(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 December 2004 (23.12.2004)

PCT

(10) International Publication Number
WO 2004/111809 A1

(51) International Patent Classification[7]: G06F 1/00, H04Q 7/22

(21) International Application Number: PCT/SE2003/001053

(22) International Filing Date: 18 June 2003 (18.06.2003)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: NOREFORS, Arne [SE/SE]; Hantverkargatan 44, S-112 21 Stockholm (SE). SCHUBERTH, Ulf [SE/SE]; Jakob Westinsgatan 6, 4tr, S-112 20 Stockholm (SE).

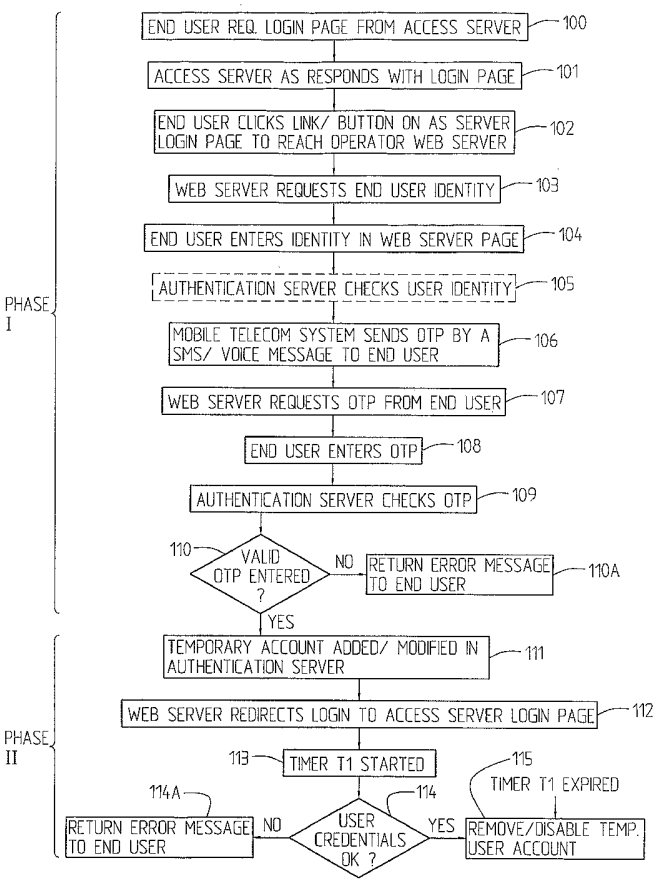
(74) Agents: BERGENTALL, Annika et al.; Cegumark AB, P.O. Box 53407, S-400 14 Göteborg (SE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: AN ARRANGEMENT AND A METHOD RELATING TO IP NETWORK ACCESS



(57) Abstract: The present invention relates to an arrangement and a method respectively for providing an end user with access to an IP network (login). It comprises a user station, an access server of an access network, a web server and an authentication server. The end user station comprises first means for communication with the access server and second means for communication over a mobile telecommunication system with the authentication server. The access/login procedure comprises a first and a second phase, the authentication server controls the first phase comprising a one-time-password (OTP) login sequence, and, if the one time password (OTP) is valid, the second login phase is performed in order to login the end user at the access server, by creating a temporary account for which user credentials are defined.

WO 2004/111809 A1

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Title:
AN ARRANGEMENT AND A METHOD RELATING TO IP NETWORK ACCESS

FIELD OF THE INVENTION

The present invention relates to an arrangement and a method for providing an end user with access to an IP network, i.e. here for end user login. The invention also relates to an access server of an access network over which access is provided, i.e. over which the end user can log in at the IP network.

STATE OF THE ART

To get access to some kind of a service in general, entering of password and username is needed. However, in the society of today the number of passwords etc. that one single user needs to remember, keep stored safely etc. is high, and might increase still further. There might e.g. be a particular password for WLAN access, for Internet services etc.

WISPs (Wireless Internet Service Providers) offer IP network access based on a web dialogue with the user for login and Radius communication with a Radius server. The typical procedure is to use a username and a static password. There are described preferred practises for how this could be done e.g. from Wi-Fi Alliance industry forum in the WISPr best practice document. The involved protocols are HTTP and Radius as defined by IETF (www.ietf.org). However, a static username is normally used at login. A static user name can easily be copied and hence be used by several persons. One attempt to solve this problem consists in using a one-time password (OTP), which only can be used during a limited time period, thereafter it is blocked. To get access or login to Internet at e.g. public places, such as airports, railway

stations, hotels etc. generally a WLAN may be used as access network. Generally the coverage is not so large and depends on construction etc. of the building, and moreover there are not so many frequencies available. The building and integration of radio networks is complicated and expensive. Access issues are thus complicated for serveral reasons, both for operators, users and network owners.

SUMMARY OF THE INVENTION

What is needed is therefore an arrangement through which access to an IP network, login, can be provided for in an easy manner, both from the point of view of the end user and from the point of view of the operator. An arrangement is also needed through which login can be provided with a minimum risk of abuse, e.g. through copying of usernames, finding usernames written down somewhere or similar. Further yet an arrangement is needed through which access/login can be provided without substantial impact on access servers, and through which existing access servers can be used without requiring access server upgrading. This is an important aspect since the organisation running the access server can be a different from the operator that controls the web and authentication nodes, and has the commercial relation with the user. Reuse of existing access network is especially advantageous when a radio based access is used as an additional radio network might cause interference with the already installed one. Still further a method is needed through which one or more of the above mentioned objects can be achieved. Further yet an access server is needed through which one or more of the objects referred to can be achieved, and which can be used to provide login.

