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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 January 2017 (12.01.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/004711 A1

(51) International Patent Classification:
H04L 9/06 (2006.01) *H04L 9/32* (2006.01)
H04L 9/08 (2006.01)

(21) International Application Number:
PCT/CA2016/050783

(22) International Filing Date:
5 July 2016 (05.07.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/188,951 6 July 2015 (06.07.2015) US

(71) Applicant: **CRYPTOMILL INC.** [BB/BB]; First Floor, Mall Internationale Office, Haggatt Hall 11063 (BB).

(72) Inventors; and
(71) Applicants *(for US only)*: **JOLLY, Nandini** [CA/CA]; c/o CryptoMill Technologies Ltd., 372 Bay Street, Suite 2000, Toronto, Ontario M5H 2W9 (CA). **BATTY, Chris** [CA/CA]; c/o CryptoMill Technologies Ltd., 372 Bay Street, Suite 2000, Toronto, Ontario M5H 2W9 (CA). **SERRAO, Canute** [CA/CA]; c/o CryptoMill Technologies Ltd., 372 Bay Street, Suite 2000, Toronto, Ontario M5H 2W9 (CA). **FILJI, Deepu** [CA/CA]; c/o CryptoMill Technologies Ltd., 372 Bay Street, Suite 2000, Toronto, Ontario M5H 2W9 (CA). **DAI, David** [CA/CA]; c/o CryptoMill Technologies Ltd., 372 Bay Street, Suite 2000, Toronto, Ontario M5H 2W9 (CA).

(74) Agents: **NAUMAN, David** et al.; Borden Ladner Gervais LLP, World Exchange Plaza, 100 Queen Street, Suite 1100, Ottawa, Ontario K1P 1J9 (CA).

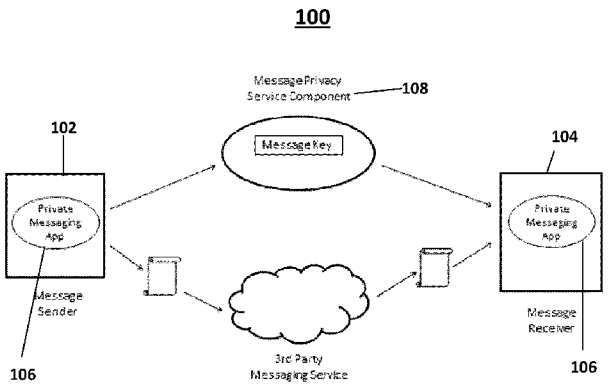
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, 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, ST, 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, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

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

(54) **Title**: SYSTEM AND METHOD FOR PROVIDING PRIVACY CONTROL TO MESSAGE BASED COMMUNICATIONS

FIG. 1 Top-Level Context



(57) **Abstract**: A system and method for controlling access to a message after communication. A sender sends an encrypted message to a recipient. The sender also sends an encryption key and the identity of the recipient to a services component. The recipient authenticates its access rights with the services component to obtain the encryption key. The key is held for a period of time for the recipient to access the encrypted message. The recipient may re- authenticate with the services component to again obtain the key to subsequently access the message. The sender may revoke or reinstate the receiver's access to the message by updating the service component.

WO 2017/004711 A1

SYSTEM AND METHOD FOR PROVIDING PRIVACY CONTROL TO MESSAGE BASED COMMUNICATIONS

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of priority of U.S. Provisional Patent Application No. 62/188,951 filed July 6, 2015, which is hereby incorporated by reference in its entirety.

FIELD

[0002] The embodiments disclosed herein relate generally to the field of data security and information privacy, and more specifically to a method of securely sending data communications (for example, email messages) such that only the designated recipient is able to read the message, but is not permitted to share the communication with others.

BACKGROUND

[0003] Across various industries, data security is an ever increasing concern. The protection of information is an important concern for corporations, individuals, and other legal entities. Corporations, for example, generally deal with vast amounts of sensitive information whether it be customer lists, personal information of clients, trade-secrets or other sensitive information. It is important to keep such information safe and secure. It is also desirable to share such information between authorized persons but still maintain some control over the information once it has been shared. It is, therefore, desirable to provide a method and system for providing such control to message based communications.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] Embodiments of the present disclosure will now be described, by way of example only, with reference to the attached figures.

[0005] Figure 1 is a schematic diagram illustrating the top-level Context Model of an example embodiment.

[0006] Figure 2 is a flow chart illustrating a method of composing a message, according to an embodiment.

[0007] Figure 3 is a flowchart diagram illustrating a method of receiving a message, according to an embodiment.

[0008] Figure 4 is a flowchart diagram illustrating a method of checking a read status, according to an embodiment.

[0009] Figure 5 is a flow chart diagram illustrating the process of recalling a message, according to an embodiment.

[0010] Figure 6 is a flowchart diagram illustrating the process of recalling a message, according to an embodiment.

[0011] Figure 7 is a schematic diagram illustrating a Protected Message Data Format according to an embodiment.

[0012] Other aspects and features of the present disclosure will become apparent to those ordinarily skilled in the art upon review of the following description of specific embodiments in conjunction with the accompanying figures.

DETAILED DESCRIPTION

[0013] Various embodiments described herein provide the ability for individuals to send messages to specified recipients, ensuring that the message content is private, cannot be forwarded onto others, and optionally expiring after viewing has occurred. Some of the embodiments disclosed herein can allow a user to be able to confidently communicate potentially sensitive messages, without worrying about the content getting into the hands of anyone but the intended recipient. Various of the embodiments disclosed herein are useful to individuals either working on their own, or in small-to-large organizations, in any field of endeavor.

[0014] Some embodiments disclosed herein provide controls over the data communication after it has been received by the recipient. Embodiments of the disclosed system and method prevent the message from being forwarded to others. In various embodiments, where possible on specific platforms, actions which make a copy of message content (e.g. select text and copy to a clipboard, screen shot capture) are disabled. Similarly, side-effects of message transmission which may copy message content (e.g. caching of files attached to an email) are mitigated by bringing all attached data in-line, into the message itself.

