An arrangement (106), such as a server apparatus or a plurality of at least functionally connected server and/or other apparatuses, for controlling access to a network service, such as a cloud service, utilizing multi-factor, at least two-factor, authentication, comprising a processing entity (150) and a memory entity (152) for processing and storing data, respectively, and a data transfer entity (156) for receiving and sending data, the arrangement being configured to transmit a code (143c), preferably as browser data such as web page data, during a communication session associated with a predetermined user of the service for visualisation and subsequent uttering by the user, receive sound data (143g) indicative of the uttered code, determine on the basis of the sound data and voiceprint data associated with the predetermined user whether the code has been uttered by the predetermined user (143h), and provided that this seems to be the case, raise the gained authentication status of the predetermined user regarding at least the current communication session (143i), wherein raising the authentication status optionally includes at least one action selected from the group consisting of: enabling a new service feature, enabling the use of a new application, enabling a new communication method, and enabling the adjustment of service settings or preferences. A corresponding method is presented.
ARRANGEMENT AND METHOD FOR ACCESSING A NETWORK SERVICE

FIELD OF THE INVENTION

Generally the invention pertains to computers and related communications infrastructure. In particular, however not exclusively, the invention concerns logging into a service provided by a remote computer system and associated authentication.

BACKGROUND

Access control in conjunction with network services may imply user identification, which can be generally based on a variety of different approaches. For example, three categories may be considered including anonymous, standard and strong identification. Regarding anonymous case, the service users do not have to be and are not identified. Standard, or 'normal', identification may refer to what the requestor for access knows, such as a password, or bears such as a physical security token. Such a token may include password-generating device (e.g. SecurlD™), a list of one-time passwords, a smart card and a reader, or a one-time password transmitted to a mobile terminal. Further, strong identification may be based on a biometric property, particularly a biometrically measurable property, of a user, such as a fingerprint or retina, or a security token the transfer of which between persons is difficult, such as a mobile terminal including a PKI (Public Key Infrastructure) certificate requiring entering a PIM (Personal Identification Number) code upon each instance of use.

On the other hand, network service-related authentication, i.e. reliable identification, may also be implemented on several levels, e.g. on four levels, potentially including unnecessary, weak, strongish, and strong authentication, wherein the strongish authentication, being stronger than weak, thus resides between the weak and strong options. If the user may remain anonymous, authentication is unnecessary. Weak authentication may refer to the use of single standard category identification means such as user ID/password pair. Instead, strongish authentication may apply at least two standard identification measures utilizing different techniques. With strong authentication, at least one of the identification measures should be strong.
Notwithstanding the various advancements taken place during the last years in the context of user and service identification, authentication, and related secure data transfer, some defects still remain therewith and are next briefly and non-exhaustively reviewed with useful general background information.

Roughly, access control methods to network services include push and pull methods. In pull methods, a user may first identify oneself anonymously to a network service providing a login screen in return. The user may then type in the user ID and a corresponding password, whereupon he/she may directly access the service or be funneled into the subsequent authentication phase. In push methods, a network server may first transmit information to the e-mail address of the user in order to authorize accessing the service. Preferably only the user knows the password of the e-mail account.

The users are often reluctant to manually manage a plurality of user IDs and corresponding passwords. As a result, they may utilize the very same user ID and/or password in multiple services and/or use rather obvious and thus easy-to-crack words, numbers or expressions as passwords. Even if the access control management systems require using a strong password, i.e. hard-to-remember password, a risk that the user writes the password down increases considerably and the authentication level turns ultimately weak.

Yet, the utilization of a password is typically enabled by access control management entity that may also store the password locally. If the security of the data repository is later jeopardized, third parties may acquire all the passwords stored therein. Also if the user forgets the password or it has to be changed for some other reason, actions have to be taken by the user and optionally service provider. The user has to memorize the new password.

Further, the adoption of a personal, potentially network service-specific token such as a smartcard, e.g. SecurlD™, and a related reader device may require intensive training. The increase in the use of smart cards correspondingly raises the risk of thefts and provision of replacement cards. In case the personal tokens apply a common (distributed) secure algorithm, the theft of such algorithm would cause tremendous security issues and trigger massive update operations regarding the associated elements such as tokens in order to recover at least part of the original security.
Particularly, in the context of cloud services such as cloud virtual-desktop services that may be regularly, e.g. daily, utilized by a user, the nowadays available access control procedures, especially identification and authentication solutions applied upon logging in to a service, are typically either inadequate in terms of the achieved data security or awkward from the standpoint of usability with reference to the aforesaid lengthy and strong, i.e. complex and thus hard-to-remember, passwords.

SUMMARY OF THE INVENTION

The objective is to at least alleviate one or more problems described hereinabove regarding the usability issues and security risks, such as authentication risks, associated with the contemporary remote computer systems and related network services.

The objective is achieved by the arrangement, such as an apparatus or a plurality of at least functionally connected apparatuses, and method in accordance with the present invention disclosing service access technology and technique, respectively, preferably incorporating e-mail account and mobile device-related communication resulting in at least two-factor authentication in conjunction with the overall procedure, which provides both trustworthy authentication and pleasant use experience. A myriad of electronic services such as cloud computing services, remote desktop services, and customer portal services may be accessed and related documents programmatically transmitted from a database to registered recipients, for instance.

Accordingly, in an aspect of the devised solution an arrangement, such as a server apparatus or a plurality of at least functionally connected server and/or other apparatuses, for controlling access to a network service, such as a cloud service, utilizing multi-factor authentication, comprises a processing entity and a memory entity for processing and storing data, respectively, and a data transfer entity for receiving and sending data, the arrangement being configured to transmit a code, preferably as browser data such as web page data, during a communication session associated with a predetermined user of the service for visualization and subsequent uttering by the user,

receive sound data indicative of the uttered code,
determine on the basis of the sound data and voiceprint data associated with the predetermined user whether the code has been uttered by the predetermined user, and provided that this seems to be the case,

raise the gained authentication status of the predetermined user regarding at least the current communication session.

Preferably the sound data is received from a mobile (terminal) device. The mobile device is further preferably associated with the predetermined user. Optionally, the code is received and indicated to the user via a first terminal device such as a laptop or desktop computer, and the sound data is obtained via a second terminal device, preferably a mobile device like a cellular phone or communications-enabled PDA/tablet, configured to capture sound such as the user's voice and convert it into digital sound data forwarded towards the arrangement.

The determination tasks may include a number of mapping and/or comparison actions according to predetermined logic by which the match between the obtained sound data and existing voiceprint data is confirmed, i.e. the authentication is considered successful in the light of the voice-based authentication factor. In case no match, i.e. failed voice-related authentication, the authentication status may remain as is or be lowered (or access completely denied).

Optionally, raising the gained (current) authentication status in connection with successful voice-based authentication may include at least one action selected from the group consisting of: enabling a new service feature, enabling the use of a new application, enabling a new communication method, and enabling the (user) adjustment of service settings or preferences.

Optionally, the code is numeric and preferably contains between four and eight digits (numbers). Alternatively or additionally, the code may include one or more letters.

In preferred embodiments, the arrangement may be configured to send an e-mail notice to an e-mail address associated with a predetermined user, the e-mail
notice including a preferably secure link for a browser, such as an Internet browser,

receive an indication of the activation of the preferably secure link, such as a data request like a web resource request sent via a browser, in response to which the arrangement being further configured to

send
- first browser data, such as web page data, requesting the user of the browser to input a secret, and
- a one-time password (OTP) to a mobile device associated with the predetermined user,

receive user input relative to the request for secret,

determine whether the user input matches the sent OTP, and

provided that such condition is fulfilled, enable the user of the browser and related terminal device, the user being thus authenticated as the predetermined user, to access the service.

In some preferred embodiments, the enablement may generally include sending data such as second browser data, e.g. a UI (web) page of the associated network service or other service data, which may further enable the user to access the service and/or fetch a desired electronic document via a download link, for instance. In a preferred embodiment the enablement incorporates or basically is about providing service access -enabling data to the user (terminal). The transferred enabling data may include at least one element selected from the group consisting of: a browser executable program, a Java entity such as a Java applet, an executable such as a binary executable, and a service password or related data required for generating it preferably in encrypted form.

The data may be transferred via the browser connection, and/or through other connection. The service password may be used for accessing such as logging in to the network service. Multiple data elements may be transferred substantially simultaneously, e.g. one substantially after each other, or during a longer period. The service password, the resulting authentication, e.g. log-in, action and/or the resulting service connection may be associated with a predetermined or dynamic
validity or expiration condition such as a period. The service password may be user and/or terminal device-specific. In some embodiments, the service password may be embedded in the transferred other data such as transferred program or transferred (other) file.

