(19) österreichisches patentamt

(10) **AT 12 796 U1 2012-11-15**

(12) **Gebrauchsmusterschrift**

(21) Anmeldenummer: GM 668/2010
(22) Anmeldetag: 29.10.2010
(24) Beginn der Schutzdauer: 15.09.2012
(45) Veröffentlicht am: 15.11.2012

(51) Int. Cl. : ***G06F 21/00*** (2006.01)
H04L 29/06 (2006.01)

(56) Entgegenhaltungen:
US 5956400 A EP 2199907 A1
WO 2005117481 A1

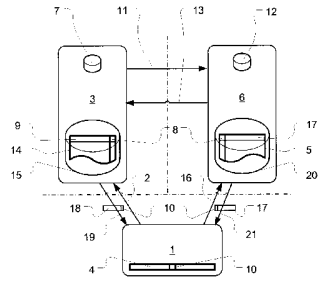
Spitzer et al.; 'Securing a Web-Based Teleradiology Platform According to German Law and "Best Practices".' In: Medical Informatics in a United and Healthy Europe - Proceedings of MIE 2009, The XXIInd International Congress of the European Federation for Medical Informatics, Sarajevo, Bosnia and Herzegovina, August 30 - September 2, 2009. Edited by Adlassnig et al., IOS Press, 2009. Vol. 150, p. 730-734

(73) Gebrauchsmusterinhaber:
RESEARCH INDUSTRIAL SYSTEMS ENGINEERING (RISE) GMBH
2320 SCHWECHAT (AT)

(54) **VERFAHREN UND VORRICHTUNG ZUR PSEUDONYMISIERTEN DATENVERARBEITUNG**

(57) Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur pseudonymisierten Datenverarbeitung wobei das abzufragende Informationsobjekt (4) getrennt auf zumindest einem ersten Server (3) und einem zweiten Server (6) vorliegt und die beiden Server untereinander über eine gesicherte Verbindung (Koordinierungsdatenstrom) für jede Client-Sitzung (Session) und jedes abgefragte Informationsobjekt ein ausschließlich für diese Client-Sitzung (Session) gültiges Session Pseudonym (SID) vereinbaren, welches an den Client zur Identifikation des jeweiligen Informationsobjektes und folglich zur Zusammenführung der beiden Teilinformationsobjekte übermittelt werden kann.

Fig. 1



AT 12 796 U1 2012-11-15

Beschreibung

VERFAHREN UND VORRICHTUNG ZUR PSEUDONYMISIERTEN DATENVERARBEITUNG

[0001] Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur pseudonymisierten Datenverarbeitung.

[0002] In der elektronischen Datenverarbeitung ist es oft notwendig, Benutzerdaten in Untergruppen aufzuteilen, beispielsweise in personalisierte Daten über den Benutzer selbst, wie etwa Name, Geburtsdatum, etc. und diesem Benutzer zugeordnete Prozessdaten, beispielsweise Kontonummern, Warenkorb oder Gesundheitsdaten in einem medizinischen Datenbestand. Die Kenntnis jeweils einer Untergruppe der Daten hat für sich wenig Aussagekraft, da die wesentliche Verknüpfung der personalisierten Daten mit den Prozessdaten fehlt. Erst die Verknüpfung enthüllt das vollständige Bild über eine Person und die zugeordneten Daten, und entsprechend soll es vermieden werden, dass unberechtigte Personen diese Verknüpfung, beispielsweise durch Abfangen des Datenverkehrs, herstellen können.

[0003] Eine beispielhafte Anwendung ist die Aufteilung von Gesundheitsdaten in einem medizinischen Datenbestand, welcher lediglich Behandlungs- und Dokumentationsdaten beinhaltet und in einen Datenbestand mit den entsprechenden demographischen Daten zu den jeweiligen Patienten. Somit kann bei Kenntnis des ersten Datenbestandes nicht auf die Person der Patienten geschlossen werden und bei Kenntnis des zweiten Datenbestandes keinerlei medizinische Information zu den entsprechenden Patienten gewonnen werden. Die Zusammenführung der beiden Teildatenbestände erfolgt über eindeutige Pseudonyme als Identifikatoren, welche in jedem Teildatenbestand zum jeweiligen Datensatz persistent mitgespeichert werden.

[0004] Derartige Verfahren sind bekannt. Insbesondere ist es bekannt, die jeweiligen Teildatenbestände auf physisch getrennten, unabhängigen Servern abzulegen. Ein Client benötigt für die Zusammenführung der beiden Teilinformationsobjekte jedoch einen beschriebenen Identifikator, um das korrespondierende zweite Teilinformationsobjekt nach Erhalt des ersten Teilinformationsobjekts vom zweiten Server nachladen zu können.

[0005] Genau dieser Identifikator, der als statisches Pseudonym (PID) bezeichnet wird, stellt in diesem Datentrennungskonzept bzw. -verfahren jedoch einen potentiellen Angriffspunkt dar, da einer unberechtigten Person (z. B. Angreifer, Hacker, Cracker, etc.) dieses statische Pseudonym unter Umständen zur Kenntnis gelangen könnte und somit Daten gegebenenfalls unbefugt von einem der beiden Server, oder von beiden Servern, abgegriffen werden könnten.

[0006] Die technische Aufgabe der Erfindung ist es demnach, ein verbessertes Verfahren zur pseudonymisierten Datenverarbeitung vorzusehen. Insbesondere ist es eine Aufgabe der Erfindung, den zu speichernden Gesamtdatenbestand derart in zwei Teildatenbestände aufzuteilen, dass jeder Teildatenbestand für sich alleine keine relevanten Informationen preisgibt, und dass es einer unbefugten Person auch bei Kenntnis des relevanten Identifikators nicht möglich ist, beim Abfangen der jeweiligen Nachrichten auf die Kombination der Teildaten zu schließen.