[0015] In addition, in some embodiments, the sender has the option of specifying whether or not that the message will self-destruct such that it is automatically removed from memory a period of time after the recipient has reviewed or accessed the message. Various of the embodiments disclosed herein provides the ability to audit whether or not the recipient

has read a sent message, as well as providing the ability to recall the message, effectively withdrawing the recipient's ability to view the message.

[0016] Reference is made to Figure 1, where the top-level Context Model 100 of an example embodiment of the present invention is shown. The various elements of this context are described below.

[0017] Two computing devices 102, 104 are shown, each containing an instance of the private messaging application software 106. The term "computing devices" as used herein can include, but is not limited to, a desktop computer, a laptop, a notebook computer, a tablet, a smart phone, phablet or any other suitable computing or mobile communications device. Accordingly, various of the embodiments disclosed herein can be used with a variety of different types of computing devices while some embodiments are specific to a given type of computing device. One of the computing devices represents the message sender role 102, the other computing device represents the message receiver role 104. When sending a message, the private messaging application 106 encrypts the message contents, sends the encryption key to the messaging privacy service component, and then sends the encrypted message to the recipient. The recipient, upon receiving the encrypted message, contacts the messaging privacy service component 108 to obtain the encryption key for the service. In various embodiments, the message privacy service component 108 comprises a computing device, such as for example, a server. The various computing devices can communicate through one or more networks, including, for example but not limited to, the internet, wireless networks, and cellular networks.

[0018] The following paragraphs example use cases where users interact with various of the embodiments disclosed herein. These serve to illustrate typical uses and the utility provided by some of the embodiments.

[0019] Setting up the Application

[0020] In an example embodiment, in order to use the disclosed features, the user downloads an application, such as a mobile application, for their computing device. Once the application is downloaded, it will ask the user to provide credentials for their email account. In some embodiments, the user's email account credentials are stored on their device, and are used to send protected private emails through that email account. As a security and user-acceptance feature, in some embodiments, the user's email account credentials are never sent to the service component.

[0021] Once the user has provided their email account credentials, they proceed to set up an account on the service component. In some embodiments, the user provides a separate, new account password for the service. In various embodiments, the service account password is hashed and salted before being stored in the service components data store.

[0022] Using the Application to Compose and Send

[0023] Using the application, the user can now compose a message (e.g. email) and send it. By clicking the "Send" button, the application creates a new unique encryption key and encrypts the message with it. The message can have attachments such as image files or other files. The encryption key and the target recipient list is then sent to the message privacy service component 108. In various embodiments, only the recipients of the email, and the user, can request the key from the message privacy service component 108. In some embodiments, for security and privacy reasons, at no point are the message contents sent to the message privacy service component – not even in encrypted form. The user's (encrypted) message is then sent via the regular messaging account to its recipients.

[0024] Reference is made to Figure 2, which is a flowchart 200 illustrating a method of composing a message, according to an embodiment. The method may be carried out by software executed, for example, by a physical processor of the sender's computing device 102. Coding of software for carrying out such a method is within the scope of a person of ordinary skill in the art given the present description. The method may contain additional or fewer processes than shown and/or described, and may be performed in a different order. Computer-readable code executable by at least one processor of the system to perform the method may be stored in a computer-readable storage medium device or apparatus, which may be a non-transitory or tangible storage medium.

[0025] In an embodiment, the user composes a message 202 in the private messaging application, specifying the desired recipients. In some embodiments, upon selecting the Send action, the application generates a 256-bit random number 206 to be used as an AES 256-bit key, K1. In other embodiments, a different sized random number and key are used. The message body is encrypted 208 using the AES key K1. The application then transmits the AES Key K1 and the recipient list 210 to the message privacy service component 108. The message privacy service component 108 assigns a unique ID to the message, and records the message ID, key K1 and recipient list in its database 212. The message ID is returned 214 to the private messaging application 108. Upon successful

feedback from the message privacy service component 108, the private messaging application proceeds to encrypt 216 the message, and then passes that message on to User's messaging service provider 218. The messaging service provider distributes the message as it normally does.

[0026] Using the Application to View Messages

[0027] In some embodiments, a recipient who receives an encrypted message protected by the present invention will also receive instructions describing how to download and install the corresponding mobile application. If the user has already installed the application, they can use the application to open the message to read it. At this point, their application contacts the message privacy service component 108 and requests the cryptographic key corresponding to that particular message. Upon receiving such a request, the message privacy service component 108 poses an authentication challenge to the requesting user, verifying their service account password. After successfully authenticating, the service component 108 furnishes the cryptographic key for the message. Their application holds the message key temporarily, while using it to decrypt the message.

[0028] For messages marked for expiry, the application displays the message to the recipient for the time period, which in some embodiments can be set by the sender. In some embodiments, the sender can specify a specific expiry time for the message. In some embodiments, the user can specify that the message can be only be viewed for a maximum length of time by the receiver. For example, in an embodiment the message can be viewed for a maximum 20 seconds. In various embodiments, the user can select the amount of time. In some embodiments, the system may suggest a length of time to the sender given the length of the message. In some embodiments, the message can be viewed only once and only for the maximum time period. Accordingly, in such embodiments, if the viewer opens the message and views it for less than the maximum time period before closing it, they will not be able to view the message again despite the fact that they have not viewed it for the full maximum time period. After the time period has passed, the application closes the message display, and immediately 'forgets' the message key. For example, in some embodiments, the encryption key is stored on a server and when the message expires the key is erased from the server. For messages that have had their viewing time period expire, if the recipient tries to open the message again, the service component will refuse to send them the message key.

