(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. Juni 2011 (16.06.2011)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2011/069492 A1

(51) Internationale Patentklassifikation:
*H04L 29/06* (2006.01) *G06F 21/00* (2006.01)

(21) Internationales Aktenzeichen: PCT/DE2010/001435

(22) Internationales Anmeldedatum:
9. Dezember 2010 (09.12.2010)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2009 057 800.5
10. Dezember 2009 (10.12.2009) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **EBERHARD KARLS UNIVERSITÄT TÜBINGEN** [DE/DE]; Geschwister-Scholl-Platz, 72074 Tübingen (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **BORCHERT, Bernd** [DE/DE]; Ludwig-Schriever-Str. 16, 48480 Lünne (DE). **REINHARDT, Klaus** [DE/DE]; Weissdornweg 14 /151, 72076 Tübingen (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, 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, RO, RS, RU, 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, 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).

**Erklärungen gemäß Regel 4.17**:

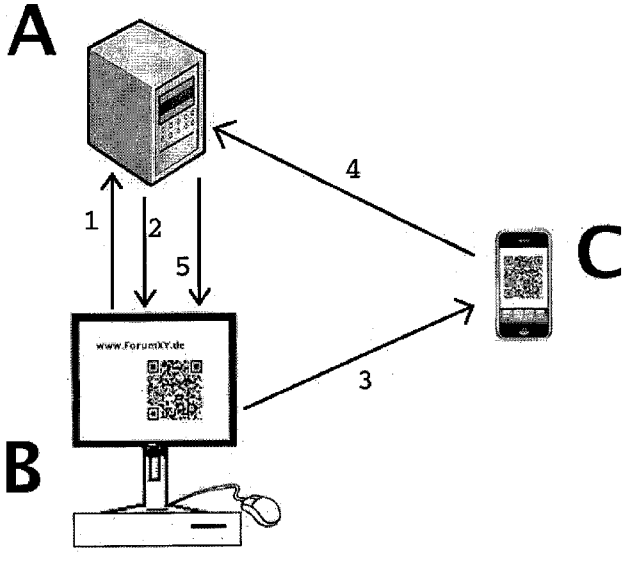
— *hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii)*

*[Fortsetzung auf der nächsten Seite]*

(54) **Title**: METHOD FOR PROVIDING A SECURE AND CONVENIENT ACCESS TO ONLINE ACCOUNTS VIA REMOTE FORWARD

(54) **Bezeichnung** : VERFAHREN UND COMPUTERPROGRAMMPRODUKTE ZUM AUTHENTISIERTEN ZUGANG ZU ONLINE -ACCOUNTS

Abb. 1




(57) **Abstract**: The invention relates to a method for providing a secure and convenient access to a document in a computer network, especially to online user accounts (online accounts), these accounts especially being access-restricted user accounts requiring authorization. In addition to a server computer and a client computer which are located in the same computer network, the method requires a mobile communication device having a camera, a processing unit with memory and means for communication (e.g. a mobile phone with Internet access and built-in camera). The method comprises the following steps: upon inquiry (1) of the client computer (B), the server computer (A) transmits information (2) to the client computer (B) which information is displayed on the client display as information (3); information (3) is read and processed by the mobile communication device (C); the result is transmitted to the server computer (A) as information (4); if the result of examination of the data is positive, information (5) is forwarded to the client computer (B) which then provides the local access. The method allows the convenient and secure handling of access information to a plurality of user accounts, such as e.g. passwords, user names, and login addresses. Since no permanent passwords are used but only single-use passwords which are only valid for seconds, the method remedies the problem of password overload and identity theft through electronic eavesdropping by Trojans.

(57) **Zusammenfassung**:

*[Fortsetzung auf der nächsten Seite]*

WO 2011/069492 A1

— *Erfindererklärung (Regel 4.17 Ziffer iv)*

**Veröffentlicht**:

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

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

Die Erfindung betrifft ein Verfahren zum Bereitstellen eines sicheren Zugangs zu Online-Benutzerkonten. Es handelt sich dabei um zugangsbeschränkte Benutzerkonten, die eine Autorisierung benötigen. Für das Verfahren werden neben einem Server-Rechner und einem Klienten-Rechner noch zusätzlich ein mobiles Kommunikationsgerät mit einer Kamera benötigt. Das Verfahren beinhaltet folgende Schritte: der Server-Rechner (A) schickt nach Anfrage (1) des Klienten-Rechners (B) die Informationen (2) an den Klienten-Rechner (B), die am Klienten-Bildschirm als Informationen (3) dargestellt werden; die Informationen (3) werden vom mobilen Kommunikationsgerät (C) mittels der Kamera eingelesen und verarbeitet; das Ergebnis wird als Information (4) zum Server-Rechner (A) übertragen; nach positiver Prüfung der Daten werden die Informationen (5) zum Klienten-Rechner (B) geschickt, der dort den Zugang bereitstellt. Mit dem Verfahren wird es ermöglicht, Zugangsinformationen zu mehreren Benutzerkonten, wie z. B. Passwörter, Benutzernamen, Login -Adressen, bequem und sicher zu handhaben. Dabei werden keine Dauer-Passwörter verwendet werden, sondern nur noch Einmal-Passwörter, die nur wenige Sekunden gültig sind.

