A method of operating computing apparatus comprises receiving an instruction to initiate an authenticated voice call or an authenticated video call between a first user and a second user, transmitting an identifier to a first device, the first device being associated with the first user, the identifier being uniquely associated with the first user, thereby to allow the computing apparatus to be authenticated by the device or by the first user, receiving user-generated information from the first device, using the user-generated information to authenticate the first user, and causing an authenticated voice call or an authenticated video call to be in place between a second device, the second device being associated with the second user, and the first device or a third device, the third device being associated with the first user.
Authenticated Voice or Video Calls

Field of the Invention
The invention relates to methods of operating computing apparatus, devices and
systems, in particular computing apparatus, devices and systems for use in
authenticated telecommunications. The invention relates also to a computing
apparatus and computer readable code, in particular computing apparatus and
computer readable code for use in authenticated telecommunications.

Background to the Invention
Institutions such as banks are required by modern data protection laws to verify the
identity of the customer with whom they are communicating prior to handing out
sensitive data. As such, the customer is often required to provide personal details
to allow verification to occur. Fraudsters can make use of this fact in order to
illegally obtain personal information, with a view to identity theft or another similar
fraud. Thus, it is very common to receive fraudulent emails from entities
purporting to be banks or other trusted institutions. These emails often include
requests for the victim to provide various different types of personal information
such as usernames, passwords, dates of birth and addresses. Other types of
telecommunication, such as telephone calls, are also used by fraudsters in order to
illegally obtain personal information. This type of activity is commonly known as
phishing.

The invention was made within this context.

Summary of the Invention
According to a first aspect, the present invention provides a method of operating
computing apparatus, the method comprising receiving an instruction to initiate an
authenticated voice call or an authenticated video call between a first user and a
second user, transmitting an identifier to a first device, the first device being
associated with the first user, the identifier being uniquely associated with the first
user, thereby to allow the computing apparatus to be authenticated by the device or
by the first user, receiving user-generated information from the first device, using
the user-generated information to authenticate the first user, and causing an authenticated voice call or an authenticated video call to be in place between a second device, the second device being associated with the second user, and the first device or a third device, the third device being associated with the first user.

According to a second aspect, the present invention provides a method of operating a device, the method comprising receiving an identifier from computing apparatus, the identifier being uniquely associated with a user of the device, comparing the received identifier to a stored identifier, authenticating the computing apparatus only if there is correspondence between the received identifier and the stored identifier, subsequent to the authenticating the computing apparatus, receiving a user-generated information input, sending the user-generated information to the computing apparatus, thereby to allow the computing apparatus to authenticate the user, and subsequent to sending the user-generated information allowing the user to participate in an authenticated voice call or an authenticated video call initiated by the computing apparatus.

According to a third aspect, the present invention provides a method of operating a device, the method comprising receiving an identifier from computing apparatus, the identifier being uniquely associated with a user of the device, outputting the received identifier to a user, subsequent to outputting the received identifier, receiving a user input confirming or denying authentication of the computing apparatus, subsequent to receiving the user input, receiving a user-generated information input, sending the user-generated information to the computing apparatus, thereby to allow the computing apparatus to authenticate the user, and subsequent to sending the user-generated information, allowing the user to participate in an authenticated voice call or an authenticated video call initiated by the computer apparatus.

According to a fourth aspect, the present invention provides a method of operating a system, the system comprising a first device and a second device, each of the first and second devices being associated with a user, the method comprising receiving at the first device, an identifier from computing apparatus, the identifier being
uniquely associated with the user, outputting the received identifier to the user, subsequent to outputting the received identifier, receiving a user input confirming or denying authentication of the computing apparatus, subsequent to receiving a user input confirming authentication of the computing, receiving a user-generated information input, sending the user-generated information to the computing apparatus, thereby to allow the computing apparatus to authenticate the user, and subsequent to sending the user-generated information, the second device receiving an authenticated voice call or an authenticated video call initiated by the computer apparatus.

According to a fifth aspect, the present invention provides a method of operating a system, the system comprising a first device and a second device, each of the first and second devices being associated with a user, the method comprising receiving at the first device, an identifier from computing apparatus, the identifier being uniquely associated with the user, comparing the received identifier to a stored identifier, authenticating the computing apparatus only if there is correspondence between the received identifier and the stored identifier, subsequent to the authenticating the computing apparatus, receiving a user-generated information input, sending the user-generated information to the computing apparatus, thereby to allow the computing apparatus to authenticate the user and, subsequent to sending the user-generated information, the second device receiving an authenticated voice call or an authenticated video call initiated by the computer apparatus.

According to a sixth aspect, the present invention provides computer readable code, optionally stored on a medium, which, when executed by computer apparatus, causes the computer apparatus to perform the method of any of the first to fifth aspects of the present invention.

According to a seventh aspect, the present invention provides computing apparatus comprising processing apparatus and memory, the memory having stored thereon computer readable code which when executed by the processing apparatus causes
the processing apparatus to perform the method of any of the first to fifth aspects of the present invention.