An arrangement is also needed through which a uniform login interface is achieved, even if the end user is served by different WISP:s, independent of each other.

Therefore an arrangement as initially referred to is provided which comprises a user station, an access network access server, a web server and an authentication server having the characterizing features of claim 1. Thus, the user station may here be seen as comprising two means, a first means, e.g. a PC, and a second means, e.g. a mobile telephone, the main thing however being that a one-time-password or similar that is used during the first phase is provided or transferred to the user over a mobile telecommunications network and that the login procedure is performed in two steps, or phases. A method for providing end users with access (logging in) to an IP network is also provided which has the characterizing features of claim 26.

Therefore also an access server for an access network is provided which communicates with an end user station for providing said end user station with access to an IP network, and with a web server and an authentication server. The access server has the characterizing features of claim 24.

Preferred or advantageous implementations are given by the appended subclaims.

According to the invention is thus an arrangement, for providing an end user station, an access server of an access network, a web server and an authentication server suggested. It comprises an end user station with first means for communication with an access server, second means for communication with an authentication server over a mobile telecommunications system and the access/login procedure comprises a first and a second phase. The authentication server controls the first phase, said first phase comprising a one-time password (OTP) login sequence, and the second login phase is performed by creating/modifying a temporary account for which user credentials are defined in order to log in

the end user at the access server. Particularly the second login phase only is performed if the OTP is valid. For the second phase a user account is created/modified in the authentication server, which particularly is temporary, i.e. that it allows login only for a limited time period. The access server (AS) is particularly run by an Internet Service Provider or a WISP. The one-time-password (OTP) used in the first phase is in one implementation reused in the second phase. Particularly the one-time-password (OTP) is created by, and transfered from, the authentication server to the second means of the end user station over the mobile telecommunication system. The first means of the user station may comprise a PC, and the second means may comprise a mobile telephone. Other alternatives are also possible.

The OTP is most particularly transfered by an alfa numeric text message, e.g. a SMS or a voice message to the second means (e.g. mobile telephone) of the user station. When transferred to the user station (mobile telephone), the OTP is to be entered on the first means of the user station (PC) and provided to the authentication server for authentication/validation. If the OTP is valid, the OTP from the first phase may be reused in the second phase. If the OTP is valid, a user name and a password of the created/modified account are particularly defined, which are uniquely tied to the OTP sequence. The second phase can be performed on different ways, and user name and password can be used in different ways.

In one embodiment, in the second phase, the same user name is used as in the first phase and the OTP is used as password. In another embodiment a dynamic user name is used and the OTP (of the first phase) is used as password. Still further a static user name (common for all users) may be used and the OTP (of the first phase) may be used as password. In still another embodiment a static user name (common for all users) is used and a random number is used as password. Still further a dynamic user name may

be used and a random value can be used as password. Other alternatives are also possible.

Advantageously the web server redirects the login message to the access server login page when an account has been created/modified in the authentication server and a timer is set to a given time period during which user credentials are checked, and if they are not valid, an error message is returned to the user. Particularly, if the user credentials comprise user name and password, and if they are verified/authenticated within the given time period, the user is given access and the added/modified temporary user account is removed/disabled. In one implementation the authentication server comprises a Radius server, in another a Diameter server. However, any appropriate authentication server can be used. In some embodiments one or more proxy servers are provided between the access server (AS) and the authentication (Radius, Diameter etc.) server. The access network particularly comprises a WLAN, an Ethernet or similar.

Advantageously login syntax is stored in the access server, and the login syntax is transferred to the web server to subsequently form part of a redirect message. Alternatively login syntax is stored with the operator, which however is more difficult to administrate since the operator needs detailed knowledge about the different access servers of the (W)ISP:s. (For an operator normally access servers of several manufacturers are to be used.)

The invention also discloses an access server in an access network communicating with an end user station, for providing said end user station with an end user station, for providing said end user station with access to an IP network, with a web server and with an authentication server. The access server allows any user to perform an access attempt to the web server, e.g. by using a white list function, a login link to the operator, and supports authentication server roaming. The access server supports a second

phase of a login procedure following on a first phase during which a one-time-password is given. For said second phase a temporary user account is created/modified, the password and user name of which are defined and uniquely associated with the one-time-password given by the authentication server and provided to the user station over a mobile communication system e.g. as an SMS, voice message or similar in the first phase. It may e.g. be an access server of a WLAN, an Ethernet or similar, run by an Internet Service Provider, e.g. a wireless ISP.

The invention also suggests a method for providing an end user with access to an IP network over an access network comprising an access server. For the login procedure, the method comprises the steps of:

- performing a first phase of a login procedure whereby a one-time-password (OTP) is provided by an authentication server and transferred to the end user over a mobile communication system, e.g. by a SMS or voice message,
- checking the validity/authenticity of the one-time-password, (and if valid),
- adding/modifying a temporary account in the authentication server, for a second phase of the login procedure,
- defining a user name and a password uniquely tied to the one-time-password of the first phase,
- checking the validity of the user name and the password in the authentication server, and if valid,
- allowing the user login request,
- removing/disabling the temporary user account after lapse of a predetermined time period.

