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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 March 2015 (05.03.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/028339 A1

(51) International Patent Classification:
*G06Q 20/32* (2012.01) *G06Q 20/38* (2012.01)

(21) International Application Number:
PCT/EP2014/067595

(22) International Filing Date:
18 August 2014 (18.08.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13182220.7 29 August 2013 (29.08.2013) EP

(71) Applicant: **KONINKLIJKE PHILIPS N.V.** [NL/NL]; High Tech Campus 5, NL-5656 AE Eindhoven (NL).

(72) Inventors: **BRUEKERS, Alphons Antonius Maria Lambertus**; c/o High Tech Campus 5, NL-5656 AE Eindhoven (NL). **DENG, Mina**; c/o High Tech Campus 5, NL-5656 AE Eindhoven (NL). **GORISSEN, Paulus Mathias Hubertus Mechtildis Antonius**; c/o High Tech Campus 5, NL-5656 AE Eindhoven (NL). **TOLHUIZEN, Ludovicus Marinus Gerardus Maria**; c/o High Tech Campus 5, NL-5656 AE Eindhoven (NL). **SCHEPERS, Hendrik Jan Jozef Hubertus**; c/o High Tech Campus 5, NL-5656 AE Eindhoven (NL).

(74) Agents: **KROEZE, Johannes Antonius** et al.; Philips IP&S, P.O Box 220, NL-5600 AE Eindhoven (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, 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, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

*[Continued on next page]*

(54) Title: MOBILE TRANSACTION DATA VERIFICATION DEVICE AND METHOD OF DATA VERIFICATION

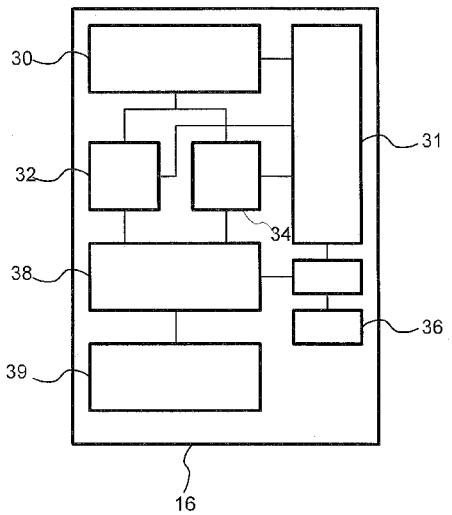


Fig.3

(57) Abstract: A mobile transaction data verification device is provided that can be used by a user to ensure authenticity of information displayed by a terminal during image-based transactions. The mobile transaction data verification device contains a camera for obtaining a captured image of the terminal during a transaction. Furthermore, the mobile transaction data verification device has a visual object recognition module such as an optical character reader, coupled to the camera and a code reader module such as a QR code decoder. An authentication module computes authentication data from a recognition result obtained from the visual object recognition module and a code value obtained from the code reader module, and optionally transaction time distinguishing data. The mobile transaction data verification device signals an authentication result based on the authentication data. Optionally, the mobile transaction data verification may apply its own signature to the captured image and keep it stored to provide evidence that the user verified the transaction data.

WO 2015/028339 A1

**Declarations under Rule 4.17**:

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

**Published**:

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

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

# Mobile transaction data verification device and method of data verification

## FIELD OF THE INVENTION

The invention relates to a mobile transaction data verification device, a data verification system, a method of verifying transaction data, a tangible medium with a computer program for executing the method.

## BACKGROUND

Image-based transactions at terminals, such as ATMs or PCs used for home banking, display information that a user must be able to rely on. The transaction may require a user to enter data that needs to be kept confidential in response to the displayed information. There is a need to protect the reliability of the displayed information against attacks. For example, confidentiality may be compromised by a "man-in-the-middle attack" wherein the user is enticed to accept or decline displayed image content that simulates image content from a lawful counterparty, or to enter confidential data intended for the lawful counterparty in response to the display.

Authentication techniques have been designed to enable detection of such attacks. Image-data authentication provides for proof of the identity of the party that generated an image. US 2012138679 discloses a method of generating an image with a QR code comprising data entangled with biometric data that has been captured from a user. This makes it possible to verify involvement of this user with the creation of the image.

