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

(19) **World Intellectual Property Organization**
International Bureau

(43) **International Publication Date**
7 October 2010 (07.10.2010)

PCT

(10) **International Publication Number**
WO 2010/114459 A1

(51) **International Patent Classification**:
H04L 9/32 (2006.01)

(21) **International Application Number**:
PCT/SE2010/050172

(22) **International Filing Date**:
15 February 2010 (15.02.2010)

(25) **Filing Language**: English

(26) **Publication Language**: English

(30) **Priority Data**:
12/414,957 31 March 2009 (31.03.2009) US

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

(72) **Inventors**: **SCHULTZ, Göran**; Vågtoppen 7 B 47, FIN-02320 ESBOO, Finland, FIN-02320 Espoo (FI). **SALMELA, Patrik**; Kuninkaantie 5-7 B 20, FIN-02400 Kirkkonummi (FI). **AMIN, Parth Ileshkumar**; 2B Pratima Park, Ahmedabad 380013 (IN). **SUSITAIVAL, Riikka**; Mannerheimintie 82 A 13, FIN-00250 Helsinki (FI). **WAGER, Stefan**; Gårdsgränden 8 H, FI-FUN-02360 Espoo (FI).

(74) **Agent**: **HASSELGREN, Joakim**; Ericsson AB, Patent Unit LTE, Torshamnsgatan 23, S-164 80 Stockholm (SE).

(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

[Continued on next page]

(54) **Title**: METHOD AND APPARATUS FOR EMAIL COMMUNICATION

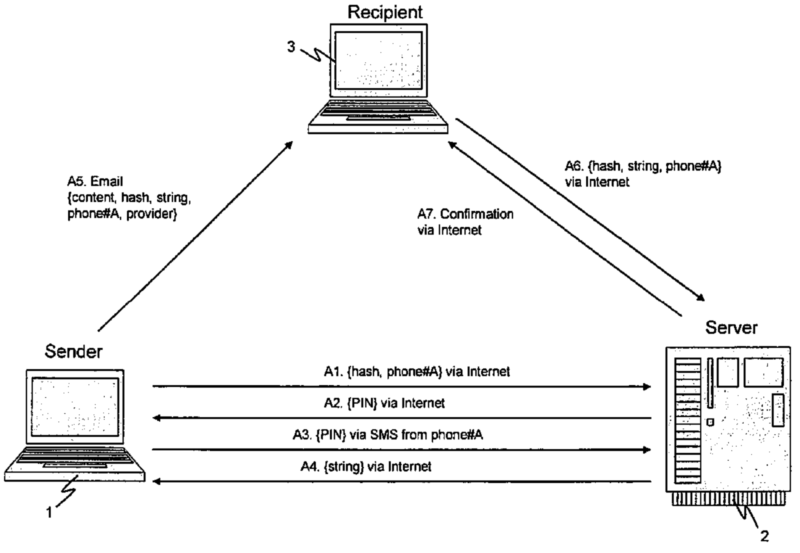
Recipient
3
A5. Email {content, hash, string, phone#A, provider}
A6. {hash, string, phone#A} via Internet
A7. Confirmation via Internet
Server
Sender
A1. {hash, phone#A} via Internet
A2. {PIN} via Internet
A3. {PIN} via SMS from phone#A
A4. {string} via Internet
1
2

Figure 1

(57) **Abstract**: According to the present invention there is provided a method of verifying to a recipient of an email that a sender of the email possesses a mobile telecommunications device associated with a specific telephone number. The method comprises using a Short Message Service message, sent from the sender to a server (A3), to verify to the server that the sender of the email has access to the telephone number, and, following receipt of the email, the recipient contacting the server (A6) to obtain confirmation that the sender of the received email has access to the telephone number (A7).

WO 2010/114459 A1

Published:

— *with international search report (Art. 21(3))*

METHOD AND APPARATUS FOR EMAIL COMMUNICATION

Technical Field

The present invention relates to a method and apparatus for email communication. More particularly, the invention relates to verifying, to a recipient of an email, that the sender possesses a specific phone number.

Background

Today a large proportion of people have at least one email (electronic mail) account, and there are a variety of ways in which an individual can obtain an email account. For example, a user's employer may provide them with an email account, or when a user subscribes to an Internet Service Provider (ISP) they will usually be provided with at least one email account. In addition, a user can create an email account with one of a number of email services, such as Google's Gmail®, Microsoft's Hotmail ® etc.

Each email account is associated with at least one email address that is unique to that account, and therefore allows any emails sent to this address to be delivered appropriately. Email addresses take the form "local-part@domain", wherein the domain identifies the entity/entities that host the account associated with the email address, and the local-part identifies the individual email account to the host (see, for example, IETF RFC 5321).

When creating an email account, it is often the case that a user is free to define what the local-part of their email address will be, provided that it is unique to the host. As such, a recipient of an email cannot necessarily rely on the email address as a means for correctly identifying the sender. For example, an email sent from the email address "john.smith@emailservice.com" may not be from an individual whose name is actually John Smith. Furthermore, even if the local-part of the email address does in some way accurately represent the actual name of the sender, the recipient of the email can not be certain which particular individual the email is from. This is particularly true of those email addresses wherein the domain part of the email address identifies a host that allows anybody to create an email address.

Summary

The present invention provides a method of verifying to a recipient of an email that a sender of the email possesses a mobile telecommunications device associated with a specific telephone number. The method comprises using a Short Message Service message, sent from the sender to a server, to verify to the server that the sender of the email has access to the telephone number, and, following receipt of the email, the recipient contacting the server to obtain confirmation that the sender of the received email has access to the telephone number.

According to a first aspect of the present invention there is provided a method of verifying to a recipient of an email that a sender of the email possesses a mobile telecommunications device associated with a specific telephone number. The method comprises at the sender, sending an identifier of the email content and the telephone number to a server via the Internet, at the server, receiving the identifier and the phone number from the sender, generating a verification code, sending the verification code to the sender via the Internet, and storing the verification code with the identifier and the telephone number, at the sender, receiving the verification code from the server and returning the verification code to the server in a Short Message Service message sent by said mobile telecommunications device, at the server, confirming that the received verification code and the telephone number from which the Short Message Service message originated match the stored telephone number and verification code, and then using the telephone number and the identifier to generate an authentication string, and sending the authentication string to the sender via the Internet, at the sender, receiving the authentication string from the server, and sending the email including said authentication string and said telephone number to the recipient via the Internet, at the recipient, receiving the email, and forwarding the authentication string, the telephone number and the identifier of the received email content to said or another server, and at the receiving server, receiving the authentication string, the telephone number and the identifier, generating an authentication string using the received telephone number and identifier, confirming that the received authentication string is the same as the generated authentication string, and sending confirmation to the recipient.