Particularly the steps of performing the first phase of the login comprises the steps of:

- sending a login request to an access server from the user station,
- receiving a response from the access server if the user station enabling activation of a link to the operator web (login) server,
- accessing the web server,
- entering end user station identity in web server,
- providing a one-time-password (OTP) to the user station from the authentication server and transferring it to the user station over the mobile communications system, e.g. by SMS or a voice message;
- requesting the one-time-password by web server,
- verifying validity/authenticity of the one-time-password, whereas the second phase advantageously comprises the steps of:
- redirecting the login request to the login page of the access server;
- setting a timer,
- checking the validity/authenticity of the user credentials, e.g. password, user name, in authentication server, and if valid,
- removing/disabling the temporary account at expiry of the set timer.

Particularly the same user name may be used in the second phase as in the first phase, and the OTP may be used as password. In one embodiment the method comprises the steps of; in the second phase:

- using a dynamic user name,
- using the OTP of the first phase as password.

Alternatively it comprises the steps of:

- using a static user name common for all users,

- using the OTP of the first phase or random number as password.

Further still it may comprise the steps of, in the second step:

- using a dynamic user name,
- using a random value as password.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will in the following be further described, in a non-limiting manner, and with reference to the accompanying drawings, in which:

Fig. 1 is a very schematical block diagram illustrating an arrangement according to the invention,

Fig. 2 is a schematical flow diagram describing the inventive concept,

Fig. 3 is a signalling diagram describing one implementation of the invention concept.

DETAILED DESCRIPTION OF THE INVENTION

Fig. 1 shows a user 1 with a user station 2 comprising a first means, a terminal, e.g. PC 2A and a second means, a mobile telephone 2B. The terminal 2A communicates with access server AS 3 which is run by an ISP (Internet Service Provider) or a WISP (Wireless ISP). The access server 3 is an AS of an access network, e.g. a WLAN (Wireless Local Access Network) or an Ethernet, communicating with a web server 4 and an authentication server 5. Through the implementation of the inventive concept substantially any access server can be used in principle without modification, it only needs some reconfiguration. Only limited, slight requirements are put on the access server, such as addition of a login link to the operator, support of authentication server roaming and the provisioning of a white list or similar, i.e. the user can reach the web server prior to successful authentication. The authentication server 5 may e.g.

be a Radius (Remote Access Dial-in server) server or a Diameter server or similar. Radius is described in Radius, IEEE RFC (Request for Comments) 2865 which herewith is incorporated herein by reference. There may also be more than one authentication server. For example there can be two authentication servers, each supporting one phase in the login procedure.

The mobile telecommunications system 6 with SMS-C (Short Message Service Center) 7 is here used to provide the user with an OTP as will be further described below.

To initiate the procedure the terminal, e.g. a PC 2A establishes communication with the access server 3 run by an (W)ISP, which enables user contact with the web server 4, through which an OTP can be requested from authentication server 5. Authentication server then provides an OTP and transfers it to the user station (second means, mobile telephone 2B) over mobile telephony system 6 by means of SMS-C 7. The login procedure is handled in a first and a second phase, of which the first is an OTP sequence controlled by the authentication server 5. If this first phase is successful, i.e. when an OTP is delivered and verified, the second login phase follows that logs in the user at the access server 3. The OTP obtained and used in the first phase may be reused in the second phase. Other alternatives are however also possible as will be further described below.

According to the invention operators owning networks and having a large amount of customers are enabled to offer branded services based on OTP to their customers based on partnership agreements with access network providers having access servers, without there being any considerable requirements on the access servers. Login to different types/brands of access servers can easily be managed since the login syntax is handled by a (W)ISP. According

to the invention a temporary account allowing access during a limited time period is provided and used during the second login phase.

In the flow diagram of Fig. 2 a general implementation of the invention concept is illustrated. Thus it is supposed that communication is established between the end user station (i.e. the first means of the end user station, e.g. a PC) and the access server by the user requesting a login page, 100. The access server reponds to the request by furnishing the end user with a login page, 101. The user then clicks an operator link/button on the access server login page to reach the web server, 102. The web server then requests a user identity from the end user, 103. The end user identity is then entered by the user in the web server page, 104. Subsequently an authentication server may check the user identity. This, however, is an optional step, the box of step 105 is therefore indicated within dashed lines in the figure. Unless a valid user identity was given, the procedure is interrupted, and the user receives an error message.

The authentication server is in an advantageous implementation a Radius server. In another embodiment it comprises a Diameter server. It may however be any authentication server.

The authentication server subsequently via a mobile telephony system sends an OTP e.g. by SMS or as a voice message to the end user, 106. (Also here the procedure is interrupted, e.g. an error message sent to the receiver unless a valid user identity was given within a predetermined time period.) Subsequently the web server reqests the OTP from the end user, 107, who enters the OTP received by e.g. SMS, 108. Thereupon the authentication server checks the OTP, 109. If a valid OTP was entered, 110, it is proceded with the second phase of the login procedure as will be

described below. (Thus, the first phase of the login procedure comprises steps 100-110.) If no valid OTP was entered, an error message is returned to the user, 110A, and the procedure is interrupted.

In the second phase of the login procedure (supposing a valid OTP was entered by the user), a temporary account is added/modified by the authentication server, 111. User credentials (e.g. user name and password) are given for the temporary account. The web server then redirects the login request message to the access server login page, 112. Then also a timer T1 is started, 113. An authentication request is then sent from the access server to the authentication server, which checks the user credentials, 114, to verify if they are valid. If not, an error message is returned to the end user, 114A. If yes, e.g. at expiry of the timer T1 (or earlier), the temporary user account is removed or disabled, 115.