More generally, a basic authentication technique requires the entitled counterparty to provide authentication information with or in a message, using authentication information that is the result of a one way computation from message data and secret information that is available only to the entitled counterparty. The secret information can be biometric data, but more generally it can be any data. A private encryption key is another example. Furthermore, basic authentication technique requires a receiver to compute an authentication result from the message and the authentication information. Known authentication techniques make it possible to do this in a way that ensures that a positive authentication result is only possible if the correct secret information has been used.

In practice, computation of the authentication result is usually performed by the terminal (receiver) that has to display the message, the terminal suppressing message display or adding a warning, if the authentication result is not positive. This means that user security depends on protection against tampering with the terminal that displays the message to the user.

SUMMARY

Among others, it is an object to provide for increased security for user transactions at a transaction terminal with an image display for displaying information such as text.

A mobile transaction-data verification device according to claim 1 is provided. The mobile transaction-data verification device may be a mobile telephone provided with a camera and a computer program to process images from the camera for example. The device provides its user with a verification result signal obtained on the basis of one or more images of the transaction terminal. In support of the device, a transaction generation system makes the transaction terminal transmit a code value for use to authenticate image information such as text displayed on the display of the transaction terminal.

The mobile transaction data verification device uses one or more captured images and the code value to verify that the code corresponds to the object or objects displayed on the display of the transaction terminal.

The mobile transaction data verification device comprises a camera for obtaining a captured image during a transaction and a visual object recognition module coupled to the camera for obtaining a recognition result from the captured image, and optionally further images captured during the transaction, for example by means of optical character recognition. Furthermore the mobile transaction data verification device comprises a code reader module for obtaining the code value and an authentication module configured to compute authentication data from the recognition result and the code value. The authentication data serve to ensure that data such as stated amount of money is correct (data authentication) and/or that the data is from the source that it pretends to be from (data origin authentication, also known as entity authentication). The mobile transaction data verification device uses a sound, video, vibration, a transmitted message or other output to signal an authentication result to the user based on the authentication data. In this way the mobile transaction data verification device supports a form of authentication beyond the reach of

those who might have tampered with the transaction terminal or a part of the transaction generation system behind the transaction terminal.

In an embodiment the code reader module is a visual code reader module coupled to the camera. In this embodiment the code value may be decoded by the visual code reader module being configured to decode from said captured image or a further image captured during the transaction. Thus, no additional input is necessary and the possibility of tampering with a separate code value channel is avoided. In other embodiments, the code value may be transmitted from the transaction terminal as a separate signal, for example in a Bluetooth message.

In an embodiment the object recognition and the code value are determined from the same image. This requires a minimum of image data. In another embodiment the recognition result is determined from a plurality of successively captured images in a time interval, such as video data, and the code value may be determined dependent on an image captured during the time interval. In this way time dependent output at the transaction terminal may be verified.

In an embodiment, to prevent replay attacks the code value may depend on session identifying data. The session identifying data may be transaction time distinguishing data such as a clock time value during the transaction or audio, video, movement and/or force signals produced by the user during the transaction. In an embodiment, the authentication module is configured to obtain the transaction time distinguishing data on the basis of a clock time during the transaction. In this way a simple time stamp can be obtained. In a further embodiment the device may comprise a clock circuit to provide the time. In another embodiment the mobile transaction data verification device may comprise an audio, video, movement and/or force input for obtaining the transaction time distinguishing data. Thus, the user may provide the transaction time distinguishing data by making a sound during the transaction, directing the camera at an object, such as the user's person, moving the device in an arbitrary manner or exerting an arbitrary time-dependent force on the device. Data based on observation of such input may be used in the transaction generation system, i.e. the source system that generates the code value, for generation of the code value in the mobile transaction data verification device to authenticate the displayed information. A separate input device may be used to obtain such data, but preferably the mobile transaction data verification device inputs the data and transmits it to the transaction generation system for generation of the code value.

In an embodiment a mobile transaction data verification device according to any of the claims is provided with a control circuit configured to cause data representing the captured image to be kept stored after the transaction. This may be done at least partly in response to the result of authentication for example. Thus authenticated data is kept for later retrieval, for example to serve as evidence that the user had a right to rely on the displayed information. Preferably, the mobile transaction data verification device is configured to generate further authentication data, tied to the captured image and the time of the transaction. In this way, the stored information is made more robust as evidence that the user had a right to rely on the displayed information.

