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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 April 2014 (10.04.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/054009 A1

(51) International Patent Classification:
H04L 12/58 (2006.01)

(21) International Application Number:
PCT/IB2013/059072

(22) International Filing Date:
2 October 2013 (02.10.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2012/07351 2 October 2012 (02.10.2012) ZA

(71) Applicant: **ENTERSEKT (PTY) LTD** [ZA/ZA]; Neutron House, 3 Neutron Street, Technopark, 7600 Stellenbosch (ZA).

(72) Inventors: **BRAND, Christiaan Johannes Petrus**; 12 Haakdoring Street, Welgevonden Estate, 7600 Stellenbosch (ZA). **VAN TONDER, Albertus Stefanus**; Eikenbosch 8, Karee Street, 7600 Stellenbosch (ZA). **MARITZ, Gert Stephanus Herman**; 43 Valliant Road, 7130 Somerset West (ZA).

(74) Agents: **VON SEIDELS INTELLECTUAL PROPERTY ATTORNEYS** et al.; PO Box 440, Century City, 7446 Cape Town (ZA).

(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, BN, 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, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, 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, RS, SE, SI, SK, SM,

[Continued on next page]

(54) Title: SECURE EMAIL MESSAGING SYSTEM AND METHOD

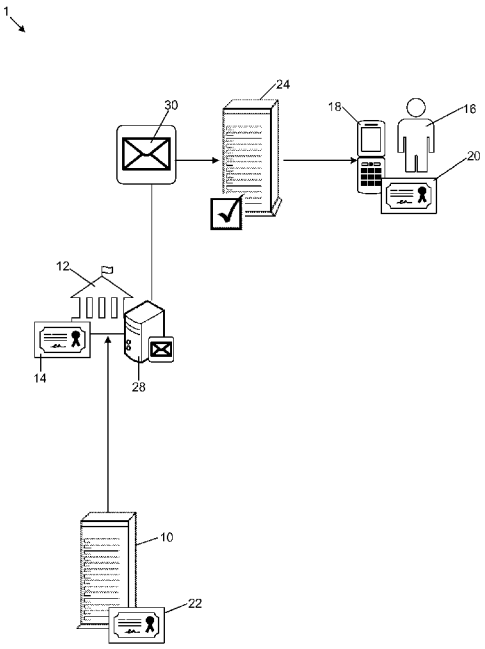

Figure 1

(57) Abstract: The invention provides a system (1) and method of transmitting secure end- to-end encrypted email messages (30) between sending email clients (28) and mobile devices (18) of users (16) of the system. The method includes encrypting the email message (30) with public cryptographic keys associated with mobile devices, signing the encrypted messages (30) with private cryptographic keys associated with sending email clients (28), and transmitting the signed, encrypted email messages (30) to recipient email servers (24) identified from email addresses associated with the users (16), for onward delivery to email accounts operable by the users from the mobile devices (18).

WO 2014/054009 A1

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, 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))*

— *of inventorship (Rule 4.17(iv))*

Published:

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

SECURE EMAIL MESSAGING SYSTEM AND METHOD

FIELD OF THE INVENTION

This invention relates to the transmission of secure messages. More specifically, it relates to the transmission of secure email messages from a sending email server to a mobile device of a user.

BACKGROUND TO THE INVENTION

Email messaging systems are a critical component to most businesses. With the prevalence of email across virtually all industries, email privacy and security has become a significant requirement for most businesses.

Many email users falsely believe that email messages containing potentially sensitive information are secure, while in fact this is not the case. This has led, and still leads to, security breaches resulting in sensitive information becoming known to unintended or unscrupulous third parties. Risks to users of unsecured email communication include, but are not limited to, the leaking of company or client confidential information, the fraudulent modification of email messages, the dissemination of corrupted or virus infected files or documents, the impersonation of email senders, spam, phishing attacks, the dissemination and installation of so-called spyware and the like.

To the applicant's knowledge, a number of email security solutions are commercially available. However, in order to provide a reasonable level of email privacy, all routers in an email pathway, as well as all connections between them, must be secured. One way of improving email security is by means of data encryption. One of the currently used methods of encrypting email is known as Secure/Multipurpose Internet Mail Extensions (S/MIME). S/MIME provides cryptographic security services for electronic messaging applications. The implementation of secure S/MIME systems, like most

commercially available email security solutions, however, require cumbersome and often complicated installation on devices used by both the senders and recipients of the messages.

