



(51) International Patent Classification:

G06F 17/30 (2006.01) G06Q 10/10 (2012.01)
G06F 21/62 (2013.01)

(21) International Application Number:

PCT/NL2014/000046

(22) International Filing Date:

28 November 2014 (28.11.2014)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

N2011857 28 November 2013 (28.11.2013) NL

(72) Inventor; and

(71) Applicant : VAN DER KAMP, Jaap [NL/NL];
Kerkbuurt 22, NL-1551 AD Westzaan (NL).

(72) Inventor: DE HAAN, Eduart Martinus Maria; Adres:
Winterkoning 5, Zuid-Scharwoude 1722 CA (NL).

(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).

Declarations under Rule 4.17:

— of inventorship (Rule 4.17(iv))

Published:

— with international search report (Art. 21(3))
— with amended claims (Art. 19(1))

(54) Title: SECURE SINGLE SIGN-ON EXCHANGE OF ELECTRONIC DATA

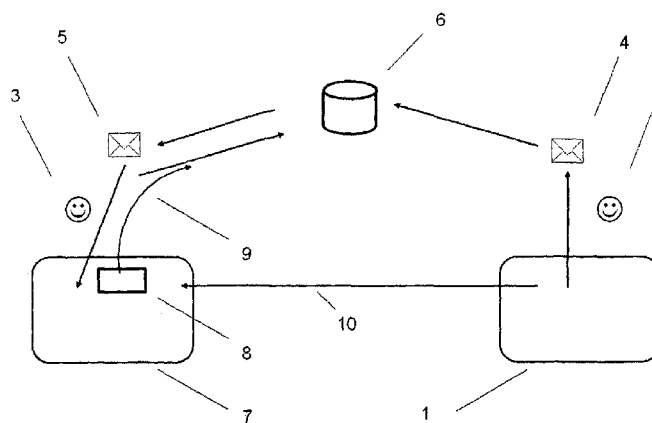


Figure 1

(57) Abstract: A method is disclosed for secure exchange of electronic data using single sign-on. According to the method an outgoing e-mail message is provided with a first pass code. The message is placed on a secure server, and the recipient receives a notification message comprising a link to the message on the server. The recipient enters a second pass code, which provides access to the e-mail on the secure server. According to the method at least one of the steps of providing a first pass code to the e-mail message and of providing a second pass code to the server is automated. In a preferred embodiment both steps are automated. Users having signed on to a secure environment can send and/or receive pass code protected e-mail messages without manually entering pass codes. In addition to e-mail as a means to send a notification, the notification also can be sent by means of social media, sms message or portable storage like an usb stick or a laptop. The address of the recipient can be an email address, a mobile phone number or another kind of destination. The content to be disclosed by the described single sign-on process can be stored encrypted in an email message, on a server in the cloud, on a device at the recipient, on a device at the sender or on portable storage. The encryption can be on file level or on the level of the container of the file such as an email message, a folder or a portable device..

SECURE SINGLE SIGN-ON EXCHANGE OF ELECTRONIC DATA

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0001] The invention relates generally a method for secure exchange of electronic data
5 and more specifically to such a method not requiring at least one of the sender and the
recipient of the electronic data to take affirmative security steps. The invention is restricted
to situations in which data packages and access codes are communicated separately.

2. Description of the Related Art

[0002] Prior art processes are known in which the sender of an electronic data package
10 associates the data package with a pass code, requiring the recipient to enter the pass code
before the data package can be received. These prior art processes have serious drawbacks.

[0003] One drawback of the prior art processes is that a pass code must be communicated
to the recipient. This is often done by electronic mail, which poses a security risk if the
message containing the pass code is intercepted by a hacker. This risk is amplified if the pass
15 code is sent in the same e-mail as the electronic data package. The risk is mitigated
somewhat if the pass code and the electronic data package are sent in separate e-mails, but
this is inconvenient to both the sender and the recipient. Moreover, this practice is still far
from risk free, because the two e-mail messages are typically sent within minutes or even
seconds from each other, and therefore subject to interception by a single hacker, who then
20 gains access to both the electronic data package and the pass code.

[0004] Another drawback of the prior art processes is that the sender may make a
typographical error when associating the pass code to the electronic data package and/or
when communicating the pass code to the recipient. Such error causes the recipient to
make several failed attempts at accessing the electronic data package, necessitates further
25 communication between the recipient and the sender, and delay on the electronic data
transfer.

[0005] Sender and recipient may pre-agree on a fixed pass code, which they then use for
all their data communications. This practice does not alleviate the problem of potential

typographical error on the part of the sender. In addition, the use of fixed pass codes, which are often stored in unsecured places, is inherently vulnerable to security attacks.

[0006] Perhaps the most serious drawback of the prior art processes is that they are perceived as cumbersome by the users, prompting them to bypass the security measures altogether. This practice, which is unfortunately very common, completely undermines the security of the system.