In an embodiment a method of providing data verification during a user transaction at a user terminal is provided, using a mobile transaction data verification device, the method comprising the following steps executed by the mobile transaction data verification device:

- capturing an image of at least part of a display screen of the user terminal with a camera of the mobile transaction data verification device;
- applying a visual object recognition operation such as optical character recognition to the captured image;
- obtaining a code value, for example from the captured image;
- computing authentication data from a recognition result obtained from the visual object recognition operation, transaction time distinguishing data such as clock time information, and the code value;
- rendering a signal to the user dependent on an authentication result derived from the authentication data. In an embodiment a representation of the captured image and/or the authentication data are stored dependent on the authentication result. This information thereby made available as evidence of the transaction with valid authentication.

The image for applying the visual object recognition operation may be captured for example in response to a user command to perform the verification, or the user may shoot the image before entering the user command. The user may direct the camera to the transaction terminal before entering this command, e.g. by pressing a snapshot button. In another embodiment, the method comprises capturing data representing successive images; testing whether the successive images show indicia that indicate that at least one of the successive images shows at least part of a display screen; and if so using the at least one of the successive images as the captured image in said step of applying the visual object recognition operation. Thus user control of direction of the mobile device is less critical.

In another aspect, a transaction generation system is provided, comprising a message data generator system, and a transmitter for transmitting transaction data based on message data from the message data generator system to a transaction terminal, the transaction generation system comprising

- an authentication data generator configured to generate a code value from message data for transmission of the code value to a mobile transaction data verification device,

- an image data generator (106) configured to generate image data representing an image comprising visual objects, such as text characters, representing the message data, the transmitter (108) being configured to include the image data in the transmitted transaction data.

For example, the authentication data generator is configured to generate the code value from message data in dependence on session identifying data.

## BRIEF DESCRIPTION OF THE DRAWING

These and other objects and advantageous effects will become apparent from a description of exemplary embodiments with reference to the following figures.

Figure 1 shows a transaction processing system

Figure 2 shows a flow chart of a message generation process

Figure 3 shows a mobile transaction data verification device

Figure 4 shows a flow-chart of transaction data verification

## DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

Figure 1 shows a transaction processing system comprising a source system 10, a network 12, a user transaction terminal 14 and a mobile data verification device 16. Source system 10 is coupled to user transaction terminal 14 via network 12.

Source system 10 comprises a message data generator system 100, a clock circuit 102, an authentication data generator 104, an optional image data generator 106 and a transmitter 108. Authentication data generator 104 has inputs coupled to outputs of message data generator system 100 and clock circuit 102. Image data generator 106 has inputs coupled to the output of message data generator system 100 and an output of authentication data generator 104. Image data generator 106 has an output coupled to network 12 via transmitter 108.

User terminal 14 comprises a transceiver 140, an image controller 142, a display screen 144, a user entry keypad 148 and a processor 146. Image controller 142 has an input coupled to transceiver 140 and an output coupled to display screen 144. Processor 146 has an input/output interface coupled to transceiver 140 and an input coupled to user entry keypad 148.

In operation, the transaction processing system processes an image based transaction wherein image data from source system 10 is used at user terminal 14. In an image based transaction, a human user needs to be able to rely on the authenticity of displayed image information, because the user may need to commit him or herself relying on that information.

As used herein, an image based transaction is a process wherein information is supplied to a human user by means of display of image information. Examples of image based transactions are a cash withdrawal transaction, a transaction for ordering goods or services in return for payment, but also unilateral transactions that give a user a right to rely on the displayed information such as display of a credit amount, or approval to undertake a user action.

The image based transaction comprises steps of reception and display of image data at a terminal. In addition to image display, the image based transaction may further comprise an action such as entry of transaction data into a database and/or delivery of a service or product (e.g. cash, beverage etc). Hence the image based transaction may comprise a subsequent step of detection of a user response at the terminal, such as entry of user data at the terminal for performing the action dependent on the entered user data. Herein at least a part of the action may be performed by the terminal (e.g. delivery of cash) and/or the terminal may transmit transaction data that causes at least part of the action to be performed elsewhere.

