenhang mit Figur 4 werden die unterschiedlichen Möglichkeiten nochmals detaillierter beschrieben, wie die Registry REG auf eine Registrierungsanfrage seitens der Datenquelle Q oder der Datensenke S antworten kann. Dies betrifft die Nachrichten S2 (für die Datenquelle Q) und R2 (für die Datensenke S).

Als Antwort auf eine Registrierungsanfrage seitens der anfragenden Instanzen (Datenquelle Q, Datensenke S) wird auf der Registry REG ein Sicherheitstoken bzw. Pseudonym PS generiert. Erfindungsgemäß sind nun unterschiedliche Möglichkeiten vorgesehen, wie das Antwortsignal in Schritt S2 bzw. R2 an die anfragenden Instanzen weitergeleitet werden kann. In einem ersten Fall wird lediglich das Pseudonym PS weitergeleitet. Dies ist in Figur 4 mit dem durchgehend gezeichneten Pfeil gekennzeichnet. Alternative Möglichkeiten sind in Figur 4 mit einer Punktlinie gekennzeichnet. Eine Möglichkeit besteht in der Übertragung einer Kombinationsnachricht aus Identifikator und Pseudonym. Dabei kann es sich z.B. um ein (digitales) Datentupel oder um einen per Post übersandten Kombinationsbrief handeln. Alternativ sind hier zwei kombinierte Nachrichten denkbar. Der Identifikator bezieht sich dabei auf einen systeminternen Identifikator, der von Registry REG und/oder Repository REP verwendet wird. Eine weitere Möglichkeit besteht darin, das Signal aus der Registrie-

rungsanfrage aufzunehmen und eine Kombinationsnachricht zurückzusenden, umfassend demographische Daten DD aus der Anfragenachricht (in Schritt S1 bzw. R1 übermittelt) und die mit dem zugewiesenen Pseudonym PS zu kombinieren.

Falls keine Kombinationsnachricht, sondern nur das zugewiesene Pseudonym PS alleine übersendet wird, ist es Aufgabe der anfragenden Instanz Q, S eine Zuordnung zwischen den Daten aus der Registrierungsanfrage (S1, R1) mit dem erhaltenen Pseudonym PS zu verknöpfen. Dies kann über eine zeitliche Zuordnung oder über eine Adressfunktion ausgeführt werden.

Grundsätzlich ist es bei der erfindungsgemäßen Lösung vorgesehen, dass vor einem Zugriff auf das Repository REP (bzw. auf sicherheitskritische Daten SD des Repository's REP) immer eine Registrierungsanfrage an die Registry REG erfolgt, um das Pseudonym PS für den Zugriff auf das Repository REP zu erhalten. Der Zugriff auf das Repository REP setzt also immer einen vorhergehenden Zugriff auf die Registry REG voraus. Es ist jedoch auch möglich, dass Datenquelle Q oder Datensenke S lediglich auf solche Daten zugreifen wollen, die in der Registry REG gespeichert sind und ein geringeres Sicherheitsprofil aufweisen. Beispielsweise würde dies ein Zugriff auf den Geburtsort für einen bestimmten Patienten umfassen. In diesem Fall ist es vorgesehen, dass die Registry REG auf die Registrierungsanfrage lediglich eine erste Mappingfunktion ausführt, die nämlich von den demographischen Daten DD oder einem Teil davon, die Bestandteil der Registrierungsanfrage S1, R1 waren, den jeweiligen Datensatz herausfiltert. Der so indizierte Datensatz kann dann an die anfragende Instanz als Antwort zurückgegeben werden. Dies deckt beispielsweise auch Fälle ab, in denen die Datenquelle Q oder die Datensenke S ihre Registrierungsdaten einem Update unterziehen wollen. Das Generieren eines Pseudonyms PS kann unterbleiben und ebenso die nachgelagerten Schritte mit dem Zugriff auf das Repository REP.

Es ist somit vorgesehen, dass nicht notwendigerweise alle Schritte des beanspruchten Verfahrens ausgeführt werden müssen.

Aufgrund des asynchronen Protokolls ist es möglich, dass die ausgetauschten Nachrichten bezüglich des Datenaustauschs (z.B. Zeit) unabhängig voneinander sind. Dies hat zur Folge, dass die Datenquelle Q beispielsweise gleichzeitig Nachrichten an die Registry REG oder das Repository REP senden kann wie die Datensenke S.