SUMMARY OF THE INVENTION

In accordance with the invention there is provided a method of transmitting a secure end-to-end encrypted email message between a sending email client and a mobile device of a user, the method including the steps of:

retrieving from a certificate authority, a device certificate including a public cryptographic key uniquely associated with the mobile device of the user, the device certificate having previously been issued to the mobile device by the certificate authority ;

encrypting the email message using the public cryptographic key;

signing the encrypted email message with a private cryptographic key uniquely associated with the sending email client, the private cryptographic key being associated with a sending email client certificate having previously been issued to the sending email client by the certificate authority; and

transmitting the signed, encrypted email message to a recipient email server identified from an email address associated with the user, for onward delivery to an email account operable from the mobile device.

Further features of the invention provide for the step of transmitting the email message to include determining the email address from a user identifier uniquely associated with an account held by the user with a service enterprise utilising the sending email client; for the step of determining the email address from the user identifier to be conducted by the service enterprise utilizing a service enterprise database in doing so; and for the method to include the step of routing the signed, encrypted email message via an intermediary server en route to the recipient email server.

The invention further provides a system for transmitting a secure end-to-end encrypted email message between a sending email client and a mobile device of a user of the system, the system comprising:

a certificate authority operable to issue a digital certificate to the sending email client and the mobile device; and

at least one recipient email server operable to receive the email message over a communications network and deliver it to an email account of the user;

wherein the sending email client is associated with at least one service enterprise, and the sending email client is operable to:

retrieve a device certificate including a device public cryptographic key associated with the mobile device from the certificate authority, the device certificate having previously been issued to the mobile device by the certificate authority;

encrypt the message using the device public cryptographic key;

sign the encrypted message with a private key uniquely associated with the sending email client, the private key being further associated with an email client certificate previously issued to the sending email client by the certificate authority; and

transmit the signed, encrypted message over the communications network to the recipient email server for onward delivery to the email account of the user which, in turn, is operable by the user from the mobile device.

Further features of the invention provide for the sending email client to be operable to transmit the signed, encrypted message to an email address of the email account of the user, and to determine the email address from a user identifier uniquely associated with an account held by the user with the service enterprise utilising the sending email client; and for the sending email client to be further operable to determine the email address of the email account of the user by looking up the user identifier in a secure service enterprise database of the service enterprise containing user information.

Still further features of the invention provide for the sending email client to be operable to route the message via an intermediary server en route to the recipient email server; for one or both of the recipient email server and the intermediary server to be configured to verify a signature of the sending email client, applied to the encrypted email message during signing thereof by the sending email client, using a sending email client public key associated with the sending email client private key; for the recipient email server to be configured to remove the signature of the sending email client; and for one or both of the recipient email server and the intermediary server to be configured to check the sending email client against a list of authorised sending email clients registered for use of the system, and upon locating the sending email client in the list of authorised sending email clients, relay the email message to the email account of the user.

A yet further feature of the invention provides for the recipient email server to be a recipient email client resident on the mobile device.

Further features of the invention provide for the intermediary server to be associated with an authentication service provider tasked with authenticating transactions conducted between the mobile device and the service enterprise; for the authentication server to be adapted to operate as an email server and substitution for the recipient email server; and for the user to be registered for use of the system with the service enterprise and the user identifier to be issued to the user at the time of registration of the user and stored in an account held by the user with the service enterprise.

Still further features of the invention provide for the mobile device of the user to have installed thereon a software application associated with the service enterprise; for the device certificate to be issued to the mobile device as part of the installation of the software application on the mobile device; and for the device certificate to have associated therewith a device private cryptographic

key uniquely associated with the public cryptographic key, the device private cryptographic key being used by the mobile device to decrypt the encrypted message received from the sending email client.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will now be described, by way of example only with reference to the accompanying representations in which:

Figure 1 is a schematic illustration of a secure email messaging system in accordance with the invention; and

Figure 2 is a schematic illustration of an alternative embodiment of a secure email messaging system in accordance with the invention.

DETAILED DESCRIPTION WITH REFERENCE TO THE DRAWINGS

Figure 1 shows a system (1) for transmitting an end-to-end encrypted email message (30) from a sending email client (28) to a mobile device (18) of a user (16). The sending email client (28) is associated with a service enterprise (12), in the current example a bank, and is used by the bank (12) for managing at least outgoing email communication. It should immediately be apparent that the sending email client (28) may be a physical email server forming part of the bank's architecture or may be an independent email server providing email services to the bank (12), or simply an instance of a software application tasked at least with managing email communications out of the bank, forming part of the larger system architecture of the bank. Even though the example that follows deals mainly with email communication out of the bank it should be appreciated that it may also include email communication coming into the bank.