Figure 2 shows a flow chart of an exemplary message generation process executed by source system 10. In a first step 21, message data generator system 100 generates basic message data. This may include data for use in a financial transaction for example. In a second step 22, authentication data generator 104 samples a time stamp from clock circuit 102. In a third step 23, authentication data generator 104 generates authentication data from the basic message data and the time stamp. The time stamp is used to make replay attacks difficult. The use of a time stamp may be omitted for example if replay attacks are not a problem. Although an example is given wherein a time stamp is used to address replay attacks, it should be appreciated that other data may be used that is tied to

the time of the transaction. More generally, if replay attacks are a problem, any other type of session identifying data may be used, such as a session ID. In another embodiment source system 10 may provide for information that defines predetermined successive session IDs, and authentication data generator 104 may be configured to use a first unused session ID.

The authentication data may serve to ensure that data is correct (data authentication) and/or that the data is from the source that it pretends to be from (data origin authentication, also known as entity authentication). Any known algorithm may be used for generating authentication data. Message authentication is well known in the art and is for example discussed in Chapters 11 and 12 of "Cryptography and Network Security – Principles and Practices", 4-th edition by W. Stallings, Pearson-Prentice Hall, 2006. The methods include message authentication based on hash functions, on the DES algorithm, and on SHA-512. Authentication data generator 104 may generate a signature of the basic message data and optionally the session identifying data using a private encryption key for example. In a simple example, the concatenation of the symbols from the basic message data and a time stamp is used as a number M. In this embodiment authentication data generator 104 may generate authentication data V according to V = (a*M+ b) mod p. Herein "mod" is the modulo operation, p is a prime number, and a and b are randomly selected integer numbers with "a" and "b" unequal to zero and "a" unequal to one mod p. The larger the prime number "p", the more robust the authentication. It should be emphasized that this is only one example of generation of authentication data: many others may be used, for example algorithms using a private encryption key of source system to encrypt data computed from the symbols from the basic message data and the time stamp.

In a fourth step 24, transmitter 108 transmits the basic message data and the authentication data to user terminal 14 via network 12. In one example, the authentication data generator is configured to select authentication data such that the application of a predetermined authentication computation to the combination of the basic message data and the authentication data will yield a predetermined result.

Optionally, the basic message data and the authentication data may be transmitted as image data. In this case an optional fifth step 25 is executed before fourth step 24, wherein optional image data generator 106 generates image data based on the basic message data and the authentication data. Although an exemplary embodiment will be described in terms of an image, it should be appreciated that instead a series of images (video data) may be used. In the exemplary embodiment, the image data defines an image, for example in terms of a collection of pixel values for respective locations in the image. The

pixel values may be encoded in any known way, for example as a BMP file, a GIF file, a JPEG file or part of an MPEG stream. Any other type of image representation may be used.

In an embodiment, image data generator 106 may be configured to represent text characters in the image dependent on symbols from the basic data message. Furthermore, image data generator 106 is configured to include a machine readable a code in the image, which represents the authentication data in the image. The image data generator 106 may generate a QR code image part or a bar code image part for example. The text characters and the code may be represented in mutually different image parts respectively. But in other embodiments overlapping representations may be used, or the information may be displayed on different display screens. In a sixth step 26, transmitter 108 transmits the image data from image data generator 106 to user terminal 14 via network 12.

Image controller 142 receives the basic message data and the authentication data. or the image data, via transceiver 140 and controls display screen 144 dependent on the data. When only basic message data and the authentication data are sent, image controller 142 generates the image instead of image data generator 106. Although an exemplary embodiment will be described in terms of an image, it should be appreciated that instead a series of images (video data) may be used. After a start of display of the image data processor 146 receives user input from user entry keypad 148 and uses this data to generate a response message for transmission via network 12.

In an embodiment, mobile data verification device 16 may be a mobile telephone programmed with special program code to perform data verification. The program code may be configured to make a processing system of the mobile telephone perform the functions of a control module, a visual object recognition module, a visual code reader module and an authentication module.