According to an eighth aspect, the invention provides a method of operating computing apparatus, the method comprising: receiving an instruction to initiate an authenticated voice call or an authenticated video call between a first user and a second user; transmitting an identifier to a first device, the first device being associated with the first user, the identifier being uniquely associated with the first user, thereby to allow the computing apparatus to be authenticated by the device or by the first user; subsequent to transmitting the identifier, receiving user-generated information from the first device; using the user-generated information to authenticate the first user; and causing an authenticated voice call or an authenticated video call to be in place between a second device, the second device being associated with the second user, and the first device or a third device, the third device being associated with the first user.

According to a ninth aspect, the invention provides a method of operating computing apparatus, the method comprising: receiving an instruction to initiate an authenticated voice call or an authenticated video call between a first user and a second user; transmitting an identifier to a first device, the first device being associated with the first user, the identifier being uniquely associated with the first user, thereby to allow the computing apparatus to be authenticated by the device; receiving user-generated information from the first device; using the user-generated information to authenticate the first user; and causing an authenticated voice call or an authenticated video call to be in place between a second device, the second device being associated with the second user, and a third device, the third device being associated with the first user.

The identifier described with reference to the above aspects of the present invention may be stored in a database associated with the computing apparatus during registration by the first user with the computing apparatus. The identifier may be known to the first user or the device associated with the first user. The identifier may be received from the user. Alternatively the identifier may be
selected by the first user. Still alternatively the identifier may be selected by the
computer apparatus and may be transmitted during registration to the device
associated with the first user. In any of these cases the identifier may be agreed
during negotiation between the device associated with the first user and the
computer apparatus. The primary purpose of the identifier is to allow the user or
the device to authenticate the computing apparatus and to this end it is of primary
importance that the identifier is known by the user or the device prior to the
authenticated call being initiated.

In order that the invention may be more fully understood, embodiments thereof will
now be described by way of illustrative example with reference to the accompanying
drawings.

Brief Description of the Drawings

In the drawings:

Figure 1 shows a typical telecommunications system within which the present
invention can reside; and

Figures 2, 3 and 4 illustrate methods according to aspects of the present invention.

In the Figures, like references numerals refer to like elements throughout.

Detailed Description of Preferred Embodiments

The telecommunication system 1 of Figure 1 comprises caller-side
telecommunications apparatus 10. In this example, the caller-side
telecommunications apparatus 10 is located within a business or financial
institution, such as a bank. The caller-side telecommunications apparatus 10
comprises a communication and network infrastructure 12 and a plurality of
telecommunications devices 14 connected thereto. The communication and
network infrastructure 12 may include one or more of the following: a proxy for
aggregating communication the plurality of telecommunications devices 14, a
private branch exchange (PBX) or other type of telephony switch, an ISDN to voice
protocol converter, routers, switches, databases and servers or appliances for
running call centre software such as call management, integrated voice recognition, queue management, autodialing, customer relations management and the like.

The telecommunications devices 14 may include computers, such as desktop PCs 14a and laptops 14b, telephone devices such as landline telephones 14c, mobile or cellular telephones 14d, and voice over internet protocol (VOIP) or other devices 14e allowing voice to be transmitted via a PC or network. It will be appreciated that the telecommunications devices 14 may include other types of device such as personal digital assistants (PDAs), internet tablets etc. The telecommunications devices 14 may be in physical and/or wireless connection with the communication and network infrastructure 12. The telecommunications devices 14 and the communication and network infrastructure 12 may or may not be on the same premises. Associated with the telecommunications devices 14 are callers 40, for instance employees of the business or financial institution.

The telecommunications system 1 of Figure 1 also includes recipient-side telecommunications apparatus 20. Associated with the recipient-side telecommunications apparatus 20 are recipients 42, for instance customers of the business or financial institution. It will be appreciated, however, that the recipient 42 could alternatively be people at, for instance employees of, another business or financial institution. The recipient-side telecommunications apparatus 20 includes, for example, computers 22 connected to the internet 32, internet-protocol telephones 24a, 24b connected to the internet 32 via the computers 22, and telephones 24c, 24d, 24e connected wirelessly or physically to a public switched telephone network (PSTN) or ISDN or other network 34. The internet-protocol telephones 24a, 24b and the telephones 24c, 24d, 24e can be denoted a recipient side telecommunications device 24 in the following.

Also included in the telecommunications framework 1 is an authentication server 36. The authentication server 36 provides an authentication service for enabling authenticated telecommunication between a caller 40 and a recipient 42. The authentication server (36) comprises one or more processors 36a for executing computer-readable code such as software. The authentication server 36 also
comprises memory means, such as ROM or RAM, for storing the computer executable code. The methods described hereafter which are performed by the authentication server 36 may be caused by computer executable code which is optionally stored on the memory means 36b being executed by the one or more processors 36a. Similarly, method steps carried out by any of the other devices described with reference to Figure 1 may also be caused by computer executable code, such as software, being executed by processors 24c-1, 22-1 and optionally being stored on memory means 24c-2, 22b. The authentication server 36 may also to be operable to provide one or more of the following functionalities: the recording of the calls, the recording of participant data, time stamping, GPS stamping, encrypting and tamper evident signing.