# VERFAHREN UND COMPUTERPROGRAMMPRODUKTE ZUM AUTHENTISIERTEN ZUGANG ZU ONLINE-ACCOUNTS

Die vorliegende Erfindung betrifft ein Verfahren zum Bereitstellen eines sicheren und komfortablen Zugangs zu einem Dokument in einem Rechnernetz, insbesondere zu Online-Benutzerkonten (Online-Accounts).

Viele Internet-Benutzer kennen das Problem der *Passwort-Flut*: die vielen Passwörter (und auch die Benutzer-Namen und Login-Adressen) für die Online-Benutzerkonten können sich viele Benutzer kaum merken.

Es gibt improvisierte Methoden, mit der Passwort-Flut zurecht zu kommen. Eine davon ist, sich die Passwörter auf dem eigenen Handy abzuspeichern. Entsprechende Handy-Programme gibt es schon für einige Handy-Typen. Es bleibt aber bei der manuellen Eingabe der Benutzerdaten auf dem Bildschirm. Auch das im Folgenden beschriebene Problem der Sicherheit bei der Passwort-Eingabe ist dadurch nicht gelöst, denn es handelt sich dabei weiterhin um Dauer-Passwörter.

Das Eintippen eines Passworts am Computerbildschirm ist unsicher gegenüber dem Abhören durch Trojaner („*Identitäts-Diebstahl*" durch sog. „keylogger"): Der Trojaner beobachtet, welche Tasten bei der Passwort-Eingabe gedrückt werden. Auch wenn das Passwort per Mausklicks auf einer Tastaturanzeige am Bildschirm eingegeben wird, kann ein Trojaner es mittels Bildverarbeitung abhören. Wenn das Passwort auf dem Rechner abgespeichert ist und automatisch in das Passwort-Feld eingetragen wird, ist es sogar noch problematischer, denn der Trojaner kann es jederzeit aus dem Rechnerspeicher herauslesen oder aber bei der Eingabe abhören (auch wenn auf dem Bildschirm nur Sternchen oder andere verdeckende Zeichen angezeigt werden, kann ein Trojaner das Passwort dennoch innerhalb des Softwaresystems finden).

Abgelauschte Passwörter können vom Trojaner per Rechnetz heimlich verschickt werden, z.B. an Zentralen, in denen die gestohlenen Identitäten gesammelt werden, um sie dann für Missbrauch-Zwecke weiterzuverkaufen.

Es gibt Methoden gegen den Identitätsdiebstahl durch Trojaner, z.B. das Foto-PIN-Verfahren mit dem Fotohandy, siehe Patentanmeldung DE-2007029759.

Es ist bislang jedoch kein Verfahren für eine sichere und gleichzeitig für den Benutzer bequeme Handhabung von Passwörtern für Online-Benutzerkonten bekannt.

Der vorliegenden Erfindung lag somit die Aufgabe zugrunde, ein Verfahren zum sicheren und gleichzeitig komfortablen Zugang zu Online-Dokumenten, z.B. Benutzerkonten, bereit zu stellen, insbesondere für zugangsbeschränkte Benutzerkonten, die eine Autorisierung benötigen. Mit dem Verfahren soll es außerdem möglich sein, Zugangsinformationen zu mehreren Benutzerkonten, wie z.B. Passwörter, Benutzernamen, Login-Adressen, bequem und sicher zu handhaben.

Diese Aufgabe wird erfindungsgemäß durch ein Verfahren gelöst, bei dem neben einem Server-Rechner und einem Klienten-Rechner, die sich im gleichen Rechnernetz befinden, noch zusätzlich ein mobiles Kommunikationsgerät mit einer Kamera, einem Prozessor mit Speicher und Mitteln zur Kommunikation mit einem Server-Rechner benötigt wird. Das mobile Kommunikationsgerät kann insbesondere ein Handy mit Internet-Zugang und eingebauter Kamera sein.

Um sich den Zugang zu einem Dokument, z.B. ein Online-Benutzerkonto, auf dem Klienten-Rechner zu verschaffen, werden folgende Schritte ausgeführt (**Abb.1**).

Als erstes wird vom Benutzer eine Anfrage (Informationen 1) an den Server-Rechner übertragen. Das kann beispielsweise durch das Aufrufen einer sog. URL für ein Dokument (eine Internetseite) durch ein sog. Browser-Programm, das auf dem Rechner des Benutzers (Klienten-Rechner) läuft, geschehen.

Nach dem Empfang dieser Anfrage durch den Server-Rechner wird von diesem eine Antwortnachricht (Informationen 2) generiert und auf den Klienten-Rechner übertragen.