The method may further comprise, at the server, when sending the verification code to the sender via the Internet, starting a timer, when the verification code is received from the sender, determining if the timer has expired, and only confirming that the received verification code and the telephone number from which the Short Message Service message originated match the stored telephone number and verification code if the timer has not expired.

The method may further comprise, at the sender, including the identifier of the email content in the email sent to the recipient. Alternatively, if the identifier of the email content comprises a hash value of the email content, then the method may further comprise generating the hash value of the email content.

According to a second aspect of the present invention there is provided method of operating a user terminal connected to the Internet. The method comprises, prior to sending an email from the user terminal to a recipient, sending an identifier of the email content and a telephone number to a server, receiving a verification code from the server via the Internet, receiving an authentication string from the server via the Internet, including the authentication string and the telephone number in the email; and sending the email to the recipient.

The method may further comprise, including the identifier of the email content in the email sent to the recipient. Alternatively, if the identifier of the email content comprises a hash value of the email content, then the method may further comprise generating the hash value of the email content.

An email client of the user terminal may automatically perform the steps of generating the hash value of the email content and sending the hash value and the telephone number to the server. These steps may be performed automatically upon an input from a user of the user terminal. The step of including the authentication string and the telephone number in the email may also be performed automatically, by an email client of the user terminal, when the authentication string is received.

According to a third aspect of the present invention there is provided method of operating a server. The method comprises receiving, from a sender of an email, an identifier of the email content and a telephone number, generating a verification code, sending the verification code to the sender via the Internet, storing the verification code with the identifier and the telephone number, receiving the verification code that has been returned to the server in a Short Message Service message, determining if the received verification code and the telephone number from which the Short Message Service message originated match a verification code and telephone number, and, if so, using the telephone number and the identifier to generate an authentication string, and sending the authentication string to the sender via the Internet.

When sending the verification code to the sender via the Internet the method may further comprise, starting a timer, and then, when the verification code is received from the sender, determining if the timer has expired, and only confirming that the received verification code and the telephone number from which the Short Message Service message originated match the stored telephone number and verification code if the timer has not expired.

According to a fourth aspect of the present invention there is provided method of operating a server. The method comprises receiving, from a recipient of an email, a string, a telephone number and an identifier of the email content, generating an authentication string using the received telephone number and identifier, determining if the received string is the same as the generated authentication string, and sending a message to the recipient confirming whether or not the sender of the email content possesses a mobile telecommunications device associated with the telephone number.

According to a fifth aspect of the present invention there is provided a method of operating a user terminal connected to the Internet. The method comprises receiving an email from a sender, said email including a string and a telephone number, sending the string, the telephone number and an identifier of the email content to a server, and receiving a message from the server confirming whether or not the sender of the email content possesses a mobile telecommunications device associated with the telephone number.

If the identifier of the email content comprises a hash value of the email content, the method may further comprise, generating the hash value of the email content.

The step of sending the string, the telephone number and an identifier of the email content to a server may be performed automatically, by an email client of the user terminal, when the email including a string and a telephone number is received. This step may be performed automatically upon an input from a user of the user terminal.

According to a sixth aspect of the present invention there is provided an apparatus configured to operate as a user terminal. The apparatus comprises an email client for generating an email to a recipient, and for inserting an authentication string and a telephone number into the email prior to sending the email, a transmitter for sending an identifier of email content and the telephone number to a server, a receiver for receiving a verification code from the server and for receiving the authentication string for the email from the server, and a transmitter for sending the email including the authentication string and the telephone number to the recipient.

The email client may be arranged to generate the identifier by applying a hash function to the email content.

According to a seventh aspect of the present invention there is provided an apparatus configured to operate as a server. The apparatus comprises a receiver for receiving, from a sender of an email, an identifier of the email content and a telephone number, a code generation unit for generating a verification code, a transmitter for sending the verification code to the sender via the Internet, a memory for storing the verification code with the identifier and the telephone number, a receiver for receiving a verification code that has been returned to the server in a Short Message Service message, a processing unit for determining if the received verification code and the telephone number from which the Short Message Service message originated match a stored verification code and telephone number, and, if so, for using the telephone number and the identifier to generate an authentication string, and a transmitter for sending the authentication string to the sender via the Internet.

The apparatus may further comprise a timer that is started when the verification is sent to the sender, wherein the processing unit is arranged to determine if the timer has expired when the verification code is received from the sender, and to only confirm that the received verification code and the telephone number from which the Short Message Service message originated match the stored telephone number and verification code if the timer has not expired.

According to an eighth aspect of the present invention there is provided an apparatus configured to operate as a server. The apparatus comprises a receiver for receiving, from a recipient of an email, a string, a telephone number and an identifier of the email content, a processing unit for generating an authentication string using the received phone number and identifier, a processing unit for determining if the received string is the same as the generated authentication string, and a transmitter for sending a message to the recipient, the message confirming whether or not the received string is the same as the generated authentication string.

According to a ninth aspect of the present invention there is provided apparatus configured to operate as a user terminal. The apparatus comprises a receiver for receiving an email from a sender, the email including a string and a telephone number, an email client for extracting the string and the telephone number, a transmitter for sending the string, the telephone number and an identifier of the email content to a server, and a receiver for receiving, from the server, a message indicating whether or not the sender of the email content possesses a mobile telecommunications device associated with the telephone number.

If the email from the sender also includes the identifier, the email client may be arranged to extract the identifier from the email. Alternatively, the email client may be arranged to generate the identifier by applying a hash function to the email content.

According to a tenth aspect of the present invention there is provided a method of operating an email client. The method comprises prior to sending an email to a recipient, generating an identifier of the email content, sending the identifier and a telephone number to a server, receiving a verification code from the server, displaying the verification code to the user, receiving an authentication string from the server, including the authentication string and the telephone number in the email, and sending the email to the recipient.

The method may further comprise including the identifier of the email content in the email sent to the recipient. Alternatively, the identifier of the email content may be generated comprises a hash value generated by applying a hash function to the email content.

According to an eleventh aspect of the present invention there is provided method of operating an email client. The method comprises upon receipt of an email including a string and a telephone number, sending the string, the telephone number and an identifier of the email content to a server, and receiving a message from the server confirming whether or not the sender of the email content possess a mobile telecommunications device associated with the telephone number.

If the identifier of the email content comprises a hash value of the email content, the method may further comprise generating the hash value of the email content.