[0007] Diese Aufgabe wird erfindungsgemäß dadurch gelöst, dass ein abzufragendes Informationsobjekt getrennt auf zumindest einem ersten Server und einem zweiten Server vorliegt und die beiden Server untereinander über eine gesicherte Verbindung (Koordinierungsdatenstrom) für jede Client-Sitzung (Session) und jedes abgefragte Informationsobjekt ein ausschließlich für diese Client-Sitzung (Session) gültiges Session Pseudonym (SID) vereinbaren, welches bedenkenlos an den Client zur Identifikation des jeweiligen Informationsobjektes und folglich zur Zusammenführung der beiden Teilinformationsobjekte übermittelt werden kann.

[0008] Das erfindungsgemäße Verfahren erlaubt die aufgetrennte Verarbeitung eines Informationsobjekts in einer ersten Datenbank betrieben auf einem ersten Server und einer zweiten Datenbank betrieben auf einem zweiten Server, bei welchem die Zusammenführung des ersten Teilinformationsobjekts mit dem zweiten Teilinformationsobjekt mittels eines Session Pseudonyms und ausschließlich am Client erfolgt. Der Client sendet an den ersten Server eine Client-

Server-1-Anfrage zur Durchführung einer bestimmten Transaktion. Bildet diese Anfrage einen Abruf des Informationsobjekts, fragt der erste Server zum Statischen Pseudonym des ersten Teilinformationsobjekts das Session Pseudonym im ersten Session Store ab, falls dieses dort noch nicht existiert, sendet der erste Server eine Anfrage an den zweiten Server, welcher das Session Pseudonym generiert, im zweiten Session Store abspeichert und als Antwort an den ersten Server übermittelt, der das Session Pseudonym zusammen mit dem Statischen Pseudonym ebenfalls in seinem ersten Session Store speichert.

[0009] Konkret umfasst das erfindungsgemäße Verfahren folgende Schritte:

[0010] Zuerst wird vom Client eine Anfrage an den ersten Server übermittelt, auf Grund welcher der erste Server zusammen mit dem zweiten Server eine Transaktion betreffend das Informationsobjekt durchführen soll. Der erste Server leitet den Client an den zweiten Server weiter, welchem der Client die das zweite Teilinformationsobjekt darstellenden Daten in Form einer Anfrage übermittelt. Der zweite Server generiert ein Statisches Pseudonym, ein Session Pseudonym sowie eine eindeutige TransaktionsID, speichert diese Daten in seinem Session Store und speichert das zweite Teilinformationsobjekt zusammen mit dem Statischen Pseudonym in seiner (zweiten) Datenbank ab.

[0011] Der Client wird unter Übermittlung der TransaktionsID an den ersten Server zurückgeleitet, welcher unter Übermittlung der TransaktionsID das Statische Pseudonym und das Session Pseudonym beim zweiten Server abfragt, der wiederum nach Übermittlung der Antwort die TransaktionsID invalidiert.

[0012] Der erste Server ruft das erste Teilinformationsobjekt aus seiner Datenbank ab und verpackt dieses zusammen mit dem Session Pseudonym und bestimmten Metadaten, welche für die Abfrage des zweiten Teilinformationsobjekts beim zweiten Server notwendig sind, in eine Datenstruktur, welche er an den Client als Client-Server-1-Antwort übermittelt.

[0013] Der Client fragt auf Grund der erhaltenen Datenstruktur beim zweiten Server das zweite Teilinformationsobjekt ab und fügt die beiden Teilinformationsobjekte zum gesamten Informationsobjekt zusammen.

[0014] Es kann erfindungsgemäß vorgesehen sein, dass sich das erste Teilinformationsobjekt in einer ersten Datenbank auf dem ersten Server und das zweite Teilinformationsobjekt in einer zweiten Datenbank auf dem zweiten Server befinden und zusammen das gesamte Informationsobjekt bilden.

[0015] Es kann weiters vorgesehen sein, dass das erste Teilinformationsobjekt im ersten Teildatenbestand und das zweite Teilinformationsobjekt im zweiten Teildatenbestand durch dasselbe statische Pseudonym identifiziert werden.

[0016] Es kann weiters für jede Sitzung (Session) zwischen Client und erstem Server sowie Client und zweitem Server ein nur für diese Session gültiges Session Pseudonym generiert werden, welches dem Client zur Zusammenführung des ersten Teilinformationsobjekts und des zweiten Teilinformationsobjekts zum gesamten Informationsobjekt dient.

[0017] Die Zuordnung Statisches Pseudonym und Session Pseudonym für ein Informationsobjekt im ersten Server im ersten Session Store und im zweiten Server im zweiten Session Store kann persistent gehalten werden.

[0018] Der erste Teildatenbestand kann in der ersten Datenbank am ersten Server und der zweite Teildatenbestand kann in der zweiten Datenbank auf dem zweiten Server gespeichert werden, wobei diese beiden Teildatenbestände zusammen die Gesamtheit aller mit diesem Verfahren verarbeiteten Informationsobjekte darstellen.

[0019] Der erste Server kann bei der Abfrage eines Informationsobjekts durch den Client im ersten Schritt im ersten Session Store Nachschau halten, ob dort zu diesem Informationsobjekt und dessen Statischen Pseudonym bereits ein Session Pseudonym existiert, widrigenfalls dieses mittels einer Anfrage vom zweiten Server angefordert wird, anschließend vom diesem generiert wird, die Zuordnung Statisches Pseudonym - Session Pseudonym in einer Antwort an

den ersten Server übermittelt wird und sowohl im zweiten als auch im ersten Session Store gespeichert werden.

[0020] Der erste Server kann den Client bei einer Anfrage zur Neuanlage eines Informationsobjekts oder Suche eines Informationsobjekts auf Grund von Merkmalen aus dem zweiten Teilinformationsobjekt an den zweiten Server weiterleiten, worauf der Client die entsprechenden vom zweiten Server zu speichernden oder zu suchenden Daten in einer Anfrage an den zweiten Server übermittelt, dieser die entsprechende Transaktion durchführt, ein Session Pseudonym zum Statischen Pseudonym und eine TransaktionsID generiert, diese Zuordnung einschließlich TransaktionsID im zweiten Session Store speichert und den Client unter Beifügung der TransaktionsID an den ersten Server zurückleitet.