The system further includes a certificate authority (10), which is tasked with issuing digital certificates (14, 20) to both service enterprises (12) as well as mobile devices (18). As is commonplace in the art, each digital certificate issued by the certificate authority (10) has associated therewith a cryptographic key pair including a private cryptographic key, which is only known to the entity to which the certificate was issued, as well as a public cryptographic key which is incorporated into the digital certificate by the certificate authority at the time of issuing. The certificate authority (10) likewise has its own private cryptographic key (22) which it uses to sign each digital certificate issued by it and a corresponding public cryptographic key which interested parties can use to verify the authenticity of the certificates issued by the certificate authority (10).

The system further includes a recipient email server (24) responsible for delivering email messages to the user's email account. It should be appreciated that the email account is operable by the user (16) from his or her mobile phone (18). In the example of the invention described here, messages sent by the sending email client (28) to the user (16) are therefore sent to the recipient email server (24) prior to being delivered to the intended user (16) on his or her mobile phone (18). The recipient email server (24) may, however, also be a recipient email client resident and operating on the mobile device itself, in which case the email message from the sending email client (28) will be sent directly to the device itself.

Before first use of the system, both the bank (12) and the user's mobile device (18) have to be provided with digital certificates (14, 20) by the certificate authority (10). On the mobile device side this is accomplished by the user (16) registering his or her mobile device for use with the bank (12). To do so, the user installs a software application on the mobile device (18) and provides suitable registration information for inclusion in an account held by the user (16) with the bank (12). The information may be entered by the user or may be gathered from the mobile device (18) by the application itself.

In the process, the user is also assigned a user identifier by which it is capable of being identified by the bank (12). As part of the registration process, the certificate authority (10) issues a digital device certificate to the mobile device. This device certificate (20) includes a device public key which is associated with a device private key which, in turn, is securely communicated to and stored on the device (18). The certificate authority (10) also stores a copy of the device certificate (20) in its own database for future reference. Likewise, the bank (12) or sending email client (28), as the case may be, is also issued with an email client certificate (14) containing an email client public key associated with an email client private key known only to the sending email client (28). It should be noted that the events associated with the issuing of the sending email client and mobile device digital certificates do not have to be linked in any way, and may happen independently. What is important for the system to function is that both the sending email client and the user's mobile device must have had digital certificates previously issued to them.

In the present embodiment of the invention, the recipient email server (24) also stores a list of registered sending email clients, preferably including copies of their digital certificates as issued by the certificate authority (10).

In use, if the service enterprise (12) wishes to send a secure email message to the user's mobile device (18), the sending email client (12) requests and receives from the certificate authority (10) a copy of the device certificate (20) of the user's mobile device (18), the certificate being identified by means of the user's user identifier. From the device certificate (20), the public cryptographic key (20) associated with the user's device (18) can be obtained. The sending email client (28) then encrypts the email message (30) with the user's device public cryptographic key and signs the encrypted message (30) using its own unique private cryptographic key (14). The signed, encrypted email message is then sent to an email address of the

user (16) identified by means of the user's unique user identifier, and which directs it to the recipient email server (24).

Upon receipt of the signed, encrypted message by the recipient email server (24), the recipient email server (24) verifies the signature of the sending email client (28) using the sending email client's public cryptographic key, which is available from its certificate (14). It also checks the sender against the list of registered sending email clients and if the sending email client can be verified and is one of the registered senders, the encrypted message (30) is relayed to the user's mobile device (18). It should be noted that a sending email client appearing as a registered user at the recipient email server may automatically be regarded as a safe sender. If, however, a sending email client is not found in the list of registered sending email clients, the email message may be discarded by the recipient email server.

At the time of verifying the signature of the sending email client (28) it should be appreciated that the email client signature may be removed by the recipient email server if the signature can be positively verified. Even after removal of the signature, the email message will still be encrypted with the mobile device public key (20) that the sending email client (28) received from the certificate authority (10).

Once received at the mobile phone (18) the mobile phone has the unique capability of fully decrypting the message (30) by using the private cryptographic key (20) associated with its certificate (20). The message will then be readable by the user on his or her mobile phone. It should, however, also be apparent that the sending email client signature could likewise be removed at the mobile phone (18) if it is in possession of the sending email client's public cryptographic key. However, by removing the signature at the recipient email server it alleviates the computational load on the mobile device.