Figure 3 shows a functional diagram of mobile data verification device 16. The device comprises a camera 30, a control module 31, a visual object recognition module 32, a visual code reader 34 module, a clock circuit 36, an authentication module 38, and a signal output device 39. Signal output device 39 may comprise a display screen or an audio output device for example. Camera 30 may comprise a memory for storing data representing a captured image. Additionally or alternatively, control module 31 may be configured to communicate information representing the captured image to a storage system, such as a storage device at home, or in a network. Control module 31 has an input coupled to camera 30 and outputs coupled to visual object recognition module 32 and visual code reader module 34. When QR codes are used, visual code reader 34 module may be a QR code reader module

for example. Control module 31, visual object recognition module 32 and visual code reader module 34 may be implemented using one or more programmable processors and program modules to make the one of more processors perform their functions, in which case the connections between the modules represent data and control exchange. Authentication module 38 has inputs coupled to visual object recognition module 32, code reader module 34 and clock circuit 36. Authentication module 38 has an output coupled to signal output device 39. QR code reading algorithms and other code reading algorithms are known per se and may involve determining the location and/or size of relatively lighter and darker areas in the image and computing or looking up a code value from these locations and or size. Similarly, visual object recognition algorithms are known per se and they may involve optical character recognition (OCR) for example. Similarly, authentication algorithms are known per se and they may involve computing a check value from data that must be authenticated and comparison of the check value with a reference value.

In operation, the user may direct camera 30 at display screen 144 of user terminal 14 in order to obtain an authentication of image data shown on that display screen 144. Based on the image, mobile data verification device 16 provides user feedback on the authenticity of the image.

Figure 4 shows a flow-chart of generation of user feedback on the authenticity of image by mobile data verification device 16. In a first step 41, control module 31 receives a command to perform authentication. In a second step 42 control module 31 captures image data from camera 30. In an embodiment, this step may be performed after waiting for a separate user command to capture the image. In this embodiment second step 42 may also be performed before first step 41. When no separate user command is used to capture the image, the image may be captured effectively in response to the user command of first step 41.

This may lead to problems if the camera is not directed at the screen at the time of the command. In an embodiment shown in figure 4, images may be captured without specific user commands to capture the images. In this embodiment control module 31 performs a third step 43, of testing whether the image represented by the data contains locations showing a display screen. In an embodiment wherein the image shown by display screen 144 contains a QR code, visual code reader is a QR code reader and control module 31 may feed the image data to this QR code reader and obtain a QR code location detection from that QR code reader to detect whether the image represented by the data contains locations showing a display screen including the QR code. Alternatively, control module 31 may use other ways to do so. For example, fiducia marks may be provided in user terminal 14 or in

the displayed image and control module 31 may be configured to detect the fiducia marks. Control module 31 may repeat second and third step 42, 43 until it detects that the image represented by the data contains locations showing a display screen, optionally timing out if this does not occur within a predetermined time period.

If a user command is used to select the time of capturing the image, or if control module 31 detects that the image represented by the data contains locations showing a display screen in third step 43, control module 31 causes visual object recognition module 32 to perform a fourth step 44, wherein object recognition is applied to image data for the location of the display screen. Optical character recognition may be applied for example, which produces text data representing text, such as a sequence of text characters, numbers and/or words recognized in the image data.

Furthermore, control module 31 causes visual code reader 34 to perform a fifth step 45, wherein a code such as a QR code is read from the image data for the location of the display screen. In a sixth step 46, control module 31 causes a time stamp from clock circuit 36 to be sampled, for example in a register.

In a seventh step 47 authentication module 38 applies an authentication computation to the object recognition output from visual object recognition module 32 (e.g. one or more detected character strings), a code value read by visual code reader 34 and the time stamp. The authentication computation of seventh step 47 corresponds to algorithm that is used by authentication data generator 104. Of course, use of the time stamp may be omitted if source system 10 does not use it, or other session identifying data may be used when source system 10 uses that. When session IDs are used, mobile data verification device 16 may store information to indicate what the current session ID may be.