[0021] Der zweite Server kann bei einer Anfrage zur Neuanlage eines zweiten Teilinformationsobjekts die vom Client übermittelten Daten als zweites Teilinformationsobjekt unter Beifügung des neu zu generierenden Statischen Pseudonyms in der zweiten Datenbank speichern.

[0022] Der erste Server kann mittels einer Anfrage unter Beifügung der TransaktionsID beim zweiten Server die Zuordnung Statisches Pseudonym- Session Pseudonym für diese Session anfragen, worauf der zweite Server diese Information im zweiten Session Store ermittelt und in einer Server-Server-Antwort an den ersten Server übermittelt, welcher diese Information in seinem eigenen Session Store speichert.

[0023] Die Antwort des zweiten Servers kann die Zuordnung Statisches Pseudonym -Session Pseudonym beinhalten, wenn sich der Client zum Zeitpunkt der Anfrage bereits beim zweiten Server authentifiziert hat, und anderenfalls eine „leere" Antwort übermitteln.

[0024] Der zweite Server kann nach Übermittlung der Antwort an den ersten Server die TransaktionsID invalidieren, wodurch mit dieser keine weitere Anfrage mehr möglich ist.

[0025] Der erste Server kann entsprechend der Anfrage des Clients das entsprechende Teilinformationsobjekt aus seiner ersten Datenbank abrufen und dieses zusammen mit dem Session Pseudonym in eine Datenstruktur einschließlich bestimmter Metadaten, welche die Abfrage des Clients des zweiten Teilinformationsobjekts beim zweiten Server ermöglichen, einbetten und diese in einer Antwort an den Client übermitteln, wobei diese Datenstruktur keinerlei Daten aus dem zweiten Teilinformationsobjekt enthält.

[0026] Der Client kann nach Erhalt der Datenstruktur in der Antwort vom ersten Server in einer Anfrage mittels des in diese Datenstruktur eingebetteten Session Pseudonyms und der Metadaten beim zweiten Server das Teilinformationsobjekt abfragen und dieses unter Beifügung des Session Pseudonyms in einer Antwort übermittelt erhält, wodurch dem Client unter Verwendung des Session Pseudonyms die Zusammenführung des ersten Teilinformationsobjekts und des zweiten Teilinformationsobjekts zum gesamten Informationsobjekt möglich ist.

[0027] Sämtliche Anfragen als auch sämtliche Antworten können aus Sicherheitsgründen ausschließlich über gesicherte HTTPS-Verbindungen übermittelt werden.

[0028] Bildet die Transaktion die Neuanlage eines Informationsobjekts oder das Suchen eines solchen, leitet der erste Server den Client an den zweiten Server weiter, welchem per Anfrage die Daten des zweiten neu anzulegenden oder zu suchenden Teilinformationsobjekts übermittelt werden. Der zweite Server generiert ein Statisches Pseudonym bei einer Neuanlage oder ermittelt dieses auf Grund von Suchkriterien, generiert ein Session Pseudonym sowie eine TransaktionsID und fragt das zweite Teilinformationsobjekt in seiner zweiten Datenbank ab oder generiert dort ein solches neu. Dann leitet der zweite Server den Client unter Beifügung der TransaktionsID an den ersten Server zurück, welcher über eine Anfrage beim zweiten Server das Statische Pseudonym und das Session Pseudonym abfragt, wobei beim zweiten Server die TransaktionsID invalidiert. Nun übermittelt der erste Server dem Client das erste Teilinformationsobjekt mit dem Session Pseudonym in einer Datenstruktur als Antwort.

[0029] Der Client ruft in einer zweiten Anfrage an den zweiten Server das zweite Teilinformationsobjekt ab und fügt es unter Zuhilfenahme des Session Pseudonyms zum gesamten Infor-

mationsobjekt zusammen.

[0030] Erhält nun ein Server eine Anfrage von einem Client unter Beifügung dieses Session Pseudonyms (SID), so kann dieser auf das korrespondierende Statische Pseudonym (PID) schließen, das entsprechende Teilinformationsobjekt aus seiner Datenbank laden und an den Client übermitteln.

[0031] Sollte es nun trotz aller technischen Sicherheitsmaßnahmen einem Angreifer gelingen, ein solches Session Pseudonym (SID) abzufangen, so kann dieser nach Beendigung der jeweiligen Client-Session mit diesem SID keine Datensätze mehr identifizieren oder abfragen, da die SID invalidiert ist und mit dieser nicht mehr auf das Statische Pseudonym (PID) geschlossen werden kann.

[0032] Neben dem technisch notwendigen Koordinierungsdatenstrom, der über eine gesicherte Verbindung zwischen dem ersten Server und dem zweiten Server geführt wird, werden zwischen diesen beiden Servern keinerlei Inhaltsdaten von Teilinformationsobjekten ausgetauscht oder von einem Server - in welcher Form auch immer - über den jeweils anderen Server zum Client durchgeleitet.

[0033] Beim Aufbau dieses Koordinierungsdatenstroms authentifizieren sich die beiden Server je dem anderen gegenüber, wodurch sichergestellt werden kann, dass jeder Server stets tatsächlich auch mit dem „richtigen" Server des Systems kommuniziert (beiderseitige Authentifizierung).

[0034] Das Verfahren ermöglicht eine Vielzahl von Transaktionen, welche im Prinzip alle die Abarbeitung derselben technischen Schritte erfordern. Abhängig von der durchzuführenden Transaktion können bestimmte Schritte auch entfallen.

[0035] Das Verfahren ermöglicht die aufgetrennte pseudonymisierte Speicherung beliebiger Informationsobjekte auf zwei voneinander unabhängigen Computersystemen (Servern), durch jeweilige Auftrennung eines Informationsobjekts in zwei Teilinformationsobjekte, wobei jedes dieser Teilinformationsobjekte jeweils auf einem unabhängigen Server verarbeitet wird.