[0007] Thus, there is a need for a method for electronic data exchange that relieves at least one of the sender and the recipient, and preferably both, from the inconveniences of sending or receiving pass code protected communications.

[0008] The above mentioned drawbacks pertain to secure e-mail but also to pass code protected file transfer, storage and retrieval of pass code protected data 'in the cloud' and sending pass code protected files in unprotected e-mail.

[0009] Another kind of prior art processes is secure e-mail with only the data transfer being secured, leaving the data in the mailboxes relatively unprotected. The risk of data leakage is obvious, taking into account a too broad authorization to the mailboxes, synchronization of e-mail to smart phone, auto-forwarding to a less secure mailbox over an unprotected connection and the mailbox being hacked. It may be clear that a process in which only the data transfer process is protected, is not secure. This corroborates the need for a data transfer process supported by a pass code to protect the mails, but without the said inconveniences.

[0010] Related prior art examples are the use of a SAML token or OpenID to get easy access to applications 'in the cloud'. SAML and OpenID are based on a user using a web browser or an app. Although a method like SAML realizes single sign-on, this is not the single sign-on to be used in secure email, which is described here in this invention. However, this invention is applicable to situations in which the user has logged on using SAML or OpenID and then accesses the secure mail using single sign-on.

[0011] Related prior art in which single sign-on access to the sent data package is realized, is Identity Based Encryption (IBE). However, the drawback of IBE is that a secure email which

has been sent to a wrong email address, can be opened by the corresponding wrong recipient. This drawback is based on the fact that the encryption method of IBE is based on the mail addresses of the sender and recipient. The scope of the invention described here is restricted to situations in which data packages and access codes are communicated
5 separately, which is not the case in IBE.

[0012] Regarding the items to be transported, discerned can be data packages, notifications and access codes.

[0013] Data packages normally are sent by means of email or by means of a file transfer process. In the case of a file transfer process the data package firstly is sent to a server in
10 the cloud and secondly, after authentication of the recipient, is sent to the recipient or is displayed to the recipient. Another option is that the data package is stored firstly on the network of the sender, for example on an extranet. The invention described here pertains on all mentioned transport methods.

[0014] The access codes can be distributed using a broad range of methods, from a simple
15 agreement between sender and recipient on a permanent or temporary pass code to distribution of pass codes from a central point over a restricted community. A first pass code originated in the sending process can be translated into a second pass code to be used by the recipient. For the invention it is important that the recipient needs an access code to open the data package to be received. The access code which the recipient virtually skips
20 using the SSO invention described here is not chosen by the recipient himself. If the recipient himself chooses the access code, the invention would be a classical single sign-on construct.

[0015] Data packages, notifications and access codes can be transported by a diversity of means of transport such as email, EDI, usb stick, sms, umts et cetera. The invention applies
25 to all options.

[0016] The data package can be encrypted on various levels, for example file level, folder level or device level. The invention applies to all options.

[0017] The invention described here can be implemented as an add-on to an existing method of data transfer, as an add-on to an existing method for secure transfer of data packages or can be implemented as an independent method for secure transfer of data packages. An example of an add-on to an existing method of data transfer is an outlook
5 plug-in.

BRIEF SUMMARY OF THE INVENTION

[0018] The present invention addresses the mentioned drawbacks by providing a method for secure exchange of electronic data using single sign-on, said method comprising the
10 steps of:

- a. preparing a data package by a sender for electronic transfer to a recipient;
- b. associating the data package with a first pass code;
- c. placing the data package on a server which is accessible by the recipient;
- d. sending an electronic message to the recipient, said electronic message comprising a link
15 to the data package;
- e. obtaining a second pass code;
- f. retrieving the data package from the server using the second pass code;

wherein at least one of steps b. and e. is carried out automatically.

[0019] Another aspect is a secure network comprising means for implementing the
20 method of the invention.

[0020] Yet another aspect is a means for making a secure network capable of implementing the method of the invention.

BRIEF DESCRIPTION OF THE FIGURE

[0021] Figure 1 schematically represents an embodiment of the method of the invention.

DETAILED DESCRIPTION OF THE INVENTION

5 [0022] The following is a detailed description of the invention.

Definitions

[0023] The term "computer" as used herein means any device capable of sending and/or receiving electronic data via a network or the Internet. As used herein the term encompasses devices such as mainframe computers; desktop computers; laptop computers; 10 tablets, such as iPads; smart phones; and the like.

[0024] The term "data package" as used herein means any collection of digital information capable of being transferred via a network or the Internet. The term includes files in any electronic format, such as .doc; .docx; jpeg; xls; pdf; ppt; html; and the like. It includes both messages and any attachments to such messages. A data package can be 15 secured totally or partially.