Prior to providing the authentication service, the caller 40 and the recipient 42 register with the authentication server 36. The registration details of the caller 40 and recipient 42 may be stored on a database 36-1 associated with the authentication server. When registering, the registrant 40, 42 provides various personal details including, for example, their name and one or more of their telephone number and their email address. The registrant may provide plural telephone numbers, and optionally may indicate which of those numbers can be used to make or receive authenticated calls. The registrant may also provide one or more instant messaging identifiers, software serial numbers or other identifiers through which the authentication server 36 may contact the user. Other details also may be provided when registering. During registration, the registrant 40, 42 and the server 36 agree one or more unique identifiers. The one or more unique identifiers are used during the authentication process. Advantageously, the unique identifier is easily recognisable by the registrant 42. For example, the unique identifier may be an audio clip that is personal to the user. More specifically, the audio clip may be a recording of the registrant reciting a phrase, for instance a phrase meaningful to the registrant 40, 42. The unique identifier need not be provided by the registrant 40, 42, but should be known and recognisable by the registrant 40, 42. For example, the unique identifier may be a password or passphrase.
The authentication server 36 may be located in any appropriate place. For example, the authentication server 36 may be located at the caller side on the premises of the business or financial institution. The authentication server 36 may instead be located remotely from both the caller-side and the recipient-side apparatuses 10, 20.

The authentication server 36 may be communicatively coupled to the caller- and user-side apparatuses in any suitable way. For example, the authentication server 36 may be communicatively coupled to the caller- and user-side apparatuses by physical connection (particularly if the authentication server is located at same premises as the caller-side apparatus), via the PSTN 34, by the Internet, other network or by any combination thereof.

A method according to certain aspects of the invention will now be described with reference to Figure 2.

In step S1, the caller 40 provides an input instruction to the caller side telecommunications device 14. The input indicates to the caller side telecommunications device 14 that the caller 40 wishes to begin an authenticated communication with the recipient 42. The input may include the telephone number of the recipient’s device 24, or any other information uniquely identifying the recipient 42. The indication that the caller 40 wishes to begin an authenticated communication with the recipient 42 may be made by contacting the authentication server 36, for instance by dialling a telephone number associated with the authentication server 36. The caller side telecommunications device 14 may know based on a pre-stored parameter associated with the recipient’s telephone number that calls to the recipient 42 should be authenticated by the authentication server 36.

Following the receipt of the input instruction, in step S2 a telephone call is initiated between the caller side telecommunications device 14 and the authentication server 36.
The authentication server 36 then begins a process of authenticating the caller 40. This includes sending to the caller side telecommunications device 14 a request S3 for the input of information which identifies the caller 40.

In response to the request S3 from the authentication server 36, in step S4 the caller 40 supplies the requested identification information to the authentication server 36, either via a keypad (not shown) of the caller side telecommunications device 14, or via the IVR platform of the authentication server 36. Authentication of the caller 40 may be performed in any appropriate way, for example by way of the user supplying one or more characters or digits of a secret password or passcode. Advantageously, authentication of the caller 40 by the authentication server 36 may be performed using the “PINsafe™ authentication system”. The operation of this system is described in UK Patent 2,366,966. The authentication of the caller 40 may be performed by the authentication server 36 itself or alternatively may be performed by another associated server 38 (see Figure 1), for example the “PINsafe™” server.

In step S5, when the authentication server 36 has authenticated the caller 40, the authentication server 36 initiates a telephone call to the recipient side telecommunications device 24.

In step S6, when the recipient 42 answers the telephone call, the authentication server 36 transmits to the recipient side telecommunications device 24 the unique identifier that is stored at the database 36-1 and is associated with the recipient 42. In this example, the unique identifier is an audio clip of the recipient 42 reciting a line from their favourite film. In this example, the recipient hears themselves reciting “Live long and prosper”. The authentication server 36 then requests the recipient to indicate whether they wish to receive a telephone call from the caller 40. The authentication server 36 may also provide the recipient 42 with the option to reschedule the authenticated call.

If the recipient 42 recognises the audio clip as being their own voice reciting their memorable phrase, they can immediately know that the call is coming via the
authentication server 36 and thus can trust that the caller 40 is who they purport to be. Put another way, the recipient 42 can authenticate the authentication server 36. Thus, the recipient 42 can accept the phone call confident that the caller 40 is not a fraudster.

If the recipient 42 does not recognise the unique identifier that is transmitted by the authentication server 36, they may terminate the call.