[0029] In some embodiments, the recipient receives a notification indicating that they have received an encrypted message. In some embodiments, the notification indicates whether the message is set to expire. The notification may also indicate the length of the time period for which the message may be viewed.

[0030] In some embodiments, a countdown indicator is displayed for messages that are set to expire. In some embodiments, the countdown indicator is a countdown bar that is displayed in relation to the message. The countdown indicator can, for example, display a length of time or the number of times which the message can be viewed. In an embodiment where the countdown indicator displays a length of time, the countdown indicator is displayed and updated while the recipient views the message allowing him/her to see how much longer they can view the message.

[0031] Reference is made to Figure 3, which is a flowchart diagram illustrating a method of receiving a message 300, according to an embodiment. The method 300 may be carried out by software executed, for example, by a physical processor of the receiver's computing devices 104. Coding of software for carrying out such a method is within the scope of a person of ordinary skill in the art given the present description. The method may contain additional or fewer processes than shown and/or described, and may be performed in a different order. Computer-readable code executable by at least one processor of the system to perform the method 300 may be stored in a computer-readable storage medium device or apparatus, which may be a non-transitory or tangible storage medium.

[0032] The receiving user runs the private messaging application to read a protected message that has been received. The encrypted email is scanned to determine its message ID. The private messaging application contacts the message privacy service component 108, supplying the message ID and message privacy service authentication info 302. The message privacy service component authenticates 304 the user and determines if that user account is authorized to read the specified message. Any user account that is in the message's recipient list is so authorized. If authorized, the message Key K1 is retrieved, and passed back to the private messaging application 306. Upon receipt of the message Key K1, the private messaging application decrypts 308 the message, and then displays it to the user on the screen of the computing device 310. If the message metadata indicates that the message has an expiry time, a countdown timer is started 312. Otherwise, the message remains displayed until the user closes the message. After the countdown timer reaches zero, the message is automatically deleted 314.

[0033] Using the Application to Check Read Status

[0034] In some embodiments, the sending user can obtain a listing of messages that they have sent in the past. The application provides this information under a Sent Items' area. In some embodiments, if the user selects a particular message that they have sent previously, they can also check to see which of their recipients have read that message, and if so, when the most recent access occurred.

[0035] Reference is made to Figure 4, which is a flowchart diagram illustrating a method of checking a read status 400, according to an embodiment. The method 400 may be carried out by software executed, for example, by physical processors of the sender's 102 and receiver's 104 computing devices. Coding of software for carrying out such a method is within the scope of a person of ordinary skill in the art given the present description. The method may contain additional or fewer processes than shown and/or described, and may be performed in a different order. Computer-readable code executable by at least one processor of the system to perform the method may be stored in a computer-readable storage medium device or apparatus, which may be a non-transitory or tangible storage medium.

[0036] Navigating through the list of Sent Items 402, a user can select a previously-sent message for checking read status. The message is first opened 404, using a process similar to that used when Receiving a Message. The selected encrypted message is scanned to determine its message ID. The private messaging application contacts the message privacy service component 108, supplying the message ID and message privacy service authentication info 406. The message privacy service component authenticates the user and determines if that user account is authorized to read the specified message 408. In various embodiments, any user account that is in the message's recipient list is so authorized. If authorized, the message Key K1 is retrieved, and passed back to the private messaging application 410. Upon receipt of the message Key K1, the private messaging application decrypts the message 412, and then displays it to the user 414. When reviewing the message, the user has the option to check the read status 416.

[0037] The private messaging application contacts the message privacy service component 108, supplying the message ID and message privacy service authentication info 418. The message privacy service component authenticates the user and then fetches the recipient read status 420 for all users in the messages recipient list. In some embodiments, only the user that sent the message can be authenticated to view the read status of the

message. This read status is passed back 422 to the private messaging application. The private messaging application then displays the read status.

[0038] Using the Application to Recall a Message

[0039] In addition, in some embodiments, the sending user is able to recall the message, making it ineligible for future reading. As a result, any recipient that has not already read the message, will no longer be able to read it. When recalling a message, the message privacy service component erases the key that was used to encrypt the message.

[0040] Reference is made to Figure 5, which is a flow chart diagram illustrating the process of recalling a message 500, according to an embodiment. The method may be carried out by software executed, for example, by physical processors of the sender's 102 and receiver's 104 computing devices. Coding of software for carrying out such a method is within the scope of a person of ordinary skill in the art given the present description. The method may contain additional or fewer processes than shown and/or described, and may be performed in a different order. Computer-readable code executable by at least one processor of the system to perform the method may be stored in a computer-readable storage medium device or apparatus, which may be a non-transitory or tangible storage medium. The message sender has the ability to recall a message. This action renders the message no longer readable.

[0041] Using the Application to Revoke a User

[0042] In some embodiments, the sending user is provided with the option of selectably revoking one or more recipients from the message recipient list. This feature provides the sending user with the option of selecting a particular recipient and making the message ineligible for further reading by that recipient. With this option, other recipients are unaffected by the revoke action. As a result, if the selected recipient hasn't already read the message, they will not be able to read it at all.

[0043] Reference is made to Figure 6, which is a flowchart diagram illustrating the process of recalling a message 600, according to an embodiment. The method may be carried out by software executed, for example, by physical processors of the sender's 102 and receiver's 104 computing devices. Coding of software for carrying out such a method is within the scope of a person of ordinary skill in the art given the present description. The method may contain additional or fewer processes than shown and/or described, and may be performed in a different order. Computer-readable code executable by at least one processor

of the system to perform the method may be stored in a computer-readable storage medium device or apparatus, which may be a non-transitory or tangible storage medium.