[0036] Lediglich auf Abruf eines Clients und ausschließlich auf diesem werden die beiden Teilinformationsobjekte vom jeweiligen Server abgerufen und am Client zusammenführt, wobei mittels eines Pseudonyms, welches zu jedem dieser beiden Teilinformationsobjekte ebenfalls gespeichert wird, definiert wird, welche beiden Teilinformationsobjekte zusammen das gesamte Informationsobjekt bilden.

[0037] Inhaltsdaten bzw. Teilinformationsobjekte des einen Computersystems werden zu keiner Zeit an das jeweils andere Computersystem übermittelt.

[0038] Auch eine Durchleitung eines Teilinformationsobjekts über das jeweils andere Computersystem erfolgt nicht.

[0039] Da die Zusammenführung der beiden Teilinformationsobjekte stets nur am Client erfolgt, werden die zusammengehörigen Teilinformationsobjekte immer und ausschließlich außerhalb der technischen und organisatorischen Sphäre der beiden Daten haltenden Computersysteme (Server) zusammengefügt.

[0040] Eine weitere charakteristische Eigenschaft dieses Verfahrens ist es, dass einem Client niemals das Statische Pseudonym (PID) übermittelt wird, welches ein Informationsobjekt identifiziert und der Zusammenführung der beiden Teilinformationsobjekte zum gesamten Informationsobjekt dient.

[0041] Sämtliche Kommunikationen zwischen den beiden Servern erfolgen ausschließlich über eine verschlüsselte, identitäts- und integritätsgesicherte Verbindung (z. B. HTTPS, SOAP over HTTPS). Jeder Server, der bei dem jeweils anderen Server eine Abfrage durchführen möchte, muss sich diesem gegenüber authentifizieren. Es erfolgt beim Verbindungsaufbau folglich eine beiderseitige Authentifizierung (z. B. mittels eines gültigen Zertifikats).

[0042] Bei der Kommunikation zwischen einem Client und einem der beiden Server kommen

ausschließlich integritätsgesicherte und verschlüsselte Verbindungen zum Einsatz (z.B. HTTPS). Diese werden bereits beim ersten Verbindungsaufbau vom Client zu einem Server hergestellt und somit noch vor Übermittlung der Authentifikationsdaten eines Benutzers.

[0043] Für jedes Informationsobjekt wird ein Statisches Pseudonym (PID) vergeben, welches dieses sowohl in der Datenbank des ersten Servers als auch in jener des zweiten identifiziert. An Clients wird dieses Statische Pseudonym (PID) jedoch niemals übermittelt, sondern pro Session wird für jedes abgefragte Informationsobjekt ein ausschließlich für diese Session gültiges Session Pseudonym (SID) generiert, mittels welchem von jedem der beiden Server auf das Statische Pseudonym (PID) geschlossen werden kann. Lediglich dieses Session Pseudonym (SID) wird an den Client zur Abfrage des korrespondierenden Teilinformationsobjekts übermittelt. Zusätzlich muss diese Zuordnung PID - SID über eine gesicherte Verbindung (Koordinierungsdatenstrom) auch dem jeweils zweiten Server bekannt gegeben werden, damit auch dieser das korrekte Mapping PID - SID im Zuge einer Clientabfrage vornehmen kann.

[0044] Weitere erfindungsgemäße Merkmale sind den Ansprüchen, der Beschreibung und den Zeichnungen zu entnehmen.

[0045] Das erfindungsgemäße Verfahren wird nun an Hand der Figur 1 detailliert beschrieben. Fig. 1 zeigt einen Client 1, einen ersten Server 3 und einen zweiten Server 6.

[0046] Schritt 0: Der Client 1 verbindet sich mittels einer gesicherten Verbindung (z. B. HTTPS) zum ersten Server 3. Im Anschluss identifiziert bzw. authentifiziert sich der Client 1 beim ersten Server 3 (z. B. Übermittlung von Benutzername/Passwort oder mittels Zertifikat, Smartcard, Fingerprint, etc.).

[0047] Schritt 1: Der Client 1 übermittelt an den ersten Server 3 eine Client-Server-1-Anfrage 2 zur Durchführung einer der folgenden Transaktionen: Anlegen eines Informationsobjektes 4, Abfrage eines Informationsobjektes 4, Suchen eines Informationsobjektes 4 auf Grund von Merkmalen des zweiten Teildatenbestands 5 auf dem zweiten Server 6.

[0048] Falls die Client-Server-1-Anforderung 2 an den ersten Server 3 in Schritt 1 eine Abfrage eines Informationsobjektes 4 ist, folgt Schritt 1a:

[0049] Schritt 1a: Der erste Server 3 prüft in seinem ersten Session Store 7 nach, ob zum Statischen Pseudonym 8 des abzurufenden Teilinformationsobjekts 9 bereits ein Session Pseudonym 10 existiert. Falls dies nicht der Fall ist, folgt Schritt 1a I:

[0050] Schritt 1a I: Der erste Server 3 stellt beim zweiten Server 6 über eine gesicherte Verbindung eine Server-Server-Anfrage 11, um zum Statischen Pseudonym 8 des ersten Teilinformationsobjektes 9 ein Session Pseudonym 10 zu erhalten.

[0051] Schritt 1a II: Hat sich der Client 1 auch bereits beim zweiten Server 6 authentifiziert, generiert der zweite Server 6 zu diesem Statischen Pseudonym 8 ein Session Pseudonym 10, speichert diese Zuordnung in seinem zweiten Session Store 12 und übermittelt das Tupel Statisches Pseudonym 8 - Session Pseudonym 10 über die gesicherte Verbindung mittels einer Server-Server-Antwort 13 an den ersten Server 3. Der erste Server 3 speichert nun ebenfalls die Zuordnung Statisches Pseudonym 8 - Session Pseudonym 10 in seinem ersten Session Store 7 ab. Ist der Client 1 zum Zeitpunkt der Server-Server-Abfrage 11 noch nicht beim zweiten Server 6 authentifiziert, wird ein leeres Tupel mittels einer Server-Server-Antwort 13 an den ersten Server 3 zurückgegeben.