Depending on the embodiment, the utilization of the service password, or 'service code', may be substantially transparent or invisible from the standpoint of the user, i.e. it may be handled automatically for log-in purposes so that after providing the OTP the user may omit substantive further manual actions in order to access the service, or the required action(s) are minimal such as a number of simple confirmation actions like click or button press-type actions. The service password may also be lengthy, e.g. of available maximum length as advantageously, the user does not have to manually play with it or even know it. The password generation may be of 'black box' type, i.e. a specific entity may be configured to generate it in a non-transparent manner. Likewise, the password may be afterwards operated via a number of black box entities. The password may remain secret from the service operator even though the service operator may advantageously trigger resetting the password upon need. The password may be stored as encrypted. Preferably the password remains secret to the user, operator and third parties. In some embodiments, the tasks of password or related data provision, verification (receipt and checking) and/or service provision may be executed by different entities. A certain network entity comprising a number of network devices of the arrangement may thus take care of OTP and/or service password provision and/or verification. A certain other network entity may provide the network service. The entities may also overlap as to the included devices.

In a supplementary embodiment, also the service password may be a one-time password and/or a temporally limited password. It may be created dynamically. For example, a new service password may be created and/or transferred when necessary. In some embodiments, the new password may be provided upon each instance of a service log in procedure after the mobile-based OTP authentication as described herein.

In one supplementary or alternative embodiment, the established service connection (access) is maintained based on a number of security measures the outcome of which is used to determine the future of the service connection, i.e. let it remain, terminate it, or change it, for example. In some scenarios,
fingerprint methodology may be applied. The client terminal may initially, upon service log-in, for instance, provide a fingerprint based on a number of predetermined elements, such as browser data such as version data, OS data such as version data, obtained Java entity data such as version data, and/or obtained executable data such as version data. Version data may include ID data such as version identifier or generally the identifier (application or software name, for example) of the associated element. The arrangement may be configured to request new fingerprint in response to an event such as a timer or other temporal event (timed requests, e.g. on a regular basis). Alternatively or additionally, the client may provide fingerprints independently based on timer and/or some other event, for instance.

In response to the received new fingerprint, the arrangement may utilize the most recent fingerprint and a number of earlier fingerprints, e.g. the initial one, in a procedure such as a comparison procedure. The procedure may be executed to determine the validity of the current access (user). For example, if the compared fingerprints match, a positive outcome may be determined indicating no increased security risk and the connection may remain as is. A mismatch may trigger a further security procedure or terminating the connection.

In another supplementary or alternative embodiment, the arrangement is location-aware advantageously in a sense it utilizes location information to authenticate the user. A number of predetermined locations may be associated with each user of the arrangement. For example, the location may refer to at least one element selected from the group consisting of: address, network address, sub-network, IP (Internet Protocol) address, IP sub-network, cell, cell-ID, street address, one or more coordinates, GPS coordinates, GLONASS coordinates, district, town, country, continent, distance to a predetermined location, and direction from a predetermined location. Each of the aforesaid addresses may refer to an address range.

Failed location-based authentication may result in a failed overall authentication (denied access), or alternatively, a limited functionality such as limited access to the service may be provided. The same applies to other authentication factors. Each authentication factor may be associated with a characterizing weight (effect) in the authentication process.
In some embodiments, the arrangement may be configured to transmit another code, preferably as browser data such as web page data, during a communication session associated with a predetermined user of the service for visualization and subsequent input by the user. Further, the arrangement may be configured to receive data indicative of the inputted code and of the location of the terminal device applied for transmitting the data, determine on the basis of the data and predetermined locations associated with the user whether the user currently is in allowed location, and provided that this seems to be the case on the basis of the data, raise the gained authentication status of the user regarding at least the current communication session.

Preferably the data is received from a mobile (terminal) device. The mobile device is further preferably associated with the predetermined user. Optionally, the code is received and indicated to the user via a first terminal device such as a laptop or desktop computer, and the data is obtained via a second terminal device, preferably a mobile device like a cellular phone or communications-enabled PDA/tablet, configured to capture the code via the UI of the device.

In some embodiments, a single code could be utilized both for location and voice-based authentication. The code received by the user could (or should in some embodiments) be input to terminal (application) as sound data via microphone and optionally also (i.e. in addition to the voice input regarding the very same code) input, typically typed in, via the keypad or touchscreen. The user(s) could be provided with opportunity to adjust personal preferences or service settings relating to the application of location- and/or voice-based authentication (e.g. on/off, use separately or jointly or both, use order in the case of separate application, relationship with security/authentication levels) and optionally the input methods of codes.

A certain location may be associated with a certain user by "knowing" the user, which may refer to optionally automatically profiling and learning the user via monitoring one's habits such as location and optionally movements. As a result, a number of common, or "allowed", locations may be determined and subsequently utilized for authentication purposes. Additionally or alternatively, the user may manually register a number of allowed locations for utilizing the solution in the arrangement. Generally, in various embodiments of the present invention, knowing the user and/or his/her gear and utilizing the related information such as location information in connection with access control,
conducting automated attacks such as different dictionary attacks against the service may be made more futile.

In some scenarios, the location of the user (terminal) and/or data route may be estimated, e.g. by the arrangement, based on transit delay and/or round-trip delay. For example, delays relating to data packets may be compared with delays associated with a number of e.g. location-wise known references such as reference network nodes, which may include routers, servers, switches, firewalls, terminals, etc.

In one other, either supplementary or alternative, embodiment the secure link may include a URI with an applicable scheme such as a HTTPS scheme implying the use of SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocol for encrypting traffic between the browser and the server. Alternatively, the traffic may be encrypted utilizing some other method. The link may include an address of a web page including the first browser data for user input. The address may contain a secure element that is practically impossible to guess or deduce. The secure element may include a hash such as an MD5 (Message-Digest algorithm 5) hash, for instance, for the determination of which service or document data and secret key of the server may have been applied.

In a further, either supplementary or alternative, embodiment the notice (e-mail) may be provided as digitally signed utilizing a substantially S/MIME-compliant (Secure/Multipurpose Internet Mail Extensions) identity certificate, OpenPGP (Pretty Good Privacy, RFC 4880)-compliant identity certificate, and/or X.509-compliant identity certificate. The options are not necessarily mutually exclusionary. E.g. X.509-compliant certificate may be utilized in connection with S/MIME e-mails.

Still in a further, either supplementary or alternative, embodiment a text message, such as an SMS-compliant (Short Message Service) message, is utilized as a carrier of the OTP. Alternatively other message such as a multimedia message, e.g. an MMS (Multimedia Messaging Service) message, may be exploited.

Yet in a further, either supplementary or alternative embodiment, the network service is a cloud service (running in a cloud). Additionally or alternatively, the service may arrange virtual desktop and/or remote desktop to the user.
In another aspect, a method for controlling access to a network service such as a cloud virtual-desktop service, utilizing multi-factor authentication, comprises transmitting a code, preferably as browser data such as web page data, during a communication session associated with a predetermined user of the service for visualization and subsequent uttering by the user,

receiving sound data indicative of the uttered code,

determining on the basis of the sound data and voiceprint data associated with the predetermined user whether the code has been uttered by the predetermined user, and provided that this is the case according to a number of predetermined criteria,

raising the gained authentication status of the predetermined user regarding at least the current communication session.

Further, the method may include sending an e-mail to an e-mail address associated with a predetermined user, said e-mail including a preferably secure link for a browser, receiving an indication of the activation of the preferably secure link, sending first browser data, such as web page data, requesting the user of the browser to input a secret, sending a one-time password (OTP) to a mobile device associated with the user, receiving user input relative to the request for secret, determining whether the user input matches the sent OTP, and provided that that this is the case, enabling the user of the browser and related terminal, thus authenticated as the predetermined user, to access the service, wherein said enabling includes sending enabling data to the terminal optionally via the browser-related connection such as HTTP (Hypertext Transfer Protocol) connection.

Particularly, the actual execution order of the first browser data and OTP sending items may differ depending on the embodiment, which is also described in further detail hereinafter.

The previously presented considerations concerning the various embodiments of the arrangement may be flexibly applied to the embodiments of the method mutatis mutandis, and vice versa, as being appreciated by a skilled person.
The utility of the present invention follows from a plurality of issues depending on each particular embodiment. The suggested solution potentially enables applying e.g. strongish authentication such that the use experience is improved, security risks are mitigated, and the supply chain of services and/or digitally transferable documents such as bills or account statements among numerous other options is shortened. Indeed, at least strongish if not strong authentication is achieved with minimal additional costs. One rather fundamental biometric property, i.e. voice, may be exploited as an authentication factor. Also location data indicative of the location of the user (terminal) may be harnessed for authentication purposes.