[0025] The term "pass code" as used herein refers to any form of electronic identification or protection by an access code. The term includes strings of numbers, letters or symbols in any combination. The term further includes alternate identifiers, such as mathematical formulas, biometric data based on a user's retina, fingerprint or other uniquely personal 20 feature; and the like.

[0026] The term "notification" as used herein means a message to a recipient which refers to the securely sent data package. In nowadays technology the notification is often realized by an email containing a link to the data package or to a logon window to open the data package. In the invention described here the notification can be every kind of electronic 25 message and the pass code to the link can be every kind of signal, from a string of digits to the voice recognized words "you open sesame".

[0027] The term “secure network” as used herein means a network having access limited to authorized users. Generally an authorized user may gain access to the secure network using a sign-on procedure or protocol. The sign-on procedure may include entering a user id and a password, and may involve additional security measures, such as correctly responding to a challenge, answering specific security questions only an authorized user is supposed to know, entering a code transmitted to the authorized user’s phone, etc. The sign-on procedure may be dependent on the location from which the user seeks access to the network. For example, an employee of a company may get wired access to the company’s secure network from a computer at a work location using a sign-on procedure requiring only entering a user id and a password, whereas the same employee seeking wireless access from a remote location may in addition need to respond to a randomly generated challenge. The term “secure network” can also mean an individual computer, as defined above, having access limited to an authorized user or users. Access to the secure network can be realized by a logon code and password, by a stronger authentication, but also by a code to enter a mobile device, a key ring application, an authentication application in the cloud or another type of authentication method.

[0028] The term “single sign-on” or “SSO” as used herein refers to a feature of the invention allowing a user of the inventive method send, or to gain access to, pass code protected data packages after signing on to, for example, a secure network or a secure software package. Because the pass code or pass codes required by the user is or are retrieved or calculated by the secure network or the secure software, the user only needs to sign on to the secure network or the secure software in order to make use of the method of the invention. It will be understood that the user’s connection to the secure network may automatically terminate after a predetermined time after sign-on or after a predetermined time of inactivity, requiring the user to sign on again. This is considered to be within the definition of single sign-on.

[0029] In its broadest aspect the present invention relates to a method for secure exchange of electronic data using single sign-on, said method comprising the steps of:

a. preparing a data package by a sender for electronic transfer to a recipient;

- b. associating the data package with a first pass code;
- c. placing the data package on a server which is accessible by the recipient;
- d. sending an electronic message to the recipient, said electronic message comprising a link to the data package;

5 e. obtaining a second pass code;

- f. retrieving the data package from the server using the second pass code;

wherein at least one of steps b. and e. is carried out automatically.

[0030] In a first main embodiment step b. is carried out automatically. This can be accomplished by using an e-mail software package that automatically attaches a pass code to an electronic data transfer. The software package may additionally include a notification in the e-mail message to alert the recipient that the data transfer is protected by a pass code. In this embodiment the recipient needs to obtain a second pass code in order to gain access to the electronic data package. The second pass code may be identical to the first pass code, or it may be different from the first pass code. In the latter case, the second pass code is associated with the first pass code such that it is recognized as the proper key for providing access to the data package.

[0031] In a preferred execution of this embodiment the sender is connected to a secure network, which contains a monitoring software package that imposes the use of a pass code on outgoing e-mail, and attaches pass codes to each outgoing e-mail message, or to selected e-mail messages identified as confidential. The said monitoring software uses a parameter as input, for instance the pass code itself. In a preferred execution of this embodiment the pass code is stored in the single sign on mechanism of the sender. Advantages are that the pass code parameter can be used both to send and to receive, and that the pass code can be used to protect both sent messages and attachments to such messages.

[0032] The recipient may obtain the second pass code in one of several ways. For example, the second pass code may have been previously communicated to the recipient, and memorized by the recipient or stored by the recipient in some form of memory, be it in analog form (as for example written down on paper) or in digital form. Or the second pass

word may be communicated to the recipient within minutes from the sending of the message, for example by separate e-mail, by voice telephone call, in a telephone text message, or the like. Or the recipient may have access to software comprising an algorithm for calculating the second pass code. In a preferred embodiment the e-mail message received by the recipient may contain a seed code used by the algorithm to calculate the second pass code. The recipient needs to manually enter the second pass code in order to gain access to the data package.

[0033] This embodiment has the advantages that the sender can only send messages that are protected by a pass code. In addition, there is no risk transmitting an incorrect pass code due to a typographical error on the part of the sender. In addition, providing a pass code does not require any additional action by the sender, removing any incentive on the part of the sender to try and circumvent the security measures.