[0052] Schritt 1b: Der erste Server 3 fragt nun das vom Client 1 angeforderte erste Teilinformationsobjekt 9 aus seinem Ersten Teildatenbestand 14, welcher permanent in der ersten Datenbank 15 gespeichert ist, ab.

[0053] Schritt 1c: Fortsetzung mit Schritt 10

[0054] Schritt 2: Der erste Server 3 leitet nun die Verbindung zwischen diesem 3 und dem Client 1 mittels Redirect an den zweiten Server 6 weiter, wodurch im Folgenden auch eine gesicherte Verbindung (z. B. HTTPS zwischen Client 1) und dem zweiten Server 6 geöffnet wird.

[0055] Schritt 2a: Hat sich der Client 1 noch nicht gegenüber dem zweiten Server 6 authentifiziert, so muss sich der Client 1 nun auch gegenüber dem zweiten Server 6 authentifizieren (z. B. durch Übermittlung von Benutzername/Passworts oder sonstige Authentifizierungsmechanismen).

[0056] Schritt 3: Der Client 1 übermittelt an den zweiten Server 6 nun mittels einer Client-Server-2-Anfrage 16 die Daten für das neu anzulegende zweite Teilinformationsobjekt 17 oder beliebige Suchkriterien des zu suchenden zweiten Teilinformationsobjekts 17.

[0057] Schritt 3a: Soll ein zweites Teilinformationsobjekt 17 hinzugefügt werden, generiert der zweite Server 6 ein Statisches Pseudonym 8, mittels welchem die Zuordnung erstes Teilinformationsobjekt 9 - zweites Teilinformationsobjekt 17 für die gesamte Speicherdauer dauerhaft erfolgen und kann in späterer Folge dem Client 1 effektiv zur Zusammenführung des Informationsobjekts 4 dient.

[0058] Schritt 4: Aus dem Statischen Pseudonym 8 wird nun ein ausschließlich für diese beiden Client-Sitzungen (Sessions) (Client 1 und erster Server 3 sowie Client 1 und zweiter Server 6) gültiges Session Pseudonym 10 generiert und zusammen mit dem Statischen Pseudonym 8 im zweiten Session Store 12 vom zweiten Server 6 gespeichert.

[0059] Schritt 5: Der zweite Server 6 generiert nun eine TransaktionsID und verknüpft diese TransaktionsID mit dem Tupel Statisches Pseudonym 8 - Session Pseudonym 10.

[0060] Schritt 6: Der zweite Server 6 leitet den Client 1 nun mittels Redirect unter Beifügung der TransaktionsID an den ersten Server 3 zurück.

[0061] Schritt 7: Der erste Server 3 fragt nun über eine gesicherte Verbindung mittels einer Server-Server-Anfrage 11 beim zweiten Server 6 das dieser TransaktionsID entsprechende Tupel Statisches Pseudonym 8 - Session Pseudonym 10 ab.

[0062] Schritt 8: Der zweite Server 6 übermittelt dem ersten Server 3 mittels einer Server-Server-Antwort 13 die in Schritt 7 angeforderten Informationen und invalidiert im Anschluss die entsprechende TransaktionsID.

[0063] Schritt 9: Der erste Server 3 legt nun abhängig von der Client-Server-1-Anforderung 2 aus Schritt 1 entweder ein leeres erstes Teilinformationsobjekt 9 unter Beifügung des vom zweiten Server 6 erhaltenen Statischen Pseudonyms 8 in seiner ersten Datenbank 15 an oder fragt entsprechend des vom zweiten Server 6 erhaltenen Statischen Pseudonyms 8 das entsprechende in der ersten Datenbank 15 gespeicherte erste Teilinformationsobjekt 9 ab.

[0064] Schritt 10: Der erste Server 3 generiert nun aus dem ersten Teilinformationsobjekt 9 unter Beifügung des Session Pseudonyms 10 eine entsprechende Datenstruktur 18, welche am Client 1 (z. B. durch Anzeige am Display) verarbeitet werden soll. In diese Datenstruktur werden auch entsprechende Metadaten eingebettet, welche dem Client 1 eine Abfrage des korrespondierenden zweiten Teilinformationsobjekts 17 auf dem zweiten Server 6 mittels des Session Pseudonyms 10 ermöglichen, wobei diese Datenstruktur 18 keinerlei Daten aus dem zweiten Teildatenbestand 5 beinhaltet.

[0065] Schritt 11: Die in Schritt 10 generierte Datenstruktur 18 wird über die gesicherte Verbindung mittels einer Client-Server-1-Antwort 19 an den Client 1 übermittelt.

[0066] Schritt 12: Der Client 1 fragt nun über eine Client-Server-2-Anfrage 16 beim zweiten Server 6 durch Übermittlung des Session Pseudonyms 10 und der vom ersten Server 3 in der Datenstruktur 18 erhaltenen Metadaten das zweite Teilinformationsobjekt 17 beim zweiten Server 6 ab.

[0067] Schritt 13: Der zweite Server 6 sucht nun in seinem Session Store 12 das dem Session Pseudonym 10 entsprechende Statische Pseudonym 8 und fragt das entsprechende zweite Teilinformationsobjekt 17 in seiner Datenbank 20 ab.

[0068] Schritt 14: Dieses zweite Teilinformationsobjekt 17 übermittelt der zweite Server 6 über eine Client-Server-2-Antwort 21 an den Client 1.

[0069] Schritt 15: Der Client 1 fügt nun das in der vom ersten Server 3 erhaltenen Datenstruktur 18 eingebettete erste Teilinformationsobjekt 9 und das vom zweiten Server 6 erhaltene zweite Teilinformationsobjekt 17 zum Informationsobjekt 4 zusammen (z. B. durch direkte Einbindung in den DOM-Tree mittels JavaScript).

[0070] Die Erfindung umfasst das beschriebene Verfahren sowie eine Vorrichtung zur Implementierung des Verfahrens mit zumindest einem Client und zumindest zwei Servern, sowie ein Computerprogrammprodukt welches ein Programm zur Realisierung des beschriebenen Verfahrens implementiert.