Message authentication verification is well known in the art and is for example discussed in Chapters 11 and 12 of "Cryptography and Network Security – Principles and Practices", 4-th edition by W. Stallings, Pearson-Prencice Hall, 2006. The methods include message authentication based on hash functions, on the DES algorithm, and on SHA-512. For example, a signature may be verified using the public key corresponding to a private key used by authentication data generator 104 to generate the signature. In one example, if the authentication data V was generated according to $V = (a*M+ b) \bmod p$, authentication module 38 may use the concatenation of the symbols obtained from the object recognition of fourth step 44, and the time stamp as a number M'. In this embodiment authentication module 38 computes $(a*M'+ b) \bmod p$ using values of a, b and p that it has for the source system 10 and returns a positive authentication result only if a code value V obtained in fifth

step 45 equals (a*M'+ b) mod p. If another algorithm was used to generate of authentication data, a correspondingly different computation may be used. For example, this may involve decryption using a public encryption key of source system 10 and/or computations using the symbols obtained from the object recognition of fourth step 44, and the a time stamp from the basic message data and the time stamp. Authentication may comprise applying a predetermined authentication computation (e.g. a one-way computation) to the combination of the basic message data and the authentication data yields, and testing that this results in a predetermined value.

In an eight step 48, control module 31 tests whether authentication module 38 has produced a positive authentication result. If so, control module 31 makes signal output device 39 output a first signal in ninth step 49. The first signal may be a predetermined audio signal for example, or a rendition of a predetermined image (e.g. an image showing a green field). If not, control module 31 makes signal output device 39 output no signal, or a second, perceptibly different signal.

Based on the output signal, the user may then decide whether to continue with the transaction, for example by entering the user input on user entry keypad 148 or not.

In a further embodiment, control module 31 causes data derived from the image data to be kept stored for retrieval after completion of the transaction, for example in a non-volatile memory (not shown) in mobile data verification device 16 or, via a communication channel, in a remote storage device. That is, the data is not merely kept stored for use during the transaction but it is kept for an indefinite amount of time, or at least for a predetermined time period such as at least a week or at least a month. The data may be used as evidence that the user has verified the transaction when using the mobile data verification device 16.

In an embodiment control module 31 generates further authentication data from the image data and a time stamp for the time of the transaction or, instead of the time stamp, the other data that is tied to the time of the transaction, such as the data that was used for this purpose by authentication data generator 104. In an embodiment the time stamp or other data may be an authenticated part of the image. In this case no separate time information is needed.

The control module 31 may compute an electronic signature of the mobile transaction data verification device for the data derived from the image and the data that is tied to the time of the transaction for example. Alternatively control module 31 may send the image data to a trusted third party server. In this embodiment the trusted third party server

may generate the further authentication data from the image data and a time stamp, or the other data that was used for this purpose by authentication data generator 104. The further authentication data may serve as evidence that the data derived from the image data has not been tampered with. Preferably, control module 31 is configured to cause the data to be kept at least partly in response to detection of a positive authentication result in eight step 48. Storing and generation of further authentication data may be part of ninth step 49.

The data derived from the image data may be the image data itself, or other data that represents the image represented by the image data or a part of it that is sufficient to perform the verification. In this embodiment the data that is kept stored may be used by the user as evidence of the transaction that was performed. The authentication information in the stored data may serve as evidence that the user has not generated or modified the data. The verification by control module 31 informs the user that this evidence is valid and in addition it may be used to select the image data that should be kept stored.

Although an example has been described wherein a time stamp is used, it should be appreciated that other data may be used that is tied to the time of the transaction. Any information may be used that is not known in advance of the transaction time. For example, mobile data verification device 16 may generate and display arbitrary data for this purpose, the user entering the displayed data into user terminal 14 at the time of the transaction for use instead of, or in addition to the time stamp. Instead the user may select the arbitrary data and enter it into the mobile data verification device 16 as well. Instead of entered data, audio, visual or tactile data captured by mobile data verification device 16 and source terminal 14 at the time of the transaction may be used. For example, detection of timing and/or signal data of a sound produced by the user may be used, or of an image supplied by the user, or of video showing gestures that the user shows both to mobile data verification device 16 and a camera (not shown) of user terminal 14, or a temporal pattern of detected touches of mobile data verification device 16 against user terminal 14.

Although an exemplary embodiment using an image has been described, it should be appreciated that instead a series of images may be used. In this case, the object recognition of fourth step 44 may be applied to the series of images, for example to recognize characters of successively different text messages that are displayed successively. Accordingly, the characters of the text message may be used both in the source system and mobile data verification device 16 in the authorization computations.