Encryption may be flexibly utilized for information transfer. Existing, proprietary network services may be cultivated by adding at least two-factor authentication thereto as a front-end solution without necessarily causing a need to make major changes to the already established, underlying authentication/log-in practice of the service. A service may be practically ready for exploitation by the user as soon as the one has received the notification e-mail. As the e-mail contains only a link to access the OTP-requesting front-end of the network service, potential lack of e-mail encryption does not expose any confidential information. The password of e-mail account and the control over mobile account are used as authentication factors among other options such as location information. The risk of undesirably lowering the authentication level due to careless management of passwords practically disappears. Spyware-related risks may be overcome, for example. The arrangement may store information such as e-mail addresses and cell phone numbers of the users of the provided services, but such information is not typically considered as particularly confidential and would be stored anyway in respect of customer records as desirable contact details. As a relatively ordinary mobile device may be applied as a security token, proprietary new tokens do not have to be obtained.

The expression "a number of" refers herein to any positive integer starting from one (1), e.g. to one, two, or three.

The expression "a plurality of" refers herein to any positive integer starting from two (2), e.g. to two, three, or four.
The expression "data transfer" may refer to transmitting data, receiving data, or both, depending on the role(s) of a particular entity under analysis relative a data transfer action, i.e. a role of a sender, a role of a recipient, or both.

The terms "a" and "an" do not denote a limitation of quantity, but denote the presence of at least one of the referenced item.

The terms "first" and "second" do not denote any order, quantity, or importance, but rather are used to distinguish one element from another.

Different embodiments of the present invention are disclosed in the dependent claims.

**BRIEF DESCRIPTION OF THE RELATED DRAWINGS**

Next the invention is described in more detail with reference to the appended drawings in which

Fig. 1a illustrates the concept of the present invention via both block and signaling diagram approaches relative to an embodiment thereof.

Fig. 1b illustrates one possibility for providing remote service access to the user of a client terminal after successful OTP-based authentication.

Fig. 1c is a block diagram representing an embodiment of selected internals of the arrangement according to the present invention.

Fig. 1d illustrates an embodiment of location data and/or voice data exploitation in connection with the present invention.

Fig. 1e represents one example of service UI for user authentication.

Fig. 1f represents one example of adaptive service UI (menu or screen) for service feature selection.

Fig. 2 is a flow chart disclosing an embodiment of a method in accordance with the present invention.

Fig. 3 is a flow chart disclosing an embodiment of enabling the user to access a remote service in response to a successful authentication in accordance with the present invention.

Fig. 4 is a flow chart disclosing items of an embodiment incorporating location/voice data exploitation in accordance with the present invention for authentication.
DETAILED DESCRIPTION OF THE EMBODIMENTS

In the context of the present invention, the user preferably has an e-mail account (advantageously private e-mail), a browser application, network access such as Internet accessibility, a mobile (communications) device and a mobile subscription. Further, the user may have a desktop, a laptop, a thin-client or a hand-held computer for e-mail, browsing and/or various other purposes, for instance. Alternatively or additionally, the mobile device may be utilized also for such use. For example, many contemporary and forthcoming higher end mobile terminals such as so-called "smartphones" bear necessary capabilities for both e-mail and web surfing purposes. Also a number of various other software solutions, e.g. clients, may be run on the mobiles. Advantageously, the e-mail address and mobile number of the user are stored in the arrangement for future use.

The user may have to be supplied with service data such as virtual desktop and/or financial reports requiring at least strongish authentication. In the latter case, a related document may be, e.g. upon first instance of use (fetch by a recipient) converted into a target format such as the PDF format and/or digitally signed.

The potential users of the provided arrangement and method include different network service providers, operators, cloud operators, virtual and/or remote desktop service providers, software manufacturers, financial institutions, companies, and private persons in the role of a service provider/data sender, intermediate entity, or user/recipient, for example. The invention is thus generally applicable in a wide variety of different use scenarios and service/document delivery applications.

In some embodiments the service may include customer portal service and the service data may correspondingly include customer portal data. Through the portal, a user may inspect the available general data, company or other organization-related data or personal data such as data about rental assets, estate or other targets. Associated reports may be obtained via the service.

Figure 1a illustrates the overall concept of the present invention according to an embodiment thereof. The embodiment may be related, by way of example only, to the provision of a network service such as a virtual desktop service or document delivery service, e.g. delivery of a bill including a notice of maturity
regarding a bank loan. Entity 102 refers to the service user (recipient) and associated devices such as a desktop or laptop computer and/or a mobile device utilized for accessing the service in the role of a client, for instance. The device(s) preferably provide access to a network 108 such as the Internet. The mobile device, such as a mobile phone (e.g. a smartphone) or a PDA (personal digital assistant) may preferably be wirelessly connected to a compatible network, such as a cellular network. Optionally the Internet may be accessed via the mobile device. The mobile device may comprise a browser. Entity 106 refers to a network arrangement of a number of at least functionally connected devices such as servers for user verification and service provision and/or document delivery. In some embodiments, the entity 106 may only participate in user authentication and thus service access, but the service provision is then taken care of by a number of further devices. In some other embodiments, the entity 106 may also contain a number of devices actually in charge of service (data) provision after authentication/log-in phase. Hereinafter the entity 106 is called as NAS (Network access server) or ‘server’ without any limiting purpose, however. The communication between the entities 102 and 106 may take place over the Internet and underlying technologies, for example. Preferably the entity 106 is functionally also connected to a mobile network.

At 126, the NAS 106 stores information about a service to be provided to users and/or documents such as bills to be delivered to them in a number of databases for preferably permanent storage. Further, user data may be obtained and managed. At 128, a notice regarding the service and/or document is sent, as digitally signed by S/MIME, for example, and utilizing a first communication technique, preferably e-mail, to the registered e-mail address of the intended recipient. Further, the e-mail may be encrypted. With e-mail it is referred to Internet e-mail, for example. Also other electronic mail systems or platforms may be applied. The applied protocol may be SMTP (Simple Mail Transfer Protocol), for example. At 130, the user 102 receives the e-mail notice informing about a possibility to access the service or e.g. fetch a new bill via NAS 106. The notice may be received via a desktop computer or a portable, e.g. laptop or palm-top, computing device such as a smartphone as mentioned above. Optionally a plurality of authentication options may be provided to the user as described in more detail hereinafter. The user 102 may verify the sender of the e-mail by referring to the digital signature to avoid spammers' notices. Thereafter, the user 102 may select a secure link included in the notice and comprising a unique, optionally one-time accessible, URI for proceeding further with accessing the
service or e.g. e-bill stored in the NAS server 106, which takes place in item 132 utilizing e.g. HTTPS for establishing a secure channel to the server 106. Item 148a illustrates the simplified screen view visualizing the notice and the embedded link(s) to the user 102. The used e-mail client may include a stand-alone application (UI) or e.g. a webmail application.

Alternatively or additionally, anonymous pull-type login could be applied by the user for accessing the service in some embodiments. The user may, for instance, first access the network server 106 anonymously. A related service (web) page may then provide a registration and/or login screen. The server 106 may subsequently send a notice such as the aforesaid e-mail notice to the e-mail address of the user. The notice may include a link such as an URI for service access. The URI may be stored as a bookmark for facilitated logins in case the link is substantially permanent or of a longer term/multiple uses anyway. In addition to service address provided by the URI the user 102 may have to utilize a personal user ID and/or password optionally each time upon entering the service. Even the use of OTPs may be omitted with the increased security risks. Thus the obtainable overall security level in the context of present invention is fully scalable ranging from the use of permanent service links and user ID/password pairs to one-time links, mobile-transferred OTPs and optional further security factors such as the location-factor.

Reverting to the embodiment visualized in Figure 1a, at 134 the server 106 preferably validates the URI address based on e.g. the secure element thereof. At 136, the server 106 sends browser data for representing an initial login screen to the user 102 (again e.g. HTTPS may be applied) and, optionally in response to a specific request by the user 102 e.g. via the login screen, an OTP preferably to the mobile device (e.g. cell phone number) associated with him/her e.g. in an SMS message delivered via an SMS gateway, for instance. At least part of the transmission path to the mobile device is preferably wireless and the air interface of a wireless, e.g. cellular, network compatible with the mobile device is applied. At least partially different (second) communications technique may be thus exploited in contrast to the delivery of the e-mail notice. Accordingly, 2-factor/2-channel authentication may be achieved. The message and/or the OTP may be encrypted utilizing a predetermined encryption technique.

At 138, the user 102 receives the login screen that is visualized on his/her terminal device, see the example at 148b. At 138b, the OTP is received
preferably with the mobile device. At 140, the user 102 types the OTP in the login screen. Again, the related communication may apply HTTPS (TTL/SSL), for instance. At 142, access control logic of the server 106 compares the received OTP and the reference OTP (correct OTP sent at 138b), and in case these two match and optional additional conditions are fulfilled as well, transmits, at 144, data for enabling the user to access the service or document received at 146.