BEZUGSZEICHENLISTE

1 Client
2 Client-Server-1-Anfrage
3 Erster Server
4 Informationsobjekt
5 Zweiter Teildatenbestand
6 Zweiter Server
7 Erster Session Store
8 Statisches Pseudonym (PID)
9 Erstes Teilinformationsobjekt
10 Session Pseudonym (SID)
11 Server-Server-Anfrage
12 Zweiter Session Store
13 Server-Server-Antwort
14 Erster Teildatenbestand
15 Erste Datenbank
16 Client-Server-2-Anfrage
17 Zweites Teilinformationsobjekt
18 Datenstruktur
19 Client-Server-1-Antwort
20 Zweite Datenbank
21 Client-Server-2-Antwort

Ansprüche

1. Verfahren zur pseudonymisierten Datenverarbeitung, **dadurch gekennzeichnet**, dass das abzufragende Informationsobjekt (4) getrennt auf zumindest einem ersten Server (3) und einem zweiten Server (6) vorliegt und das Verfahren folgende Schritt umfasst:
   a. zuerst wird vom Client (1) eine Anfrage (2) an den ersten Server (3) übermittelt, auf Grund welcher der erste Server (3) zusammen mit dem zweiten Server (6) eine Transaktion betreffend das Informationsobjekt (4) durchführen soll;
   b. der erste Server (3) leitet den Client (1) an den zweiten Server (6) weiter, welchem der Client (1) die das zweite Teilinformationsobjekt (17) darstellenden Daten in Form einer Anfrage (16) übermittelt;
   c. der zweite Server (6) generiert ein Statisches Pseudonym (8), ein Session Pseudonym (10) sowie eine eindeutige TransaktionsID, speichert diese Daten in seinem Session Store (12) und speichert das zweite Teilinformationsobjekt (17) zusammen mit dem Statischen Pseudonym (8) in seiner (zweiten) Datenbank (20) ab;
   d. der Client (1) wird unter Übermittlung der TransaktionsID an den ersten Server (3) zurückgeleitet, welcher unter Übermittlung (11) der TransaktionsID das Statische Pseudonym (8) und das Session Pseudonym (10) beim zweiten Server (6) abfragt, der wiederum nach Übermittlung der Antwort (13) die TransaktionsID invalidiert;
   e. der erste Server (3) ruft das erste Teilinformationsobjekt (9) aus seiner Datenbank (15) ab und verpackt dieses zusammen mit dem Session Pseudonym (10) und bestimmten Metadaten, welche für die Abfrage des zweiten Teilinformationsobjekts (17) beim zweiten Server (6) notwendig sind, in eine Datenstruktur (18), welche er an den Client (1) als Client-Server-1-Antwort (19) übermittelt;
   f. der Client (1) fragt auf Grund der erhaltenen Datenstruktur (18) beim zweiten Server (6) das zweite Teilinformationsobjekt (17) ab und fügt die beiden Teilinformationsobjekte zum gesamten Informationsobjekt (4) zusammen.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, dass sich das erste Teilinformationsobjekt (9) in einer ersten Datenbank (15) auf dem ersten Server (3) und das zweite Teilinformationsobjekt (17) in einer zweiten Datenbank (20) auf dem zweiten Server (6) befinden und zusammen das gesamte Informationsobjekt (4) bilden.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet**, dass das erste Teilinformationsobjekt (9) im ersten Teildatenbestand (14) und das zweite Teilinformationsobjekt (17) im zweiten Teildatenbestand (5) durch dasselbe statische Pseudonym (8) identifiziert werden.

4. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet**, dass an den Client (1) niemals das Statische Pseudonym (8) übermittelt wird, sondern für jede Sitzung (Session) zwischen Client (1) und erstem Server (3) sowie Client (1) und zweitem Server (6) ein nur für diese Session gültiges Session Pseudonym (10) generiert wird, welches dem Client (1) zur Zusammenführung des ersten Teilinformationsobjekts (9) und des zweiten Teilinformationsobjekts (17) zum gesamten Informationsobjekt (4) dient.

5. Verfahren nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet**, dass die Zuordnung Statisches Pseudonym (8) und Session Pseudonym (10) für ein Informationsobjekt (4) im ersten Server (3) im ersten Session Store (7) und im zweiten Server im zweiten Session Store (12) persistent gehalten werden.

6. Verfahren nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet**, dass der erste Teildatenbestand (14) in der ersten Datenbank (15) am ersten Server (3) und der zweite Teildatenbestand (5) in der zweiten Datenbank (20) auf dem zweiten Server (6) gespeichert werden, wobei diese beiden Teildatenbestände zusammen die Gesamtheit aller mit diesem Verfahren verarbeiteten Informationsobjekte (4) darstellen.

7. Verfahren nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet**, dass der erste Server (3) bei der Abfrage (2) eines Informationsobjekts (4) durch den Client (1) im ersten

Schritt im ersten Session Store (7) Nachschau hält, ob dort zu diesem Informationsobjekt (4) und dessen Statischen Pseudonym (8) bereits ein Session Pseudonym (10) existiert, widrigenfalls dieses mittels einer Anfrage (11) vom zweiten Server (6) angefordert wird, anschließend vom diesem generiert wird, die Zuordnung Statisches Pseudonym (8) - Session Pseudonym (10) in einer Antwort (13) an den ersten Server (3) übermittelt wird und sowohl im zweiten (12) als auch im ersten (7) Session Store gespeichert werden.

8. Verfahren nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet**, dass der erste Server (3) den Client (1) bei einer Anfrage (2) zur Neuanlage eines Informationsobjekts (4) oder Suche eines Informationsobjekts (4) auf Grund von Merkmalen aus dem zweiten Teilinformationsobjekt (17) an den zweiten Server (6) weitergeleitet wird, der Client (1) die entsprechenden vom zweiten Server (6) zu speichernden oder zu suchenden Daten in einer Anfrage (16) an den zweiten Server (6) übermittelt, dieser die entsprechende Transaktion durchführt, ein Session Pseudonym (10) zum Statischen Pseudonym (8) und eine TransaktionsID generiert, diese Zuordnung einschließlich TransaktionsID im zweiten Session Store (12) speichert und den Client (1) unter Beifügung der TransaktionsID an den ersten Server (3) zurückleitet.