Brief Description of the Drawings

Figure 1 illustrates schematically an example of the process by which the sender of an email can verify, to the recipient, that he/she has access to a specific phone number;
Figure 2 is a flow diagram illustrating the process implemented by the sender of an email;
Figure 3 is a flow diagram illustrating the process implemented by a verification server when interacting with a sender of an email;
Figure 4 is a flow diagram illustrating the process implemented by the recipient of an email;
Figure 5 is a flow diagram illustrating the process implemented by a verification server when interacting with a recipient of an email;
Figure 6 illustrates schematically an example of the user terminal of a sender of an email;
Figure 7 illustrates schematically an example of a verification server; and
Figure 8 illustrates schematically an example of user terminal of a recipient of an email.

Detailed Description

It is recognised here that a large proportion of individuals have access to a mobile telecommunication device, and that it will often be the case that most, if not all, of the people that an individual is likely to contact will know and trust the telephone number belonging to this individual. As such, there will now be described a method by which the sender of an email can verify, to the recipient, that he/she possesses a specific telephone number, therefore providing the recipient with means for confirming the identify of the sender. The method involves using a Short Message Service (SMS) message, sent from the sender of an email to a server, to verify to the server that the sender has access to a specific telephone number. The server can then confirm this to the recipient of email.

Figure 1 illustrates schematically an example of the process of associating an email with a telephone number of the sender, and verifying this to the recipient. The steps performed are as follows:

A1. The sender 1 generates the content of an email that he/she wishes to send. The email client at the sender 1 then generates an identifier for the email content. For example, the sender 1 can apply a hash function to this content to generate a hash value. This hash value is then sent, together with the sender's telephone number, to a verification server 2 via the Internet.

A2. The server 2 receives the hash value and telephone number from the sender 1, generates a short verification code or PIN, stores the PIN together with the hash value and the telephone number, and returns this PIN to the sender 1 via the Internet. At the same time the server 2 starts a timer that runs for a predefined time. The PIN sent to the sender 1 is only valid for the duration of this timer.

A3. When the sender 1 receives the PIN from the server 2, he/she uses a mobile telecommunications device that is associated with the telephone number to return the PIN to the server 2 in a SMS message. Alternatively, the sender 1 could use their mobile telecommunications device to call a number associated with the server 2 and, once connected, to type or dial in the PIN.

A4. When the server 2 has received the PIN it determines whether or not the timer has expired. Provided that the timer has not yet expired, the server 2 then verifies that the received PIN and the telephone number from which the SMS originates matches the PIN and telephone number stored in the server's memory. Provided that this is the case, the server 2 then uses the phone number and the hash value as inputs to some process or function, that generates an authentication string. The authentication string should be unique to that combination of hash value and telephone number. For example, the authentication string could be generated by the application of a hash function to the concatenation of the hash value of the email content and the telephone number. The server 2 returns this authentication string to the sender 1 via the Internet.

A5. When the sender 1 receives the authentication string, they can then include this authentication string, the hash value of the email content and their telephone number in the email. The email is then sent to the recipient 3. The email should also include the identity of the service provider that the recipient 3 should contact in order to verify the association between the authentication string, the hash value, and the telephone number.

A6. When the recipient 3 receives the email they can then forward the authentication string, the hash value and the telephone number to the server 2. The recipient 3 can use the identity of the service provider, which was also sent with the email, to determine the appropriate server 2 to contact.

A7. The server 2 then uses the telephone number and the hash value received from the recipient 3 as inputs to the same process or function, as that used in step A4, in order to generate a string. The server 2 then determines if this generated string is the same as the string received from the recipient 3. If so, the server 2 can confirm, to the recipient, that the sender 1 of the email content possesses a mobile telecommunications device associated with that telephone number.

In addition, by applying the same hash function to the content of the received email, the recipient 3 can then compare this with the received hash value to confirm that the email content is the same as that originally verified by the server. Alternatively, if the email from the sender did not include the hash value, the recipient could make use of the same hash function as used by the sender to generate the hash value. This hash value would then be sent to the server together with the telephone number and the authentication string. In this case, only if the content of the received email is the same as that used to create the hash value sent to the server by the sender, will the generated string match the string sent with the email.

Figure 2 is a flow diagram illustrating the process implemented by the sender of an email in order to verify that they have access to a specific telephone number. The steps performed are as follows:

B1. The sender 1 generates the content of an email to be sent.

B2. The email client, or some other application, of the sender 1 can then apply a hash function to this content to generate a hash value.

B3. The sender then sends this hash value together with the sender's telephone number to a server 2 via the Internet.

B4. The sender 1 then receives a verification code or PIN from the server 2.

B5. The sender 1 then returns the PIN to the server 2 in a Short Message Service message from the mobile telecommunications device associated with the sender's telephone number. Alternatively, the sender 1 could use their mobile telecommunications device to call a number associated with the server 2 and, once connected, to type or dial in the PIN.

B6. The sender 1 then receives confirmation from the server 2 that the sender's telephone number has successfully been verified, the confirmation including an authentication string.

B7. The email client at the sender 1 then automatically includes this authentication, the identifier and the sender's telephone number in the email and sends the email to the recipient.

Figure 3 is a flow diagram illustrating the process implemented by the verification server in order to verify that the sender of an email possesses a specific telephone number. The steps performed are as follows:

C1. The server 2 receives a hash value and a telephone number from the sender 1

C2. The server 2 generates a short verification code or PIN, sends this PIN to the sender 1 via the Internet, stores the PIN together with the hash value and the phone number, and starts a timer.

C3. The server 2 receives a PIN that has been sent in a SMS message.

C4. The server 2 then determines if the timer has expired.

C5. If the timer has expired, the server 2 notifies the sender that the verification has failed, and erases the record of the hash value, the telephone number and the PIN from its memory.

C6. If the timer has not expired, the server 2 then determines if the received PIN and the telephone number from which the SMS originated matches a PIN and a telephone number stored in its memory.

C7. If it is determined that the received PIN and the telephone number from which the SMS originated does not match a PIN and telephone number stored in the memory, then the server 2 notifies the sender 1 that the verification of the phone number has failed.

C8. If it is determined that the received PIN and the telephone number from which the SMS originated does match a PIN and telephone number stored in the memory, then the server 2 makes use of the telephone number and hash value as inputs to some process or function in order to generate an authentication string. For example, the authentication string could be generated by the application of a hash function to the concatenation of the hash value of the email content and the telephone number. The server 2 then sends the authentication string to the sender 1 via the Internet.