One implementation will now somewhat more thoroughly be described with reference to the signalling diagram of Fig. 3. First a HTTP request is sent from the user station (first means) to the access server, 1. The request goes to the login page of the access server. The access server returns a response with the login page to the user, 2. The login page contains a button or similar, the activation of which results in a link to the login server of the operator. The user is subsequently supposed to click the link and then reaches the web server of the operator, since the access to this web server is open in the access server by configuration, 3. Particularly the syntax of the login message to be used in the second phase of the login procedure may be transferred in this message. Then the web server request the user identity, 4, and in response thereto the user enters his identity, e.g. MSISDN 5. This is forwarded to the authentication server, 6, which provides an OTP and forwards it to SMS-C of a mobile communications

system, which transfers the OTP to the user e.g. by an SMS, 7. Information thereon is provided to the authentication server and the web server, 8, and the user is requested to enter the OTP by the authentication server, 9, over the web server, 10. The user then enters the OTP given by e.g. SMS or a voice message on the first means of the user station (e.g. a PC), and the OTP is via the web server provided to the authentication server, 11, 12. The authentication server then verifies the OTP to see if it is valid. If yes, a message with information to that fact is sent to the web server, 13. (In one implementation a dynamic account could be created before a correct OTP has been returned, e.g. for reasons of performance.) At this stage of the login procedure the first phase is terminated and it is proceeded with the second login phase.

Then, in this implementation, a temporary user account is created or modified to an account with a user id and with OTP as password, 14. A redirect message is then sent to the user station with the login URL, e.g. http://<access server IP address>/ login ? user name = <username> & <password = OTP where anything between < > is replaced with current values, 15. The login message is then sent to the access server run by the (W)ISP, 16. An authentication request is subsequently sent to the authentication server, possibly relayed by one or more proxy servers, 17. In this particular embodiment the authentication server comprises a Radius server, as refered to earlier in the application. The Radius server (in this case) responds with an access accept message to the access server and the access server opens the communication, after verifying that the user credentials are correct, 18. The user receives the response when/if the authentication is successful, 19. It may contain a forced web portal and a session window branded by the operator.

Finally the credentials stored for the second login phase are removed or blocked after a delay corresponding to a given time period to prevent multiple logins, unless immediately followed by the OTP login sequence, 20. In one implementation a timer is used for this purpose. Other ways are also possible.

The second phase of the login procedure can be performed in different manners. The credentials (e.g. user name and password) of the temporary account can be defined in different manners according to different embodiments. They may have static or dynamic values. The combination of user name and password must be uniquely tied to the earlier OTP sequence (of the first login phase). In one implementation the same user name as for the first phase (OTP part) is used, and the OTP is used as password. In another implementation a dynamic user name is used and the OTP is used as password.

Still further a dynamic user name may be used, whereas a random value is used as password. According to still another embodiment a static user name that is common for all users is used. Then may e.g. the OTP be used as password, or alternatively a random value may be used as password. A number of other alternatives are also possible. Also in other aspects the invention is not limited to the specifically illustrated embodiments, but it can be varied in a number of ways within the scope of the appended claims.

CLAIMS

1. An arrangement, for providing an end user with access to an IP network, comprising a user station, an access server of an access network, a web server and an authentication server, c h a r a c t e r i z e d i n that it comprises an end user station with first means for communication with an access server and a web server, second means for communication with an authentication server over a mobile telecommunications system, and in that the access/login procedure comprises a first and a second phase, that the authentication server controls the first phase, said first phase comprising a one-time password (OTP) login sequence, and in that the second login phase is performed by creating/modifying a temporary account for which user credentials are defined in order to log in the end user at the access server.

2. An arrangement according to claim 1, c h a r a c t e r i z e d i n that for the second phase a user account is created/modified in the authentication server.

3. An arrangement according to claim 2, c h a r a c t e r i z e d i n that said created/modified account is temporary, i.e. that it allows login only for a limited time period.

4. An arrangement according to any one of claims 1-3, c h a r a c t e r i z e d i n that the access server (AS) is run by an Internet Service Provider.

5. An arrangement according to claim 4,
c h a r a c t e r i z e d i n
that the Internet Service Provider offers a wireless service (i.e. is a WISP).

6. An arrangement according to any one of claims 1-5,
c h a r a c t e r i z e d i n
that the one-time-password (OTP) used in the first phase is reused in the second phase.

7. An arrangement according to any one of claims 1-6,
c h a r a c t e r i z e d i n
that the first means of the user station comprises a PC, and in that the second means comprises a mobile telephone.

8. An arrangement according to any one of the preceding claims,
c h a r a c t e r i z e d i n
that the one-time-password (OTP) is created by, and transfered from, the authentication server to the second means of the end user station over the mobile telecommunication system.

9. An arrangement according to claim 8,
c h a r a c t e r i z e d i n
that the OTP is transfered by an alfa numeric text message, e.g. a SMS or a voice message to the second means of the user station.

10. An arrangement according to claim 7 or 8,
c h a r a c t e r i z e d i n
that the OTP is entered on the first means of the user station and provided to the authentication server for authentication/validation.

11. An arrangement according to claim 10,
c h a r a c t e r i z e d i n
that if the OTP is valid, the OTP from the first phase is reused in the second phase.