[0044] When displaying a message 602, the user may check the read status 604. The request for read status on the specified message ID, along with the user authentication information, is sent 606 to the message privacy service component 108. The service determines if the user is authorized 608 to obtain read status information pertaining to the message, and if so, returns 610 that information. Upon receipt of the read status information, the private messaging application will display the read status 612, with one entry for each recipient. For each recipient shown, the option is made available to revoke 614 that user from the authorized recipient list. If the user chooses this option, a request is made 616, to the message privacy service component 108, to revoke the selected user. This request, along with user authentication information, is sent to the message privacy service component 108 to perform this revoke action 618. Upon successful completion, this action renders the message no longer readable by the specified recipient.

[0045] Protected Message Data Format

[0046] Reference is made to Figure 7, which illustrates the data format of a Protected Message, according to an embodiment.

[0047] In the example embodiment, a protected message 700 is composed of three distinct parts:

[0048] • Message Container 702

[0049] • Data Header 704

[0050] • Data Content (or payload) 706

[0051] The actual placement and ordering of these parts 702, 704, 706, within the overall message data, is not important to the overall functioning of the embodiments disclosed herein.

[0052] In various embodiments, the Message Container 702 is simply the skeleton or envelope that allows the private message to be sent and transported through the usual, regular messaging system. For example, if the messaging system is SMTP Email, the message container is a validly formatted SMTP-compatible email body. The actual encoded message would be contained within this envelope.

[0053] In some embodiments, the Data Header 704 serves to identify the message as a protected message, and provides a unique Message ID.

[0054] In various embodiments, the Data Content 706 is the part of the protected message that contains the encryption payload. The Data Content 706 is the same size as the original unencrypted message. The Data Content 706 is encrypted using the Data Encryption Key (DEK). The Data Encryption Key is a random number value, generated prior to the message being sent.

[0055] Seamless Access and Transparency

[0056] Email-Based Approach

[0057] To meet the need for transparent secured message distribution, an example embodiment of the present invention protects data within a standard message format used by the messaging system. This allows for the transport of the encrypted message through arbitrarily complex messaging systems, without the need for involvement by the third parties.

[0058] Transparent Message Encryption

[0059] This same example embodiment of the present invention encrypts messages deemed to be sensitive when they are sent from the computing device. So that there are no extra steps or interruptions to normal use, this encryption (and any subsequent decryption) is performed "on-the-fly". This is also known as "transparent encryption/decryption" – emphasizing that the user is not aware that the data transformation (plaintext to ciphertext, or ciphertext to plaintext) is happening. This is achieved by encrypting the message data as it is sent out, and decrypting it as a message is opened. In the present disclosure, this transparent encryption and decryption takes place, so long as the protected data is being accessed by the legitimate recipient, who must be in possession of, or be able to obtain, the appropriate cryptographic key for that particular message. Otherwise, to all other parties and actors, the message can be merely moved around, or copied, as an opaque, but otherwise meaningless, stream of bytes.

[0060] Cryptographic Security

[0061] Key Management

[0062] In some embodiments, when an email is sent, the list of people to whom the email is addressed (the "recipient list") is transmitted, along with the Message Key, to the message privacy service component. When suitably stored, the message privacy service component returns a Message ID for the message.

[0063] In some embodiments, to retrieve the Message Key, the recipient's private messaging application performs the following:

[0064] a) Successfully authenticate to the message privacy service component using a valid user account and password, and

[0065] b) Furnish the Message ID of the desired message.

[0066] In some embodiments, only if the specified message contains the requesting User's ID in its recipient list, will the Message Key be returned to the recipient's private messaging application.

[0067] In the preceding description, for purposes of explanation, numerous details are set forth in order to provide a thorough understanding of the embodiments. However, it will be apparent to one skilled in the art that these specific details are not required. In other instances, well-known electrical structures and circuits are shown in block diagram form in order not to obscure the understanding. For example, specific details are not provided as to whether the embodiments described herein are implemented as a software routine, hardware circuit, firmware, or a combination thereof.

[0068] Embodiments of the disclosure can be represented as a computer program product stored in a machine-readable medium (also referred to as a computer-readable medium, a processor-readable medium, or a computer usable medium having a computer-readable program code embodied therein). The machine-readable medium can be any suitable tangible, non-transitory medium, including magnetic, optical, or electrical storage medium including a diskette, compact disk read only memory (CD-ROM), memory device (volatile or non-volatile), or similar storage mechanism. The machine-readable medium can contain various sets of instructions, code sequences, configuration information, or other data, which, when executed, cause a processor to perform steps in a method according to an embodiment of the disclosure. Those of ordinary skill in the art will appreciate that other instructions and operations necessary to implement the described implementations can also be stored on the machine-readable medium. The instructions stored on the machine-readable medium can be executed by a processor or other suitable processing device, and can interface with circuitry to perform the described tasks.

[0069] The above-described embodiments are intended to be examples only. Alterations, modifications and variations can be effected to the particular embodiments by those of skill in the art. The scope of the claims should not be limited by the particular embodiments set forth herein, but should be construed in a manner consistent with the specification as a whole.

WHAT IS CLAIMED IS:

1. A method as substantially described herein.

2. A system as substantially described herein.

3. A computer readable medium including instructions for executing a method as substantially described herein.

4. A method of reading an encrypted message, the method comprising:

receiving the encrypted message at a client device;

scanning the encrypted message to determine its message ID;

supplying the message ID and message privacy service authentication information to a message privacy service component;

authenticating a user at the privacy service component and determining if the user is authorized to read the message;

if authorized, retrieving a message Key K1 and transmitting the message keey to the private messaging application; and

at the client device, upon receipt of the message Key K1, decrypting the message, and displaying it to the user on a screen of the client computing device.