Once the sender of an email has verified their phone number to the server, and received an authentication string, the sender can then send the email to the recipient. The sender must at least include the verified phone number and the authentication string in the email. Figure 4 is a flow diagram illustrating the process implemented by the recipient of an email in order to verify that the sender of the email possesses a mobile telecommunications device associated with the telephone number that has been included with the email. The steps performed are as follows:

D1. The recipient 3 receives an email from a sender. The email includes a telephone number, a hash value, a string and the identity of a service provider.

D2. The recipient 3 makes use of the identity of the service provider to identify a server 2 to contact. The recipient 2 then sends the string, the hash value and the telephone number to the identified server 2. This could be performed automatically by the recipient's email client.

D3. The recipient 3 receives a response from the server 2 confirming whether or not the sender of the email possesses a mobile telecommunications device associated with the telephone number.

Figure 5 is a flow diagram illustrating the process implemented by the verification server in order to confirm, to the recipient of an email, that the sender of the email possesses a specific telephone number. The steps performed are as follows:

E1. The server 2 then receives a hash value, a string and a telephone number from a recipient 3.

E2. The server 2 then uses the telephone number and the hash value received from the recipient 3 as inputs to a process or function, which is the same as that used in step C8 above, in order to generate a string.

E3. The server 2 then determines if this generated string is the same as the string received from the recipient 3.

E4. If the generated string is not the same as the received string, then the server 2 notifies the recipient 3 that the verification of the phone number has failed.

E5. If the generated string is the same as the received string, then the server sends confirmation to the recipient 3 that the sender 1 of the email content possesses a mobile telecommunications device associated with the telephone number.

As previously described, by applying the same hash function to the content of the received email, the recipient 3 can then compare this with the received hash value to confirm that the email content is the same as that originally verified by the server. Alternatively, if the email from the sender did not include the hash value, the recipient could make use of the same hash function as used by the sender to generate the hash value. This hash value would then be sent to the server together with the telephone number and the authentication string. In this case, only if the content of the received email is the same as that used to create the hash value sent to the server by the sender, will the generated string match the string sent with the email.

The method described above allows the sender of an email to provide the recipient with means for confirming the identity of the sender, by verifying that he/she possesses a mobile telecommunications device associated with a specific telephone number. The server used to provide this verification will usually belong to a service provider trusted by both the sender and the recipient. In providing that the verification code or PIN is returned to the server in an SMS message, or by means of a telephone call made using the telecommunications device, the method provides that the server can verify that the sender possesses the telephone number. Furthermore, by providing that the PIN must be sent from the sender's telecommunication device to the server, the service provider has means for charging the sender for the verification service.

The generation of the authentication string using the hash value of the email content and the sender's telephone number provides that the server does not need to store this string, thereby reducing the burden on the server's memory. As such, when the server is required to provide confirmation to the recipient, it can simply use the hash value and telephone number received from the recipient to re-create the authentication string. Only if the hash value and telephone number are the same as those used to create the received string, will the generated string match the received string. The function or process used to create the authentication string should therefore ensure that the string will be unique for the particular combination of email content and telephone number, and should also be such that it cannot easily be inverted. For example, the authentication string could be generated by the application of a hash function, known only to the server, to the concatenation of the hash value of the email content and the telephone number.

Figure 6 illustrates schematically an example of user terminal 4 to be used to send an email, and suitable for implementing the method described above. The user terminal 4 can be implemented as a combination of computer hardware and software. The user terminal 4 comprises an email client 5, a transmitter 6 and a receiver 7. The email client 5 is suitable for generating an email from the user to a recipient and for applying a hash function to the email content to generate a hash value. The transmitter 7 is suitable for sending the hash value of the email content and a phone number to a server, and for sending the email together with a unique string and the phone number to the recipient. The transmitter 7 may also be suitable for sending the hash value of the email content with the email to the recipient. The receiver 8 is suitable for receiving a PIN from the server and for receiving a unique string for the email from the server.

Figure 7 illustrates schematically an example of a verification server 2 suitable for implementing the method described above. The server 2 can be implemented as a combination of computer hardware and software. The server 2 comprises a receiver 8, a code generation unit 9, a transmitter 10, a memory 11, a SMS client 12 and a processing unit 13. The receiver 8 is suitable for receiving, from a sender of an email, a hash value of the email content and a phone number. The PIN generation unit 9 is suitable for generating a PIN. The transmitter 10 is suitable for sending the PIN and for sending a unique string to the sender via the Internet. The memory 11 is suitable for storing the PIN with the hash value and the phone number. The SMS client 12 is suitable for receiving a Short Message Service message including a PIN. The processing unit 13 is suitable for verifying the phone number if the received PIN matches the stored PIN, and, if so, for using the phone number and the hash value to generate the unique string for the email. The server 2 may also comprise a timer 14 that is started when the PIN is sent to the sender. The processing unit 13 will then only verify the phone number if a Short Message Service message including the PIN is received prior to expiration of the timer 14.

In addition, the receiver 8 is also suitable for receiving, from a recipient of an email, a string, a phone number and a hash value of the email content. The processing unit 13 is also suitable for determining if the received string is the same as a unique string generated using the received phone number and hash value, and, if so, verifying that the sender of the email content has access to the phone number, and the transmitter 10 is also suitable for sending a message to the recipient, the message indicating whether or not the verification has been successful.

Figure 8 illustrates schematically an example of user terminal 15 used to receive an email, and suitable for implementing the method described above. The user terminal 15 can be implemented as a combination of computer hardware and software. The user terminal 15 comprises a receiver 16, a transmitter 17 and an email client 18. The receiver 16 is suitable for receiving an email from a sender, together with a string and a phone number, and for receiving, from the server, verification that the sender of the email content has access to the phone number. The transmitter 17 is suitable for sending the string, the phone number and a hash value of the email content to a server. The email client 18 is suitable for applying a hash function to the email content to generate the hash value, and for automatically extracting the string and the telephone number from the email.

It will be appreciated by the person of skill in the art that various modifications may be made to the above-described embodiments without departing from the scope of the present invention.

Claims

1. A method of verifying to a recipient of an email that a sender of the email possesses a mobile telecommunications device associated with a specific telephone number, the method comprising:

at the sender, sending an identifier of the email content and the telephone number to a server via the Internet;

at the server, receiving the identifier and the phone number from the sender, generating a verification code, sending the verification code to the sender via the Internet, and storing the verification code with the identifier and the telephone number;

at the sender, receiving the verification code from the server and returning the verification code to the server in a Short Message Service message sent by said mobile telecommunications device;

at the server, confirming that the received verification code and the telephone number from which the Short Message Service message originated match the stored telephone number and verification code, and then using the telephone number and the identifier to generate an authentication string, and sending the authentication string to the sender via the Internet;

at the sender, receiving the authentication string from the server, and sending the email including said authentication string and said telephone number to the recipient via the Internet;

at the recipient, receiving the email, and forwarding the authentication string, the telephone number and the identifier of the received email content to said or another server; and

at the receiving server, receiving the authentication string, the telephone number and the identifier, generating an authentication string using the received telephone number and identifier, confirming that the received authentication string is the same as the generated authentication string, and sending confirmation to the recipient.