12. An arrangement at least according to claim 2 and 10,
c h a r a c t e r i z e d i n
that if the OTP is valid, the user name and a password of the created/modified account are defined, which are uniquely tied to the OTP sequence.

13. An arrangement according to claim 12,
c h a r a c t e r i z e d i n
that in the second phase the same user name is used as in the first phase and in that the OTP is used as password.

14. An arrangement according to claim 12,
c h a r a c t e r i z e d i n
that for the second phase a dynamic user name is used and in that the OTP (of the first phase) is used as password.

15. An arrangement according to claim 12,
c h a r a c t e r i z e d i n
that for the second phase a static user name (common for all users) is used and in that the OTP (of the first phase) is used as password.

16. An arrangement according to claim 12,
c h a r a c t e r i z e d i n
that for the second phase static user name (common for all users) is used and in that a random number is used as password.

17. An arrangement according to claim 12, characterized in that for the second phase a dynamic user name is used and in that a random value is used as password.

18. An arrangement according to any one of the preceding claims, characterized in that the web server redirects the login message to the access server login page when an account has been created/modified in the authentication server and in that a timer is set to a given time period during which user credentials are checked, and if they are not valid, an error message is returned to the user.

19. An arrangement according to claim 18, characterized in that if the user credentials comprise user name and password, and if they are verified/authenticated within the given time period, the added/modified temporary user account is removed/disabled.

20. An arrangement according to any one of the preceding claims, characterized in that the authentication server comprises a Radius server or an Diameter server.

21. An arrangement according to claim 20, characterized in that one or more proxy servers are provided between the access server (AS) and the authentication (Radius, Diameter etc.) server.

22. An arrangement according to claim 21, characterized in that the access network comprises a WLAN, an Ethernet or similar.

23. An arrangement accordning to any one of the preceding claims,
c h a r a c t e r i z e d i n
that login syntax is stored in the access server and in that the login syntax is transferred to the web server to subsequently form part of a redirect message.

24. An access server in an access network communicating with an end user station for providing said end user station with access to an IP network, with a web server and with an authentication server,
c h a r a c t e r i z e d i n
that the access server allows any user to perform an access attempt to the web server, e.g. by using a white list function, a login link to the operator, and supports authentication server roaming, and in that the access server supports a second phase of a login procedure following on a first phase during which a one-time-password is given, and in that for said second phase a temporary user account is created/modified, the password and user name of which are defined and uniquely associated with the one-time-password given by the authentication server and provided to the user station over a mobile communication system e.g. as an SMS, voice message or similar in the first phase.

25. An access server according to claim 24,
c h a r a c t e r i z e d i n
that it is an access server of a WLAN, an Ethernet or similar and in that it is run by an Internet Service Provider, e.g. a wireless ISP.

26. A method for providing an end user with access to an IP network over an access network comprising an access server,

c h a r a c t e r i z e d i n
that it, for the login procedure, comprises the steps of:

- performing a first phase of a login procedure whereby a one-time-password (OTP) is provided by an authentication server and transferred to the end user over a mobile communication system, e.g. by a SMS or voice message,
- checking the validity/authenticity of the one-time-password, and if valid,
- adding/modifying a temporary account in the authentication server, for a second phase of the login procedure,
- defining a user name and a password uniquely tied to the one-time-password of the first phase,
- checking the validity of the user name and the password in the authentication server, and if valid,
- allowing the user login request,
- removing/disabling the temporary user account after lapse of a predetermined time period.

27. A method according to claim 26,
c h a r a c t e r i z e d i n
that the steps of performing the first phase of the login comprises the steps of:

- sending a login request to an access server from the user station,
- receiving a response from the access server if the user station enabling activation of a link to the operator web (login) server,
- accessing the web server,
- entering end user station identity in web server,
- providing a one-time-password (OTP) to the user station from the authentication server and transferring it to the user

station over the mobile communications system, e.g. by SMS or a voice message;

- requesting the one-time-password by web server,
- verifying validity/authenticity of the one-time-password.

28. A method according to claim 26 or 27, c h a r a c t e r i z e d i n that the second phase comprises the steps of:

- redirecting the login request to the login page of the access server;
- setting a timer,
- checking the validity/authenticity of the user credentials, e.g. password, user name, in authentication server, and if valid,
- removing/disabling the temporary account at expiry of the set timer.

29. A method according to any one of claims 26-28, c h a r a c t e r i z e d i n that it comprises the steps of:

- using the same user name in the second phase as in the first phase,
- using the OTP as password.

30. A method according to any one of claims 26-28, c h a r a c t e r i z e d i n that it comprises the steps of; in the second phase:

- using a dynamic user name,
- using the OTP of the first phase as password.

31. A method according to any one of claims 26-28, c h a r a c t e r i z e d i n

that it comprises the steps of, in the second step:

- using a static user name common for all users,
- using the OTP of the first phase or a random number as password.

32. A method according to any one of claims 26-28, characterized in that it comprises the steps of, in the second step:

- using a dynamic user name,
- using a random value as password.

33. A method according to any one of claims 26-32, characterized in that the access network comprises a WLAN, an Ethernet or similar, and in that the authentication server comprises e.g. a Radius server or a Diameter server.