Vorzugsweise ist es in einer Konfigurationsphase vorgesehen, dass Sicherheitsparameter für den Datenaustausch festgelegt werden können. Dabei ist es beispielsweise möglich, die Gültigkeitsdauer für die Pseudonymzuweisung PS festzulegen.

Eine Sicherheitsvorkehrung gemäß einer bevorzugten Ausführungsform ist auch darin zu sehen, dass jeder Zugriff auf das Repository REP ausschließlich nach einer erfolgreichen Registrierung ausgeführt werden kann. Zugriffe auf das Repository REP können nur mittels eines Pseudonyms PS ausgeführt werden. Ein "direkter" Zugriff auf das Repository REP mit personenidentifizierenden Daten oder Teilen davon ist ausgeschlossen.

In einer bevorzugten Ausführungsform ist das Verfahren als computerimplementiertes Verfahren bereitgestellt. Dabei kann es in einer verteilten Umgebung angewendet werden, sodass einzelne Schritte des Verfahrens auf unterschiedlichen Computer-basierten Instanzen zur Ausführung kommen. Ebenso können einzelne ausführbare Programmteile lediglich auf dem jeweiligen Computer geladen werden und nicht als ausführbarer Code vorliegen.

Das Computerprogramm oder Teile davon können fest implementiert in den Hardwareinstanzen integriert sein oder sie können als separate Add-On-Module aufschaltbar sein oder sie können auf einem Speichermedium gespeichert sein.

Die Registry REG wird üblicherweise als international übergeordnete Zertifizierungsinstanz betrieben, während die Repositories REP von unterschiedlichen nationalen und/oder regionalen Instanzen betrieben werden, die bei der Registry REG registriert sind. Bei den Datenquellen Q und/oder bei den Datensenken S kann es sich um beliebige Instanzen und Applikationen im Rahmen eines Gesundheitssystems oder anderer Anwendungen handeln. Es ist auch möglich, dass Datenquelle Q und Datensenke S ihre Funktion während des Betriebs wechseln und in der jeweils anderen Rolle betrieben werden. Handelt es sich beispielsweise bei Datenquelle Q oder Datensenke S um radiologische Systeme, so können diese wahlweise als Datensender/quelle und Datenempfänger/senke fungieren. Ihre Rolle ist somit nicht festgeschrieben.

Wie eben erwähnt, können in einer bevorzugten Ausführungsform die "Rollen" von Datenquelle Q und Datensenke S wechseln. Deshalb weisen diese Instanzen vorteilhafterweise denselben Aufbau auf, sodass sich die Registrierungsmodule 22, 32 in funktionaler Hinsicht entsprechen. Dasselbe gilt für die Zugriffsmodule 24, 34.

Ebenso ist es möglich, dass das erfindungsgemäße Zugriffssystem nur auf eine bestimmte Zugriffsart beschränkt sein soll. Falls es nur für einen STORE-Zugriff beschränkt sein soll, besteht es lediglich aus Registry REG, Datenquelle Q und Repository REP. Falls es nur für ein RETRIEVE ausgelegt sein soll, besteht das System nur aus Registry REG, Datensenke S und Repository REP. Auch Teile des vorstehend beschriebenen Systems und die einzelnen Instanzen sollen im Rahmen dieser Anmeldung unter Schutz gestellt sein.

Vorzugsweise ist es vorgesehen, dass die Registry REG vollautomatisch betrieben werden kann. Für den Betrieb der Registry sind keine Benutzerinteraktionen notwendig. Damit können sowohl Kosten als auch Verwaltungsaufwand eingespart werden.

Ein Vorteil der erfindungsgemäßen Lösung ist auch darin zu sehen, dass das System insofern skalierbar ist, als dass einzelne Instanzen zu jeder Zeit hinzugefügt gelöscht, oder verändert werden können. Damit können auch während des Betriebs Datenquellen Q, Datensenken S oder weitere Repositories REP hinzugefügt werden.

Ein weiterer Vorteil ist auch darin zu sehen, dass die Registrierung und damit verbundene Prozesse nicht unnötig ausgeführt werden. Erst wenn die Datenquelle Q bzw. Datensenke S einen Zugriff auf das Repository REP planen, wird eine Registrierung seitens der Registry angefordert und ausgeführt. Auf der Registry REG werden somit keine unnötigen Registrierungsdaten generiert und müssen demnach auch nicht verwaltet werden müssen.