2. A method as claimed in claim 1, and further comprising:

at the server, when sending the verification code to the sender via the Internet, starting a timer, when the verification code is received from the sender, determining if the timer has expired, and only confirming that the received verification code and the telephone number from which the Short Message Service message originated match the stored telephone number and verification code if the timer has not expired.

3. A method as claimed in any preceding claim, and further comprising:

at the sender, including the identifier of the email content in the email sent to the recipient.

4. A method as claimed in any preceding claim, wherein the identifier of the email content comprises a hash value of the email content, and the method further comprises generating the hash value of the email content.

5. A method of operating a user terminal connected to the Internet, the method comprising:

prior to sending an email from the user terminal to a recipient, sending an identifier of the email content and a telephone number to a server;

receiving a verification code from the server via the Internet;

receiving an authentication string from the server via the Internet;

including the authentication string and the telephone number in the email; and sending the email to the recipient.

6. A method as claimed in claim 5, and further comprising:

including the identifier of the email content in the email sent to the recipient.

7. A method as claimed in any of claims 5 or 6, wherein the identifier of the email content comprises a hash value of the email content, and the method further comprises generating the hash value of the email content.

8. A method as claimed in claim 7, wherein an email client of the user terminal automatically performs the steps of generating the hash value of the email content and sending the hash value and the telephone number to the server.

9. A method as claimed in any of claims 5 to 8, wherein the step of including the authentication string and the telephone number in the email is performed automatically, by an email client of the user terminal, when the authentication string is received.

10. A method of operating a server, the method comprising:

receiving, from a sender of an email, an identifier of the email content and a telephone number;

generating a verification code;

sending the verification code to the sender via the Internet;

storing the verification code with the identifier and the telephone number;

receiving the verification code that has been returned to the server in a Short

Message Service message; and

determining if the received verification code and the telephone number from which the Short Message Service message originated match a stored verification code and telephone number, and, if so, using the telephone number and the identifier to generate an authentication string, and sending the authentication string to the sender via the Internet.

11. A method as claimed in claim 10, and further comprising:

when sending the verification code to the sender via the Internet, starting a timer, when the verification code is received from the sender, determining if the timer has expired, and only confirming that the received verification code and the telephone number from which the Short Message Service message originated match the stored telephone number and verification code if the timer has not expired..

12. A method of operating a server, the method comprising:

receiving, from a recipient of an email, a string, a telephone number and an identifier of the email content;

generating an authentication string using the received telephone number and identifier;

determining if the received string is the same as the generated authentication string; and

sending a message to the recipient confirming whether or not the sender of the email content possesses a mobile telecommunications device associated with the telephone number.

13. A method of operating a user terminal connected to the Internet, the method

comprising:

receiving an email from a sender, said email including a string and a telephone number;

sending the string, the telephone number and an identifier of the email content to a server; and

receiving a message from the server confirming whether or not the sender of the email content possesses a mobile telecommunications device associated with the telephone number.

14. A method as claimed in claim 13, wherein the identifier of the email content comprises a hash value of the email content, and the method further comprises generating the hash value of the email content.

15. An apparatus configured to operate as a user terminal, the apparatus comprising:

an email client for generating an email to a recipient, and for inserting an authentication string and a telephone number into the email prior to sending the email;

a transmitter for sending an identifier of email content and the telephone number to a server;

a receiver for receiving a verification code from the server;

a receiver for receiving the authentication string for the email from the server; and

a transmitter for sending the email including the authentication string, and the telephone number to the recipient.

16. An apparatus as claimed in claim 15, wherein the email client is arranged to generate the identifier by applying a hash function to the email content.

17. An apparatus configured to operate as a server, the apparatus comprising:

a receiver for receiving, from a sender of an email, an identifier of the email content and a telephone number;

a code generation unit for generating a verification code;

a transmitter for sending the verification code to the sender via the Internet;

a memory for storing the verification code with the identifier and the telephone number;

a receiver for receiving a verification code that has been returned to the server in a Short Message Service message;

a processing unit for determining if the received verification code and the telephone number from which the Short Message Service message originated match a stored verification code and telephone number, and, if so, for using the telephone number and the identifier to generate an authentication string; and

a transmitter for sending the authentication string to the sender via the Internet.

18. An apparatus as claimed in claim 17, the apparatus further comprising:

a timer that is started when the verification is sent to the sender, wherein the processing unit is arranged to determine if the timer has expired when the verification code is received from the sender, and to only confirm that the received verification code and the telephone number from which the Short Message Service message originated match the stored telephone number and verification code if the timer has not expired.

19. An apparatus configured to operate as a server, the apparatus comprising:

a receiver for receiving, from a recipient of an email, a string, a telephone number and an identifier of the email content;

a processing unit for generating an authentication string using the received phone number and identifier;

a processing unit for determining if the received string is the same as the generated authentication string; and

a transmitter for sending a message to the recipient, the message confirming whether or not the sender of the email content possesses a mobile telecommunications device associated with the telephone number.

20. An apparatus configured to operate as a user terminal, the apparatus comprising:

a receiver for receiving an email from a sender, the email including a string and a telephone number;

an email client for extracting the string and the telephone number;

a transmitter for sending the string, the telephone number and an identifier of the email content to a server; and

a receiver for receiving, from the server, a message indicating whether or not the sender of the email content possesses a mobile telecommunications device associated with the telephone number.

21. An apparatus as claimed in claim 20, wherein the email from the sender also includes the identifier and the email client is arranged to extract the identifier from the

email.

22. An apparatus as claimed in claim 20, wherein the email client is arranged to generate the identifier by applying a hash function to the email content.

23. A method of operating an email client, the method comprising:

prior to sending an email to a recipient, generating an identifier of the email content;

sending the identifier and a telephone number to a server;

receiving a verification code from the server;

displaying the verification code to the user;

receiving an authentication string from the server;

including the authentication string and the telephone number in the email; and

sending the email to the recipient.

24. A method of operating an email client, the method comprising:

upon receipt of an email including a string and a telephone number, sending the string, the telephone number and an identifier of the email content to a server; and

receiving a message from the server confirming whether or not the sender of the email content possess a mobile telecommunications device associated with the telephone number.