Diese Antwortnachricht enthält einen Teil der Autorisierungsdaten, die dazu benötigt werden, um den Zugang zum Dokument auf dem Server-Rechner bereit zu stellen. Die Antwortnachricht kann insbesondere kryptographisch verschlüsselt sein. Die Antwortnachricht wird auf dem Bildschirm des Benutzers, z.B. in Form eines Barcodes, angezeigt (Informationen 3) und kann eine Identifizierung des Server-Rechners, der aufgerufenen Internetseite, und / oder eine Identifizierung des Klienten-Rechners beim Server-Rechner enthalten.

Die auf dem Bildschirm des Klienten-Rechners angezeigten Informationen 3 werden nun vom Benutzer mittels der Kamera des mobilen Kommunikationsgeräts eingelesen (aufgenommen) und in seinem Prozessor verarbeitet. Dabei werden die eingelesenen Informationen ggf. entschlüsselt und mit den vom Benutzer im Speicher abgelegten und für die Zuordnung von Identifizierungsdaten zu bestimmten Dokumenten (z.B. Internetseiten) notwendigen Daten verglichen. Bei diesem Vorgang wird der vom Benutzer angefragte Server-Rechner identifiziert und Autorisierungsdaten (Informationen 4) für den Zugang zum aufgerufenen Dokument auf dem Server-Rechner neu generiert. Bevorzugt stellen die neu generierten Autorisierungsdaten eine kryptographische Signatur dar.

Die neu generierten Autorisierungsdaten werden vom mobilen Kommunikationsgerät auf den Server-Rechner übertragen und von diesem geprüft. Wenn die Prüfung der Autorisierungsdaten positiv ausfällt und der Server-Rechner den Klienten-Rechner anhand der Autorisierungsdaten identifiziert hat, überträgt der Server-Rechner die Zugangsdaten (Informationen 5) an den Klienten-Rechner. Nach dem Empfang der Zugangsdaten durch den Klienten-Rechner wird der Zugang zum Dokument gewährt. Dies kann z.B. dadurch erreicht werden, dass auf dem Bildschirm des Klienten-Rechners eine neue Seite mit dem entsprechenden Dokument (z.B. Benutzerkonto) angezeigt wird. Alternativ schickt der Server-Rechner an den Klienten-Rechner die URL des angefragten Dokuments, ggf. einschließlich Autorisierungsdaten, so dass der Benutzer anschließend vom Server-Rechner den Zugang zum Dokument erhält.

Alle Autorisierungsdaten, die im vorliegenden Verfahren generiert werden (Informationen 2, 4, 5, 7, 8, 9 und 10), sind bevorzugt nur eine kurze Zeit, z.B. wenige Sekunden, gültig. Wenn nach Ablauf dieser festgelegten Zeit der Server-Rechner keine

Autorisierungsdaten empfängt bzw. als übereinstimmend identifiziert, werden die späteren Anfragen vom Klienten-Server nicht beantwortet. Deswegen wird durch das erfindungsgemäße Verfahren ein Missbrauch von Autorisierungsdaten erschwert.

Bei einem Rechnernetz-Protokoll wie dem World Wide Web (als Teil des Internets) sieht die Architektur nicht vor, dass ein Server-Rechner, der einem Klienten-Rechner ein Dokument geschickt hat, welches per sogenanntem Browser auf dem Bildschirm des Klienten-Rechners dargestellt wird, dieses Dokument auf dem Bildschirm des Klienten-Rechners direkt durch ein anderes ersetzen kann. Deshalb wird per sogenanntes "polling" dem Server die Möglichkeit gegeben, ein Dokument beim Klienten-Rechner zu ersetzen: das neue Dokument wird als Rückantwort auf eine Anfrage des Klienten-Rechner beim Server-Rechner gesendet. Deshalb kann erfindungsgemäß der Übertragung der Zugangsdaten (Informationen 5) vom Server-Rechner an den Klienten-Rechner zusätzlich zumindest eine Übertragung von Informationen 6 vom Klienten-Rechner an den Server-Rechner vorausgehen (**Abb. 2**). Die Informationen 5 sind in diesem Fall eine Rückantwort auf Informationen 6.

Gemäß einer weiteren Ausführungsform der Erfindung kann das mobile Kommunikationsgerät mit mindestens einem weiteren Server-Rechner (hier als Account-Rechner bezeichnet) kommunizieren (**Abb. 3**). Dabei werden Anfragen (Informationen 7) vom mobilen Kommunikationsgerät erzeugt und an einen der Account-Rechner übertragen. Der Account-Rechner generiert als Antwort Informationen 8 und überträgt sie an das mobile Kommunikationsgerät. Dort werden sie verarbeitet, wobei Informationen 4 erzeugt werden, die Autorisierungsdaten für den Zugang zu einem Dokument auf dem Account-Rechner enthalten. Nach dem Empfang der Informationen 5 überträgt der Klienten-Rechner an den Account-Rechner Informationen 9, die bevorzugt auch Autorisierungsdaten enthalten. Der Account-Rechner prüft die Autorisierung und überträgt bei positivem Ergebnis die Informationen 10 an den Klienten-Rechner, die bevorzugt das angefragte Dokument darstellen.