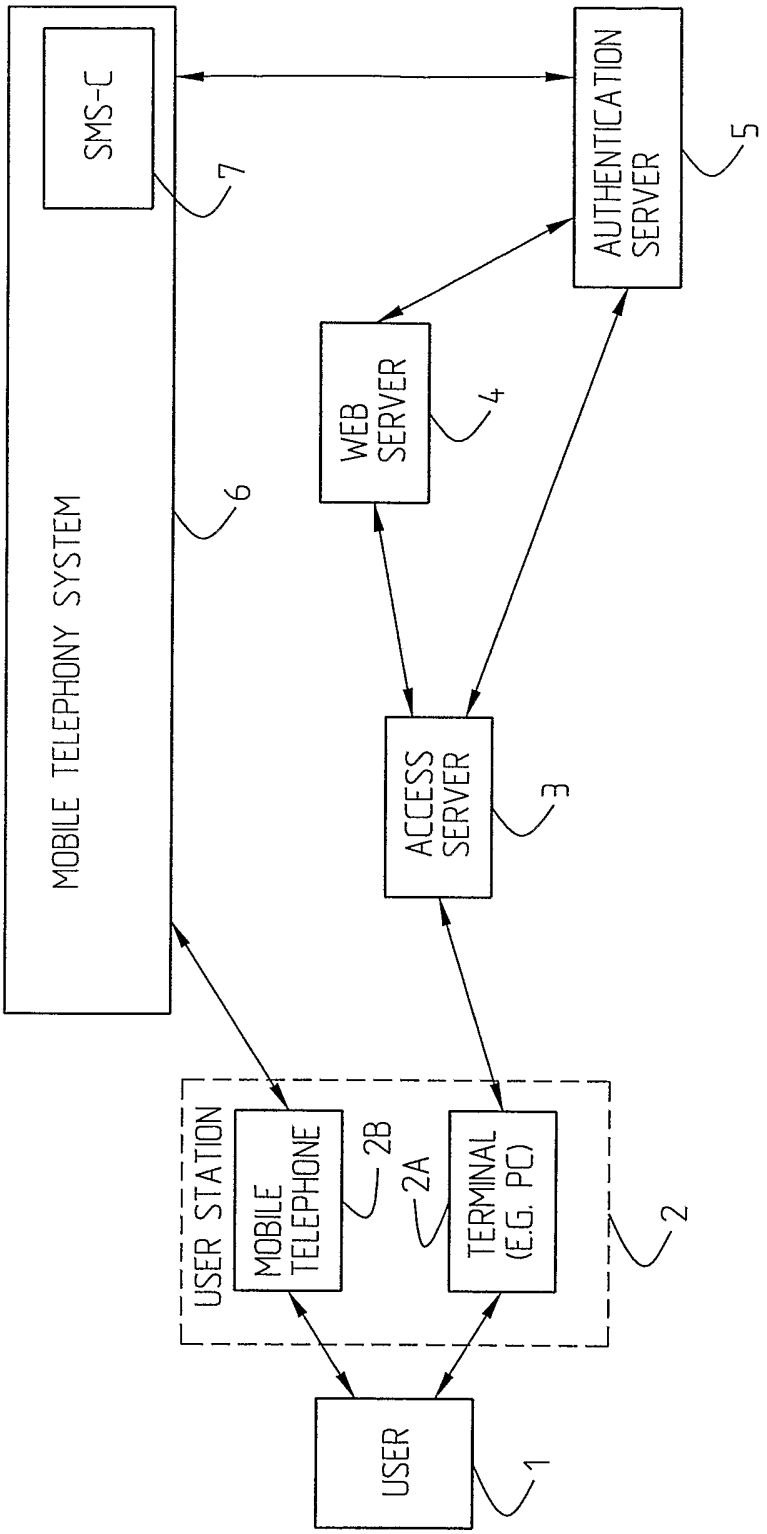

SMS-C
7
AUTHENTICATION SERVER
5
MOBILE TELEPHONY SYSTEM
6
WEB SERVER
4
ACCESS SERVER
3
USER STATION
MOBILE TELEPHONE
2B
2A
TERMINAL (E.G. PC)
2
USER
1