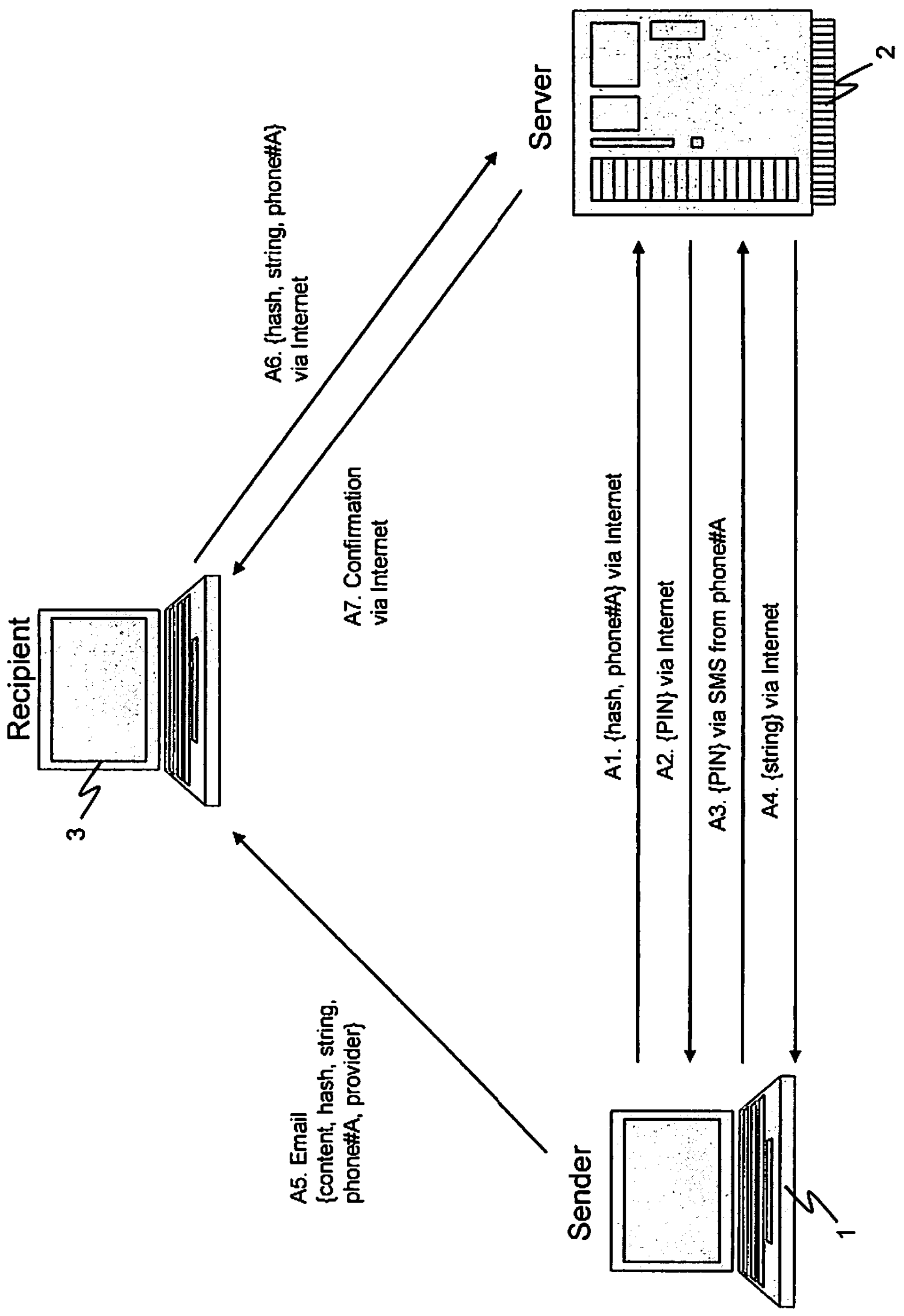
Recipient
3
A6. {hash, string, phone#A} via Internet
A7. Confirmation via Internet
Server
2
A5. Email {content, hash, string, phone#A, provider}
A1. {hash, phone#A} via Internet
A2. {PIN} via Internet
A3. {PIN} via SMS from phone#A
A4. {string} via Internet
Sender
1

Figure 1

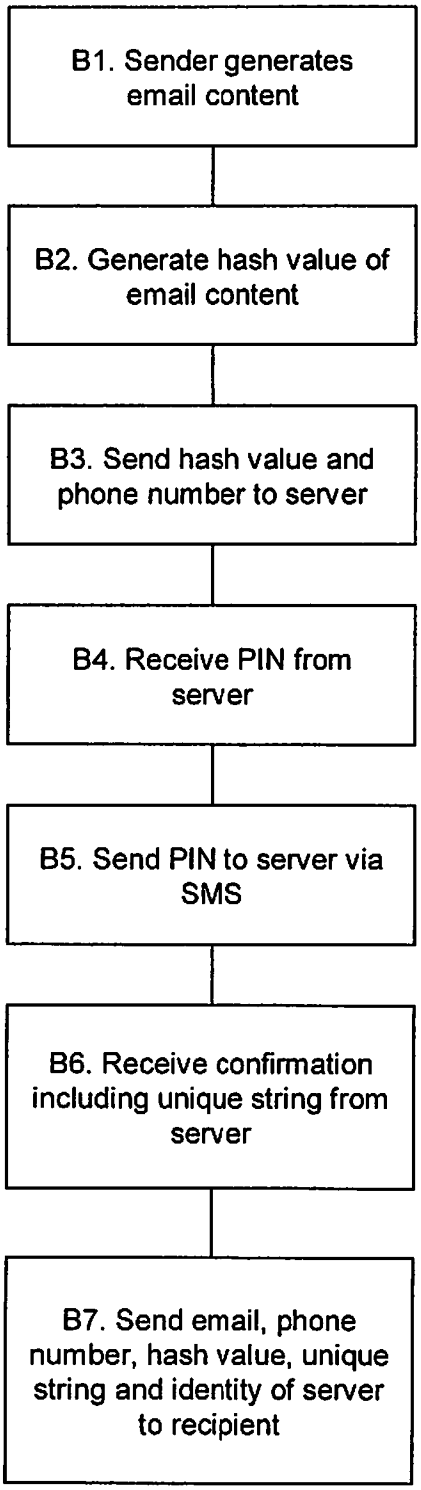
B1. Sender generates email content
B2. Generate hash value of email content
B3. Send hash value and phone number to server
B4. Receive PIN from server
B5. Send PIN to server via SMS
B6. Receive confirmation including unique string from server
B7. Send email, phone number, hash value, unique string and identity of server to recipient