Die Zuordnung der Daten auf ihren Speicherort und damit die Trennung zwischen sensitiven Daten, die auf der Registry REG und solchen, die auf dem Repository REP gespeichert werden, wird vorzugsweise von einer anderen Instanz und automatisiert ausgeführt. Vorgesehen ist es, dass demographische Daten DD, die ebenfalls personenbezogen sind keine Gesundheitsinformationen enthalten und administrativen und/oder identifizierenden Aufgaben dienen. Sie enthalten vorzugsweise den Namen, den Geburtsort, das Geburtsdatum, den Versicherungsträger, den Arbeitgeber oder andere Parameter der jeweiligen Person.

Erfindungsgemäß sind unterschiedliche Varianten zum Generieren des Sicherheitstokens PS vorgesehen. In einer ersten Variante wird das Pseudonym PS in Abhängigkeit von den Daten aus der Registrierungsanfrage erstellt. Mit anderen Worten dienen die Daten Identifikator ID und/oder alle oder ausgewählte Daten der demographischen Daten DD als Input für den Identifikator-Generator 11, um das Pseudonym PS zu generieren. Alternativ ist es auch möglich, das Pseudonym PS unabhängig von den Daten aus der Registrierungsanfrage zu gene-

rieren und hier eine konfigurierbare Generierungsvorschrift zum Generieren des Sicherheitstokens oder Pseudonyms PS vorzusehen. Dabei kann eine Hash-Funktion auf alle oder eine Auswahl der folgenden Parameter verwendet werden:

- einen eineindeutigen globalen Identifikator, zum Beispiel eine global eindeutige Zahl mit 128 Bit als sogenannten Global Unique Identifier (GUID)
- eine lokale Uhrzeit, insbesondere Systemuhrzeit,
- eine Zufallszahl und/oder
- die Ablaufzeit der Gültigkeit für das Pseudonym PS.

Wie vorstehend bereits erwähnt ist es darüber hinaus möglich, den Identifikator auf der Registry zu generieren oder alternativ auf den anfragenden Instanzen, wie Datenquelle Q oder Datensenke S. In der zweiten Alternative würden die anfragenden Instanzen für die Registrierungsanfrage gleich den Identifikator ID verwenden. Andernfalls müsste der externe Identifikator auf den systeminternen Identifikator ID „gemappt" werden.

Das Repository REP kennzeichnet sich also durch das Bereitstellen von zwei Datenstrukturen, einer statischen Datenstruktur, in der eine (fest zugewiesene) Zuordnung zwischen Identifikator ID und sicherheitskritischen Daten SD abgelegt ist und eine dynamische Datenstruktur, in der eine Zuordnung zwischen (dynamisch zugewiesenem) Pseudonym PS und Identifikator ID abgelegt ist. Das Repository umfasst des Weiteren noch Schnittstellen zum Datenaustausch mit den anderen Instanzen. Dasselbe gilt natürlich auch für die anderen Computer-basierten Instanzen.

Zusammenfassend lässt sich der vorstehend näher erläuterte Vorschlag dahingehend beschreiben, ein Schema bereitzustellen, mit dem der Datenaustausch von sensitiven Daten mit un-

terschiedlichen Sicherheitsstufen auch über das unsichere Internet ausführbar ist. Dabei werden sicherheitskritische Gesundheitsdaten SD getrennt von demographischen Daten DD gespeichert. Ein Zugriff auf die sicherheitskritischen Daten SD kann nur nach erfolgreicher Registrierung unter einem Pseudonym PS ausgeführt werden.