[0034] This embodiment has the disadvantage that it requires the recipient to take extra steps in order to gain access to the data package. In the best case this causes an inconvenience to the recipient. In case the recipient does not have access to the second pass code, for example because a memorized pass code has been forgotten, or an electronic or analog memory containing the pass code has been lost or compromised, or is at a remote location from the recipient, there can be appreciable frustration and delay in the delivery of the data package.

[0035] In a second main embodiment step e. is automated, but step b. is not. In this embodiment a data transmission is pass code protected only if the sender takes the affirmative step of associating the data package with a first pass code. The second pass code is automatically obtained for the recipient. This may be done in one of several ways. For example, software present on the recipient's computer may recognize the incoming e-mail as being pass word protected, and retrieve a previously stored pass code from the memory of the recipient's computer or from the cloud. Or the e-mail message may contain a seed value that is used on the recipient's computer to calculate the second pass code. In a preferred embodiment the recipient is connected to a secure network, which contains monitoring software that monitors incoming e-mail messages. When a pass code protected

e-mail message comes in, the monitoring software recognizes the e-mail message as being pass code protected, and retrieves the required second pass code from a secure server, or calculates the second pass code using a predetermined algorithm.

[0036] The second pass code may be communicated to the recipient, for example
5 displayed on the recipient's computer screen. For additional security the second pass code may be communicated to the recipient by a separate channel of communication, for example as a text message to the recipient's mobile phone. The recipient can then use the second pass code to gain access to the data package.

[0037] The method of this second main embodiment can be automated further by also
10 automating step f., that is, the monitoring software establishes the link to the data package on the server, communicates the second pass code to the server, and causes the data package to be downloaded to the recipient's computer.

[0038] The advantages of this second main embodiment are that the sender has control over whether a data transmission gets pass code protection, so that no pass code protection
15 is used for messages containing only non-confidential information, and that the recipient does not need to take any affirmative steps to obtain the required second pass code.

[0039] The disadvantages of this second main embodiment are that the sender needs to take affirmative steps to secure a data transmission, potentially providing the sender with an incentive to bypass the security measures.

[0040] In a third main embodiment both steps b. and e. are automated. This embodiment
20 combines the features of the first and second main embodiments. In addition step f. may also be automated, as described above in the context of the second main embodiment.

[0041] Preferably both the sender and the recipient are connected to different secure
25 networks or to one common secure network. In this embodiment the secure network comprises a means for implementing the method of the invention. The secure network may belong to a company and connect employees, contractors and consultants to the company's data and to each other. Other examples include networks of service providers having a need to communicate with their customers in a secure way and may wish to use the Internet for

such communications. Examples include hospitals, insurance companies, banks, government agencies such as tax authorities, immigration authorities, court systems, and the like.

[0042] The network can be provided with software that automatically implements the method of the invention. The actual structure of this software depends on the type of pass
5 code used for the method, as explained in more detail below.

[0043] As a first example the pass code is static and is known to all users who need to be able to send secured e-mail messages. When a new user is authorized, the new user is provided with a pass code conversion table, which may be placed on the user's computer or in a dedicated portion of a server controlled by the network. When a sender sends a pass
10 code protected e-mail message this message is placed on a server being part of a secure e-mail infrastructure, and the recipient initially only receives a notice with a link. When the recipient clicks on the link, the software retrieves the second pass code from the pass code conversion table. This second pass code enables the link. The recipient gains immediate access to the contents of the e-mail message. The pass code protocol is invisible to the
15 recipient. For added security the second pass code may be encrypted with a key based on the recipient's user id, for example.

[0044] This embodiment may be suitable for systems wherein a relatively small number of senders send pass code protected messages to a potentially large number of different recipients. The senders can be trained to apply sound judgment when deciding whether to
20 pass code protect a message, or pass code protection may be used on all outgoing messages. As the number of senders in the system is limited, the risk of loss of secrecy of the first pass code is limited. Security may be enhanced by only allowing outgoing messages from computers that are hard wired to the network.

[0045] In a second embodiment the first pass code is static, but is only known to system
25 administrators and/or the provider of the software. The first pass code is stored in a conversion table. The system automatically provides outgoing messages with the first pass code. As in the previous embodiment the recipient has been provided with a conversion table for retrieving the second pass code (which may or may not be identical to the first pass code).

[0046] As in this second embodiment the system is automated on both the sender's side and the recipient's side, their roles can be easily reversed. That is, if a recipient responds to a message, the response can be pass code protected with a first pass code retrieved from the user's conversion table, and the receiver of the response can gain access to the content of the response using a second pass code retrieved from a corresponding conversion table on his or her end.

[0047] In a third pass code embodiment, the sender and the receiver are both provided with corresponding versions of an encryption algorithm. In this embodiment each pass code is used only once. For example, an outgoing message may be provided with a date-and-time signature, which is used as a seed value for calculating the pass code. The recipient's software retrieves the date-and-time signature from the notification e-mail message, and uses it to calculate the pass code. As in other embodiments, for added security an additional unique identifier, such as the user id of the recipient, may be used for additional encryption.

