PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
G06F 1/00, H04Q 7/38, H04L 9/32

A1

(11) International Publication Number: **WO 97/31306**

(43) International Publication Date: 28 August 1997 (28.08.97)

(21) International Application Number: PCT/FI97/00067

(22) International Filing Date: 6 February 1997 (06.02.97)

(30) Priority Data:
960820 23 February 1996 (23.02.96) FI

(71) Applicant *(for all designated States except US)*: NOKIA MOBILE PHONES LTD. [FI/FI]; PI 86, FIN-24101 Salo (FI).

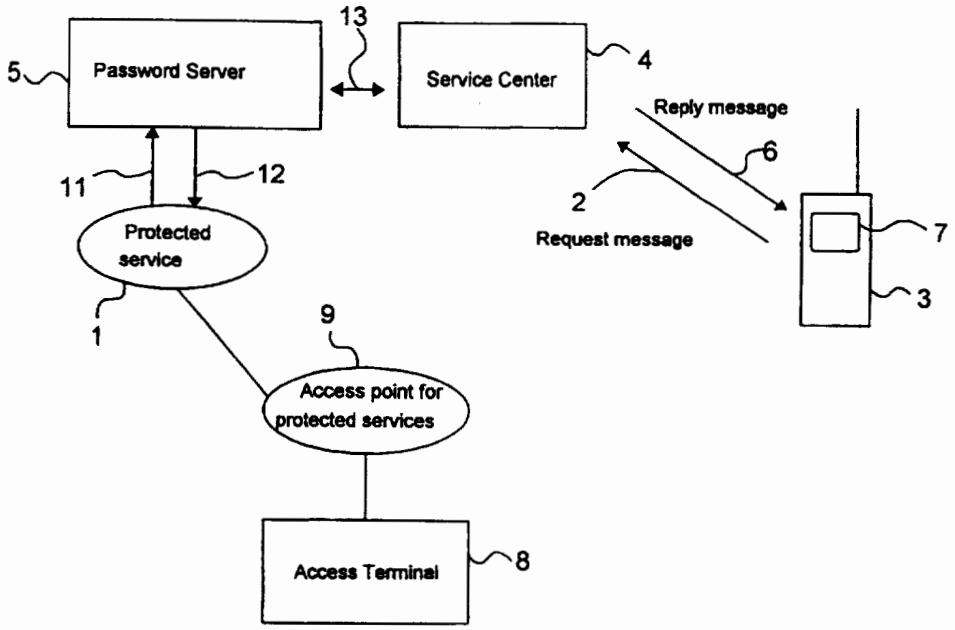
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: SORMUNEN, Toni [FI/FI]; Artturintie 6, FIN-33880 Sääksjärvi (FI). KURKI, Teemu [FI/FI]; Lahtomäenkatu 3 G 102, FIN-33580 Tampere (FI).

(74) Agents: PURSIAINEN, Timo et al.; Tampereen Patenttitoimisto Oy, Hermiankatu 6, FIN-33720 Tampere (FI).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD FOR OBTAINING AT LEAST ONE ITEM OF USER AUTHENTICATION DATA



(57) Abstract

A method for obtaining at least one item of user specific data, wherein the user specific data is obtained at least partly by using paging or a short message service.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	**GB**	United Kingdom	**MW**	Malawi
AT	Austria	**GE**	Georgia	**MX**	Mexico
AU	Australia	**GN**	Guinea	**NE**	Niger
BB	Barbados	**GR**	Greece	**NL**	Netherlands
BE	Belgium	**HU**	Hungary	**NO**	Norway
BF	Burkina Faso	**IE**	Ireland	**NZ**	New Zealand
BG	Bulgaria	**IT**	Italy	**PL**	Poland
BJ	Benin	**JP**	Japan	**PT**	Portugal
BR	Brazil	**KE**	Kenya	**RO**	Romania
BY	Belarus	**KG**	Kyrgystan	**RU**	Russian Federation
CA	Canada	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CF	Central African Republic			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SG**	Singapore
CH	Switzerland	**KZ**	Kazakhstan	**SI**	Slovenia
CI	Côte d'Ivoire	**LI**	Liechtenstein	**SK**	Slovakia
CM	Cameroon	**LK**	Sri Lanka	**SN**	Senegal
CN	China	**LR**	Liberia	**SZ**	Swaziland
CS	Czechoslovakia	**LT**	Lithuania	**TD**	Chad
CZ	Czech Republic	**LU**	Luxembourg	**TG**	Togo
DE	Germany	**LV**	Latvia	**TJ**	Tajikistan
DK	Denmark	**MC**	Monaco	**TT**	Trinidad and Tobago
EE	Estonia	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**UG**	Uganda
FI	Finland	**ML**	Mali	**US**	United States of America
FR	France	**MN**	Mongolia	**UZ**	Uzbekistan
GA	Gabon	**MR**	Mauritania	**VN**	Viet Nam

Method for obtaining at least one item of user authentication data

The invention relates to a method and system for obtaining at least one item of user specific authentication data, such as a password and/or a user name.