Patentansprüche

1. Verfahren zum gesicherten Zugriff auf Datensätze in einer unsicheren Netzwerkumgebung, wobei folgende jeweils voneinander getrennte Hardwareinstanzen miteinander in Datenaustausch stehen:
   - Eine zentrale Registry (REG)
   - Zumindest ein separat von der Registry (REG) bereitgestelltes Repository (REP)
   - Zumindest eine Datenquelle (Q) und zumindest eine Datensenke (S), die sich jeweils vorzugsweise einmalig bei der Registry (REG)zum Datenzugriff auf das Repository (REP) registrieren müssen

   wobei die Datensätze sicherheitskritische Daten (SD) und demographische Daten (DD) für eine Person umfassen und wobei die sicherheitskritischen Daten (SD) einer Person nicht zusammen mit personenidentifizierenden Daten kommuniziert werden, mit folgenden Verfahrensschritten:
   - Getrenntes Bereitstellen der sicherheitskritischen Daten (SD) und der demographischen Daten (DD), indem die demographischen Daten (DD) in der Registry (REG) und die sicherheitskritischen Daten (SD) in dem Repository (REP) gespeichert werden
   - Registrierungsanfrage (S1, R1) seitens der Datenquelle (Q) und/oder der Datensenke (S) an die Registry (REG), um für den Zugriff auf einen einer Person zugeordneten Datensatz eine Registrierung in Form einer Zuweisung eines Sicherheitstokens (PS) zu erhalten
   - Auf die Registrierungsanfrage hin wird ein Sicherheitstoken (PS) ausgegeben (S2, R2), das einem personenidentifizierenden Identifikator (ID) eindeutig zugeordnet werden kann
   - Senden einer Nachricht von der Registry (REG) an das Repository (REP), umfassend das ausgegebene Sicherheitstoken (PS) und den zugeordneten personen-

identifizierenden Identifikator (ID) als Mappingvorschrift

- Senden einer Zugriffsnachricht (S3, R3) mit dem Sicherheitstoken (PS) oder mit einer für die Anfrage eindeutigen Kennung der Datenquelle (Q) und/oder der Datensenke (S) an das Repository (REP) zum Zugriff auf in dem Repository (REP) gespeicherte sicherheitskritischen Daten (SD)
- Anwenden der Mappingvorschrift auf dem Repository (REP), um mit dem Sicherheitstoken (PS) aus der Zugriffsnachricht den personenidentifizierenden Identifikator (ID) zu berechnen und Indexierung des angefragten Datensatzes durch den personenidentifizierenden Identifikator (ID)
- Ausführen des Zugriffs auf den indexierten Datensatz.

2. Verfahren nach Anspruch 1, wobei das Sicherheitstoken (PS) temporäre Gültigkeit hat und/oder nach einer konfigurierbaren Zeitspanne verfällt.

3. Verfahren nach einem der vorstehenden Verfahrensansprüche, bei dem die Zuordnungen zwischen Sicherheitstoken (PS) und personenidentifizierendem Identifikator (ID) von der Registry (REG) und/oder von dem Repository (REP) verwaltet werden.

4. Verfahren nach einem der vorstehenden Verfahrensansprüche, bei dem die Datensätze medizinische oder gesundheitsbezogene Datensätze eines Patienten sind und die Datenquelle (Q) und/oder die Datensenke (S) medizinische Bildspeichersysteme sind.

5. Verfahren nach einem der vorstehenden Verfahrensansprüche, bei dem die sicherheitskritischen Daten (SD) nicht direkt auf dem Repository (REP) gespeichert sind, sondern nur über einen in dem Repository (REP) gespeicherten elektronischen Verweis zugreifbar sind.

6. Verfahren nach einem der vorstehenden Verfahrensansprüche, bei dem ein asynchrones und/oder ein synchrones Kommunikationsprotokoll verwendet werden.

7. Verfahren nach einem der vorstehenden Verfahrensansprüche, bei dem das Sicherheitstoken (PS) ein analoges Signal, insbesondere ein Barcode, eine Hardwarekomponente und/oder eine Softwarekomponente ist.

8. Verfahren nach einem der vorstehenden Verfahrensansprüche, bei dem der Zugriff Schreibzugriffe auf das Repository (REP) seitens der Datenquelle (Q) und Lesezugriffe auf das Repository (REP) seitens der Datensenke (S) umfasst.

9. Verfahren nach Anspruch 7, bei dem die Datenquelle (Q) zur Ausführung des Schreibzugriffs auf dem Repository (REP) in einer ersten Nachricht nur das Sicherheitstoken (PS) und in einer zweiten Nachricht nur die sicherheitskritischen Daten (SD) für den Schreibzugriff sendet und das Repository (REP) aus den so empfangenen Nachrichten die Zuordnung zwischen den sicherheitskritischen Daten (SD) und dem Sicherheitstoken (PS) herstellt oder indem die Datenquelle (Q) zur Ausführung des Schreibzugriffs eine Nachricht an das Repository (REP) sendet, umfassend Sicherheitstoken (PS) oder eine für die Anfrage eindeutige Kennung und sicherheitskritische Daten (SD).