Figure 2

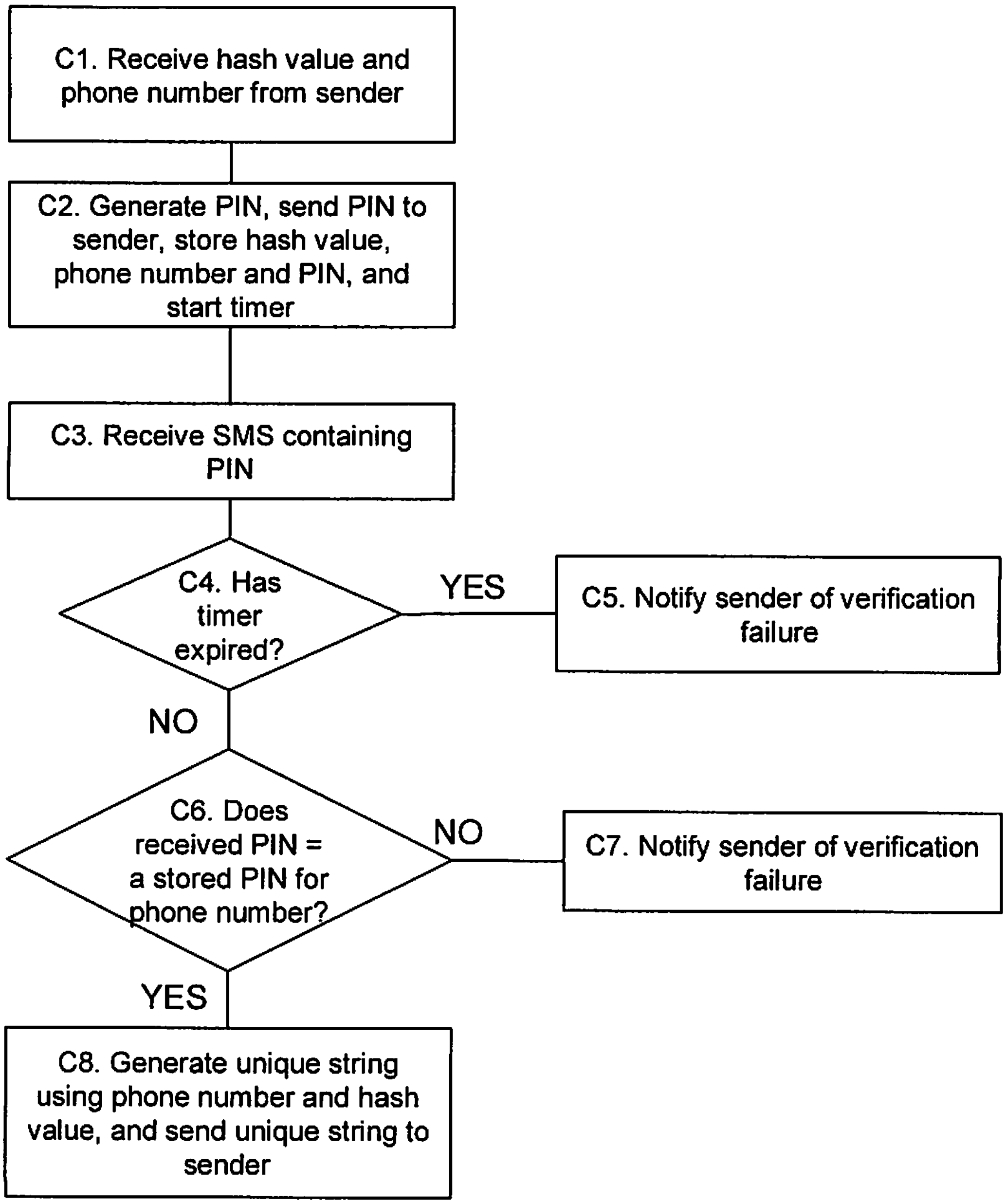
C1. Receive hash value and phone number from sender
C2. Generate PIN, send PIN to sender, store hash value, phone number and PIN, and start timer
C3. Receive SMS containing PIN
C4. Has timer expired?
YES
C5. Notify sender of verification failure
NO
C6. Does received PIN = a stored PIN for phone number?
NO
C7. Notify sender of verification failure
YES
C8. Generate unique string using phone number and hash value, and send unique string to sender

Figure 3

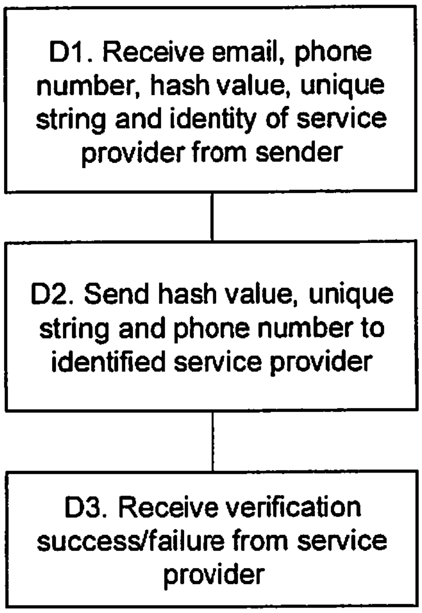
D1. Receive email, phone number, hash value, unique string and identity of service provider from sender
D2. Send hash value, unique string and phone number to identified service provider
D3. Receive verification success/failure from service provider