FIG. 1

Top-Level Context

100

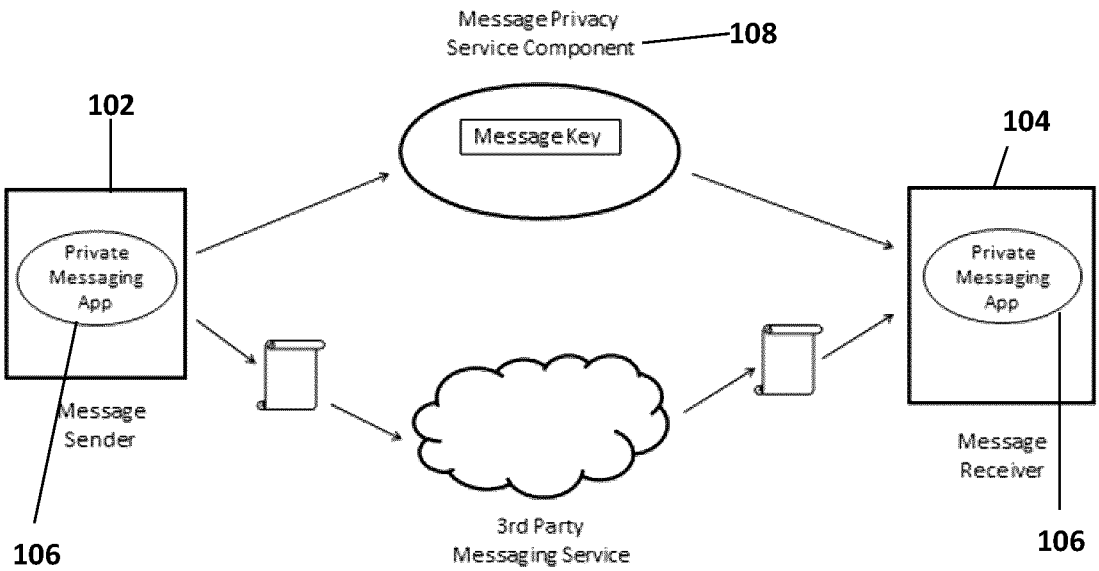


FIG. 2

Flowchart: Composing a Message

200

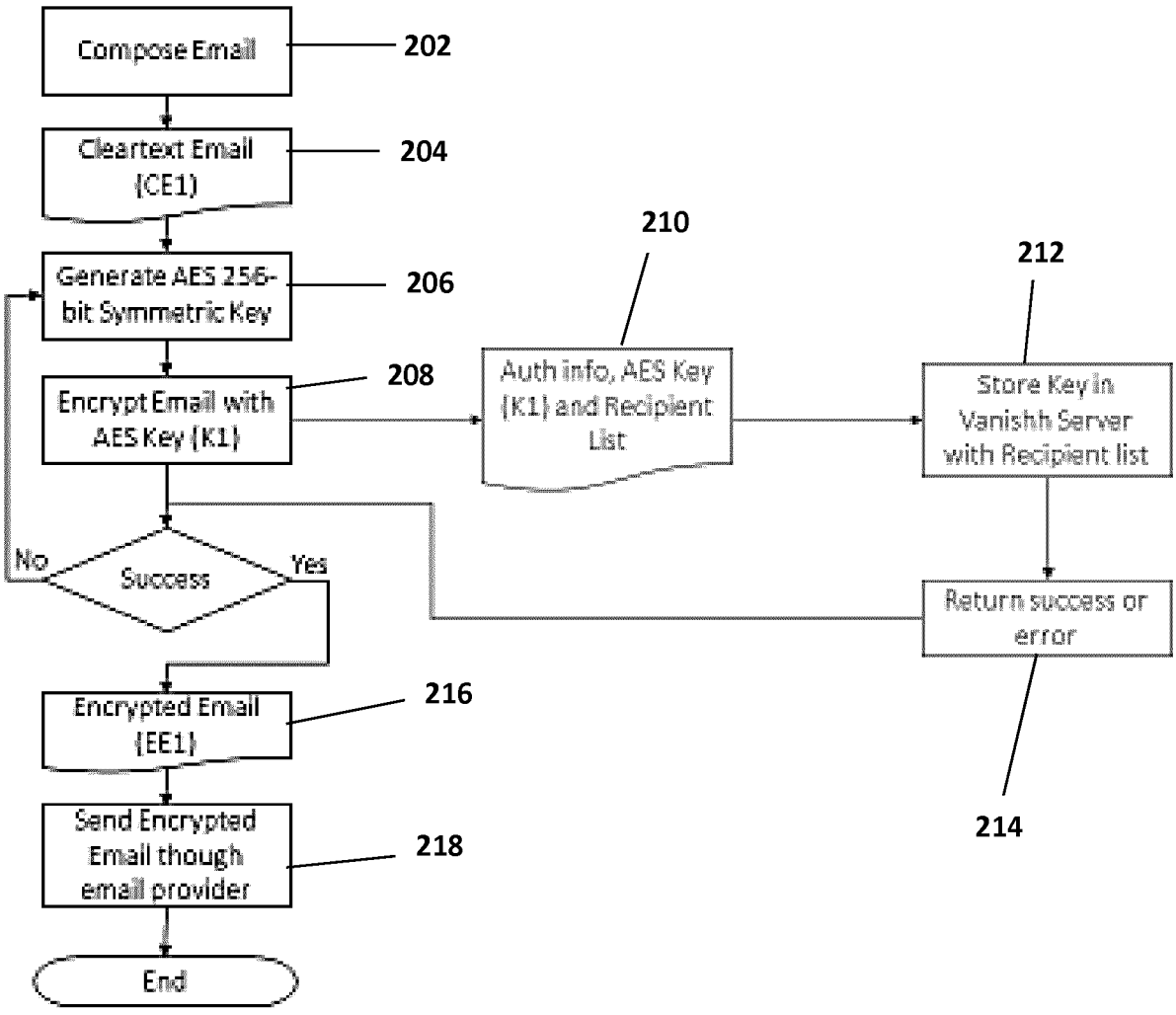


FIG. 3

Flowchart: Receiving a Message

300

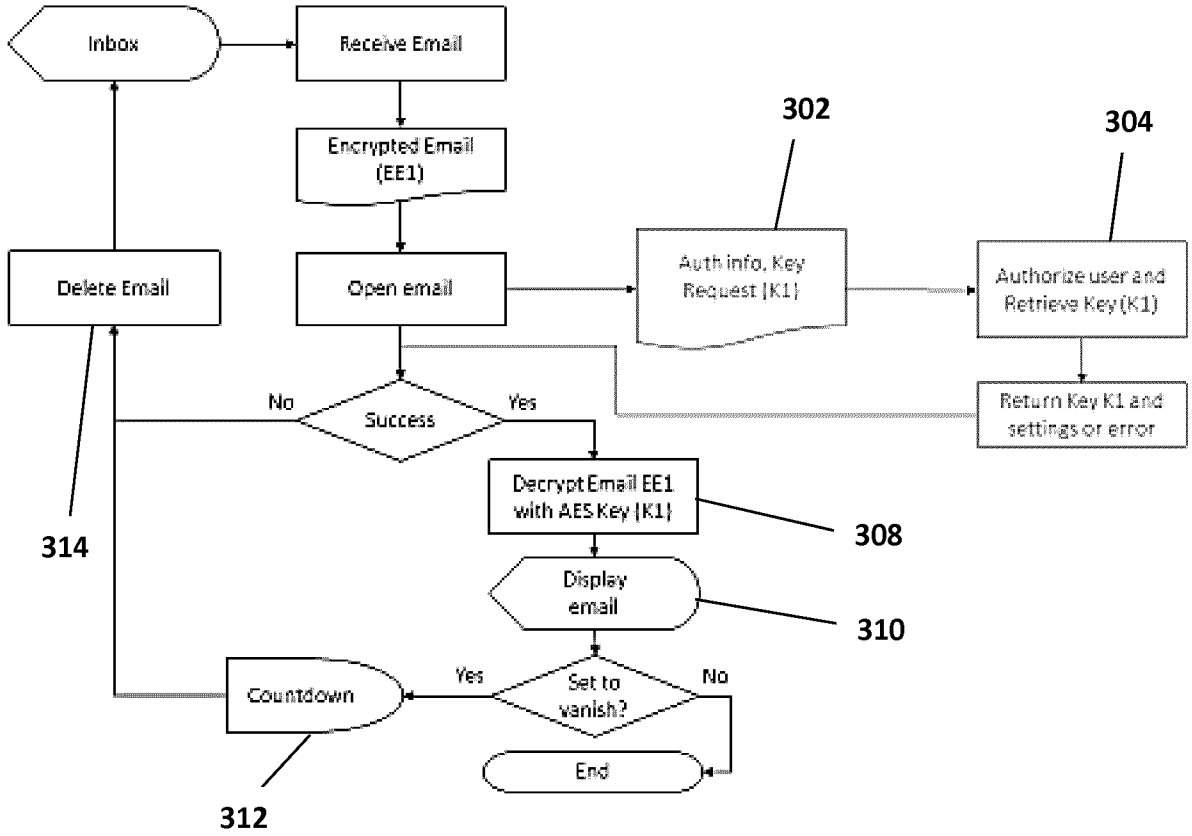


FIG. 4

Flowchart: Checking Read Status

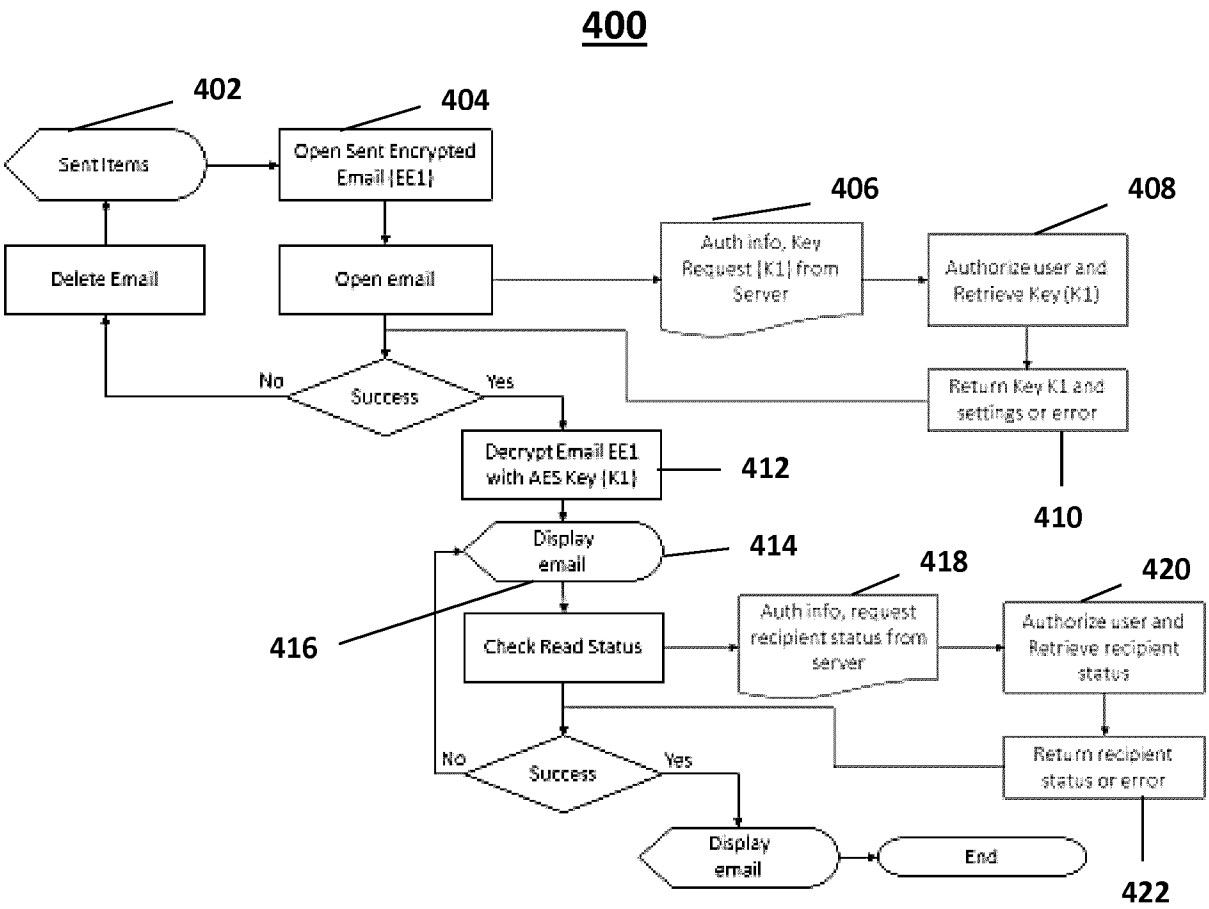


FIG. 5

Flowchart: Recalling a Message

500

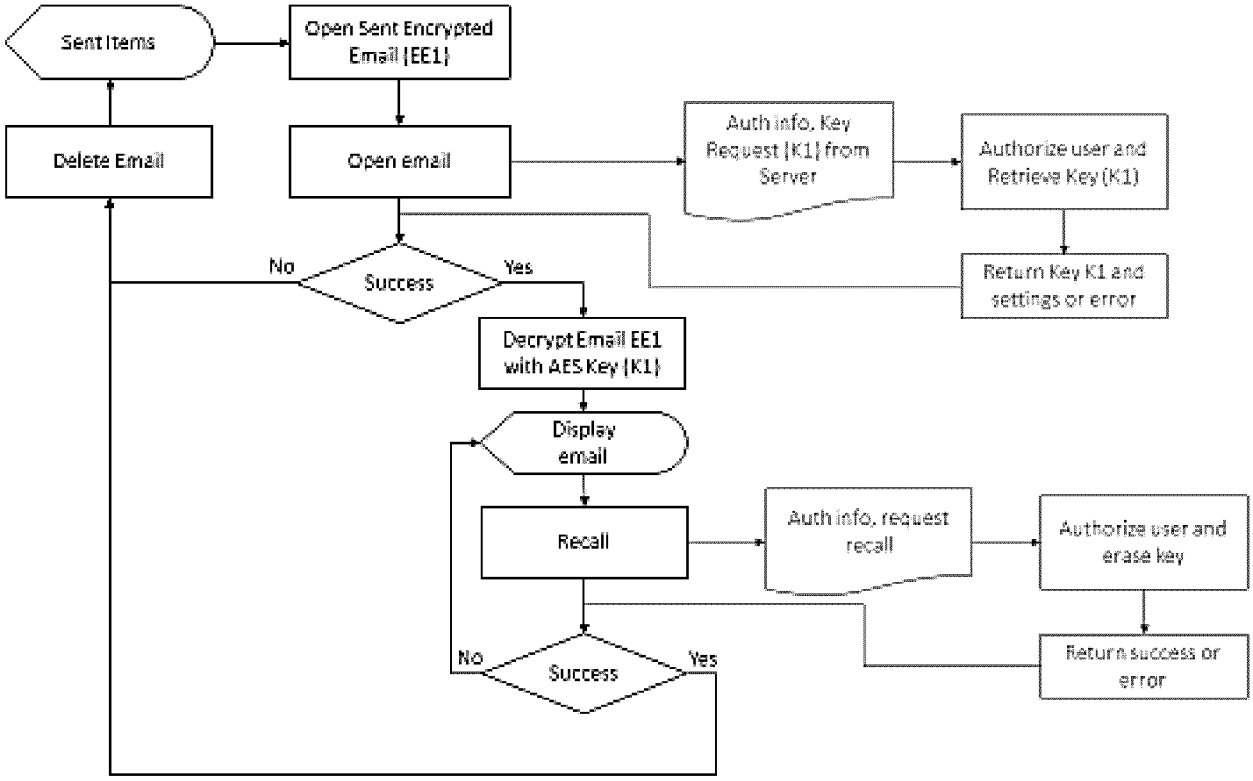


FIG. 6

Flowchart: Revoking a Recipient from a Message

600

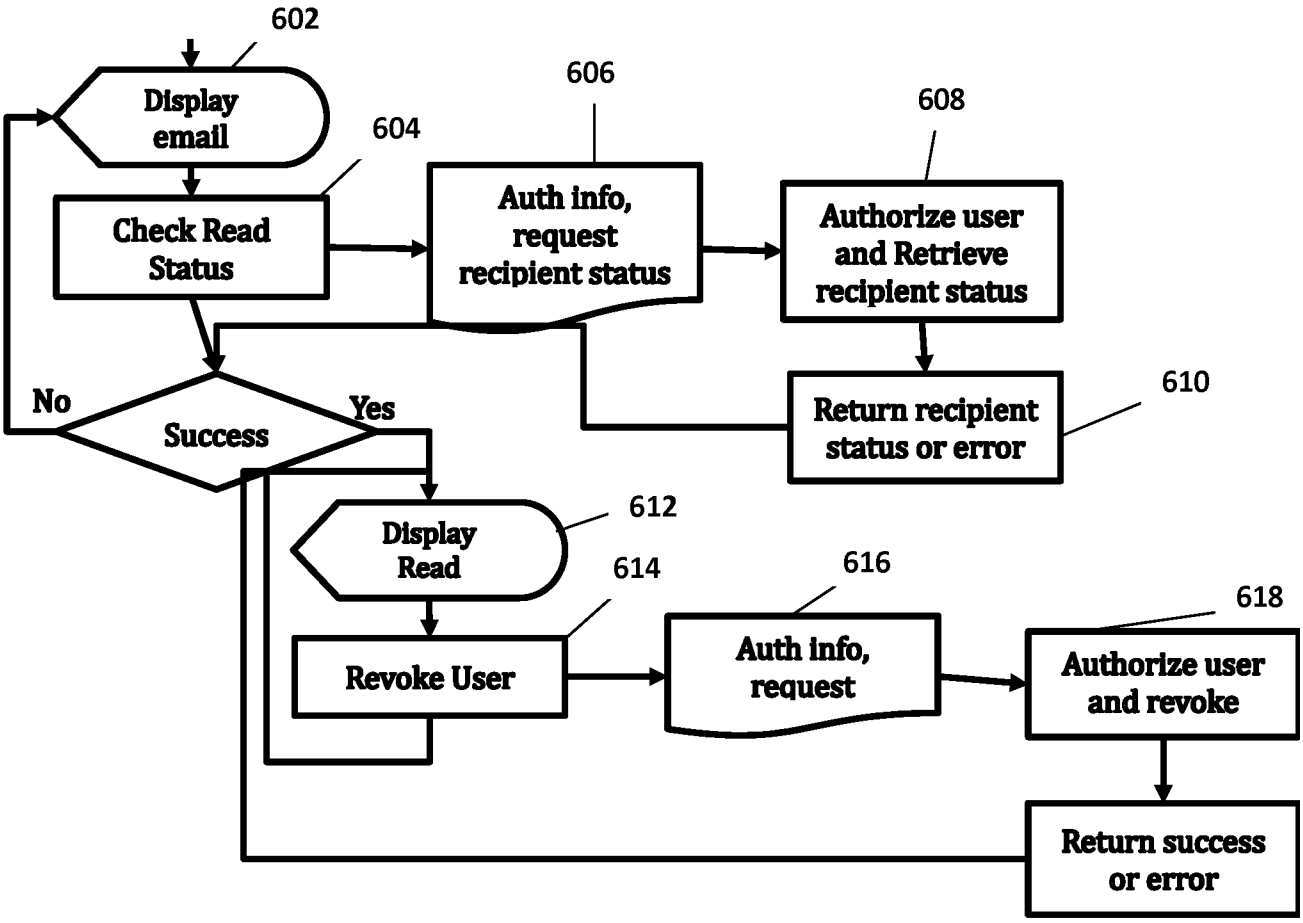
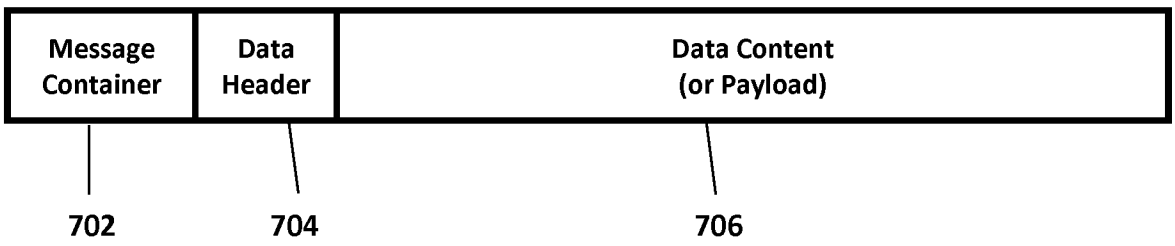


FIG. 7

Protected Message Data Format

700



INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2016/050783

A. CLASSIFICATION OF SUBJECT MATTER
IPC: ***H04L 9/06*** (2006.01) , ***H04L 9/08*** (2006.01) , ***H04L 9/32*** (2006.01)

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 9/06 (2006.01) , ***H04L 9/08*** (2006.01) , ***H04L 9/32*** (2006.01), ***H04L 9/00*** (2006.01),