10. Verfahren nach Anspruch 7 oder 8, bei dem das Repository (REP) als Antwort auf eine Zugriffsanfrage mit dem Sicherheitstoken (PS) der Datensenke (S) zur Ausführung eines Lesezugriffs nur die angefragten sicherheitskritischen Daten (SD) an die Datensenke (S) sendet oder eine Kombination aus Sicherheitstoken (PS) oder eine für die Anfrage eindeutige Kennung und angefragten sicherheitskritischen Daten (SD), vorzugsweise in einer Nachricht.

11. Verfahren nach einem der vorstehenden Verfahrensansprüche, bei dem auch während des Betriebs Repositories (REP), Datenquellen (Q) und/oder Datensenken (S) hinzugefügt, gelöscht und/oder verändert werden können.

12. System zum gesicherten Zugriff auf Datensätze (DD, SD) in einer unsicheren Netzwerkumgebung, umfassend folgende, in Datenaustausch stehende und jeweils voneinander getrennte Hardwareinstanzen:

- Eine zentrale Registry (REG) zum Speichern von demographischen Daten (DD), die auf eine Registrierungsanfrage seitens einer Datenquelle (Q) und/oder einer Datensenke (S) zur Ausgabe eines Sicherheitstokens (PS) bestimmt ist und die ein Benachrichtigungsmodul (12) umfasst, das zum Senden einer Nachricht an ein Repository (REP) bestimmt ist, wobei die Nachricht das ausgegebene Sicherheitstoken (PS) und einen zugeordneten personenidentifizierenden Identifikator (ID) umfasst
- Zumindest ein separat von der Registry (REG) bereitgestelltes Repository (REP)zum Speichern und Verwalten von sicherheitskritischen Daten (SD), umfassend ein Indexmodul (42)
- Zumindest eine Datenquelle (Q) und zumindest eine Datensenke (S), die sich jeweils bei der Registry (REG) zum Datenzugriff auf das Repository (REP) einmalig registrieren müssen und die jeweils ein Registriermodul (22, 32) und ein Zugriffsmodul (24, 34) umfassen, wobei das Registriermodul (22, 32) zum Senden einer Registrieranfrage an die Registry (REG) und zum Empfang eines Sicherheitstokens (PS) als Antwort auf die Registrieranfrage bestimmt ist und wobei das Zugriffsmodul (24, 34) zum Senden einer Zugriffsnachricht mit dem Sicherheitstoken (PS) oder mit einer für die Anfrage eindeutigen Kennung an das Repository (REP) und zum Zugriff auf die si-

cherheitskritischen Daten (SD) auf dem Repository (REP) bestimmt ist,
wobei die Datensätze sicherheitskritische Daten (SD) und demographische Daten (DD) für eine Person umfassen und wobei die sicherheitskritischen Daten (SD) einer Person nicht zusammen mit personenidentifizierenden Daten (DD, ID) kommuniziert werden.

13. Registry (REG) zur Verwendung in einem System nach Patentanspruch 12.

14. Repository (REP) zur Verwendung in einem System nach Patentanspruch 12.

15. Computerprogrammprodukt, das in einen Speicher eines digitalen Computers geladen werden kann und Computerprogrammabschnitte umfasst, mit denen alle oder ausgewählte Schritte gemäß zumindest einem der vorstehenden Verfahrensansprüche ausgeführt werden, wenn die Computerprogrammabschnitte auf einem Computer ausgeführt werden.