Fig. 1

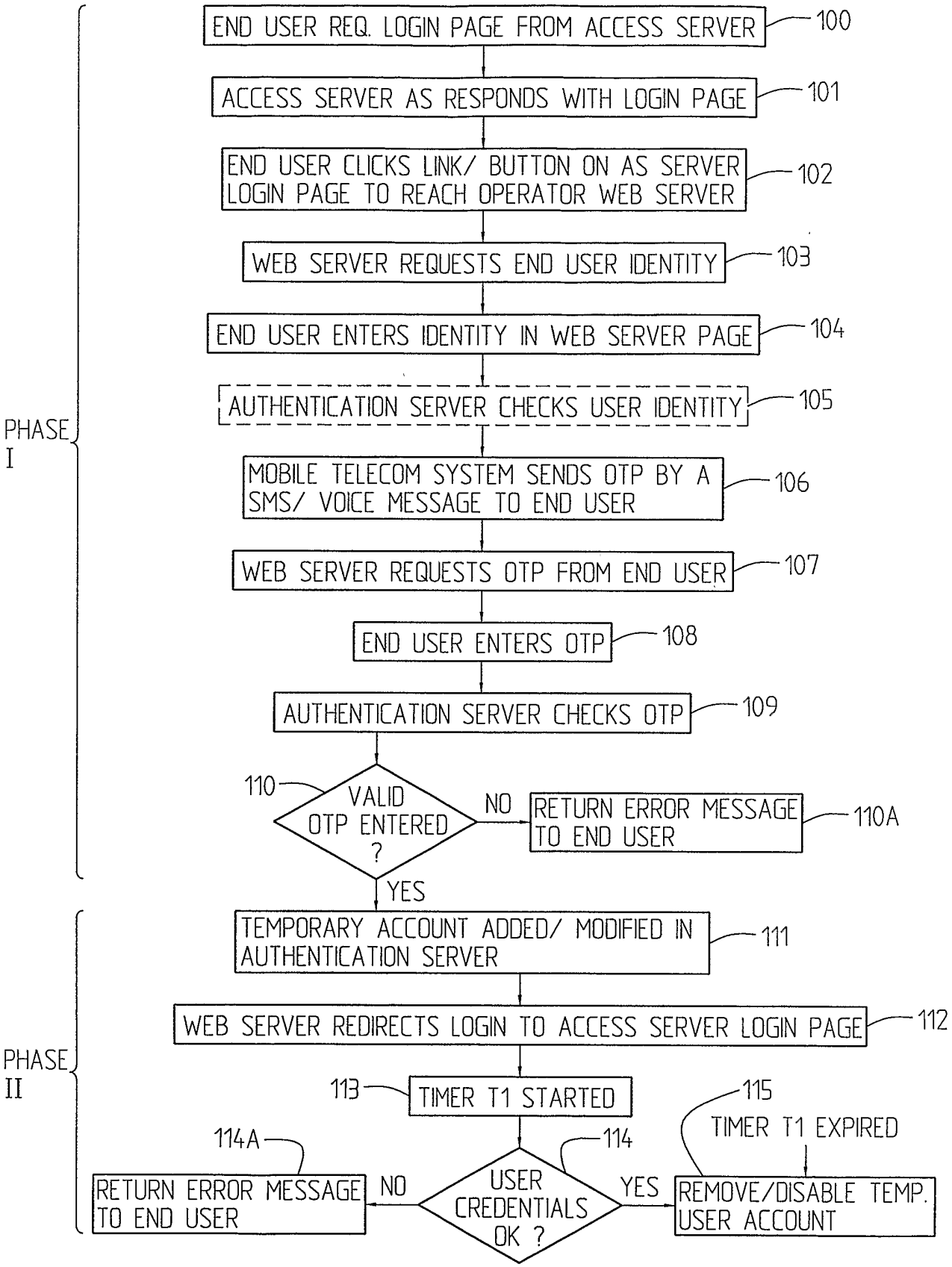

PHASE I
END USER REQ. LOGIN PAGE FROM ACCESS SERVER
100
ACCESS SERVER AS RESPONDS WITH LOGIN PAGE
101
END USER CLICKS LINK/ BUTTON ON AS SERVER LOGIN PAGE TO REACH OPERATOR WEB SERVER
102
WEB SERVER REQUESTS END USER IDENTITY
103
END USER ENTERS IDENTITY IN WEB SERVER PAGE
104
AUTHENTICATION SERVER CHECKS USER IDENTITY
105
MOBILE TELECOM SYSTEM SENDS OTP BY A SMS/ VOICE MESSAGE TO END USER
106
WEB SERVER REQUESTS OTP FROM END USER
107
END USER ENTERS OTP
108
AUTHENTICATION SERVER CHECKS OTP
109
110
VALID OTP ENTERED ?
NO
RETURN ERROR MESSAGE TO END USER
110A
YES
PHASE II
TEMPORARY ACCOUNT ADDED/ MODIFIED IN AUTHENTICATION SERVER
111
WEB SERVER REDIRECTS LOGIN TO ACCESS SERVER LOGIN PAGE
112
113
TIMER T1 STARTED
115
TIMER T1 EXPIRED
114A
114
RETURN ERROR MESSAGE TO END USER
NO
USER CREDENTIALS OK ?
YES
REMOVE/DISABLE TEMP. USER ACCOUNT