9. Verfahren nach einem der Ansprüche 1 bis 6 oder 8, **dadurch gekennzeichnet**, dass der zweite Server (6) bei einer Anfrage (16) zur Neuanlage eines zweiten Teilinformationsobjekts (17) die vom Client (1) übermittelten Daten als zweites Teilinformationsobjekt (17) unter Beifügung des neu zu generierenden Statischen Pseudonyms (8) in der zweiten Datenbank (20) speichert.

10. Verfahren nach einem der Ansprüche 1 bis 6, 8 oder 9, **dadurch gekennzeichnet**, dass der erste Server (3) mittels einer Anfrage (11) unter Beifügung der TransaktionsID beim zweiten Server (6) die Zuordnung Statisches Pseudonym (8) - Session Pseudonym (10) für diese Session anfragt, der zweite Server (6) diese Information im zweiten Session Store (12) ermittelt und in einer Server-Server-Antwort (13) an den ersten Server (3) übermittelt, welcher diese Information in seinem eigenen Session Store (7) speichert.

11. Verfahren nach einem der Ansprüche 1 bis 6, 8 bis 10, **dadurch gekennzeichnet**, dass die Antwort (13) des zweiten Servers (6) die Zuordnung Statisches Pseudonym (8) - Session Pseudonym (10) beinhaltet, wenn sich der Client (1) zum Zeitpunkt der Anfrage (11) bereits beim zweiten Server (6) authentifiziert hat, anderenfalls eine „leere" Antwort (13) übermittelt.

12. Verfahren nach einem der Ansprüche 1 bis 6, 8 bis 11, **dadurch gekennzeichnet**, dass der zweite Server (6) nach Übermittlung der Antwort (13) an den ersten Server (3) die TransaktionsID invalidiert, wodurch mit dieser keine weitere Anfrage (11) mehr möglich ist.

13. Verfahren nach einem der Ansprüche 1 bis 12, **dadurch gekennzeichnet**, dass der erste Server (3) entsprechend der Anfrage (2) des Clients (1) das entsprechende Teilinformationsobjekt (9) aus seiner ersten Datenbank (15) abruft und dieses zusammen mit dem Session Pseudonym (10) in eine Datenstruktur (18) einschließlich bestimmter Metadaten, welche die Abfrage (16) des Clients (1) des zweiten Teilinformationsobjekts (17) beim zweiten Server (6) ermöglichen, einbettet und diese in einer Antwort (19) an den Client (1) übermittelt, wobei diese Datenstruktur (18) keinerlei Daten aus dem zweiten Teilinformationsobjekt (17) enthält.

14. Verfahren nach einem der Ansprüche 1 bis 13, **dadurch gekennzeichnet**, dass der Client (1) nach Erhalt der Datenstruktur (18) in der Antwort (19) vom ersten Server (3) in einer Anfrage (16) mittels des in diese Datenstruktur (18) eingebetteten Session Pseudonyms (8) und der Metadaten beim zweiten Server (6) das Teilinformationsobjekt (17) abfragt und dieses unter Beifügung des Session Pseudonyms (10) in einer Antwort (17) übermittelt erhält, wodurch dem Client (1) unter Verwendung des Session Pseudonyms (10) die Zusammenführung des ersten Teilinformationsobjekts (9) und des zweiten Teilinformationsobjekts (17) zum gesamten Informationsobjekt (4) möglich ist.

15. Verfahren nach einem der Ansprüche 1 bis 14, **dadurch gekennzeichnet**, dass sämtliche Anfragen (2, 11 und 16) als auch sämtliche Antworten (18, 13, und 21) ausschließlich über gesicherte HTTPS-Verbindungen übermittelt werden.
16. Vorrichtung mit zumindest einem Client (1), zumindest einem ersten Server (3) und einem zweiten Server (6) welche zur Ausführung eines Verfahrens gemäß einem der Ansprüche 1 bis 15 ausgeführt ist.
17. Computerprogrammprodukt zur Ausführung einer pseudonymisierten Datenverarbeitung gemäß eines Verfahrens nach einem der Ansprüche 1 bis 15.