FIG 1

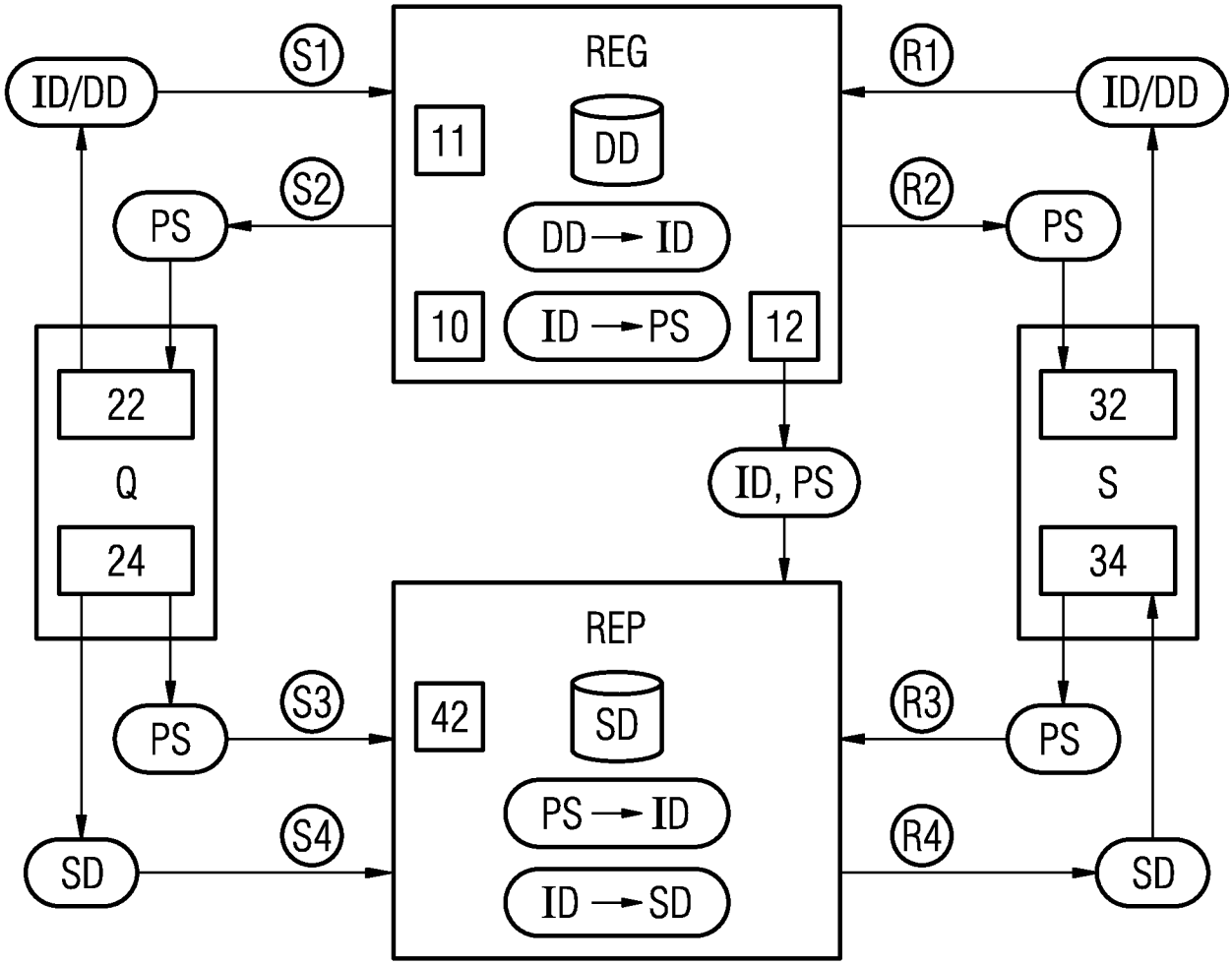

REG
11
DD
DD → ID
10
ID → PS
12
ID/DD
S1
S2
PS
R1
R2
22
Q
24
32
S
34
ID, PS
REP
42
SD
PS → ID
ID → SD
S3
S4
R3
R4
SD

FIG 2