Gemäß einer weiteren Ausführungsform kann das Verfahren zum Schutz gegen die Folgen eines Diebstahls des mobilen Kommunikationsgeräts mit einer Passwort-Abfrage beim Server kombiniert werden, entweder via die übliche Login-Webseite mit

Passwort-Abfrage, oder aber auch via trojanersichere Verfahren, z.B. das Foto-PIN-Verfahren, wie in DE-2007029759 beschrieben.

Die vorliegende Erfindung betrifft ferner Computerprogrammprodukt zur Durchführung des erfindungsgemäßen Verfahrens auf einem Prozessor im Server-Rechner.

Die vorliegende Erfindung betrifft ferner Computerprogrammprodukt zur Durchführung des erfindungsgemäßen Verfahrens auf einem Prozessor im weiteren Server-Rechner (Account-Rechner).

Die vorliegende Erfindung betrifft ferner Computerprogrammprodukt zur Durchführung des erfindungsgemäßen Verfahrens auf einem Prozessor im mobilen Kommunikationsgerät.

Mit dem erfindungsgemäßen Verfahren kann sich der Benutzer somit ohne Eintippen von Passwort und Benutzername in ein Online-Benutzerkonto am Computerbildschirm einloggen.

Ein weiterer Vorteil der Erfindung besteht darin, dass ein Identitäts-Diebstahl durch Trojaner auf dem Rechner des Benutzers praktisch ausgeschlossen wird, denn es werden dabei keine mehrfach benutzbaren Dauer-Passwörter verwendet, sondern nur noch Einmal-Passwörter, die nur wenige Sekunden gültig sind.

Weitere Vorteile, Merkmale und Anwendungsmöglichkeiten der Erfindung werden nachstehend anhand der Ausführungsbeispiele mit Bezug auf die Zeichnungen beschrieben. In den Zeichnungen zeigen:

**Abb. 1**: Der Server-Rechner **A** schickt nach Anfrage **1** des Klienten-Rechners **B** die Informationen **2** an den Klienten-Rechner **B**, die am Klienten-Bildschirm als Informationen **3** dargestellt werden. Die Informationen **3** werden vom mobilen Kommunikationsgerät **C** eingelesen und verarbeitet. Das Ergebnis wird als Information **4** zum Server-Rechner **A** geschickt. Nach positiver Prüfung der Daten werden die Informationen **5** zum Klienten-Rechner **B** geschickt, der dort den Zugang bereitstellt.

**Abb. 2**: Wenn, wie z.B. beim World Wide Web, der Server-Rechner **A** Informationen **5** nicht direkt an den Klienten-Rechner **B** schicken kann, wird dem Server-Rechner **A** durch eine vom Klienten-Rechner an den Server-Rechner geschickte Anfrage die Gelegenheit gegeben, die Information **5** als Rückantwort auf die Information **6** an den Klienten-Rechner **B** zu übertragen („polling").

**Abb. 3**: Beim mobilen Kommunikationsgerät **C** kann eine Kommunikations-Prozedur mit einem zweiten Server-Rechner (Account-Rechner) **D** stattfinden, die mindestens aus dem Übertragen von zwei Informationen **7** (hin) und **8** (zurück) besteht. Die Autorisierungsdaten zum Zugang auf diesen zweiten Server **D** kommen als Teil der Informationen **4** und **5** bei Klienten-Rechner **B** an, der diese Daten nutzt, um den Zugang beim zweiten Server **D** zu etablieren, indem er die Autorisierungsdaten als Informationen **9** an den zweiten Server **D** schickt, der dann den Zugang auf dem Bildschirm des Klienten-Rechners bereitstellt, indem er Information **10** an den Klienten-Rechner **B** überträgt.

## Ausführungsbeispiele

Das erfindungsgemäße Verfahren kann den Zugang zu Online-Benutzerkonten im Wesentlichen auf zwei Wegen ermöglichen: entweder über eine direkte (**Abb. 1 und 2**) oder über eine indirekte Fern-Weiterleitung (**Abb. 3**).

### *Verfahren zum Bereitstellen des Zugangs zu Online-Benutzerkonten mittels einer direkten Fern-Weiterleitung*

Für ein Online-Benutzerkonto, z.B. eine Download-Seite oder ein Forum, wird auf dem Fotohandy des Benutzers der Server-Name, der Konto-Name und ein geheimer krytographischer Schlüssel gespeichert. Wenn der Benutzer in das Benutzerkonto hinein will, geht er auf die Einlog-Internetseite des Benutzerkonto--Anbieters. Dort hat der Account-Server einen 2D-Code hingestellt, in dem der Server-Name und eine Session-ID stehen. Diese Information wird vom Benutzer durch Abfotografieren in das Fotohandy eingelesen. Das Fotohandy macht dann - völlig selbständig - folgendes: es sucht den abgespeicherten Benutzernamen für diesen Server-Namen; dann berechnet

es aus der Session-ID mit dem Schlüssel ein Codewort (Signatur); am Schluss geht das Handy per mobiles Internet auf eine Webseite des Account-Servers und übermittelt dem Account-Server den Benutzernamen, die Session-ID und das daraus berechnete Codewort. Der Account-Server prüft die Angaben: wenn das Codewort ok ist, schaltet der Account-Server das Benutzerkonto frei, d.h. auf dem Bildschirm des Benutzers wird die Situation wie nach dem Einloggen angezeigt.