Following acceptance of the call by the recipient 42, the method proceeds to step S7 in which the authentication server 36 begins the process of authenticating the recipient 42. This includes the authentication server 36 sending to the recipient 42, via the recipient side telecommunications device 24, a request for the input of identifying information.

In step S8, the recipient 42 provides the authentication server 36 with the requested information, thereby allowing the authentication server 36 to verify the identity of the recipient 42. The authentication process is advantageously carried out using the PINsafe™ authentication system, discussed above with reference to steps S3 and S4, although it will be understood that any suitable authentication process could be used.

Following authentication of the recipient 42, in step S9, the authentication server 36 bridges the call back from the recipient side telecommunications device 24 to the caller side telecommunications device 14. Bridging involves connecting the recipient 42 to the caller 40. In other words, the authentication server 36 initiates or otherwise connects an authenticated call between the recipient side telecommunications device 24 and the caller side telecommunications device 14. Thus, the caller 40 and the recipient 42 are able to communicate verbally with one another. If a call between the authentication server 36 and the caller side telecommunications device 14 has not been set up prior to step S9, step S9 involves the authentication server 36 connecting with the caller side telecommunications device 14 and then bridging the call.
A compliance server 39 may be in communication with the authentication server 36. The compliance server 39 may record the whole of the call, or alternatively may record only the authentication process.

In the embodiment described with reference to Figure 2, the users (i.e. the caller 40 and the recipient 42) do not require any dedicated software to be present on their devices. The only prerequisite is that the recipient 42 is registered with the authentication server 36, and if the caller 40 is to be authenticated then the caller 40 should have pre-registered with the authentication server 36.

In an alternative embodiment, one or both of the caller 40 and the recipient 42 may have dedicated authentication software, hereafter authenticated call software, installed on their devices 14, 20. Authentication may be carried out using the authenticated call software, with a telephone communication being initiated only when the authentication process is complete.

In this alternative embodiment, when the user 40, 42 is using their device 10, 20, they “log in” to the authenticated call software. “Log in” may be a manual process or may be an automatic process that occurs as soon as the device is switched on.

Following “log-in”, the user 40, 42 may remain logged-in until they provide an explicit instruction to the authentication call software to “log-out”. Alternatively the user (40, 42) may be logged-in for a predetermined session. The length of this session may be determined by the PC, the authentication call software or may last until the user switches their computer off. The method according to this embodiment of the invention will now be described with reference to Figure 3.

In step T1, the caller 40 provides an input to the caller side telecommunications device 14, for example the personal computer 14a. The input is provided using the authenticated call software that is executed by the personal computer 14a. The input indicates to the personal computer 14a that the caller 40 wishes to begin an authenticated communication with the recipient 42. The authenticated call software may store a list of recipients 42, each of whom is registered with the authentication
server 36. In this example, the input may comprise the caller 40 selecting one of the list of recipients 42.

Following the input, in step T2, the authenticated call software causes the personal computer 14a to initiate communication with the authentication server 36. The communication may be over a voice channel or a non-voice data channel. In steps T3 and T4, the authentication server 36 authenticates the caller 40. This occurs via a user interface provided by the authenticated call software. Authentication occurs if the caller 40 provides a response that is the same as an expected response. Although the PINsafe™ authentication process is preferred, any suitable authentication process may be used.

In some embodiments, the caller 40 may be required to authenticate themselves to the authentication server 36 only once for each log-in session. This single authentication may occur as soon as they log-in to the authenticated call software. In other embodiments, the caller 40 may be required to authenticate themselves to the authentication server 36 each time they make an authenticated call.

Following a successful authentication of the caller 40, in step T5, the authentication server 36 initiates communication with the recipient’s devices 20. In this example, the recipient’s devices 20 comprise the PC 22 and a mobile telephone 24b, 24c, 24e.

In this example, initiation of the communication comprises the authentication server 36 transmitting a unique identifier to the recipient’s PC 22. This may occur through the call authentication software residing on the PC 22 including an availability feature by which the authentication server can detect that the call authentication software is operational on the PC 22. This availability feature may be of the type commonly used in instant messaging applications. Alternatively, the authentication server 36 may use an instant messaging application to detect that an instant messaging application is operation on the PC 22, and thereby infer that the recipient 42 is available at the PC 22. In this case the call authentication software executed at the PC 22 may be a plug in to the instant messaging application.
In some embodiments the unique identifier comprises an audio clip of the recipient reciting a memorable phrase. As discussed with reference to Figure 2, this audio clip may have been provided by the recipient 42 upon registration with the authentication server 36. Alternatively, the identifier may be a still or animated image or graphic which has been selected or generated by or assigned to the recipient during the registration process. When the PC 22 receives the identifier it may output by the authenticated call software to the recipient 42. This allows the recipient 42 to authenticate the authentication server 36. If the recipient 42 is satisfied that the identifier is the expected identifier they may provide an input to the authenticated call software 22 which indicates that the recipient 42 is satisfied that the authentication server 36 is genuine.