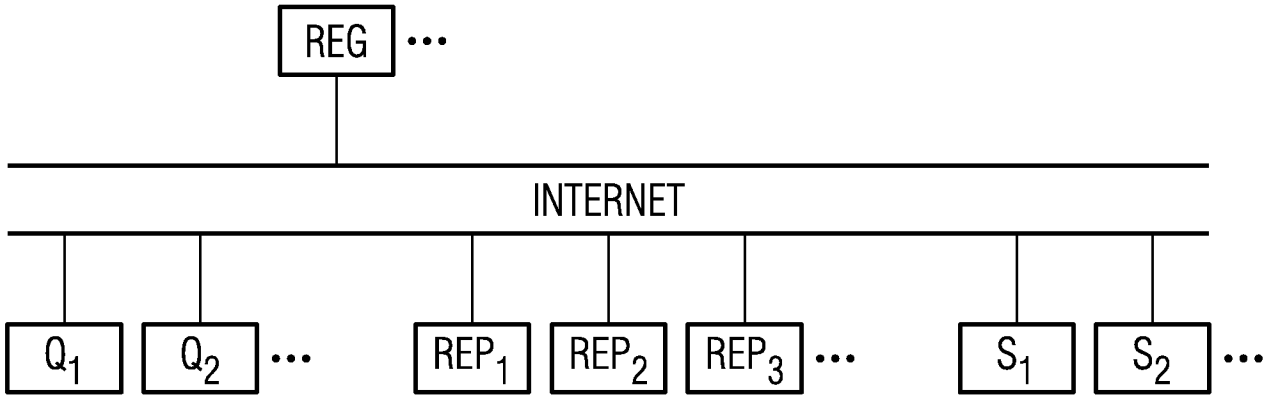

REG
INTERNET
Q1
Q2
REP1
REP2
REP3
S1
S2

FIG 3

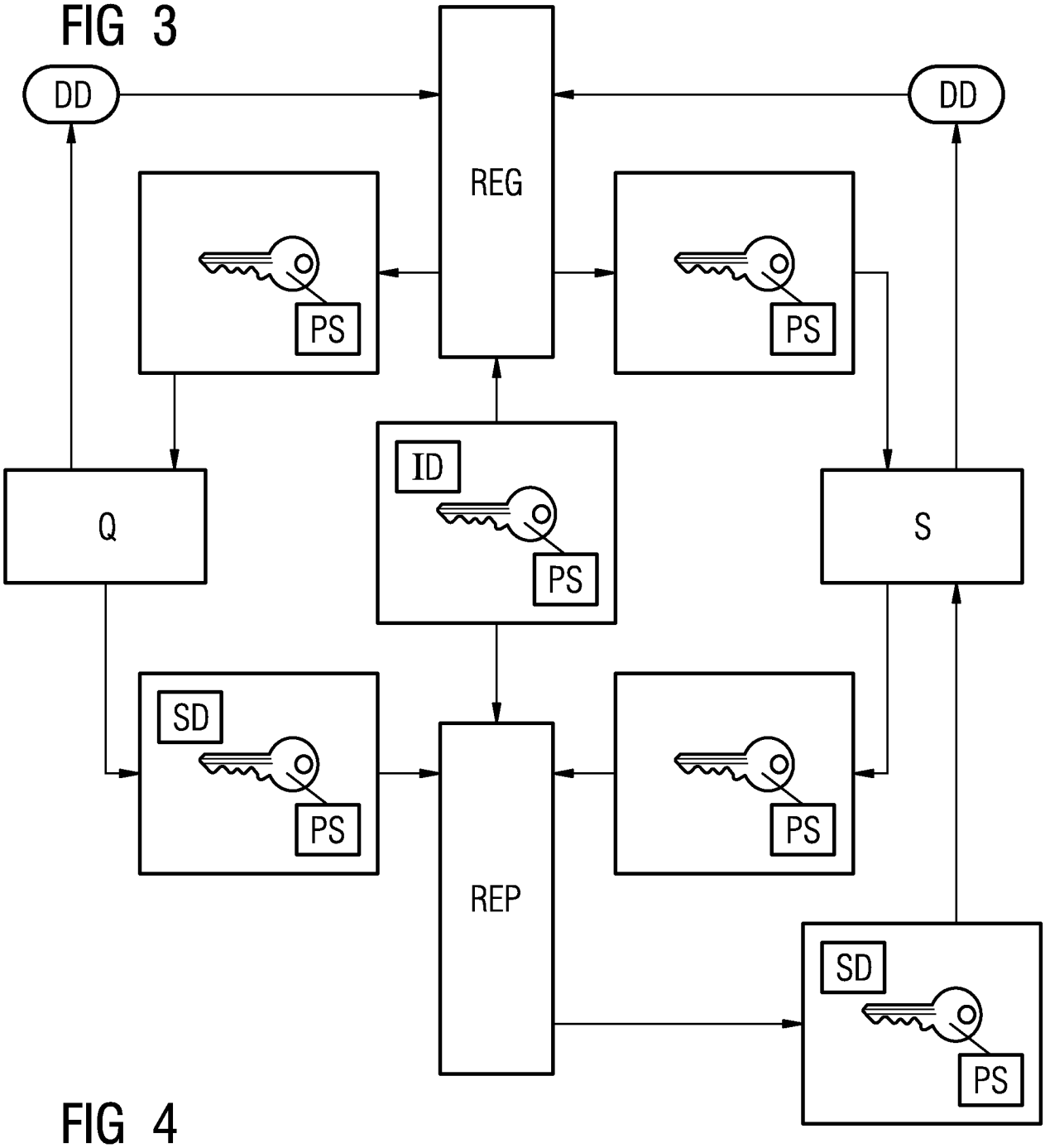
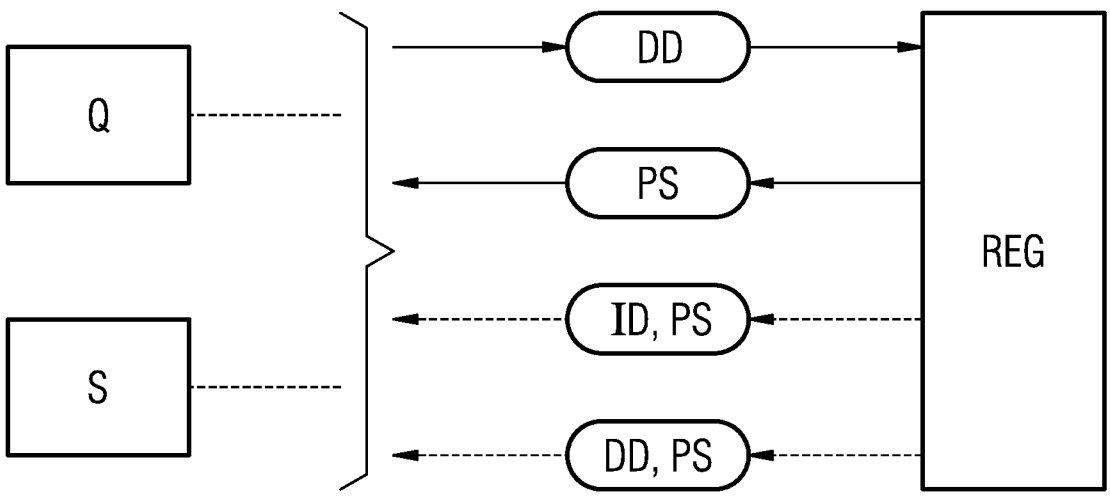