[0048] In a fourth pass code embodiment use can be made of asymmetric encryption. For example by making use of a Public Key Infrastructure ("PKI") the first and the second pass codes are different from each other, but "fit" onto each other. Depending on the type of implementation, certification may be needed on a general level, on a level of cooperating SSO providers, or on a community level.

[0049] In addition to associating an outgoing message with a pass code, a sender may be given additional tools for controlling the message. For example, the sender may limit delivery of the message to a specific computer, or to a specific time frame, to a specific geographic location, or a combination of such limitations. It is also possible for the sender to retain these capabilities even after the message has been sent. Software for implementing these additional security measures is available under the name FileSecure from Seclore of Mumbai, India.

[0050] Another aspect of the invention is a secure network capable of implementing the method of the invention. Secure networks are well known to those skilled in the art. A secure network can be provided with a secure e-mail capability available from a number of providers. Such prior art secure e-mail systems require the sender and the recipient to enter

the pass code associated with an e-mail message. The network can be upgraded to provide SSO to the sender, the recipient, or both.

[0051] To provide SSO to the sender, a pass code is stored in a sender lookup table, and the e-mail software is programmed to add the pass code to a notification e-mail that is sent to the recipient. Instead of a pass code from a lookup table, the software may contain an algorithm for calculating a pass code on an *ad hoc* basis. The e-mail message itself is not sent to the recipient, but is stored on a server that is part of the secure network. The notification e-mail contains a link to the e-mail message on the server.

[0052] The system further comprises a pass code generator on the recipient's end. This may be a simple lookup table that is placed on the recipient's computer at the time the recipient's user account on the network is created. Instead of on the recipient's computer, the lookup table may be placed in the cloud, so that the recipient has access to it when operating from different computers. The pass code generator may also be in the form of an encryption algorithm, which calculates the pass code on an *ad hoc* basis.

[0053] It is desirable to have the sender's end of the SSO system mirror the recipient's end, so that each sender can also act as a recipient, and v.v.

[0054] Yet another aspect of the invention is a plug-in for upgrading a network to SSO capability. The plug-in may be a plug-in to an existing secure e-mail system, to provide SSO capability to a network already provided with secure e-mail. The plug-in may also be a full SSO secure e-mail package, in which case the plug-in may comprise a secure e-mail module and an SSO module.

[0055] It is desirable to protect messages and attachments at the sender's end from unauthorized access. The pass code at the sender's end can be used to realize this protection. The alternative is that sent e-mails remain unprotected in the out-box of the sender.

If a secure e-mail, according to this invention, is sent to a recipient not using this invention, there is a problem. Several solutions are possible. The first is that the sender communicates separately a pass code provided manually by the supplier of the invention or by an

administrator or is originated using a token generator. A second solution is that the recipient becomes part of the community using the invention. A third solution is a fall back onto the secure e-mail mechanism without using the invention on the recipient's end.

[0056] Single sign-on access to securely sent data packages can occur in various levels of

5 granularity. A coarse implementation is that the required second pass code is static for all incoming secure mails. A finer implementation is that the required pass code depends on the mail address, phone number, MAC address, IMEI or IP address of the sender or recipient. A pass codes can be valid on individual level or on organizational level. Also the required pass code can depend on a domain or affinity which contains a certain group of
10 communicators. For incoming mails another granularity can be used than for sent mails. An extra feature is definition in time of the validity of the first or second pass code. For example, the pass code is valid from November 18th 9:14 to December 18th 9:14. An obvious feature is that the SSO mechanism for secure mail described here recognizes the secure email application which is used. An example of implementing the SSO mechanism is the
15 following table, which translates the credentials for the secure network of the recipient to the required access with which the recipient logs on in the secure email application using single sign-on.

First field: A recognition of the fact that the recipient has been logged on in his secure network;

20 Second field: The secure email application used by the sender and the recipient;

Third field: Email address of the sender;

Fourth field: Email address of the recipient;

Fifth field: Period in which the second pass code is valid;

Sixth field: Second pass code.

25 In this example the second pass code depends on the used secure email application, on the mail addresses of sender and recipient and on time. The table translates the access of the recipient on his secure network to SSO access to the securely sent data package.

[0057] Synchronization of pass codes between sender and recipient is not easy. An option is automated synchronization of changing pass codes. The pass codes of sender and

recipient can be identical but also can be synchronized whereby the two pass codes, pass code 1 and 2, remain different, which is achieved by a method which produces pass code 1 and pass code 2.

[0058] If pass code 1 or pass code 2 are contained in the application which realizes the access of the user to his secure network, such as an LDAP application, synchronization of the pass codes of the invention described here can be part of existing synchronization of the access over different secure networks, as realized in Microsoft Azure.