Fig. 2

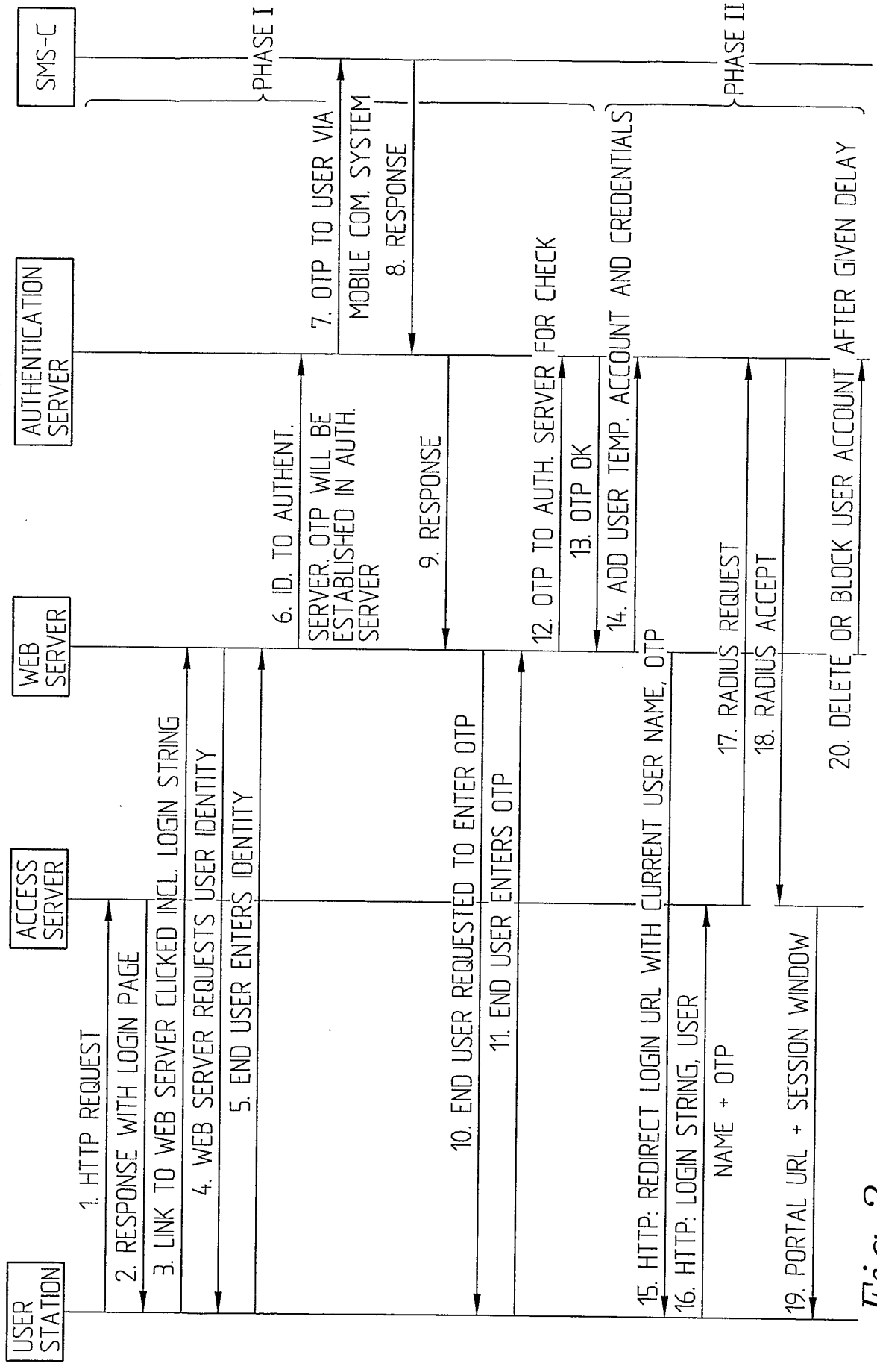

USER STATION
W(ISP) ACCESS SERVER
OPERATOR CONTROLLED WEB SERVER
AUTHENTICATION SERVER
SMS-C
PHASE I
PHASE II
1. HTTP REQUEST
2. RESPONSE WITH LOGIN PAGE
3. LINK TO WEB SERVER CLICKED INCL. LOGIN STRING
4. WEB SERVER REQUESTS USER IDENTITY
5. END USER ENTERS IDENTITY
6. ID. TO AUTHENT. SERVER. OTP WILL BE ESTABLISHED IN AUTH. SERVER
7. OTP TO USER VIA MOBILE COM. SYSTEM
8. RESPONSE
9. RESPONSE
10. END USER REQUESTED TO ENTER OTP
11. END USER ENTERS OTP
12. OTP TO AUTH. SERVER FOR CHECK
13. OTP OK
14. ADD USER TEMP. ACCOUNT AND CREDENTIALS
15. HTTP: REDIRECT LOGIN URL WITH CURRENT USER NAME, OTP
16. HTTP: LOGIN STRING, USER NAME + OTP
17. RADIUS REQUEST
18. RADIUS ACCEPT
19. PORTAL URL + SESSION WINDOW
20. DELETE OR BLOCK USER ACCOUNT AFTER GIVEN DELAY

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 2003/001053

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G06F 1/00, H04Q 7/22
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)

IPC7: G06F, H04Q, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003051041 A1 (A. KALAVADA ET AL), 13 March 2003 (13.03.2003), paragraph (0099 - paragraph (0105, paragraph (0174(- paragraph (0193; figure 4	1-33
X	WO 02084456 A2 (NETDESIGNS LIMITED), 24 October 2002 (24.10.2002), page 1, line 17 - page 8, line 33	1-33
E,X	US 2003204726 A1 (M.G. KEFFORD ET AL), 30 October 2003 (30.10.2003), paragraph (0009)- paragraph (0019)	1-33

[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 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
14 January 2004	22 -01- 2004
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Catharina Karlsson / MRo Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 2003/001053

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GB 2379040 A (INTERNATIONAL COMPUTERS LIMITED), 26 February 2003 (26.02.2003), abstract --	1-33
A	WO 03015370 A2 (CRYPTOMATHIC A/S), 20 February 2003 (20.02.2003), page 14 - page 16, abstract -- --------	1-33

US	2003051041	A1	13/03/2003	WO	03017125 A	27/02/2003
WO	02084456	A2	24/10/2002	GB	0109200 D	00/00/0000
				GB	0208362 D	00/00/0000
				GB	2377523 A,B	15/01/2003
				GB	0111528 D	00/00/0000
				GB	0126583 D	00/00/0000
				GB	0126929 D	00/00/0000
US	2003204726	A1	30/10/2003	WO	03092216 A	06/11/2003
GB	2379040	A	26/02/2003	GB	0120391 D	00/00/0000
WO	03015370	A2	20/02/2003	EP	1364508 A	26/11/2003
				GB	0119629 D	00/00/0000
				NO	20033407 D	00/00/0000