Hierzu 1 Blatt Zeichnungen

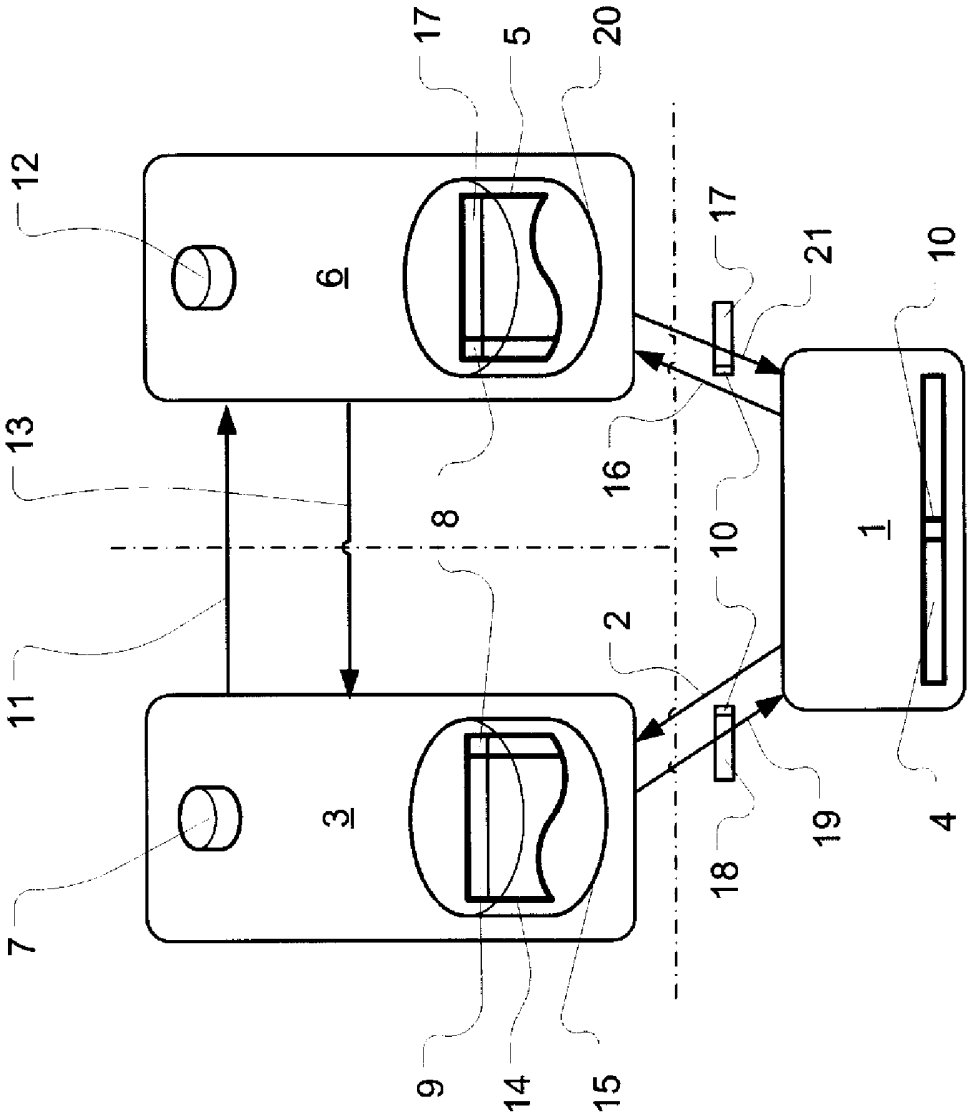


Fig. 1

Recherchenbericht zu **GM 668/2010**

österreichisches patentamt

Klassifikation des Anmeldungsgegenstands gemäß IPC: ***G06F21/00*** (2006.01); ***H04L29/06*** (2006.01)
Klassifikation des Anmeldungsgegenstands gemäß ECLA: G06F21/00N9A2P1, H04L29/06S4A
Recherchierter Prüfstoff (Klassifikation): G06F21, H04L29
Konsultierte Online-Datenbank: EPODOC, WPI, TXT
Dieser Recherchenbericht wurde zu den **am 29. Oktober 2010 eingereichten** Ansprüchen **1-17** erstellt. Die in der Gebrauchsmusterschrift veröffentlichten Ansprüche könnten im Verfahren geändert worden sein (§ 19 Abs. 4 GMG), sodass die Angaben im Recherchenbericht, wie Bezugnahme auf bestimmte Ansprüche, Angabe von Kategorien (X, Y, A), nicht mehr zutreffend sein müssen. In die dem Recherchenbericht zugrundeliegende Fassung der Ansprüche kann beim Österreichischen Patentamt während der Amtsstunden Einsicht genommen werden.

Kategorie*)	Bezeichnung der Veröffentlichung: Ländercode, Veröffentlichungsnummer, Dokumentart (Anmelder), Veröffentlichungsdatum, Textstelle oder Figur soweit erforderlich	Betreffend Anspruch
X	Spitzer et al.; 'Securing a Web-Based Teleradiology Platform According to German Law and "Best Practices".' In: Medical Informatics in a United and Healthy Europe - Proceedings of MIE 2009, The XXIInd International Congress of the European Federation for Medical Informatics, Sarajevo, Bosnia and Herzegovina, August 30 - September 2, 2009. Edited by Adlassnig et al., IOS Press, 2009. Vol. 150, p. 730-734 Gesamtes Dokument, siehe http://dx.doi.org/10.3233/978-1-60750-044-5-730 und http://person.hst.aau.dk/ska/MIE2009/papers/MIE2009p0730.pdf	1-17
A	US 5956400 A (CHAUM ET AL) 21. September 1999 (21.09.1999) Zusammenfassung, Abschnitt "BRIEF SUMMARY OF THE INVENTION", Fig. 1 und ihre Beschreibung	1-17
A	EP 2199907 A1 (KONINKLIJKE PHILIPS ELECTRONICS NV) 23. Juni 2010 (23.06.2010) Zusammenfassung, Figuren 1-4 und ihre Beschreibungen	1-17
A	WO 2005117481 A1 (KONINKLIJKE PHILIPS ELECTRONICS NV) 08. Dezember 2005 (08.12.2005) Zusammenfassung, Figur 1 und ihre Beschreibung	1-17

Datum der Beendigung der Recherche:	☐ Fortsetzung siehe Folgeblatt	Prüfer(in):
8. März 2012		PRAMHAS A.

*) **Kategorien** der angeführten Dokumente:

- **X** Veröffentlichung **von besonderer Bedeutung**: der Anmeldungsgegenstand kann allein aufgrund dieser Druckschrift nicht als neu bzw. auf erfinderischer Tätigkeit beruhend betrachtet werden.
- **Y** Veröffentlichung **von Bedeutung**: der Anmeldungsgegenstand kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren weiteren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese **Verbindung für einen Fachmann naheliegend** ist.
- **A** Veröffentlichung, die den **allgemeinen Stand der Technik** definiert.
- **P** Dokument, das **von Bedeutung** ist (Kategorien **X** oder **Y**), jedoch **nach dem Prioritätstag** der Anmeldung **veröffentlicht** wurde.
- **E** Dokument, das **von besonderer Bedeutung** ist (Kategorie **X**), aus dem ein **älteres Recht** hervorgehen könnte (früheres Anmeldedatum, jedoch nachveröffentlicht, Schutz ist in Österreich möglich, würde Neuheit in Frage stellen).
- **&** Veröffentlichung, die Mitglied der selben **Patentfamilie** ist.