Although an exemplary embodiment using character recognition has been described, it should be appreciated that instead or in addition other types of object

recognition may be used. For example, symbols indicating properties (e.g. colors, shape elements) of a image part shown in the image may be used to compute the authorization code in source system 10, and in mobile data verification device 16, the former relying on properties used to control display of the logo and the latter using properties of a logo determined from the camera image captured by mobile data verification device 16.

In a further embodiment properties of audio data symbols indicating audio data (e.g. successive spoken words) may additionally be used to compute the authorization code in source system 10 and in mobile data verification device 16. The former may rely on the properties used to control speech output at user terminal 14 and the latter may use speech recognition results determined from audio captured by mobile data verification device 16. These may be used in addition to image properties such as displayed characters.

Other variations to the disclosed embodiments can be understood and effected by those skilled in the art in practicing the claimed invention, from a study of the drawings, the disclosure, and the appended claims. In the claims, the word "comprising" does not exclude other elements or steps, and the indefinite article "a" or "an" does not exclude a plurality. A single processor or other unit may fulfill the functions of several items recited in the claims. The mere fact that certain measures are recited in mutually different dependent claims does not indicate that a combination of these measured cannot be used to advantage. A computer program may be stored / distributed on a suitable medium, such as an optical storage medium or a solid-state medium supplied together with or as part of other hardware, but may also be distributed in other forms, such as via the Internet or other wired or wireless telecommunication systems. Any reference signs in the claims should not be construed as limiting the scope.

CLAIMS:

1. A mobile transaction data verification device, comprising

- a camera (30) for obtaining image data during a transaction;

- a visual object recognition module (32) for recognizing one or more visual objects from the image data;

- a code reader module (34);

- an authentication module (38) configured to compute authentication data from

- a recognition result obtained by the visual object recognition module (32), and

- the code value obtained by the code reader module (34); and

- a signaling unit (39) configured to signal an authentication result based on the authentication data;

wherein the visual object recognition module (32) comprises an optical character recognition module, the visual object recognition module (32) being configured to provide recognition results, comprising text data recognized from an image from the camera (30), to the authentication module (38).

2. A mobile transaction data verification device according to claim 1, wherein the code reader module (34) is a visual code reader module (34) coupled to the camera (30), the visual code reader module (34) being configured to decode the code value from said image data.

3. A mobile transaction data verification device according to claim 1, wherein the visual object recognition module (32) is configured to determine the recognition result from a plurality of successive images captured in a time interval and the visual code reader module (34) is configured to determine the code value at least dependent on one of the images captured in that time interval.

4. A mobile transaction data verification device according to claim 1, wherein the visual code reader module (34) comprises a bar code or QR code decoder, the visual code reader module (34) being configured to provide code values comprising a bar code value or QR code value decoded from an image from the camera (30) to the authentication module (38).

5. A mobile transaction data verification device according to claim 1, wherein

- the authentication module (38) is configured to obtain session identifying data, and to compute authentication data from

- the recognition result obtained by the visual object recognition module (32),

- the session identifying data and

- the code value obtained by the code reader module (34).

6. A mobile transaction data verification device according to claim 5, comprising an audio, video and/or force input, wherein the authentication module (38) is configured to obtain the session identifying data on the basis of transaction time distinguishing data determined from a signal from the audio, video, movement and/or force input during the transaction.

7. A mobile transaction data verification device according to claim 6, comprising a transmitter (108) configured to transmit data obtained from the signal from the audio, video, movement and/or force input to a source system (10) for generating the image data.

8. A mobile transaction data verification device according to claim 7, comprising a control module (31) configured to cause generation of further authentication data based on captured image and the transaction time distinguishing data or further transaction time distinguishing data, and to cause data representing the captured image and the further authentication data to be kept stored after the transaction.

9. A method of providing data verification during a user transaction at a user terminal (14), using a mobile transaction data verification device (16), the method comprising the following steps executed by the transaction data verification device (16):

- capturing (42) an image of at least part of a display screen of the user

terminal with a camera (30) of the mobile transaction data verification device (16);

- applying a visual object recognition operation (44) comprising optical character recognition to the captured image;

- obtaining a code value (45);

- computing authentication data (47) from a recognition result obtained from the visual object recognition operation and the code value;

- rendering (49) a signal to the user dependent on an authentication result derived from the authentication data.