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

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
Databases: Intellect (CIPO Database), IEEE Xplore, Questel Orbit, Google Patents
Keywords: encrypt, encryption, sever, key, distribution, message, ID, transmit, request, "key request", "message ID", decrypt

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 7,246,378 (MARVIT et al.) 17 July 2007 (17-07-2007) Col 3, Line 62- Col 4, Line 6 Col 5, Line 62 – Col 6, Line 9 Col 6, Lines 15-122 Col 10, Lines 45-61	4

☐ Further documents are listed in the continuation of Box C.

☑ See patent family annex.

*	Special categories of cited documents:	"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
"A"	document defining the general state of the art which is not considered to be of particular relevance	"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
"E"	earlier application or patent but published on or after the international filing date	"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
"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)	"&"	document member of the same patent family
"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		

Date of the actual completion of the international search 03 August 2016 (03-08-2016)	Date of mailing of the international search report 16 August 2016 (16-08-2016)
Name and mailing address of the ISA/CA Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 819-953-2476	Authorized officer Giles Babin (819) 953-5259

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2016/050783

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of the first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claim Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☑ Claim Nos.: 1-3
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

The International Searching Authority has not carried out a search for claims 1-3, under Article 17(2)(b) of the PCT. The claims fail to comply with the prescribed requirements to such an extent that a meaningful search could not be carried out. Claims 1-3 so lack clarity and/or support that a meaningful search over the whole of the claimed scope is impossible. Consequently, the search has been established for the parts of the application which appear to be clear and supported, namely claim 4.

3. ☐ Claim Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claim Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claim Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US7246378B1	17 July 2007 (17-07-2007)	US7246378B1	17 July 2007 (17-07-2007)
		AU4490000A	10 November 2000 (10-11-2000)
		TW545019B	01 August 2003 (01-08-2003)
		US6625734B1	23 September 2003 (23-09-2003)
		US7096355B1	22 August 2006 (22-08-2006)
		WO0065766A2	02 November 2000 (02-11-2000)
		WO0065766A3	08 March 2001 (08-03-2001)