In document service context, the procedure may include generating a new view enabling the user 102 to access a service, download a document such as a bill or view it directly, e.g. via HTML page(s) interpreted by compatible browser and necessary browser add-on(s), optionally with supplementary data such as indication of available functionalities like change of the presentation mode. In other service contexts such as cloud service, optionally cloud-based virtual-desktop service, contexts the enablement may refer to further, e.g. security-related, operations prior to gaining an access to the service. Such operations are explained in more detail hereinafter. Yet, HTTPS and/or SSH (Secure Shell) may be applied for securing the data transfer of e.g. the bill data as browser data, for instance. Optionally, a switchover from HTML to PDF or some other presentation may be triggered.

In some embodiments, location information 143 may be utilized in the authentication process. In one embodiment, the server 106 and/or other entities external to the user's 102 terminal gear may be configured to locate one or more of the terminals the user 102 applies for accessing the service/obtaining the document, i.e. a first terminal used for e-mail and browsing/login procedure, and a second terminal used for OTP reception, if different. The location of the terminal(s) typically gives a hint about the user's 102 location. Alternatively or additionally, the terminal devices may bear an own role in the positioning process and execute at least part of the necessary positioning actions locally. Actions required to position a terminal may be shared between the terminal(s) and at least one external entity.

For instance, address information may be used in the positioning process to deduce the location of the particular terminal in question. Somewhat typically, terminal or access network addresses such as IP addresses are at least loosely associated with physical locations so that the address-based locating is at least limitedly possible. In connection with mobile devices, many other options are also available including roaming signal and data transmission-based positioning.
For example, by checking the ID of the base station(s) the mobile device is communicating with, at least approximate location of the mobile device may be obtained. Yet, through more comprehensive signal analysis, such as TOA (Time-Of-Arrival), OTD (Observed-Time-Difference), or AOA (Angle-Of-Arrival), the mobile device may be located.

In some embodiments, a satellite navigation receiver, such as a GPS (Global Positioning System) or GLONASS (GLObal Navigation Satellite System), in connection with a terminal device may be exploited. The terminal may share the locally received satellite information with external entities as such or in cultivated form (e.g. ready-determined coordinates based on received satellite signal(s)). Further, data entity such as data packet transit times or RTT times may be monitored, if possible, e.g. in relation to both the monitored user/terminal and e.g. location-wise known reference entities as described hereinbefore in order to assess the location of the user/terminal by associated comparison.

On the basis of the terminal location, the server 106 may then introduce a further factor, i.e. a location-based factor, to the authentication procedure and verify, whether the current location of the terminal in question matches with predetermined location information defining a number of allowed locations and/or banned locations in the light of the service and/or document access. Depending on the embodiment, the status of the location-based factor may be evaluated prior to the evaluation of the fulfillment of other authentication factors, in conjunction with them, or as a final check before authorizing the user to access the service and/or electronic document.

One shall remember that in some embodiments, a communications technology different from mobile technology could be applied for delivering the OTP. This might take place upon "no service" situations relative to the mobile network, for instance, as a secondary, back-up connection. The arrangement may be configured to autonomously detect the fulfillment of a triggering condition, such as mobile connection failure, for utilizing the secondary connection for OTP transfer, and/or the user may request such by selecting a related (secure) link included in the e-mail notice, for example. The secondary connection may refer to transmitting the OTP via e-mail, for instance. When secondary connection is applied for OTP transfer, the information provided in or through the document and/or the associated network service may be scaled (down) accordingly to match the achieved authentication level. Less information, e.g. less confidential,
may be available to the recipient, for example. The information may be preclassified into a number of security classes for facilitating the scaling.

In some embodiments, the user rights for the network service provided by the arrangement may be flexibly scaled via the utilization of a plurality of authentication options. The options may be indicated in the e-mail notice via links, text, graphics, and/or other means, for example. In the case of weak authentication, in some embodiments the user receiving the receipt notice may directly access the related service and/or document by activating a relating link included therein. The achieved authentication level corresponds to a traditional e-mail communication such as a transfer of a bill. In response, the arrangement may be configured to offer merely a limited, low-level functionality of the overall service to the user, such as simple access to the bill in selected format such as PDF format, and no other functions. Correspondingly, if stronger authentication is implemented via the transfer of the OTP as a new e-mail, for example, average functionality may be offered. For instance, possibility to fetch and view previously received documents may be provided. In cases wherein a mobile connection is applied for the OTP transfer, further data and/or service options may be accessible and/or changeable, such as personal contact information and/or execution of payments. As a result of offering multiple authentication options, the reception costs may be minimized and/or reception made technically more reliable in view of possible connection problems. Therefore, the use of a mobile device may be optional only. Nevertheless, it is in many use scenarios preferred.

Figure 1b illustrates one possibility for enabling a remote service access to the user of a client terminal after successful, OTP- capitalizing authentication. The service may be a virtual or remote desktop service and/or a cloud service, for example. NoMachine ™ products such as NoMachine NX may be optionally utilized for the purpose.

The disclosed items may be considered to incorporate the aforementioned items 144, 146, which is highlighted in the figure by naming the corresponding items with postfix a, i.e. 144a, 146a.

At 144a, the arrangement may provide the client device with data necessary for accessing the service, i.e. enabling data. Data transfer may still exploit the encrypted connection (e.g. HTTPS: SSL/TLS, or SSH) via the browser, for
instance. Between different instances of service access, the data may at least partially differ. For instance, upon first access, more data may be provided including e.g. software that may be stored in the terminal such that further downloads of the same software may be omitted in the future. In contrast, substantially one-time (use) data, such as a password, and/or data expiring automatically based on e.g. a temporal event such as timer expiry may be provided upon each access including the first and all or some of the subsequent accesses. Further data such as user ID may be provided. At least part of the provided data, such as the password, may be determined in response to the successful OTP-authentication just finished.

In one example, the arrangement 106 may provide data such as software for accessing the network service at 144a to the terminal 102 such as a desktop or portable computer. The software may include a Java language entity such as a Java applet or other entity that may be executable in the browser of the terminal. Additional or alternative software such as an executable may be provided. The different software entities such as the Java entity and the executable entity may cooperatively enable the user to access the network service. The data may be provided with signature(s) to facilitate verifying the source thereof at the receiving end.

At 146a, the terminal may receive the data, store it and/or take it into use/install it depending on the nature thereof. A Java entity such as applet may be obtained and executed. It may be stored in the cache of the browser for enabling rapid future use as well. In case the terminal does not contain JVM (Java Virtual Machine), it may be first instructed, by the arrangement, to install that with JRE (Java Runtime Environment) via an internal or external link, or via automatic download, for example. The data may further include additional or alternative applications such as a client executable for accessing a predetermined network service. Yet, a password may be received, preferably in encrypted form. As the connection may itself be encrypted and the password may be separately encrypted as well (e.g. included in a .nxs file that may be generally plain text but still contain an encrypted password), very high level of overall security is achievable.

At 184, the terminal 102 may, in response to the received data, process the data, executed an action associated therewith and/or transmit data 184 such as at least part of the processed data to a remote entity such as the arrangement 106. In
some embodiments, a Java client such as at least one Java applet and optionally further software such as a binary executable may cooperatively handle and/or process a received password, such as decrypt the password, and transmit the processed version securely, preferably over e.g. SSH, to a remote system such as back to the arrangement for accessing the target service. Browser-based data transfer may again be utilized. The password may be input to the GUI (Graphical User Interface) in order to log in to a virtual or remote desktop service, for example. Some, most or all the related actions may be automated such that after providing the OTP, the user may, at most, validate the execution of a number of selected actions, if necessary.

In some embodiments, the received data may include data such as a program and/or source data for generating and optionally preferably securely communicating (e.g. to the service) the service password.

In some embodiments, the network service such as a virtual or remote desktop may be or include a Windows-based ™ service. In some other embodiments, it may be or include a Linux ™, e.g. Ubuntu ™, -based service.

The arrangement 106 or other entity, such as a separate service entity, (this optional differentiation between access or authentication provision and subsequent service provision being highlighted in the figure by the broken horizontal line between item 144a and item 186) may then receive the data such as the decrypted service password at 186 and execute a related predetermined action 188 such as log the user in and provide the user with the desired target service such as virtual desktop service 188a. Associated service data may be transferred 188 between the parties. A selected method, such as device fingerprints, may be utilized to verify optionally regularly the user/terminal identity also during the service access.