Figure 4

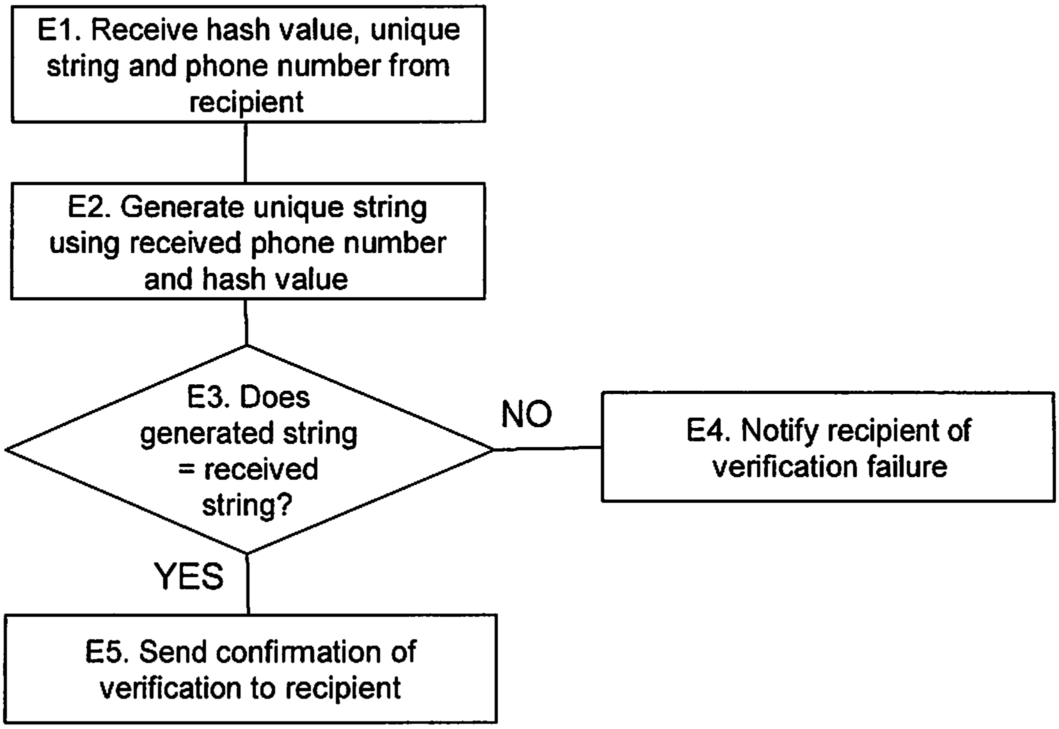
E1. Receive hash value, unique string and phone number from recipient
E2. Generate unique string using received phone number and hash value
E3. Does generated string = received string?
NO
E4. Notify recipient of verification failure
YES
E5. Send confirmation of verification to recipient

Figure 5

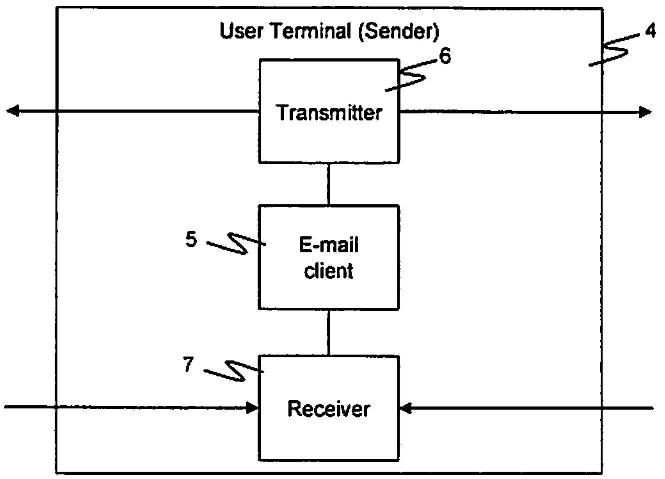

Figure 6

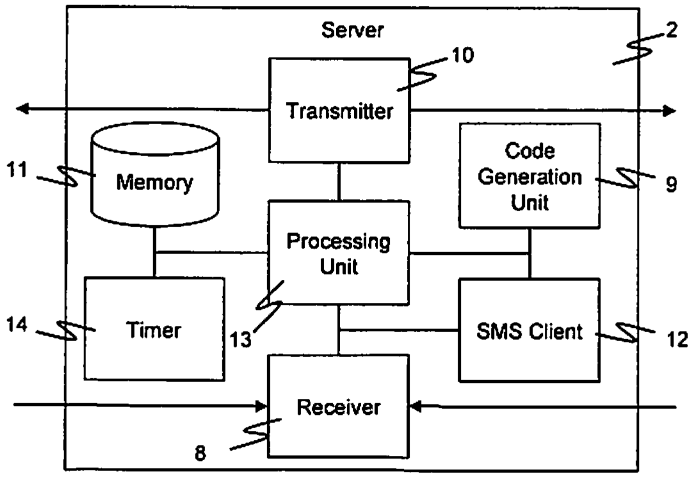

Figure 7

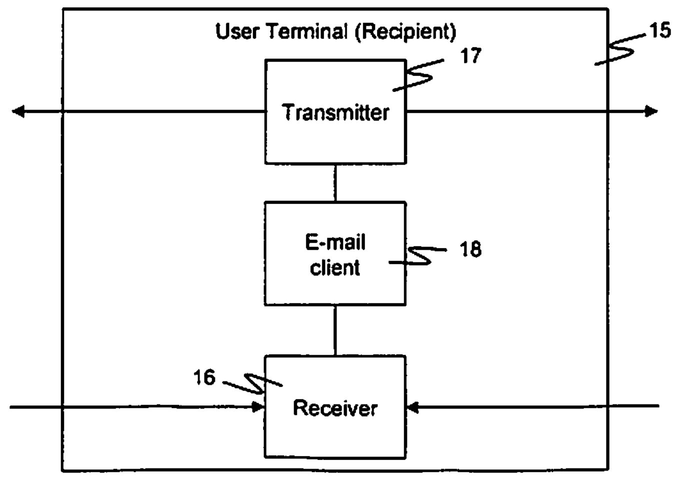

Figure 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2010/050172

A. CLASSIFICATION OF SUBJECT MATTER

IPC: 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: H04L, H04W

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

SE,DK,FI,NO classes as above

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

EPO-INTERNAL, WPI DATA, PAJ, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 20080034212 A1 (ALTIERI), 7 February 2008 (07.02.2008), figures 1-2, abstract --	1-24
A	US 20050039017 A1 (DELANY), 17 February 2005 (17.02.2005), claims 1-13, abstract --	1-24
A	US 20030204726 A1 (KEFFORD ET AL), 30 October 2003 (30.10.2003), figures 4,5A,5B, abstract, paragraphs (0012)-(0018),(0033)-(0036) -- --------	1-24

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

* Special categories of cited documents:

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

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search 15 July 2010	Date of mailing of the international search report 19 -07- 2010
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Frida Holmberg / JA A Telephone No. +46 8 782 25 00

International patent classification (IPC)

H04L 9/32 (2006.01)

Download your patent documents at www.prv.se
The cited patent documents can be downloaded:

- From "Cited documents" found under our online services at www.prv.se (English version)
- From "Anförda dokument" found under "e-tjänster" at www.prv.se (Swedish version)

Use the application number as username. The password is **RTQAIAPVZP.**

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/SE2010/050172

US	20080034212	A1	07/02/2008	NONE
US	20050039017	A1	17/02/2005	NONE
US	20030204726	A1	30/10/2003	NONE