It is envisaged that the system may be operable to enable the user (16) to reply to the email message from his or her mobile device. The reply process may entail that the message travels in the exact reverse order as described above. The reply message will accordingly be encrypted on the user's mobile phone (18) using the public cryptographic key of the email client (28) and then sent to the email server (24) for onward transmission to the email client (28). The user's mobile phone (18) also signs the encrypted message with its private key, and forwards the signed, encrypted message to the email client (28) of the service enterprise (12) via the email server (24). Upon receipt of the signed, encrypted message, the email client (28) requests a copy of the device certificate (20) of the user's device (18) from the certificate authority (10), from which the public key of the device certificate (20) may be obtained and used to verify the device signature, after which the message may be decrypted using the email client's private cryptographic key.

It should be appreciated that numerous changes and modifications may be made to the example of the invention described above, without departing from the scope of the invention. It is, for example, envisaged that the system may employ an intermediary server positioned between the sending email client and the recipient email server. This intermediary server may, for example, be associated with an authentication service provider tasked with authenticating transactions conducted between the user and the service enterprise. In such an implementation the primary function of the software installed on the user's mobile device may be to facilitate the authentication process of the transactions conducted between the user and the service enterprise. For this purpose both the user's mobile device and the service enterprise may also have had digital certificates previously issued to them by the certificate authority for use in the transaction authentication process. An authentication server associated with the authentication service provider may also have means for communicating securely with the mobile device of the user, which would further improve security of the system, and which could conveniently be adapted to allow for the additional email handling capability

of the current invention. The authentication server could also have existing databases of authorised service enterprises, their sending email clients, as well as users, and their mobile device, registered for the transaction authentication service, and may accordingly be well suited for implementing the secure end-to-end encrypted emailing functionality of the present invention. It should be noted that the mobile devices of users registered with the authentication server may be uniquely and unambiguously identifiable by the authentication server by means of a digital fingerprint representing a one-to-one relationship with the user's mobile device.

It is furthermore envisaged that the authentication server may be adapted to also operate as an email server, in which case the user may have a dedicated email account associated with the authentication server, and by means of which email messages may be sent directly between the sending email client at the service enterprise and the user's mobile device, thus alleviating the need for a separate recipient email server to be part of the system. A user may, for example, be identified by means of the user identifier issued to him or her at the time of registering for the service and his or her email address may accordingly, and by way of example, be in a format user_identifier@authentication_server.extension. It is, for example, foreseen that a user's unique user identifier may be his or her cellphone number, which would imply that the email address to which email messages may be sent could be in the format cellphone_number@authentication_server.extension. In this way the user will not need to have a separate email account with a separate email host. It should, however, be clear that unless an email client is operational on each mobile device used in the system, that a recipient email server of some sort will be required as part of the system to handle onward forwarding of email messages to the client mobile device.

An alternative embodiment of a system (2) in accordance with the invention is shown in Figure 2. In the figure, like components to those used with

reference to Figure 1 are indicated with like reference numerals. In this embodiment, a plurality of service enterprises (12) are registered for use of the system (2). Each service enterprise (12) has its own sending email client (28) which in turn has its own sending email client digital certificate (14), issued to it by the certificate authority (10). As described in the previous paragraph, the service enterprises utilise an authentication service provider (34) to authenticate transactions conducted with their users (16). The authentication service provider in this embodiment has an email server (36) associated with it which is configured to communicate email messages between the sending email clients (28) and the mobile devices (18) of registered users (16).

As the users of the various service enterprises (12) will already have been registered for transaction authentication services, the service enterprises (12) will already have records containing user identifiers of each of its registered users in a database. The user identifiers may therefore be used by the sending email clients (28) to transmit end-to-end encrypted email messages to a mobile device (18) of a registered user (16) via the email server (34). As before, each registered mobile device (18) of each user (16) of a service enterprise (12) will also have had a device certificate issued to it by the central certificate authority (10). The sending email client (28) concerned, will therefore be able to retrieve a copy of the certificate (20), and accordingly the public cryptographic key (20), of the mobile device (18) of the user (16) to which it wishes to send and end-to-end encrypted email message from the certificate authority (10) and encrypt the message as explained before with reference to Figure 1.

It should be appreciated that if the service enterprises (12) are already registered for a transaction authentication service with the authentication service provider, rolling out of the system described with reference to Figure 2 may be very easily achieved.