In alternative embodiments, the authentication server 36 may be authenticated automatically by the authentication call software. According to these embodiments, the authentication server 36 transmits a unique identifier to the authenticated call software. The unique identifier has been agreed during registration and is thus recognised by the authenticated call software. If the authenticated call software does not recognise the unique identifier or the unique identifier is different to an expected identifier, the authenticated call software does not authenticate the authentication server 36. The identifier may be a certain data sequence, and may have been created by the authenticated call software on the PC 22 or may have been created elsewhere and notified to the authenticated call software on the PC 22 at an earlier time.

In some embodiments, the software may authenticate the server 36 automatically and may also present a user-recognisable identifier to the user, thereby to provide the user with increased confidence that the server 36 is authentic.

The authentication server 36 may also provide the user with information regarding the subject of the proposed telephone call. This may be provided for consumption by the user via the authentication call software.
In step T6, following successful authentication of the authentication server 36, the authentication server 36 and the authenticated call software begin authentication of the recipient 42. This may include the authentication server 36 transmitting a request to the authenticated call software on the PC 22 for information to be provided by the recipient 42. Alternatively, the authenticated call software may automatically request the input information from the recipient 42.

In step T7, in response to the request for information, the recipient provides information to the authenticated call software on the PC 22. This information, or information derived therefrom, is then sent to the authentication server 36, which uses the information to authenticate the recipient 42. As discussed above, the PINsafe™ authentication process is preferred, although any suitable authentication process may be used.

In step T8, following a successful authentication of the recipient 42 by the authentication server 36, the authentication server 36 transmits a call identification to the PC 22. The call identification may be a number or a password or the like. The authenticated call software on the PC 22 displays this call identification to the recipient 42.

In step T9, a short period of time after step T8, for example less than a minute, the authentication server 36 initiates a voice call with the recipient’s mobile telephone 24b, 24c. When the recipient 42 answers the telephone call, the authentication server 36 transmits the call identification to the mobile telephone 24b, 24c. This may be by way of a text-to-speech conversion of the call identification, particularly if the call identification is a number or password. If the call identification transmitted to the mobile telephone 24b, 24c matches the call identification displayed by the authenticated call software, the recipient 42 can be sure that the incoming voice call is from the authentication server 36. If the call identification number transmitted to the mobile telephone 24b, 24c does not match the call identification number displayed by the authenticated call software, the recipient 42 may terminate the voice call. Optionally, the authentication server 36 may request the recipient 42 to confirm that the call identifications match each other.
According to alternative embodiments wherein the caller is from, for example, a call centre, the authentication server 36 authenticates the recipient via communication with the authentication software and may then place the and identifier relating to the recipient (such as the recipient's telephone number) at the bottom of a stack. When an existing call is finished, the identifier of the recipient with whom the existing call was in progress is removed from the top of the stack. Thus, the identifiers gradually move towards the top of the stack. When identifier of a recipient reaches the top of the stack, the authentication server 36 initiates the voice call with the telephone of that recipient. In this way, recipients can be authenticated while calls with other recipients are being carried out, thereby improving the efficiency of operation of the call centre.

Finally, in step T10 the authentication server 36 bridges the telephone call from the mobile telephone 24b, 24c of the recipient 42 to the caller-side telecommunications device 14.

In an optional step, the authentication server may carry out further authentication of the recipient 42 by ensuring that the mobile telephone 24a, 24c with which the voice call is connected is in approximately the same location as the PC 22 with which the recipient 42 was authenticated. This may be carried out by comparing a GPS location of the telephone device 14d, assuming the device 14d has GPS capability, and the IP address of the PC 14a. Since the IP address of the Internet connection associated with the PC 14a is dependent to some extent on geography, the IP address may be useable to determine the approximate geographical location of the PC 14a. Co-location of the PC 14a and the telephone device 14d can be assumed in the GPS location of the telephone device 14d matches with the approximate geographical location of the PC 14a. Alternatively the call authentication software 22 on the PC 22 may determine that the mobile telephone 14d is in proximity, for instance using Bluetooth (RTM) proximity detection, Wi-Fi proximity detection, or in any other way.
According to alternative embodiments of the method described with reference to Figure 3, the recipient’s devices may comprise a smart phone or personal digital assistant or internet tablet 24c, instead of a PC 22 and a mobile telephone 24b, 24c. In these embodiments, steps T5 to T8 are performed over a cellular telephone data link, such as a GSM or 3G data link, and steps T9 and T10 are performed using a cellular telephone voice link.

A method according to alternative embodiments will now be described with reference to Figure 4. In these embodiments, the recipient’s device is a smart phone, personal digital assistant or internet tablet 24c. For convenience, the device 24c will hereafter be referred to as a smart phone. The smart phone 24c is provided with call authentication software that is similar to the software described above as residing on the PC 22. In these embodiments, steps U1 to U4 may be substantially the same as steps S1 to S4 as described with reference to Figure 2 or steps T1 to T4 as described with reference to Figure 3.