Information services refer in this specification chiefly to electronic information services which can be used by a data processor or the like. For using an information service, a data transmission connection is formed from the data processor to the information service, which is for example an application in the computer of the information service provider. The data transmission connection can be formed for example by using a telecommunication network or a mobile communication network. Upon using an information service, usually user specific authentication data is required, for example a user name and password, which are given with a data processor at the stage when the connection to the information service is formed. The user name and the password enable the information service provider to control the user using the information service, wherein also invoicing can be directed to the users appropriately for example according to usage time. A further object of the user name and the password is to prevent unauthorized use of the information service.

A wide range of services is available for example via the Internet network. Via the network it is possible to make orders and to scan databases and articles. In addition, many banks offer their customers the possibility to pay bills and enquire account transactions using a data processor at home or even at work.

A user name is user specific and it is usually not changed in different connection set-ups. Passwords, on the other hand, can be divided into three main types:

1. One single password valid as long as the user is a registered subscriber to the service. A password of this type is used mainly in services with less need for security.

2. A list of single-connection passwords, each valid for only one connection. For the first connection, the first password is used, for the second connection, the second password is used, etc., as long as all the passwords in the list are used. Subsequently, a new set of passwords has to be ordered before the service can be further used. In some services a new list is sent within a short notice before the last password in the list is used in order to minimize the possible interruption at the list change. Passwords of this type are commonly used with information services provided especially by banks.

3. A periodical password valid for a predefined period of time. This type of password may be used within the period determined for the password regardless of how many times the connection is made. The validity period may be for example a month or a year, after which the password is to be changed into a new one.

Especially when using passwords of the type 2., the problem is that the list has to be kept safe and account of the last used password has to be kept in one way or another. Thus the possibility of abuse is great, especially if the list and the user name are preserved in the same place.

Regardless of which password type is used, it is the user of the service who is to a great extent responsible for data security, and the service provider has few possibilities to prevent and control abuse for example in case the password falls into the wrong hands.

When a new user starts using the information service, the user has to register to the information service provider. This may be done for example by a written subscription request, in which the user gives his or her personal data and other information required, most often by mail, electronic mail (e-mail) or facsimile. In due course, the new user is sent a user name and a password or a list of passwords. These are sent most commonly by mail. In some cases the information may also be sent by facsimile, but in this case it is more likely that the user name

and the password fall into the wrong hands. Also electronic mail may be used for informing a user name and a password. However, especially the Internet network is an open network in which the communicated data is in unenciphered form. Furthermore, unauthorized persons can easily read information transferred via the Internet.

In some cases, the user is mailed the information that the user specific authentication data may be dispatched from a post office or bank. In this case the identity of the user can still be checked when the authentication data is despatched.

Figure 1 shows a flow diagram of a commonly used method for obtaining user specific authentication data. The person (block 101) who wants to become a user of an information service, sends a subscription request (block 102) to the information service provider (block 103). The information service provider sends a subscription form to the user (block 104). Having filled in the form (block 105), the user sends it back to the service provider for example by facsimile or by mail (block 106). The information service provider subsequently handles the form and allots the user the user specific authentication data and sends it for instance by mail, electronic mail or facsimile (block 107). Having received the user specific authentication data, the user can start using the information service (block 108).

For example in the Internet network, some information service providers use a method for registering a new user, whereby the person who intends to become a user, forms a data transmission connection to the Internet address of the service provider. Thus in the display unit of a data processor a subscription form is produced, in which the user may fill in his or her personal data by using the keyboard of the data processor. Information to be filled in include e.g. forename, surname, a proposal for user name and password. After the information has been filled in, the data is saved to be processed in the computer of the service provider. The information service provider handles the information and, when accepting a new user, forms a record or the like for the user, in which the data of the new user is saved. After accepting the new user, the information service provider sends the information of this to the Internet address of the user. Next, the new user may form a connection

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.