The embodiment of the invention described with reference to Figure 2 therefore allows a user to communicate with a number of different service enterprises by means of secured emails to and from his or her mobile device, provided that each of these service enterprises (12), as well as the user's mobile device, have a valid digital certificate issued by a mutually trusted certificate authority (10). Even though Figure 2 shows the various sending email clients (28) to be communicating with the mobile device (18) by means of a single email server (36), it is envisaged that any number of different email servers may be available to a sending email client (28) for communication with the user's device, provided that the user has an email account registered with the applicable email server and that the mail account is operable from the user's mobile phone. A user may therefore also have a number of different email accounts, registered with different email servers, through which different service enterprises may contact him or her by means of secure email. These mail accounts may, for example, be registered with service providers with domain names such as Gmail, Yahoo, Hotmail or other, private email hosts. It should be noted that the same public encryption key associated with the user's device could be used by any sending email client (12) to encrypt email messages (30) via any number of email servers according to the invention.

It will be appreciated that the system described with reference to Figures 1 and 2 allows service enterprises, typically financial institution but not limited as such, to transmit secure, end-to-end encrypted email messages to mobile devices of their users while making only minor changes to their existing infrastructure and without requiring users to install additional software or make additional changes to their mobile devices or separately registering for use of the system with the financial institution themselves. This becomes possible because both the sending email clients of the applicable service enterprises and the mobile phones of the their users already have digital certificates including private and public cryptographic keys issued to them by an independent, mutually trusted certificate authority.

The functionality of the system will typically be incorporated and installed into an S/MIME system operational on a sending email client's mailing system. This allows the encryption and decryption of messages to take place with the minimum amount of a modification.

The invention thus provides a secure way of transmitting a message between a service enterprise and a user's mobile phone without the possibility of an external party accessing the message. The invention does not require users to register for the use of a system, since they already possess the necessary information, including the private cryptographic key, on their mobile phones, which allows them to receive the securely encrypted messages. The implementation of the invention is greatly facilitated and advantageous in an environment where the sending email clients of the various service enterprises, certificate authority or multiple certificate authorities, as the case may be, and mobile devices are all already part of the same certificate authority domain and associated public-key infrastructure ("PKI"). The implementation of the invention is further facilitated by the service enterprises having knowledge of accounts held by users with them, and them being able to easily make a connection between a given user certificate and the user's account and other details contained in the account such as, for example, the user's email address.

In another embodiment of the invention, a user may have an email client application installed on his or her mobile phone which effectively alleviates the need for a separate recipient email server in the system. An encrypted email message may accordingly be sent by a sending email client directly to the application on the user's mobile phone, typically over a communications channel such as the Internet. The mobile phone application may in turn be configured to directly contact the certificate authority, allowing it to obtain the certificates and public cryptographic keys which enable it to verify the signatures of the various sending email clients. Should a trusted sending

email client be identified, the signature of the sending email client may be verified initially, and the message afterwards decrypted with the private encryption key present on the user's mobile phone as described previously. The application on the mobile phone may also handle the discarding of messages from sending email clients, the signatures of which cannot be verified.

The foregoing description of the embodiments of the invention has been presented for the purpose of illustration; it is not intended to be exhaustive or to limit the invention to the precise forms disclosed. Persons skilled in the relevant art can appreciate that many modifications and variations are possible in light of the above disclosure.

Some portions of this description describe the embodiments of the invention in terms of algorithms and symbolic representations of operations on information. These algorithmic descriptions and representations are commonly used by those skilled in the data processing arts to convey the substance of their work effectively to others skilled in the art. These operations, while described functionally, computationally, or logically, are understood to be implemented by computer programs or equivalent electrical circuits, microcode, or the like. Furthermore, it has also proven convenient at times, to refer to these arrangements of operations as modules, without loss of generality. The described operations and their associated modules may be embodied in software, firmware, hardware, or any combinations thereof.

Any of the steps, operations, or processes described herein may be performed or implemented with one or more hardware or software modules, alone or in combination with other devices. In one embodiment, a software module is implemented with a computer program product comprising a computer-readable medium containing computer program code, which can be executed by a computer processor for performing any or all of the steps, operations, or processes described.

Finally, the language used in the specification has been principally selected for readability and instructional purposes, and it may not have been selected to delineate or circumscribe the inventive subject matter. It is therefore intended that the scope of the invention be limited not by this detailed description, but rather by any claims that issue on an application based hereon.

CLAIMS:

1. A method of transmitting a secure end-to-end encrypted email message (30) between a sending email client (28) and a mobile device (18) of a user (16), the method including the steps of:

retrieving from a certificate authority (10), a device certificate (20) including a public cryptographic key uniquely associated with the mobile device (18) of the user (16), the device certificate (20) having previously been issued to the mobile device (18) by the certificate authority (10);

encrypting the email message (30) using the public cryptographic key;

signing the encrypted email message (30) with a private cryptographic key uniquely associated with the sending email client (28), the private cryptographic key being associated with a sending email client certificate (14) having previously been issued to the sending email client (28) by the certificate authority (10); and

transmitting the signed, encrypted email message (30) to a recipient email server (24) identified from an email address associated with the user (16), for onward delivery to an email account operable from the mobile device (18).