***Verfahren zum Bereitstellen des Zugangs zu Online-Benutzerkonten mittels einer indirekten Fern-Weiterleitung***

Auf dem Fotohandy des Benutzers sind mehrere Benutzerkonten wie beim oben beschriebenen Beispiel gespeichert. Der Benutzer ruft mit seinem Browser eine feste Webseite für die indirekte Fern-Weiterleitung auf. Den auf der Seite stehenden 2D Code liest er mit einem Programm auf dem Fotohandy ein. Das Fotohandy zeigt ihm dann auf dem Display eine Liste seiner Benutzerkonten an. Der Benutzer wählt ein Benutzerkonto aus. Daraufhin setzt sich das Handy im Hintergrund mit dem entsprechenden Account-Server in Verbindung, um eine neue Session-ID („nonce“) zu erhalten, die nur wenige Sekunden gültig sein wird Die Session-ID wird auf dem Handy mit dem kryptographischen Schlüssel dieses Benutzerkontos signiert. Zusammen werden Servername, Benutzername, Session-ID und Signaturwert zum Fern-Weiterleitungs-Server geschickt, und von dort aus zum Browser am Bildschirm des Benutzers. Der Browser ruft eine Login-Seite des Account-Servers auf und schickt dabei Servername. Benutzername, Session-ID und Signaturwert als Parameter mit. Nach positiver Prüfung der Autorisierungsdaten erscheint im Browserfenster beim Benutzer das geöffnete Benutzerkonto.

**Patentansprüche**

1. Verfahren zum Bereitstellen eines Zugangs auf einem Klienten-Rechner zu einem Dokument in einem Rechnernetz von einem mobilen Kommunikationsgerät aus, wobei das mobile Kommunikationsgerät eine Kamera, einen Prozessor mit Speicher und Mittel zur Kommunikation mit einem Server-Rechner aufweist, und der Klienten-Rechner und der Server-Rechner sich im Rechnernetz befinden, gekennzeichnet durch folgende Schritte:

   (a) Erzeugung von Informationen 1 als Anfrage durch den Klienten-Rechner und Übertragung von Informationen 1 an den Server-Rechner,

   (b) Empfang von Informationen 1 durch den Server-Rechner, Erzeugung von Informationen 2 auf dem Server-Rechner, Übertragung von Informationen 2 vom Server-Rechner auf den Klienten-Rechner,

   (c) Empfang von Informationen 2 und Darstellung von Informationen 3 auf dem Bildschirm des Klienten-Rechners,

   (d) Einlesen der Informationen 3 vom Bildschirm des Klienten-Rechners durch die Kamera des mobilen Kommunikationsgeräts,

   (e) Verarbeitung der Informationen 3 auf dem mobilen Kommunikationsgerät, Erzeugung von Informationen 4 und Übertragung von Informationen 4 vom mobilen Kommunikationsgerät auf den Server-Rechner,

   (f) Empfang und Prüfung von Informationen 4 durch den Server-Rechner, Erzeugung und Übertragung von Informationen 5 für den Zugang auf den Klienten-Rechner,

   (g) Bereitstellen des Zugangs auf dem Klienten-Rechner.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das Dokument zugangsbeschränkt ist und eine Autorisierung für das Bereitstellen des Zugangs benötigt, insbesondere Online-Benutzerkonten.

3. Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass mindestens eine der Informationen 1, 2, 3, 4 und 5 Autorisierungsdaten für den Zugang zu einem Dokument auf dem Server-Rechner enthalten.

4. Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass die auf dem Bildschirm des Klienten-Rechners dargestellten Informationen 3 eine Identifizierung des Server-Rechners und / oder des Dokuments und / oder eine Identifizierung des Klienten-Rechners beim Server-Rechner beinhalten.

5. Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass der Speicher des mobilen Kommunikationsgeräts Informationen für die Zuordnung von Identifizierungsdaten von Server-Rechnern zu bestimmten Dokumenten gespeichert hat.

6. Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass der Übertragung der Informationen 5 zumindest eine Übertragung von Informationen 6 vom Klienten-Rechner an den Server-Rechner vorausgeht.