Generally, different fingerprints may be rather versatility applied also in the overall context of the present invention. Firstly, the link provided may be signed and the signature (and the related service) be verified. Secondly, the processes of user authentication may apply the various fingerprints available relating to location/address data such as IP address of the user, browser data relative to his/her terminal, OS (operating system) information, (session) cookie, calendar data, etc. to enhance the authentication accuracy. Service and authentication fingerprints may have their own validity rules.
Figure 1c is a block diagram illustrating the selected internals of an embodiment of the arrangement presented herein. The arrangement 106, such as a number of servers, may physically contain a number of at least functionally connected elements. A skilled person will naturally realize that a terminal device such as a mobile terminal utilized in connection with the present invention could include similar elements.

The arrangement 106 is typically provided with one or more processing devices capable of processing instructions and other data, such as one or more microprocessors, micro-controllers, DSP's (digital signal processor), programmable logic chips, etc. The processing entity 150 may thus, as a functional entity, comprise a plurality of mutually co-operating processors and/or a number of sub-processors connected to a central processing unit, for instance. The processing entity 150 may be configured to execute the code stored in a memory 152, which may refer to instructions and data relative to the software logic and software architecture for controlling the arrangement 106. The processing entity may at least partially execute and/or manage the execution of the aforesaid receiving, sending, determining, and/or enabling tasks.

Similarly, the memory entity 152 may be divided between one or more physical memory chips or other memory elements. The memory 152 may store program code and other data such as user contact information, electronic documents, various service data etc. The memory 152 may further refer to and include other storage media such as a preferably detachable memory card, a floppy disc, a CD-ROM, or a fixed storage medium such as a hard drive. The memory 152 may be non-volatile, e.g. ROM (Read Only Memory), and/or volatile, e.g. RAM (Random Access Memory), by nature. Software (product) 152 may be provided on a carrier medium such as a memory card, a memory stick, an optical disc (e.g. CD-ROM or DVD), or some other memory carrier.

The UI (user interface) may comprise a display or a data projector 154, and keyboard/keypad or other applicable user (control) input entity 154b such as a touch screen and/or a voice control input, or a number of separate keys, buttons, knobs, switches, a touchpad, a joystick, and/or a mouse, configured to provide the user of the arrangement with practicable data visualization and device control means, respectively. The UI may include one or more loudspeakers and associated circuitry such as D/A (digital-to-analogue) converter(s) for sound
output, and optionally a microphone with A/D converter for sound input. A
printer may be included in the arrangement for providing more permanent output.

The arrangement 106 further comprises a data interface 156 such as a number of
wired and/or wireless transmitters, receivers, and/or transceivers for
communication with other devices such as terminals and/or network
infrastructure(s). For example, an integrated or a removable network adapter may
be provided. Non-limiting examples of the generally applicable technologies
include WLAN (Wireless LAN, wireless local area network), LAN, WiFi,
Ethernet, USB (Universal Serial Bus), GSM (Global System for Mobile
Communications), GPRS (General Packet Radio Service), EDGE (Enhanced
Data rates for Global Evolution), UMTS (Universal Mobile Telecommunications
System), WCDMA (wideband code division multiple access), CDMA2000, PDC
(Personal Digital Cellular), PHS (Personal Handy-phone System), and Bluetooth.

It is clear to a skilled person that the arrangement 106 may comprise numerous
additional functional and/or structural elements for providing advantageous
communication, processing or other features, whereupon this disclosure is not to
be construed as limiting the presence of the additional elements in any manner.
Entity 158 refers to such additional element(s) found useful depending on the
embodiment.

Figure 1d illustrates one embodiment for utilizing location and/or voice data 143
in connection with the suggested embodiment, whereas Figure 1e represents one
example of service UI for user authentication and Figure 1f depicts an example
of dynamic service UI for service feature selection.

As explained hereinbefore relative to Figure 1a, location of the user as indicated
by the location of his/her terminal device such as a mobile terminal, or
alternatively/additionally, a predetermined verifiable personal biometric
property, such as voice, could be utilized as authentication factor(s).

In some embodiments, the provided service may support a plurality of security
levels. A user may progress from a level to a higher level by successfully
accomplishing one or more authentication procedures. For example, at least
three, four, or five different security levels could be provided. In the case of five
levels, the first three levels could be associated with the afore-explained
authentication procedures including the utilization of secure e-mail links, OTPs
and e.g. coarser indication of the location of the user. For example, geoIP™ or some other lower resolution solution could be applied for tracking the country and/or potentially more specific geolocation of the user based on e.g. the IP address used for accessing the service.

Further security level(s) could be achieved through the provision of more accurate location data and/or biometric property data, such as voice data, to the service for verification in desired order or in parallel.

Via the service UI 190 of Figure 1e, such as a web page, or via a generally similar UI, the user may input data regarding various identification and addressing means, and related preferences, such as user ID, e-mail address, mobile phone number, and preferred OTP delivery method. The user may request the transmittal of a secure link to the indicated e-mail address for service access. Yet, the service UI may provide a verification engine for checking the input data based on predetermined logic utilizing a number of verification rules given for each input field and data allowed therein.

Figure 1f shows a service UI 190b, such as a web page, for accessing different service features such as applications or generally 'components', 192 that may each be associated with a certain minimum security level required from the user. Only currently accessible features could be shown or alternatively, accessible features could be made visually distinguishable from the non-accessible ones. For instance, the icons of the non-accessible features could be shown as greyed or shadowed non-active features. For example, in the case of a (cloud) service for the provision of financial tools, features such as 'Reports', 'Invoices and Letters', and 'Graphical Desktop' could be selectable via the service UI 190b, each potentially associated with a certain minimum security level required for access.

Further, the UI may indicate the current security level e.g. numerically or via a number of symbols like stars, enable the user to check/update the security level and provide related instructions, see item 194, wherein codes to be used in connection with additional authentication measures are shown (positioning ID, or 'geokey', and voice recognition ID, or 'voicekey').

Still, the UI may be configured to indicate a number of service, authentication and/or e.g. session details as shown at 196. Temporal validity of the secure e-
mail link may be indicated. The number of log-ins used from the maximum amount may be indicated. Session automatic expiration time may be indicated. Allowed locations may be indicated with a desired resolution.

Reverting to Figure 1d, the shown items 143a and 143b represent potential preparatory actions preferably including providing a native mobile application to the mobile (terminal) device of the user 102 for enabling more comprehensive exploitation of location and/or biometric authentication factor in connection with the present invention.

For instance, the mobile device may be configured to download the application from the server 106 or via a (trusted) third party. Alternatively, the server 106 or the (trusted) third party might transmit the application as a push-type delivery. As a further example, the application could be provided on a physical carrier medium such as a memory card.

At 143c, the server 106 provides a location(ing) ID, a 'geokey', to the user 102 preferably through browser data such as service view, e.g. a login/authentication view or a portal view. The data is thus received by the user terminal such as desktop/laptop computer at 143d. The user 102 may then notice the (visualized) ID among the service data as a numeric code or generally a string of optionally predetermined length. The ID may be dynamic such as session-specific and/or for one-time use only.

At 143e, the user 102 provides the received ID to the obtained application by the associated device UI such as keypad or touchscreen, after which the application acquires location data according to predetermined logic based on available positioning options (typically at least partially manual, or 'human-assisted', nature of ID data transfer between items 143d and 143e being indicated by the dotted arrow in the figure). Preferably, the location data is acquired in real-time or near real-time fashion upon receipt of the ID to be current.

For example, the hosting mobile device may contain a satellite receiver such as GPS or GLONASS receiver through which location data may be obtained. In addition, the mobile device may utilize network and related signal(s) for obtaining location data such as data provided by cellular network and/or short-range wireless network, optionally WLAN. Network-assisted positioning may be
used. The mobile application may be configured to utilize available interfaces provided with the mobile operating system for acquiring the positioning data.

Location data such as longitude information, latitude information, accuracy or error estimate, the ID itself or data derived therefrom, and/or time code (or time stamp) may be then collected at 143f and transmitted to the server 106. Preferably at least part of the data is encrypted. Optionally, at least part of the above data elements may be utilized for determining a hash by means of a secret or asymmetric key, for example, in which case at least the hash is transmitted. HTTPS may be utilized for the secured transfer. The server 106 receives and optionally processes such as decodes the data at 143g. This may imply further communication with the terminal(s) as reviewed hereinafter relative to Figure 4.

At 143h, the server 106 verifies the current location of the user 102, as indicated by the data, against predetermined data indicative of e.g. allowed location(s). The resolution of the obtained data and/or related measurement error estimate may be utilized to adapt the decision-making. For example, in the case of a larger error/worse positioning accuracy, more tolerance may be allowed in verification process, and vice versa.

In one preferred embodiment, the service is configured to maintain data about allowed (and/or rejected) user locations through utilization of polygon data, i.e. geo-referenced polygon data. For example, a number of allowed postal areas represented by the corresponding polygons may have been associated with each user. The obtained location data may be mapped to a corresponding postal area polygon that is then searched from the list of allowed postal area polygons. In such an embodiment, the aforesaid adaptation may be realized by stretching or shrinking the postal area polygon boundaries, for instance.