2. A method as claimed in claim 1 wherein the step of transmitting the email message (30) includes the step of determining the email address from a user identifier uniquely associated with an account held by the user (16) with a service enterprise (12) utilising the sending email client (28).

3. A method as claimed in claim 2 wherein determining the email address from the user identifier is conducted by the service enterprise (12), the service enterprise (12) utilizing a service enterprise database in doing so.

4. A method as claimed in any one of claims 1, 2 or 3 which includes the step of routing the signed, encrypted email message (30) via an intermediary server en route to the recipient email server (24).

5. A system (1) for transmitting a secure end-to-end encrypted email message (30) between a sending email client (28) and a mobile device (18) of a user (16) of the system (1), the system comprising:

a certificate authority (10) operable to issue a digital certificate to the sending email client (28) and the mobile device (18); and

at least one recipient email server (24) operable to receive the email message (30) over a communications network and deliver it to an email account of the user (16);

wherein the sending email client (28) is associated with at least one service enterprise (12), and the sending email client (28) is operable to:

retrieve a device certificate (20) including a device public cryptographic key associated with the mobile device (18) from the certificate authority (10), the device certificate (20) having previously been issued to the mobile device (18) by the certificate authority (10);

encrypt the message (30) using the device public cryptographic key;

sign the encrypted message (30) with a private key uniquely associated with the sending email client (28), the private key being further associated with an email client certificate (14) previously issued to the sending email client (28) by the certificate authority (10); and

transmit the signed, encrypted message (30) over the communications network to the recipient email server (24) for onward delivery to the email account of the user (16) which, in

turn, is operable by the user (16) from the mobile device (18).

6. A system as claimed in claim 5, wherein the sending email client (28) is operable to transmit the signed, encrypted message to an email address of the email account of the user (16), and to determine the email address from a user identifier uniquely associated with an account held by the user (16) with the service enterprise (12) utilising the sending email client (28).

7. A system as claimed in claim 6, wherein the sending email client (28) is further operable to determine the email address of the email account of the user (16) by looking up the user identifier in a secure service enterprise database of the service enterprise (12) containing user information.

8. A system as claimed in any one of claims 5, 6 or 7, wherein the sending email client (28) is operable to route the message (30) via an intermediary server en route to the recipient email server (24).

9. A system as claimed in claim 8, wherein one or both of the recipient email server (24) and the intermediary server is configured to verify a signature of the sending email client (28), applied to the encrypted email message (30) during signing thereof by the sending email client (28), using a sending email client public key associated with the sending email client private key.

10. A system as claimed in claim 9, wherein the recipient email server (24) is configured to remove the signature of the sending email client (28).

11. A system as claimed in claim 9 or claim 10, wherein one or both of the recipient email server (24) and the intermediary server is configured to check the sending email client (28) against a list of authorised sending

email clients registered for use of the system, and upon locating the sending email client (28) in the list of authorised sending email clients, relay the email message (30) to the email account of the user (16).

12. A system as claimed in any one of claims 5 to11, wherein the recipient email server (24) is a recipient email client resident on the mobile device (18).

13. A system as claimed in any one of claims 8 to 12, wherein the intermediary server is associated with an authentication service provider tasked with authenticating transactions conducted between the mobile device (18) and the service enterprise (12).

14. A system as claimed in claim 13, wherein the authentication server is adapted to operate as an email server and substitution for the recipient email server (24).

15. A system as claimed in any one of claims 6 to 14, wherein the user (16) is registered for use of the system with the service enterprise (12) and the user identifier is issued to the user (16) at the time of registration of the user (16) and stored in an account held by the user with the service enterprise (12).

16. A system as claimed in any one of claims 5 to 15, wherein the mobile device (18) of the user (16) has installed thereon a software application associated with the service enterprise (12).

17. A system as claimed in claim 16, wherein the device certificate (20) is issued to the mobile device (18) as part of the installation of the software application on the mobile device (18).

18. A system as claimed in any one of claims 5 to 17, wherein the device certificate (20) has associated therewith a device private cryptographic key uniquely associated with the public cryptographic key, the device private cryptographic key being used by the mobile device (18) to decrypt the encrypted message (30) received from the sending email client (28).