FIG 4



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2012/051047

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
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)
H04L 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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2005/283620 A1 (KHULUSI BASSAM [US] ET AL) 22 December 2005 (2005-12-22) paragraphs [0010] - [0016]	1-15
A	EP 1 416 419 A2 (GE MED SYS INFORMATION TECH [US]) 6 May 2004 (2004-05-06) paragraphs [0003], [0004], [0006]	1-15

☐ 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
16 July 2012	23/07/2012

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	Veen, Gerardus

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2012/051047

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005283620 A1	22-12-2005	CN 101002417 A	18-07-2007
		EP 1766823 A2	28-03-2007
		EP 2418795 A1	15-02-2012
		US 2005283620 A1	22-12-2005
		WO 2006009648 A2	26-01-2006
EP 1416419 A2	06-05-2004	EP 1416419 A2	06-05-2004
		US 2004078587 A1	22-04-2004

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2012/051047

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L29/06
ADD.

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L 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

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 2005/283620 A1 (KHULUSI BASSAM [US] ET AL) 22. Dezember 2005 (2005-12-22) Absätze [0010] - [0016]	1-15
A	EP 1 416 419 A2 (GE MED SYS INFORMATION TECH [US]) 6. Mai 2004 (2004-05-06) Absätze [0003], [0004], [0006]	1-15

☐ 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
16. Juli 2012	23/07/2012

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	Veen, Gerardus

Formblatt PCT/ISA/210 (Blatt 2) (April 2005)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2012/051047

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2005283620 A1	22-12-2005	CN 101002417 A	18-07-2007
		EP 1766823 A2	28-03-2007
		EP 2418795 A1	15-02-2012
		US 2005283620 A1	22-12-2005
		WO 2006009648 A2	26-01-2006
EP 1416419 A2	06-05-2004	EP 1416419 A2	06-05-2004
		US 2004078587 A1	22-04-2004