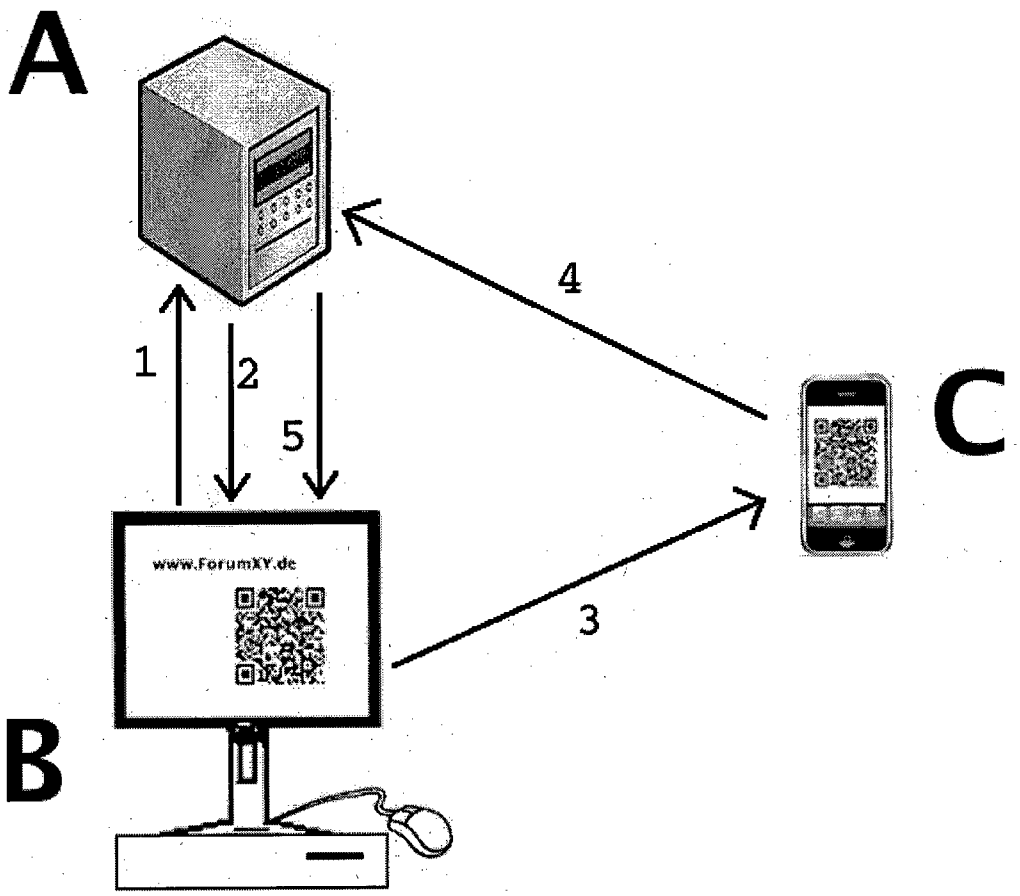
7. Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass das mobile Kommunikationsgerät mit einem zweiten Server-Rechner kommuniziert, wobei Informationen 7 von dem mobilen Kommunikationsgerät erzeugt und an den zweiten Server-Rechner übertragen werden, die Informationen 7 vom zweiten Server-Rechner empfangen werden, Informationen 8 vom zweiten Server-Rechner erzeugt und an das mobile Kommunikationsgerät übertragen werden, Informationen 8 vom mobilen Kommunikationsgerät empfangen und verarbeitet werden, wobei Informationen 4 erzeugt werden, und das Bereitstellen des Zugangs auf dem Klienten-Rechner dadurch zustande kommt, dass der Klienten-Rechner Informationen 9 an den zweiten Server-Rechner überträgt, der zweiter Server-Rechner Informationen 10 erzeugt und an den Klienten-Rechner überträgt.

8. Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass mindestens eine der Informationen 1, 2, 4, 5, 7, 8, 9 und 10 Autorisierungsdaten für den Zugang zu einem Dokument auf dem zweiten Server-Rechner enthalten.