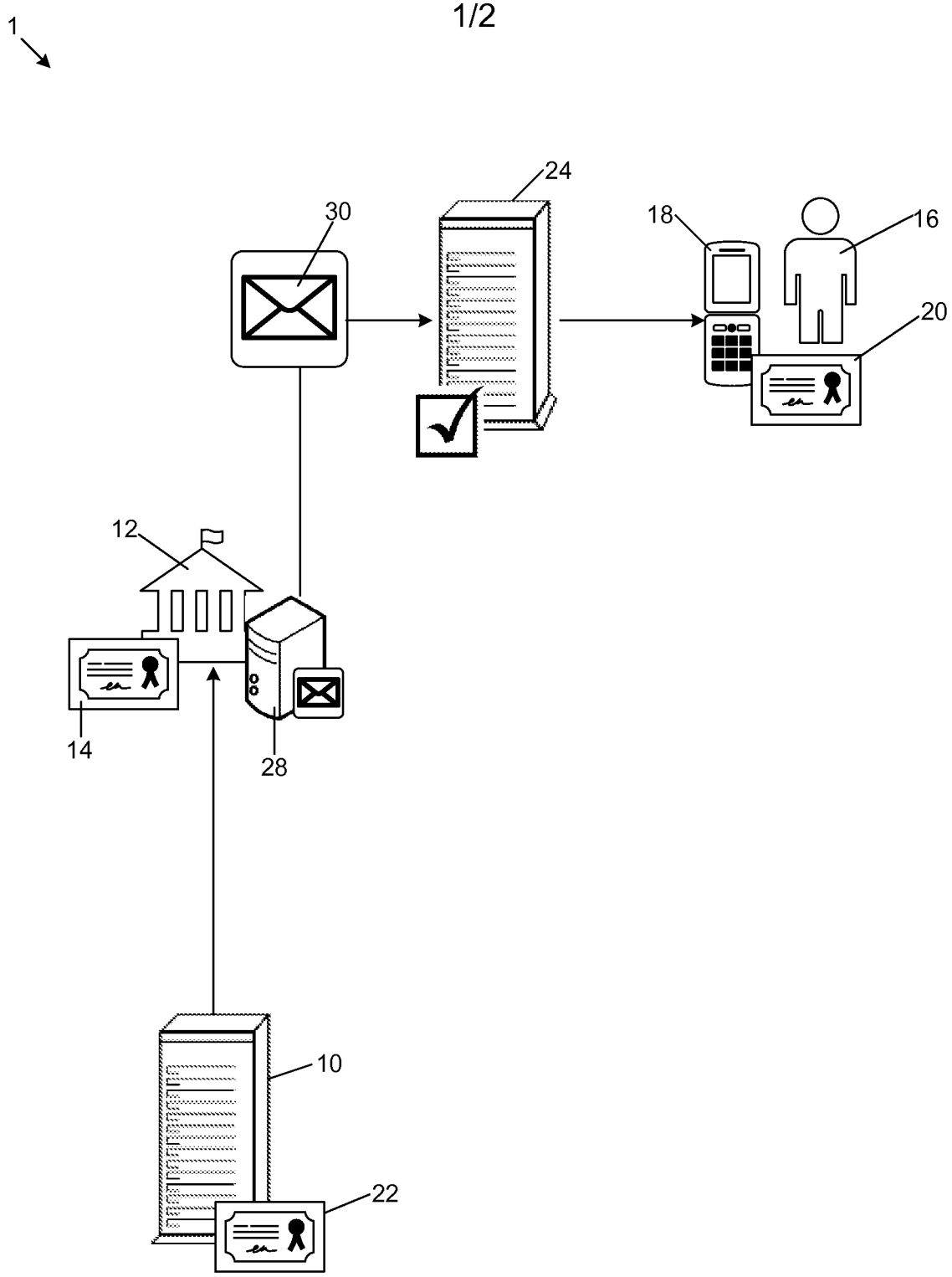

Figure 1

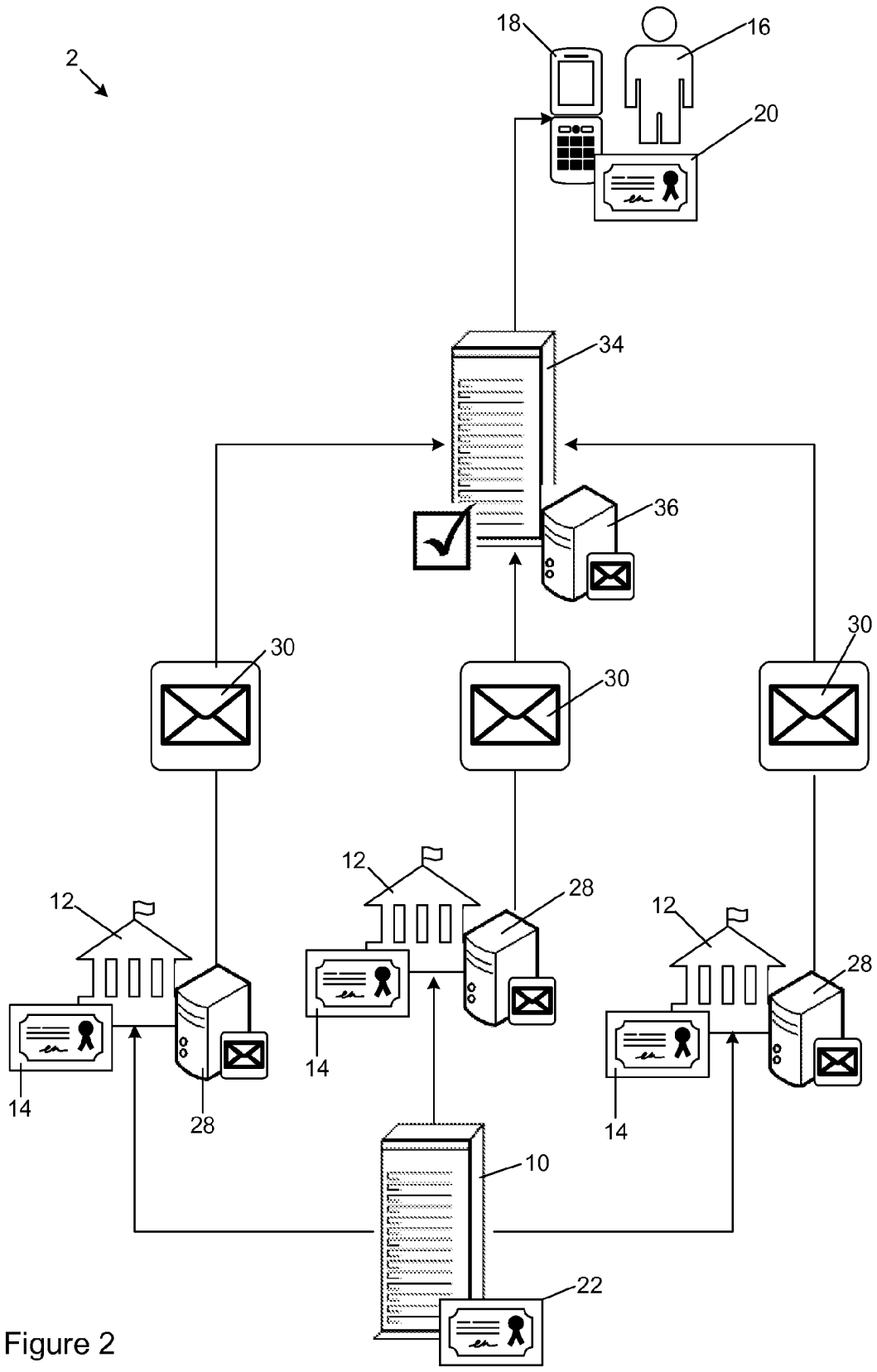

Figure 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2013/059072

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L12/58
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 practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2012/101951 A1 (LI MICHAEL [US] ET AL) 26 April 2012 (2012-04-26) abstract paragraph [0001] - paragraph [0016] paragraph [0022] - paragraph [0027] claim 1 figures 1b,1c,2,5,7	1-18
X	US 6 760 752 B1 (LIU GARY G [US] ET AL) 6 July 2004 (2004-07-06) abstract column 1, line 30 - column 2, line 30 claims 1,2 figure 2a	1-18

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 December 2013	20/12/2013

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Poggio, Francesca

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2013/059072

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 00/46952 A1 (FUNDSXPRESS INC [US]) 10 August 2000 (2000-08-10) abstract page 2, line 1 - line 13 claim 1 figure 1 -----	1-18

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2013/059072

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2012101951 A1	26-04-2012	NONE	
US 6760752 B1	06-07-2004	US 6760752 B1	06-07-2004
		US 2004249817 A1	09-12-2004
WO 0046952 A1	10-08-2000	AU 2755400 A	25-08-2000
		WO 0046952 A1	10-08-2000