In the case of a positive outcome (allowed location detected), the server 106 may update the authentication, or generally 'security', status of the user 102 accordingly and typically raise it. In practice, the user 102 may be provided with enhanced access rights to service components such as payment/finance components, higher security documents, etc. as reviewed above. Each user may be associated with session-based information such as session record dynamically keeping track of, among potential other issues, the user rights emerging from the successful authentication actions.
A notification of the raised access security level or failed authentication may be transmitted to the user at 143i e.g. as a message to be indicated such as visualized, at 143j, via the mobile application and/or through browser data.

The server 106 may now update, at 143l, the service parameters for the session automatically and provide an updated service view such as browser view to the user's terminal. Alternatively, such update may take place in response to the receipt of an update request sent, at 143k, by the user 102 via the service UI such as browser-based UI, for example, of the applied terminal device.

In some embodiments, voice recognition (speaker recognition) may be utilized to provide a further or alternative authentication element to the suggested solution.

As mentioned in connection with the description of Figure If, a voice recognition ID, or 'voicekey', may be indicated to the user via applicable information channel such as the service UI itself. The voicekey may, as the geokey, include a number of, preferably a plurality of, numbers, letters and/or symbols, most typically being a string of numbers of limited length, e.g. between 5 and 8 numbers. In some embodiments, the voicekey is shorter and/or simpler than the geokey to facilitate uttering thereof.

In order to capitalize voice-based authentication, the server 106 may be initially provided with user-specific voiceprint ('voice model' or 'voice template') data characterizing a number of preferably unique, measurable characteristics of the user's voice. For that purpose, user specific voice data for training the voice recognition engine may have to be provided. A number of predetermined characteristics may be determined from the training data for establishing the voiceprint data.

As one example, the user 102 may be instructed, optionally by the provided application through visual messaging, to audibly reproduce predetermined data. For example, digits from zero to nine may be necessary to be dictates for creating the voiceprint data. The user may first indicate the number to be dictated via the UI of the mobile device, e.g. via a corresponding key or touchscreen, and audibly reproduce the number, one number at a time. Reselecting and re-recording the same number may erase the old recording. Optionally each number or other basic unit of the training data is provided as a separate sample. The obtained, optionally pre-processed such as coded, voice data may be then sent to
the server 106 for analysis and user-specific voiceprint determination. Preferably the associated data is encrypted at least for transmission.

Voiceprint data may include a dedicated voiceprint for each user-dictated number, letter, or word, for instance. Voiceprint data may indicate fundamental frequency data, vocal tract resonance(s) data, duration/temporal data, loudness/intensity data, etc. Voiceprint data may indicate personal (physiological) properties of the user 102 and characteristics of received sample data obtained during the training being thus indicative of the way the user 102 pronounces and generally reproduces the given training data or training units such as numbers. In that sense, the voice recognition engine used in accordance with the present invention may also incorporate characteristics of speech recognition.

Cleverly, the user 102 may affect the voiceprint creation by selecting a desired language for dictation.

Additionally or alternatively, the user 102 may utilize his/her preferred personal coding scheme for the training phase and naturally the subsequent actual usage of voicekeys. For example, instead of saying 'one' while instructed to audibly reproduce '1' during training, the user 102 could state something unconventional like 'dog' or a different number such as 'two' provided that the user afterwards sticks to his own coding scheme while audibly inputting voicekeys to the mobile device for authentication purposes.

Preferably, the user 102 may re-train the server 106 also after the initial training phase when noticing, for example, that the performance of the voice recognition engine is not fully satisfactory, which may depend on somehow failed training or e.g. already forgotten personal coding scheme used during training.

Reverting to Figure 1d, at 143c, the server 106 thus could, instead or in addition to the location(ing) ID, or 'geokey', provide a voicekey to the user through browser data such as service view, e.g. a login/authentication view or a portal view. The user 102 may again notice the (visualized) ID among the service data as a numeric code or generally a string of optionally predetermined length. The ID may be dynamic such as session-specific and/or for one-time use only. Optionally, first voicekey could be provided to the user 102 utilizing registered mail or some other method that is considered secure. Such adoption of the
voicekey-type authentication could also include the training phase as discussed hereinearlier.

In some embodiments, a single ID, or 'key', could be both for location-based and voice-based authentication. The ID would be uttered by the user for enabling voice recognition but being also utilized as the ID for the obtained location data. Optionally, both the sound data and location data could be included in the same message(s) transmitted to the server 106 for voice- and location-based authentication, respectively.

At 143e, the user 102 may provide the voicekey to the obtained application by dictation. The application may show an icon with text 'Enter the voicekey' the activation of which triggers audio capturing via the microphone of the host (mobile) device. The capturing may end in response to further user input such as pressing a 'send' button, or automatically based on a timer or detection of pause in the input speech. The input signal may be coded utilizing a predetermined audio codec. The resulting audio file may be encrypted and sent at 143f to the server 106 for verification.

The server 106 receives the sound (voice) data at 143g and verifies at 143h the obtained vocal sample on the basis of available, stored voiceprint data containing a number of user-specific voiceprints. In case the sample corresponds to the predetermined voiceprint of the user according to predetermined criteria, the voicekey-based authentication may be deemed successful and the associated, typically elevating, measures executed relative to the security level, which may take place at 143l, for example. The user 102 may be informed about the outcome of voice-based authentication (143i).

Figure 2 discloses, by way of example only, a method flow diagram in accordance with an embodiment of the present invention. At 202 the arrangement of the present invention is obtained and configured, for example through loading and execution of related software, for managing the electronic service, related authentication and/or electronic document delivery system. At 204, an indication of a required authentication, such as an authentication request, is received from the current or future user of the service, or a related entity. User registration data for the service may be obtained now or it may have been obtained earlier. The data may include name/id, e-mail, and/or mobile number data, for instance. A service user may have several (sub-)accounts each optionally defining a valid e-
mail address - mobile number combination. At 206, a notification regarding the service is transmitted towards the user based on contact information available. An e-mail account associated with the user may be applied, for example. The notification may include a link (typically a hyperlink), preferably also being a secure link, the activation of which funnels the client application such as the browser of the activator to the login/password entering page for proceeding further with service access. The link may refer to a one-time or temporally limited link. The link may be associated with e.g. location and/or device restrictions that limit the application of the link respectively to certain locations (e.g. geographical such as GPS or IP verification) and/or terminal devices. Thus in some embodiments, as described hereinbefore, the link could be applied successfully multiple times by the user without need to gain a new link upon each access.

At 208, the data transmission (e.g. HTTP(S) request, such as GET) initiated by the activator reaches the arrangement and the arrangement responds by supplying an password request or potentially a more comprehensive login page (e.g. user ID may be requested) back at 210 as e.g. a web page matching the received request, for example. At 209, an OTP may be optionally specifically requested by the user. E.g. associated control functionality such as a button may be activated or triggered by the user on the associated service page potentially also provided at 209. At 212, an OTP to be provided by the user as a response to the password query is supplied utilizing e.g. cellular communication to a mobile device associated with the user and advantageously with the e-mail whereto the notification was sent.

Preferably the addresses whereto the e-mail and OTP are transmitted are indeed different to enhance the security of the overall arrangement. More preferably, the transmission techniques also at least partially differ, e.g. TCP/IP vs. cellular communication. In addition to the OTP, further data such as user ID may be provided. The order of items 210 and 212 may be reversed, or substantially simultaneous execution thereof may be preferred, as being clear to a skilled person. The issue is highlighted in the figure by the bi-directional broken arrow between the two items 210, 212. Likewise, the order of items 209 and 210 could in some embodiments be reversed or the items be combined as the password query towards the user generated at 210 may also include provision of a user-controllable functionality such as a web page control (button) for requesting the
OTP, for instance. In some embodiments, item 212 could be executed even prior to or upon item 208.

As the user authentication OTP is provided to the login screen, a corresponding data transmission is triggered towards the arrangement that, at 214, receives the transmission. At 215, further authentication factors such as location factor may be optionally considered. Optionality of the further factors is depicted by the broken outline of item 215. As deliberated hereinbefore, the exact execution instant of further authentication checks may be determined per each particular embodiment, and the illustrated position is just one feasible option. For instance, one other applicable position could reside between items 216 and 218 such that the location check would be the ultimate verification prior to authorizing access to the service and/or related electronic document.

At 216, the password entered by the user is compared against the archived one. In case the passwords do not match, a further possibility may be given to the user to enter a correct password, which is indicated by a dotted loop-back arrow. In some embodiments, a limited number of retries may be permitted. If the maximum number of tries is met without success and/or a predetermined timer is exceeded for entering a proper password, a predetermined action may be executed. For example, the service administrator or e-document sender may be informed about the service access/document delivery failure and its cause via e-mail or other electronic communication.