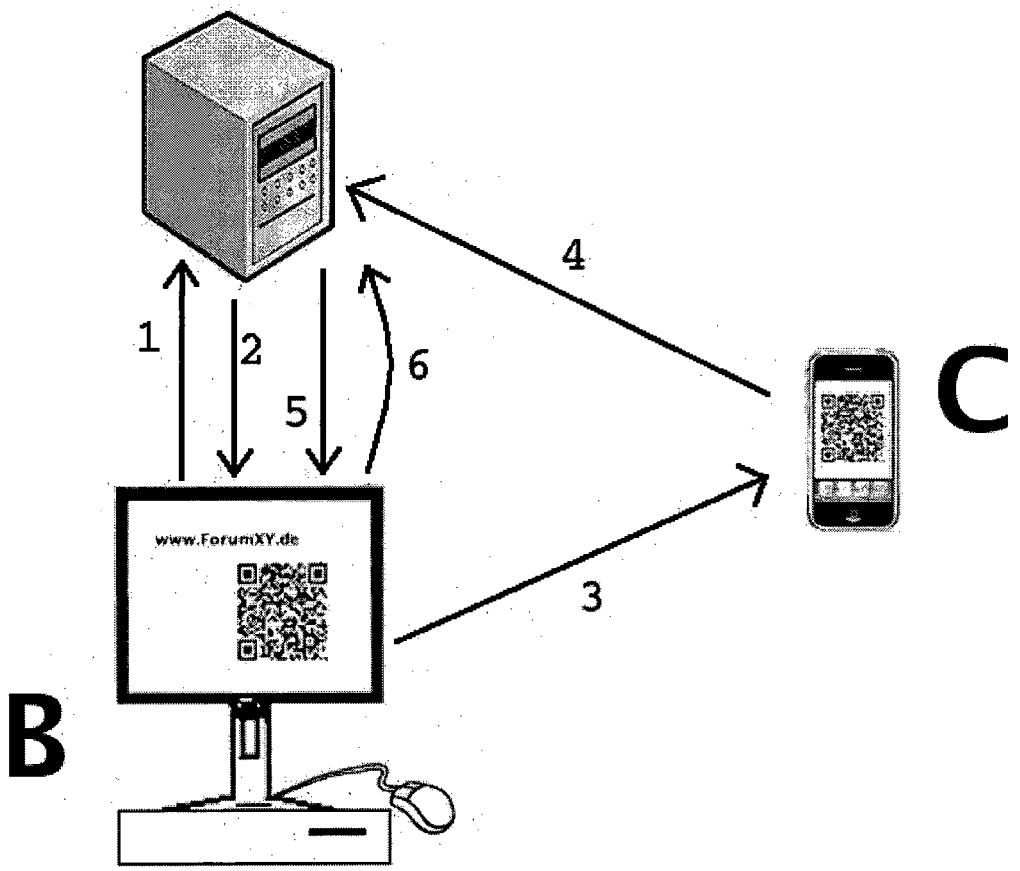
9. Verfahren nach einem der vorgehenden Ansprüche, dadurch gekennzeichnet, dass die Autorisierungsdaten für das Bereitstellen des Zugangs eine begrenzte Zeit nach ihrer Erzeugung durch den Server-Rechner und / oder durch den zweiten Server-Rechner und / oder durch das mobile Kommunikationsgerät gültig sind.

10. Computerprogrammprodukte zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 9, wenn die Computerprogramme auf einem Prozessor im Server-Rechner oder im zweiten Server-Rechner oder im mobilen Kommunikationsgerät ausgeführt werden.