[0059] The invention described here can be implemented by integration in the sign-on mechanism of the secure network of the sender or recipient such as the LDAP database, can be implemented as a plug-in in the used application to send and receive data packages and can be implemented as a standalone application stored in the secure network of the sender or recipient or stored in the cloud.

[0060] An option is that if the recipient has not implemented the invention described here, it will be implemented automatically.

[0061] In a situation that sent data packages are stored in the outbox, encrypted or not, the data packages are vulnerable to data leakage, for instance by unwanted access to the mailbox, by mail synchronization to a mobile device, by hacking or by autoforward, A solution is storage of the sent data package in the cloud followed by removing the sent data package from the outbox leaving in the outbox a pass code protected link to the data package. The pass code can be the said first pass code but can also be a third pass code. In retrieving the data package in the cloud the single sign-on mechanism of the invention described here can be used.

[0062] A feature to make the invention described here even more user friendly is that the recipient not opens the received notification mail followed by opening the data package, but only selects the received notification mail to get access to the protected email content and eventually included attachments. Thus the manual selection of the link to the securely stored data package is skipped.

[0063] When a user logs on in a mail application with weak authentication using public wifi, eavesdropping is a serious threat. When the user accesses his secure mail solution, the eavesdropping will proceed into the secure email application due to the weak authentication of the secure mail. To make the secure mail really secure at this point, the secure mail can be provided with strong authentication. The strong authentication can be based for example on an sms token, on the IMEI, on rfid, on a fingerprint or on facial recognition. The feature what is used in addition to the weak authentication can be applied for example once a day, by session or apart by mail. In the latter case the user must authenticate himself for example with his fingerprint to open each distinct mail.

[0064] The invention described here is not restricted to data packages transferred between different secure networks, but can also be applied within one secure network, for example when email between colleagues using the same secure network is sent secure.

DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS/EXAMPLES

[0065] The following is a description of certain embodiments of the invention, given by way of example only.

[0066] Figure 1 is a schematic representation of an embodiment of the method of the invention.

[0067] Sender 2 on sender's secure network 1 creates a pass code protected message 4, which is stored on server 6. At the same time sender's secure network 1 sends a notification message 10 to recipient's secure network 7. Recipient 3 clicks on a link in notification message 10, which triggers system 8 within recipient's secure network 7 to translate the network credentials of recipient 3 to a second pass code. This second pass code is communicated to server 6, and results in e-mail message 5 being downloaded to the recipient's secure network.

[0068] Thus, the invention has been described by reference to certain embodiments discussed above. It will be recognized that these embodiments are susceptible to various modifications and alternative forms well known to those of skill in the art.

- 5 [0069] Many modifications in addition to those described above may be made to the structures and techniques described herein without departing from the spirit and scope of the invention. Accordingly, although specific embodiments have been described, these are examples only and are not limiting upon the scope of the invention.

WHAT IS CLAIMED IS:

5 1. A method for secure exchange of electronic data using single sign-on, said method comprising the steps of:

- a. Preparing a data package by a sender for electronic transfer to a recipient;
- b. associating the data package with a first pass code;
- c. placing the data package on a server which is accessible by the recipient;
- 10 d. sending an electronic message to the recipient, said electronic message comprising a link to the data package;
- e. obtaining a second pass code;
- f. retrieving the data package from the server using the second pass code;

wherein at least one of steps b. and e. is carried out automatically.

15 2. The method of claim 1 wherein the recipient is connected to a secure network, and step e. is carried out automatically by the secure network.

20 3. The method of claim 1 or 2 wherein the first pass code and the second pass code are identical.

4. The method of claim 1 or 2 wherein the first pass code and the second pass code are different.

25 5. The method of any one of claims 1 through 4 wherein both steps b. and e. are carried out automatically.

6. The method of any one of the preceding claims wherein at least the first pass code is a static pass code.

7. The method of claim 6 wherein the data package is manually associated with the first pass code by the sender.

5 8. The method of any one of claims 1 through 5 wherein at least the first pass code is a dynamic pass code.

9. The method of any one of the preceding claims wherein the sender is connected to the secure network and step b. is carried out by the secure network.

10 10. The method of claim 8 or 9 wherein the second pass code is a dynamic pass code which is generated on the secure network.

15 11. The method of any one of the preceding claims wherein the sender places restrictions on receipt of the data package.

12. The method of claim 11 wherein the sender retains an ability to place or modify restrictions on receipt of the data package after the data package has been placed on the server accessible by the recipient.

20 13. The method of claim 2 or 9 wherein one pass code is used to both send and receive messages.

25 14. The method of claim 9 wherein the first pass code is used to protect sent data packages at the side of the sender against unauthorized access.