Provided the password given is correct and optional further authentication checks have been successfully executed, access to the electronic service and/or document may be authorized at 218, e.g. via the browser through which OTP was input, etc. The arrangement may transmit, in response to the correct OTP input, data enabling service access, either directly or automatically, or via optional user intervention –requiring phase(s). An embodiment of related method items is given in Figure 3 described later below. The data may generally include software required for accessing the service, e.g. Java-based software, and/or preferably user-specific service password data (e.g. password or data for generating it) optionally in encrypted form. In document delivery services, the desired electronic document(s) may be transmitted to the user via the browser connection. A separate authorization display may be first provided, for example, implying that the password was correct (and optionally that further authentication factor checks were successful as well) and access to the document is now
allowed. A link to enter the service or download the document may be simultaneously or successively presented. At 220, the method execution is ended. The execution of various method items may be naturally repeated upon need. As already alluded above, the execution order may be changed depending on the needs of the embodiment at issue.

Fig. 3 is a flow chart disclosing an embodiment of enabling the user to access a remote service in response to a successful OTP-based authentication in accordance with the present invention. The embodiment is also feasible with proprietary network services by adding at least two-factor authentication thereto without necessarily creating a need to make changes to the already established authentication/log-in interface and/or internal practice of the service. At 304, enabling data is provided to the terminal as disclosed hereinbefore. The data may include software and e.g. password or password-generation data. The password data, such as an encrypted password provided in .nxs file with reference to e.g. NoMachine™ virtual desktop solutions, may be meant for one access or log-in event only, or be applicable for a longer period such as for the time being if not substantially perpetually relative to e.g. the life cycle of the service. Software may include a number of software entities such as a browser-based entity, e.g. a Java applet, and/or a (binary) executable. The elements may be configured to communicate with each other.

At 306, the obtained data may be utilized in the terminal. In one scenario, the Java applet may access the password and provide it to the executable. The executable may optionally decrypt the password. Then the Java applet and/or other software entity such as the executable may be configured to address the optionally decrypted password to the network service for gaining access thereto, i.e. log in to the service. The network service may operate at least tangentially through the arrangement with a number of common elements or independently as mentioned hereinbefore. In more general terms, an access request utilizing the data may be provided 308 by the terminal to the network service operated through and/or by the arrangement or some other entity. The terminal may perform these actions automatically or alternatively, at least some of them may require user intervention such as confirmation. The service side, i.e. the arrangement and/or service entity external thereto, may verify the credentials and if satisfied, begin serving the terminal 310 according to the service practices. For example, a visual GUI for a virtual desktop may be provided to the terminal in connection with a corresponding kind of a network service. If the user in
question is provided with associated user rights (e.g. the role of an organization superuser), he/she may be able to modify or even add new user accounts including e.g. related e-mail - mobile number combinations and other information to the service portion, such as organization-related portion, under his/her control. As a result, new users may be conveniently added to the userbase of the service.

In some embodiments, when the service is to be accessed for the second time by the same user and terminal, the OTP authentication may be again executed generally in accordance with the embodiment of Figure 2, for instance, followed by the actual service log-in as, by way of example, represented in Figure 3. However, all the data such as Java applet or binary executable may not be necessary to re-transfer. If the service access password is of OTP nature or has expired for some other reason, a new, optionally encrypted (recalling the fact that as the connection may be encrypted itself, the password may be actually multiple times encrypted during the transfer) service password may be provided to the terminal for local use and subsequent service log-in request (308). The suggested solution may add to overall security level of the network service as an OTP-based multi-factor, at least two-factor, authentication is provided thereto.

Figure 4 is a flow chart disclosing various items of an embodiment incorporating location/voice data exploitation in accordance with the present invention. For example, such items could be executed in connection with items 215, 216 of the flow chart of Figure 2 excluding the adoption phase shown at 404 that is preferably performed earlier. Namely, at 404 the allowed (and/or forbidden) locations and/or voiceprints are established. Also the terminal application, preferably mobile application, for code input, data acquisition, notifying and/or data transfer may be installed.

At 406, locationing and/or voice recognition ID code(s), or 'keys', are transferred, preferably as browser data such as web page data, to a user terminal during a communication session associated with a predetermined user of the service for visualization and subsequent uttering by the user.

At 408, the location and/or voice (sound) data is acquired and optionally processed at the user terminal, preferably being a mobile terminal and by utilizing the installed (native) application, and transferred to the network service.
Optionally, the terminal may apply e.g. POST method for the transmission that may further optionally include location data, accuracy/error indication, geokey and/or sound data (voice file). The server may be configured to store the received information and return a salted hash 'session key' such as a salted MD5-hash using a common secret key (the one the server knows and each valid client should know; the secret key may be embedded in the associated code). The terminal may then reply with a 'session key' by GET (browser) request and provide an URL-hash computed using the same secret key (i.e. the common secret). The server may obtain the salted MD5-hash using the secret key and compare it with the received URL-hash in order to verify the validity of the terminal application prior to begin analyzing and verifying the actual location and/or voice data.

At 410, the obtained location and/or voice data may be analyzed. Ultimately, the authentication status of the concerned user may be finally adapted accordingly as deliberated hereinbefore.

A computer program, comprising a code means adapted, when run on a computer, to execute an embodiment of the desired method steps in accordance with the present invention, may be provided. A carrier medium such as an optical disc, floppy disc, or a memory card, comprising the computer program may further be provided. The program may be delivered over a communication network and a communication channel.

Consequently, a skilled person may on the basis of this disclosure and general knowledge apply the provided teachings in order to implement the scope of the present invention as defined by the appended claims in each particular use case with necessary modifications, deletions, and additions. For example, instead of HTML, a variation thereof, such as XHTML (extensible HTML), or e.g. WML (Wireless Markup Language) may be applied for document presentation, transfer and/or storage. In some embodiments, instead of a true OTP, a multi-times (still preferably a limited-times (authorizing e.g. two or three log-ins)) and/or a merely temporally limited-life password may be utilized for the mobile-enhanced authentication.
Claims

1. An arrangement (106), such as a server apparatus or a plurality of at least functionally connected server and/or other apparatuses, for controlling access to a network service, such as a cloud service, utilizing multi-factor, at least two-factor, authentication, comprising a processing entity (150) and a memory entity (152) for processing and storing data, respectively, and a data transfer entity (156) for receiving and sending data, the arrangement being configured to transmit a code (143c), preferably as browser data such as web page data, during a communication session associated with a predetermined user of the service for visualization and subsequent uttering by the user,

receive sound data (143g) indicative of the uttered code,

determine on the basis of the sound data and voiceprint data associated with the predetermined user whether the code has been uttered by the predetermined user (143h), and provided that this seems to be the case,

raise the gained authentication status of the predetermined user regarding at least the current communication session (1431), wherein raising the authentication status optionally includes at least one action selected from the group consisting of: enabling a new service feature, enabling the use of a new application, enabling a new communication method, and enabling the adjustment of service settings or preferences.

2. The arrangement of claim 1, configured to send an e-mail notice (128) to an e-mail address associated with a predetermined user, the e-mail notice including a preferably secure link for a browser, such as an Internet browser,

receive an indication of the activation of the preferably secure link (134), such as a data request like a web resource request sent via a browser, in response to which the arrangement being further configured to send
- first browser data, such as web page data, requesting the user of the browser to input a secret (136), and
- a one-time password (OTP) to a mobile device associated with the predetermined user (138b),

receive user input relative to the request for secret (140),

determine whether the user input matches the sent OTP (142), and

in the case of a match, enable the user of the browser and related terminal device, the user being thus authenticated as the predetermined user, to access the service (144, 144a, 186, 188).

3. The arrangement of claim 2, configured to send enabling data (144a) to the terminal device, such as second browser data, wherein the enabling data preferably includes at least one element selected from the group consisting of: a browser executable program, a Java entity, a Java applet, an executable, a binary executable, a password, data for generating a password, and an encrypted password.

4. The arrangement of any preceding claim, configured to further utilize the estimated location of the user as an authentication factor (143), optionally configured to receive location data together with the sound data.

5. The arrangement of claim 4, wherein the location estimate is based on the estimated location of the terminal device applied for activating the link.

6. The arrangement of any of claims 4-5, wherein the location estimate is based on the estimated location of the mobile device associated with the predetermined user.

7. The arrangement of any of claims 4-6, wherein the location estimate is compared against one or more predetermined locations.

8. The arrangement of claim 7, wherein in the case of a match between the location estimate and a predetermined location deemed as allowable, the authentication is considered successful in the light of the location-related authentication factor.
9. The arrangement of any of claims 7-8, wherein in the case of a match between
the location estimate and a predetermined location not deemed as allowable, the
authentication is considered unsuccessful in the light of the location-related
authentication factor.