In step U5, following successful authentication of the caller 40, the authentication server 36 initiates communication with the recipient’s smart phone 24c. The authenticated call software on the smart phone 24c is configured to recognise a call coming from the authentication server 36. Thus, prior to alerting the recipient 42, the authenticated call software intercepts the incoming communication from the authentication server 36. In step U6, when the authenticated call software has intercepted and answered the incoming communication from the authentication server 36, the authentication server 36 transmits a unique identifier over a voice link to the authenticated call software being executed by the smart phone 24c. The unique identifier may comprise fax noise, dual tone multi-frequency (DTMF) tones or any type of audio signal that can be interpreted or deciphered by the smart phone 24c. The unique identifier is agreed between the authentication server 36 and the smart phone 24c during registration by the recipient at the authentication server 36. The unique identifier may be generated by the call authentication software on the smart phone 24c, or it may be generated by the authentication server 36. If the smart phone 24c recognises the unique identifier as the expected unique identifier it authenticates the server 36.
In step U7, following authentication of the authentication server 36 by the smartphone 24c, the smartphone 24c alerts the recipient 42 that an authenticated call is incoming. From this alert the recipient 42 can be sure that the call authentication software has authenticated the server 36.

In step U8, after the recipient 42 has been alerted to the presence of an incoming authenticated call, the authentication server 36 begins the process of authenticating the recipient 42 by sending a request for information to the smartphone 24c. In response to this request, in step U9, the recipient inputs the requested information to the smartphone 24c which then transmits the information to the authentication server 36. The requested information may be spoken by the recipient into a microphone (not shown) of the smartphone 24c and interpreted by the authentication server 36 using voice recognition software. Alternatively, the requested information may be provided via, for example, a keypad, touch screen or other input device (not shown) of the smartphone 24c and may be communicated to the authentication server 36 using DTMF.

As discussed with reference to other embodiments, authentication via the PINSafe™ authentication process is preferred, although any authentication process may be used.

Following authentication of the recipient by the authentication server 36, in step U10 the authentication server bridges the telephone call back from the recipient’s smartphone 24c to the caller-side telecommunications device such as to connect the caller 40 and the recipient 42.

According to some embodiments in which the caller 40 is from a business or corporation, the corporation’s telecommunication server 12 may automatically initiate the authenticated communication with the recipient 42. Following authentication of the authentication server 36 by the recipient 42 or by the recipient’s device 20 and following authentication of the recipient 42 by the authentication server 36, the authentication server 36 bridges the telephone call
back to the corporation’s telecommunication server 12. The corporation’s
telecommunication server may route the call to the device of a particular individual
in the corporation, or may alternatively route the call to the device of any available
member of staff in, for example, a call centre. This enables a pool of call centre
staff to connect to recipients without a particular staff member being required to
initiate each call. Call initiation may in this case be automatic rather than manual.
Each of the call centre staff may be logged-in to the authenticated call software and
may have been authenticated at the start of their log-in session.

10 Also, the authentication server 36 on receiving an instruction to initiate an
authenticated call with a user may as a preliminary step determine whether call
authentication software associated with the user, for instance on a smart phone 24c
or a PC 22, indicates availability. Here, the authentication server 36 decides
whether to initiate communication with the call authentication software if such does
indicate availability, and initiates a call directly with the recipient’s telephone 24a,
24d if there is no availability. If the authentication server 36 attempts to initiate
communication with the call authentication software but is unsuccessful, the
authentication server may then attempt to initiate communication by dialling the
recipient’s telephone 24a, 24c, 24d.

20 The service provided by the authentication server 36 described in relation to the
above embodiments may be provided by a single server, plural distributed servers,
multiple servers within a cloud, a cluster of servers or any other suitable type of
computing apparatus.

25 In alternative embodiments, the invention may be carried out within a peer-to-peer
framework. In these embodiments, each user (i.e. the caller 40 and the recipient 42)
authenticates the other user directly without communicating with an intermediary
server, such as authentication server 36. In such embodiments, the caller’s device
14 executes authentication software similar to that executed by the authentication
server 36 described with reference to the previous embodiments. Consequently, the
caller’s device 14 includes a database containing information relating to other users
with whom they are able to carry out authenticated calling. Thus, each time a user
wishes to be able to carry out authenticated communication with a new user, the
devices of the user and the new user exchange information. This information may
include personal details such as one or more telephone numbers, one or more email
addresses or one or more instant messaging identifiers, software serial numbers or
other identifiers through which the devices may authenticate each other. The
recipient device 24 also provides the caller device 14 with unique identifiers. When
the caller wishes to initiate an authenticated communication with the recipient, the
caller device 14 initiates the communication and transmits the unique identifier
associated with the second user to the recipient device 24. Thus the recipient
device 24 or the recipient themselves can authenticate the caller device 14. The
recipient authenticates him or herself to the caller device 14 by generating
information and using the device to send it to the caller device 14, for example
using PINsafe™. In this way, authenticated communication can be provided within
a peer-to-peer framework.