15. The method of any one of claims 1 through 14 applied to pass code protected file transfer.

16. The method of any one of claims 1 through 14 applied to storage and retrieval of pass code protected data 'in the cloud'

5 17. A secure network comprising means for implementing the method of any one of the preceding claims.

18. Means for making a secure network capable of implementing the method of any one of claims 1 through 16.

10 19. A method to copy a sent data package from the outbox to the cloud and thereafter remove the data package from the outbox leaving in the outbox a pass code protected link to the said data package.

15 20. A method to skip the manual selection of a link to a securely stored data package whereby the user directly gets access to the said data package only by selecting the notification mail which contains the said reference.

20 21. A method to integrate the communication of pass codes between sender and recipient with synchronization over different secure networks of the mechanism which gives the sender and recipient access to their own secure networks.

25 22. A method to realize strong authentication in secure exchange of electronic data in which the physical part of the strong authentication, for example a fingerprint, must be applied separately to each data package to open it.

AMENDED CLAIMS

received by the International Bureau on 17 March 2015 (17.03.2015).

WHAT IS CLAIMED IS:

- 5 1. A method for secure exchange of electronic data wherein single sign-on is applied,
the secure exchange of electronic data comprising the steps of:
- a. Preparing a data package by a sender for electronic transfer to a recipient;
 - b. associating the data package with a first pass code;
 - c. placing the data package on a server which is accessible by the recipient;
 - 10 d. sending an electronic message to the recipient, said electronic message
comprising a link to the data package;
 - e. obtaining a second pass code;
 - f. retrieving the data package from the server using the second pass code;
- wherein at least one of steps b. and e. is carried out automatically.
- 15 2. The method of claim 1 wherein the recipient is connected to a secure network, and
step e. is carried out automatically by the secure network.
- 20 3. The method of claim 1 or 2 wherein the first pass code and the second pass code are
identical.
- 25 4. The method of claim 1 or 2 wherein the first pass code and the second pass code are
different.
- 30 5. The method of any one of claims 1 through 4 wherein both steps b. and e. are
carried out automatically.
6. The method of any one of the preceding claims wherein at least the first pass code is
a static pass code.

7. The method of claim 6 wherein the data package is manually associated with the first pass code by the sender.
8. The method of any one of claims 1 through 5 wherein at least the first pass code is a dynamic pass code.
9. The method of any one of the preceding claims wherein the sender is connected to the secure network and step b. is carried out by the secure network.
10. The method of claim 8 or 9 wherein the second pass code is a dynamic pass code which is generated on the secure network.
11. The method of any one of the preceding claims wherein the sender places restrictions on receipt of the data package.
12. The method of claim 11 wherein the sender retains an ability to place or modify restrictions on receipt of the data package after the data package has been placed on the server accessible by the recipient.
13. The method of claim 2 or 9 wherein one pass code is used to both send and receive messages.
14. The method of claim 9 wherein the first pass code is used to protect sent data packages at the side of the sender against unauthorized access.
15. The method of any one of claims 1 through 14 applied to pass code protected file transfer.

16. The method of any one of claims 1 through 14 applied to storage and retrieval of pass code protected data 'in the cloud'
17. A secure network comprising means for implementing the method of any one of the preceding claims.
18. Means for making a secure network capable of implementing the method of any one of claims 1 through 16.
19. The method of any one of the preceding claims wherein a sent data package, after having been copied from the outbox of the sender to a secure mail server, is removed from the outbox and is replaced by a pass code protected link to the said data package.
20. The method of any one of the preceding claims wherein the manual selection of a link to a securely stored data package is skipped because the user directly gets access to the said data package only by selecting the notification mail which contains the said link.
21. The method of any one of the preceding claims wherein the communication of pass codes between sender and recipient hitchhikes with synchronization, between different secure networks, of the mechanism which gives the sender and recipient access to their own secure networks.
22. The method of any one of the preceding claims wherein the physical part of the strong authentication, for example a fingerprint, must be applied separately to each data package to open it in order to realize strong authentication in secure exchange of electronic data.