10. The arrangement of any of claims 4-9, configured to trace user behavior, said
tracing including monitoring locations and/or movements, whereupon said
arrangement is configured to determine a number of allowed or banned locations
for accessing electronic documents at least partially based on the behavior.

11. The arrangement of any of claims 4-10, wherein the location refers to at least
one element selected from the group consisting of: address, network address,
sub-network, IP (Internet Protocol) address, IP sub-network, cell, cell-ID, street
address, one or more coordinates, GPS (Global Positioning System) coordinates,
GLONASS (GLObal Navigation Satellite System) coordinates, district, town,
country, continent, distance from a predetermined location, and direction from a
predetermined location.

12. The arrangement of any of claims 4-11, wherein the location is estimated
utilizing an indication of data transmission delay such as data packet transit or
round-trip delay relating to the terminal device of the user, such as the mobile
device or other terminal device, optionally a desktop or laptop computer.

13. The arrangement of any of claims 4-12, configured to transmit a second code,
preferably as browser data such as web page data, during a communication
session associated with a predetermined user of the service for visualization and
subsequent input by the user, further configured to receive data indicative of the
inputted code and of the location of the terminal device applied for transmitting
the data, determine on the basis of the data and predetermined locations
associated with the user whether the user is in an allowed location, and provided
that this seems to be the case on the basis of the data, raise the gained
authentication status of the user regarding at least the current communication
session.

14. The arrangement of claim 2, wherein the e-mail is provided as digitally
signed utilizing at least one certificate selected from the group consisting of:
S/MIME-compliant (Secure/Multipurpose Internet Mail Extensions) identity
certificate, OpenPGP (Pretty Good Privacy, RFC 4880) -compliant identity certificate, and X.509-compliant identity certificate.

15. The arrangement of claim 2, configured to send enabling data (144a) to the terminal device including at least one program, such as a browser-executable program optionally including a Java applet, and password data, optionally including encrypted password data, the sent data being required by the terminal device to access the network service.

16. The arrangement of claim 2, configured to send enabling data (144a) including at least part of a network service session file, such a file with nxs extension, to the terminal, said part optionally including password data for accessing the network service such as a plain text password or encrypted password.

17. The arrangement of claim 2, configured to send enabling data (144a) to the terminal device including password data for accessing the service, wherein the password data is indicative of a limited-times password, such as one-time (OTP) password, and/or a temporally automatically expiring password.

18. The arrangement of any of claims 2-17, configured to apply a predetermined digital fingerprint technique to verify the identity of the terminal during the service usage, after log in.

19. The arrangement of claim 2, configured to send enabling data (144a) to the terminal device including password data and other data for accessing the service, wherein the password data is dynamic and to be created and sent for each instance of service access by the user and the other data is static such as a computer program and to be used multiple, optionally subsequent, times for accessing the service by the user.

20. The arrangement of claim 2, configured to send the OTP embedded in a text or multimedia message, such as an SMS-compliant (Short Message Service) or an MMS-compliant (Multimedia Messaging Service) message, respectively.

21. The arrangement of any of claims 2-20, configured to host the network service, preferably a virtual or remote desktop service.
22. A system comprising the arrangement of any preceding claim and a mobile terminal device for receiving the code transmitted by the arrangement, obtaining the sound data indicative of the uttered code and transmitting the data to the arrangement.

23. A method for controlling access to a network service such as a cloud virtual-desktop service, the method utilizing at least two-factor authentication and comprising

- transmitting a code, preferably as browser data such as web page data, during a communication session associated with a predetermined user of the service for visualization and subsequent uttering by the user (406),

- receiving sound data indicative of the uttered code (408),

- determining on the basis of the received sound data and voiceprint data associated with the predetermined user whether the code has been uttered by the predetermined user, and provided that this is the case according to a number of predetermined criteria (410),

- raising the authentication status of the predetermined user regarding at least the current communication session (1431).

24. The method of claim 23, further comprising sending an e-mail to an e-mail address associated with a predetermined user, said e-mail including a preferably secure link for a browser (206),

- receiving an indication of the activation of the preferably secure link (208), optionally further receiving a user request for one-time password (OTP) (209),

- sending first browser data, such as web page data, requesting the user of the browser to input a secret (210),

- sending a one-time password (OTP) to a mobile device associated with the user (212),

- receiving user input relative to the request for secret (214),
determining whether the user input matches the sent OTP (216), and

in the case of a match, enabling the user of the browser and related terminal, the user being thus authenticated as the predetermined user, to access the service, wherein said enabling includes sending enabling data to the terminal (218, 304) optionally via the browser-related connection such as HTTP (Hypertext Transfer Protocol) connection.

25. A computer program comprising code means adapted to, when run on a computer, to execute the method items of claim 23 or 24.

26. A carrier medium comprising the computer program according to claim 25.
Authenticate Yourself for Cloud Services

1. User ID: demo
   - Ok: Demo Oy

2. Your email: martti@aplicomp.fi
   - Ok

3. Your mobile phone: 358400502157
   - Ok

4. Email identification: sdf
   - Ok

5. Password delivery method:
   - By email
   - By SMS
   - Ok

6. Verify above fields 1 - 5.
   - Verify
   - Fields 1 - 5. are Ok, click Request "button"

7. Request link into your email
   - Request
   - Authentication email has been sent to martti@aplicomp.fi

8. Link was sent to your email with subject "sdf"

Figure 1e

Comp User Portal

Reports
Invoices and Letters
Graphical Desktop

Instructions

Raise Security Level

Feed geolkey 965590 into ZEFA application
Dictate voicekey 125973 into ZEFA application
Check Current Security

This email link is valid until 19:31:23 16/06/2012
2 logins left, out of total 3
This session will expire at 21:31:23
Hollanti, Suomi, Viro

ZEFA (R)
START-UP

OBTAI NORICATION OF ACCESS REQUEST

SEND NOTIFICATION E-MAIL WITH SECURE LINK

RECEIVE INDICATION OF LINK ACTIVATION/DATA REQUEST

RECEIVE OTP REQUEST

ASK PASSWORD VIA THE BROWSER

SEND OTP TO MOBILE DEVICE

RECEIVE USER INPUT RELATIVE TO THE PASSWORD REQUEST

ACQUIRE USER (TERMINAL) LOCATION INFORMATION/ACQUIRE VOICE DATA

MATCH?

YES

NO

ENABLE ACCESS TO THE SERVICE

END

Figure 2
Figure 3
Figure 4

215, 216

404
DETERMINE ALLOWED LOCATIONS/ESTABLISH VOICEPRINTS/PROVIDE APPLICATION

406
LOCATION/VOICE ID DELIVERY

408
LOCATION/VOICE DATA ACQUISITION AND TRANSFER

410
DATA ANALYSIS
INTERNATIONAL SEARCH REPORT

INTERNATIONAL APPLICATION No.
PCT/FI2012/050630

A. CLASSIFICATION OF SUBJECT MATTER
See extra sheet

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)

IPC: G06F, H04L, G10L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
FI, SE, NO, DK

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI, XPI3E, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>US 7054819 B1 (LOVELAND SHAWN D [US]) 30 May 2006 (30.05.2006)</td>
<td>1-26</td>
</tr>
<tr>
<td></td>
<td>Fig. 8;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>column 1, lines 6-10;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>column 2, lines 44-49;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>column 11, lines 62-66;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>column 17, lines 32-37;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>column 19, line 55 - column 21, line 10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>abstract;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Figs. 1-5;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraphs [0005], [0016], [0063]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>abstract;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraphs [0041]-[0048], [0082]-[0085], [0097]</td>
<td></td>
</tr>
</tbody>
</table>

Date of the actual completion of the international search: 25 April 2013 (25.04.2013)

Date of mailing of the international search report: 03 May 2013 (03.05.2013)

Name and mailing address of the ISA/FI

National Board of Patents and Registration of Finland
P.O. Box 1160, FI-00101 HELSINKI, Finland

Facsimile No. +358 9 6939 5328

Authorized officer

Vesa-Matti Louekoski

Telephone No. +358 9 6939 500

Form PCT/ISA/210 (second sheet) (July 2009)
<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family members(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td>US 705481 9 B 1</td>
<td>30/05/2006</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1479209 A 2</td>
<td>24/1/2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2006505021 A</td>
<td>09/02/2006</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 03075540 A 2</td>
<td>12/09/2003</td>
</tr>
<tr>
<td>Int.Cl.</td>
<td>Classification</td>
<td>Date</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>----------------</td>
<td>----------</td>
<td></td>
</tr>
<tr>
<td>G06F 21/32</td>
<td>(2013.01)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H04L 9/32</td>
<td>(2006.01)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>G10L 17/00</td>
<td>(2013.01)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>