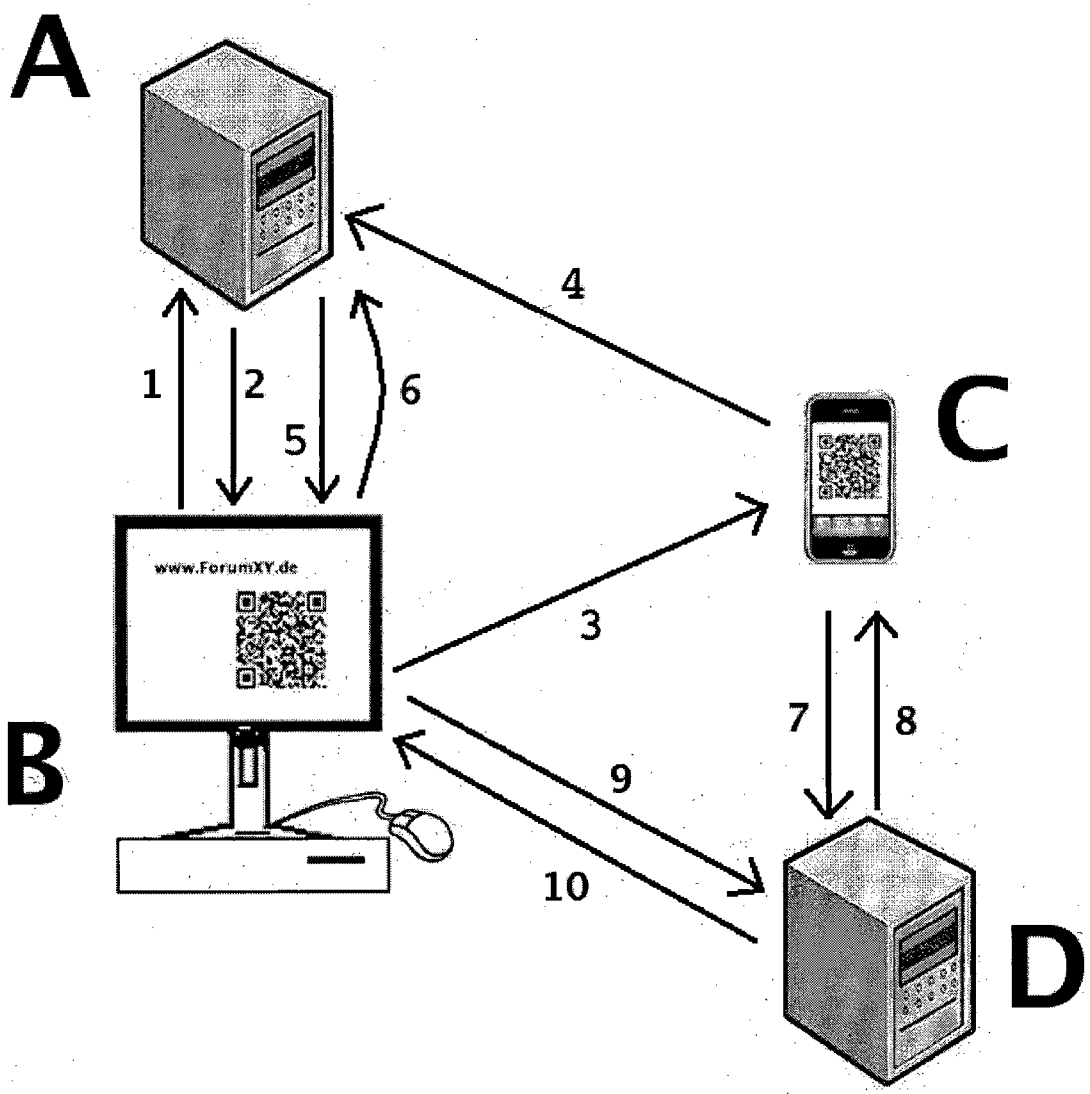
# Abb. 1



# Abb. 2



# Abb. 3



# INTERNATIONAL SEARCH REPORT

International application No
PCT/DE2010/001435

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 G06F21/00
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
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 practical, search terms used)

EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | MICHIRU TANAKA ET AL: "A Method and Its Usability for User Authentication by Utilizing a Matrix Code Reader on Mobile Phones", 28 August 2006 (2006-08-28), INFORMATION SECURITY APPLICATIONS; [LECTURE NOTES IN COMPUTER SCIENCE;;LNCS], SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 225 - 236, XP019077665, ISBN: 978-3-540-71092-9 page 226, line 33 - page 232, line 11 ----- | 1-6,9,10 |
| X | JP 2007 193762 A (TOSHIBA CORP; TOSHIBA SOLUTIONS CORP) 2 August 2007 (2007-08-02) paragraph [0005] paragraph [0012] paragraph [0028] - paragraph [0074] ----- | 1-6,9,10 |

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document 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 |
|---|---|
| 6 May 2011 | 18/05/2011 |

| Name and mailing address of the ISA/ | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040,<br>Fax: (+31-70) 340-3016 | Ströbeck, Anders |

# INTERNATIONAL SEARCH REPORT

International application No
PCT/DE2010/001435

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X,P | EP 2 166 697 A1 (GMV SOLUCIONES GLOBALES INTERN [ES]) 24 March 2010 (2010-03-24) paragraph [0030] - paragraph [0045] | 1-4,10 |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/DE2010/001435

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| JP 2007193762 A | 02-08-2007 | NONE | |
| EP 2166697 A1 | 24-03-2010 | US 2010070759 A1 | 18-03-2010 |

# INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE2010/001435

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L29/06 G06F21/00
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, INSPEC

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

| Kategorie* | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile | Betr. Anspruch Nr. |
|---|---|---|
| X | MICHIRU TANAKA ET AL: "A Method and Its Usability for User Authentication by Utilizing a Matrix Code Reader on Mobile Phones", 28. August 2006 (2006-08-28), INFORMATION SECURITY APPLICATIONS; [LECTURE NOTES IN COMPUTER SCIENCE;;LNCS], SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 225 - 236, XP019077665, ISBN: 978-3-540-71092-9 Seite 226, Zeile 33 - Seite 232, Zeile 11 ----- | 1-6,9,10 |
| X | JP 2007 193762 A (TOSHIBA CORP; TOSHIBA SOLUTIONS CORP) 2. August 2007 (2007-08-02) Absatz [0005] Absatz [0012] Absatz [0028] - Absatz [0074] ----- | 1-6,9,10 |

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, 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 anderen 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 |
|---|---|
| 6. Mai 2011 | 18/05/2011 |

| Name und Postanschrift der Internationalen Recherchenbehörde | Bevollmächtigter Bediensteter |
|---|---|
| Europäisches Patentamt, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040,<br>Fax: (+31-70) 340-3016 | Ströbeck, Anders |

# INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE2010/001435

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

| Kategorie* | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile | Betr. Anspruch Nr. |
|---|---|---|
| X,P | EP 2 166 697 A1 (GMV SOLUCIONES GLOBALES INTERN [ES]) 24. März 2010 (2010-03-24) Absatz [0030] - Absatz [0045] | 1-4,10 |

## INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/DE2010/001435

| Im Recherchenbericht angeführtes Patentdokument | Datum der Veröffentlichung | Mitglied(er) der Patentfamilie | Datum der Veröffentlichung |
|---|---|---|---|
| JP 2007193762 A | 02-08-2007 | KEINE | |
| EP 2166697 A1 | 24-03-2010 | US 2010070759 A1 | 18-03-2010 |