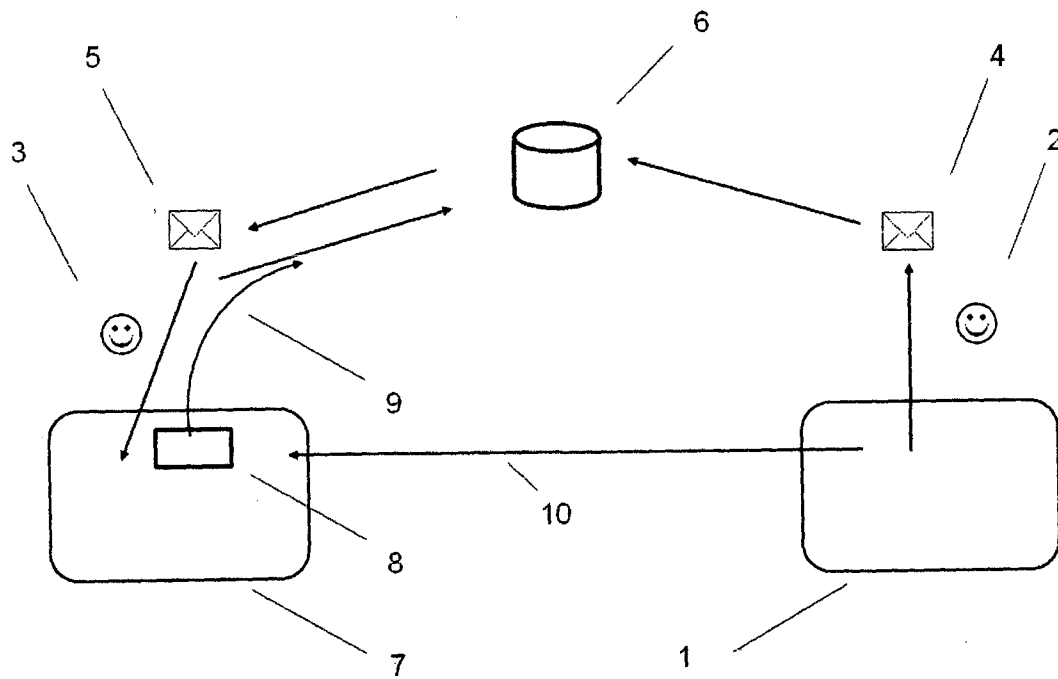


Figure 1

INTERNATIONAL SEARCH REPORT

International application No
PCT/NL2014/000046

A. CLASSIFICATION OF SUBJECT MATTER INV. G06F17/30 G06F21/62 G06Q10/10 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) G06F G06Q		
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 2013/246901 A1 (MASSAND DEEPAK [US]) 19 September 2013 (2013-09-19) abstract; claims 1-3; figures 3,4 paragraphs [0006], [0009], [0033], [0049], [0050], [0062] - [0064], [0066] - [0070]	1-18
X	----- WO 2012/177253 A1 (DROPBOX INC [US]; HOUSTON ANDREW [US]; FERDOWSI ARASH [US]; YING JONAT) 27 December 2012 (2012-12-27) abstract; claim 1; figure 1 paragraphs [0005], [0007], [0010], [0013], [0014], [0021], [0032]	1-18
X	----- US 2004/158607 A1 (COPPINGER CLIFFORD L [US] ET AL) 12 August 2004 (2004-08-12) the whole document	1-18
☐ 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 25 February 2015		Date of mailing of the international search report 05/03/2015
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Authorized officer Wolters, Robert

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NL2014/000046

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of 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. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☒ Claims Nos.: 19-22
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:
see FURTHER INFORMATION sheet PCT/ISA/210
3. ☐ Claims 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 an 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 claims 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 claims 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.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

Continuation of Box II.2

Claims Nos.: 19-22

The present application contains 22 claims, of which 7 are independent. There is no clear distinction between the independent claims because of overlapping scope. There are so many claims, and they are drafted in such a way that the claims as a whole are not in compliance with the provisions of clarity and conciseness of Article 6 PCT, as it is particularly burdensome for a skilled person to establish the subject-matter for which protection is sought.

The non-compliance with the substantive provisions is to such an extent, that the search was performed taking into consideration the non-compliance in determining the extent of the search (PCT Guidelines 9.19 and 9.25).

The search was based on the subject-matter that, as far as can be understood, could reasonably be expected to be claimed later in the procedure, and the corresponding claims, namely claims 1-18.

In addition, independent claims 19-22 have been merely stated in terms of a the desired result, without specifying any of the method steps required for coming to said desired result, rendering said claims unclear (Article 6 PCT).

The applicant's attention is drawn to the fact that claims relating to inventions in respect of which no international search report has been established need not be the subject of an international preliminary examination (Rule 66.1(e) PCT). The applicant is advised that the EPO policy when acting as an International Preliminary Examining Authority is normally not to carry out a preliminary examination on matter which has not been searched. This is the case irrespective of whether or not the claims are amended following receipt of the search report or during any Chapter II procedure. If the application proceeds into the regional phase before the EPO, the applicant is reminded that a search may be carried out during examination before the EPO (see EPO Guidelines C-IV, 7.2), should the problems which led to the Article 17(2) declaration be overcome.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/NL2014/000046

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2013246901 A1	19-09-2013	NONE	

WO 2012177253 A1	27-12-2012	CA 2840173 A1	27-12-2012
		WO 2012177253 A1	27-12-2012

US 2004158607 A1	12-08-2004	DE 10346897 A1	26-08-2004
		US 2004158607 A1	12-08-2004