According to another alternative embodiment, the methods of Figures 3 and 4 may
not require dedicated authentication software. Instead, following authentication of
the caller by the authentication server 36, a universal resource locator (URL) may be
transmitted to the recipient’s PC 22 or smart phone 24c. The recipient activates the
URL and is taken to a web page. The PC 22 or smart phone 24c may automatically
authenticate the authentication server 36 based on a pre-agreed unique identifier
that is transmitted with the URL. Alternatively or additionally, upon reaching the
web page, the authentication server 36 presents the unique identifier, such as an
audio clip etc., to the recipient via the web page. If the user recognises the unique
identifier they proceed to authenticate themselves to the authentication server 36 by
for example entering personal information to the web page. The authentication of
the recipient may be carried out, for example using PINsafe™. Once authentication
has been successfully carried out, the user is presented with a call identifier via the
web page. Subsequent to this the method may proceed as described with reference
to steps T9 and T10 of Figure 3.

The above described methods are not exclusive of one another. Thus, steps from
one method may be combined with steps from another method. For example, the
caller’s device 10 may be operating the authenticated call software as described with reference to Figure 3, but the recipient 42 may not be running the software or may not be logged in to the software. In such cases, authentication of the caller may be carried out as described in steps T1 to T4 of Figure 3 and, subsequent to
determination that the recipient’s device does not have, or is not logged into, the authentication software, the authentication process may proceed as described with reference to steps S5 to S8 of Figure 2. Also, the steps of the above methods need not be in the exact order in which they are described. For example, the caller 40 and the recipient may be authenticated by the server simultaneously, or the caller 40 may be authenticated after the recipient 42.

In the above specific examples, the caller 40 has been from a business or corporation and the recipient 42 has been a customer of the business or corporation. However, it will be understood that the methods are also applicable between two businesses or corporations, or between two individuals, who may or may not be part of one organisation. Similarly, the caller 40 may be a customer of a business or corporation who is the recipient 42 of the call.

Although the above embodiments primarily are directed to providing an authenticated telephone call between two parties, the invention is applicable also to the provision of authenticated video calls between two parties. In video call embodiments, the authentication server 36 may use face recognition technology to authenticate the caller 40 and/or the recipient 42. In these embodiments the user generates information with which they can be authenticated by directing a camera included in their device 14, 24 at their face.

It should be realised that the foregoing embodiments are not limiting. Other variations and modifications will be apparent to persons skilled in the art upon reading the present application. Moreover, the disclosure of the present application should be understood to include any novel features or any novel combination of features either explicitly or implicitly disclosed herein or any generalisation thereof and during the prosecution of the present application or of any application derived
therefrom, new claims may be formulated to cover any such features and/or combination of such features.
Claims

1. A method of operating computing apparatus, the method comprising:
   receiving an instruction to initiate an authenticated voice call or an
   authenticated video call between a first user and a second user;
   transmitting an identifier to a first device, the first device being associated
   with the first user, the identifier being uniquely associated with the first user,
   thereby to allow the computing apparatus to be authenticated by the device or by
   the first user;
   receiving user-generated information from the first device;
   using the user-generated information to authenticate the first user; and
   causing an authenticated voice call or an authenticated video call to be in
   place between a second device, the second device being associated with the second
   user, and the first device or a third device, the third device being associated with the
   first user.

2. The method of claim 1, wherein transmitting the identifier to the device and
   receiving the user-generated information are performed using a non-voice data
   channel between the computing apparatus and the first device.

3. The method of claim 2, further comprising transmitting an authenticated
   communication identifier to the first device using the non-voice data channel,
   initiating a voice call between the computing apparatus and the first device, and
   subsequently transmitting the authenticated communication identifier to the first
   device as part of the voice call.

4. The method of claim 2, further comprising, after using the user-generated
   information to authenticate the first user, conducting the authenticated voice call or
   the authenticated video call between the second device and the third device.

5. The method of claim 2, further comprising, after using the user-generated
   information to authenticate the first user, initiating a voice call between the
computing apparatus and the third device only if it is determined that the first device and the third device are proximate to one another.

6. The method of claim 4 or claim 5, further comprising transmitting an authenticated communication identifier to the first device, and subsequently transmitting the authenticated communication identifier to the third device as part of the authenticated voice call or the authenticated video call.

7. The method of claim 1, wherein causing an authenticated voice call or an authenticated video call to be in place comprises causing an authenticated voice call or an authenticated video call to be in place between the second device and the first device and wherein transmitting the identifier to the first device and receiving the user-generated information are performed using a voice channel or a video channel between the computing apparatus and the first device.

8. The method of any preceding claim, comprising receiving the identifier from the first user prior to receiving an instruction to initiate an authenticated voice call or an authenticated video call.

9. The method of claim 8, wherein the identifier is audio data.

10. The method of claim 9, wherein the audio data is a recording of the user’s voice.

11. The method of any preceding claim, wherein the instruction to initiate the authenticated telecommunication is received from the second device, the method further comprising:

   receiving user-generated information from the second device or from a fourth device, the fourth device being associated with the second user; and

   using the user-generated information to authenticate the second user.

12. The method of claim 11, further comprising bridging a voice call between the second device or the fourth device and the first device or the third device.
13. The method of any of claims 1 to 11 wherein the device associated with the second user comprises the computer apparatus.

14. A method of operating a device, the method comprising:
   receiving an identifier from computing apparatus, the identifier being uniquely associated with a user of the device,
   comparing the received identifier to a stored identifier;
   authenticating the computing apparatus only if there is correspondence between the received identifier and the stored identifier;
   subsequent to the authenticating the computing apparatus, receiving a user-generated information input;
   sending the user-generated information to the computing apparatus, thereby to allow the computing apparatus to authenticate the user; and
   subsequent to sending the user-generated information allowing the user to participate in an authenticated voice call or an authenticated video call initiated by the computing apparatus.

15. A method of operating a device, the method comprising:
   receiving an identifier from computing apparatus, the identifier being uniquely associated with a user of the device,
   outputting the received identifier to a user;
   subsequent to outputting the received identifier, receiving a user input confirming or denying authentication of the computing apparatus;
   subsequent to receiving the user input, receiving a user-generated information input;
   sending the user-generated information to the computing apparatus, thereby to allow the computing apparatus to authenticate the user; and
   subsequent to sending the user-generated information, allowing the user to participate in an authenticated voice call or an authenticated video call initiated by the computer apparatus.
16. A method of operating a system, the system comprising a first device and a second device, each of the first and second devices being associated with a user, the method comprising:

   receiving at the first device, an identifier from computing apparatus, the identifier being uniquely associated with the user;

   outputting the received identifier to the user;

   subsequent to outputting the received identifier, receiving a user input confirming or denying authentication of the computing apparatus;

   subsequent to receiving a user input confirming authentication of the computing apparatus, receiving a user-generated information input;

   sending the user-generated information to the computing apparatus, thereby to allow the computing apparatus to authenticate the user; and

   subsequent to sending the user-generated information, the second device receiving an authenticated voice call or an authenticated video call initiated by the computer apparatus.

17. A method of operating a system, the system comprising a first device and a second device, each of the first and second devices being associated with a user, the method comprising:

   receiving at the first device, an identifier from computing apparatus, the identifier being uniquely associated with the user;

   comparing the received identifier to a stored identifier;

   authenticating the computing apparatus only if there is correspondence between the received identifier and the stored identifier;

   subsequent to the authenticating the computing apparatus, receiving a user-generated information input;

   sending the user-generated information to the computing apparatus, thereby to allow the computing apparatus to authenticate the user; and

   subsequent to sending the user-generated information, the second device receiving an authenticated voice call or an authenticated video call initiated by the computer apparatus.

18. The method of claim 16 or claim 17 comprising:
subsequent to sending the user-generated information, the first device receiving an authenticated communication identifier; and
the first device outputting the authenticated communication identifier to the user.

Subsequent to the first device outputting the authenticated communication identifier, the second device receiving the authenticated communication identifier as part of the authenticated voice call or the authenticated video call.

19. Computer readable code, optionally stored on a medium, which, when executed by computer apparatus, causes the computer apparatus to perform the method of any of claims 1 to 18.

20. Computing apparatus comprising processing apparatus and memory, the memory having stored thereon computer readable code which when executed by the processing apparatus causes the processing apparatus to perform the method of any of claims 1 to 18.
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L29/06
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

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

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

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>WO 2008/002206 A1 (ERICSSON TELEFON AB L M [SE]; DAHLIN STEINAR [SE]; RYDE ANDERS [SE]) 3 January 2008 (2008-01-03) page 7, line 30 - page 8, line 29</td>
<td>1-20</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C. See patent family annex.

Date of the actual completion of the international search: 18 March 2011

Date of mailing of the international search report: 24/03/2011

Name and mailing address of the ISA/
European Patent Office, P.B. 5618 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer
Veen, Gerardus
<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td>US 2007043947 A1</td>
<td>22-02-2007</td>
<td>CN 101248643 A</td>
<td>20-08-2008</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1915846 A1</td>
<td>30-04-2008</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2009505576 T</td>
<td>05-02-2009</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KR 20080041153 A</td>
<td>09-05-2008</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 2007024455 A1</td>
<td>01-03-2007</td>
</tr>
<tr>
<td>WO 2008002206 A1</td>
<td>03-01-2008</td>
<td>CA 2675554 A1</td>
<td>03-01-2008</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 101473330 A</td>
<td>01-07-2009</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GB 2456069 A</td>
<td>08-07-2009</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SE 0850173 A</td>
<td>20-01-2009</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2010023417 A1</td>
<td>28-01-2010</td>
</tr>
</tbody>
</table>