10. A method according to claim 9, wherein the step of obtaining the code value (45) comprises obtaining the code value by applying a visual code reading operation to the captured image or a further image from a captured series of images captured during a time interval that includes a time of capturing the captured camera image.

11. A method according to claim 9, comprising the following steps executed by the transaction data verification device (16):

- capturing data representing successive images;

- testing (43) whether the successive images show indicia that indicate that at least one of the successive images shows at least part of a display screen; and if so

- using the at least one of the successive images as the captured image in said step of applying the visual object recognition operation.

12. A computer program product comprising instructions for a programmable computer system that, when executed by the programmable computer system will make the programmable computer system execute the method of any one of claims 9 to 11.

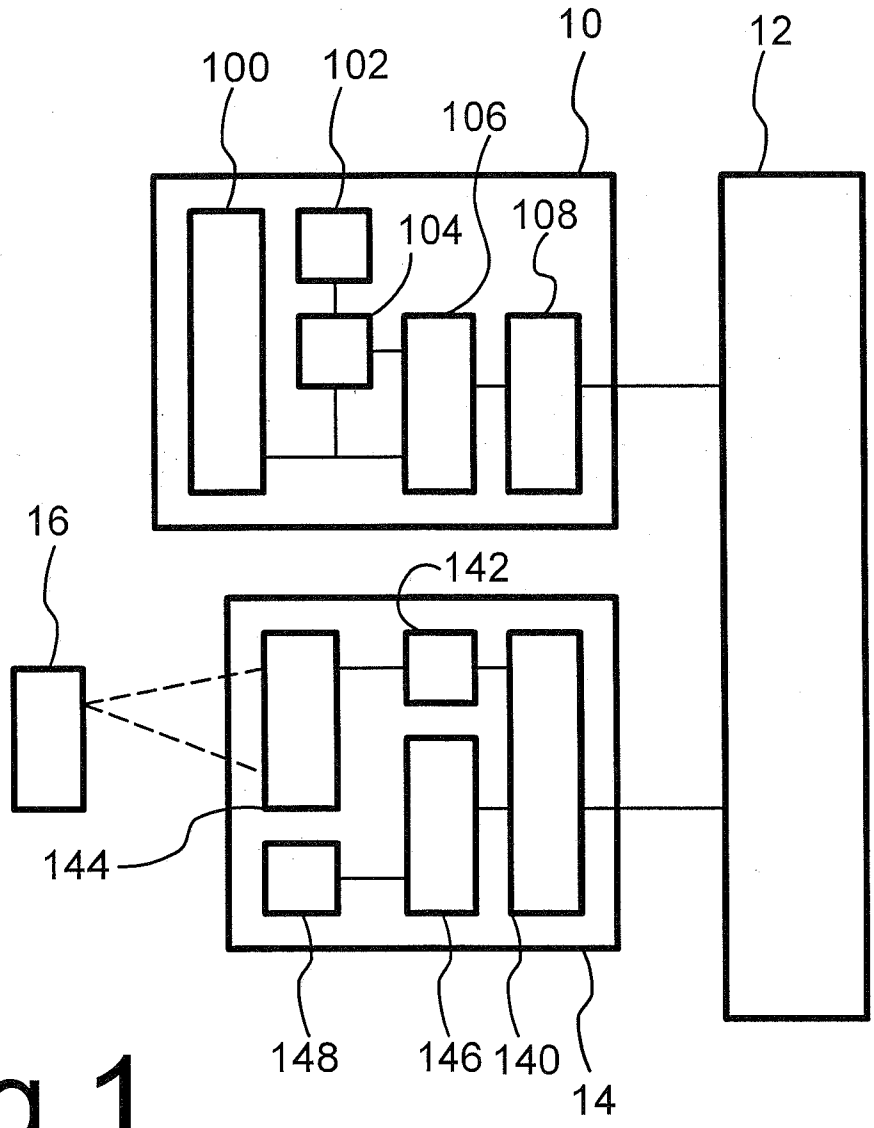


Fig.1

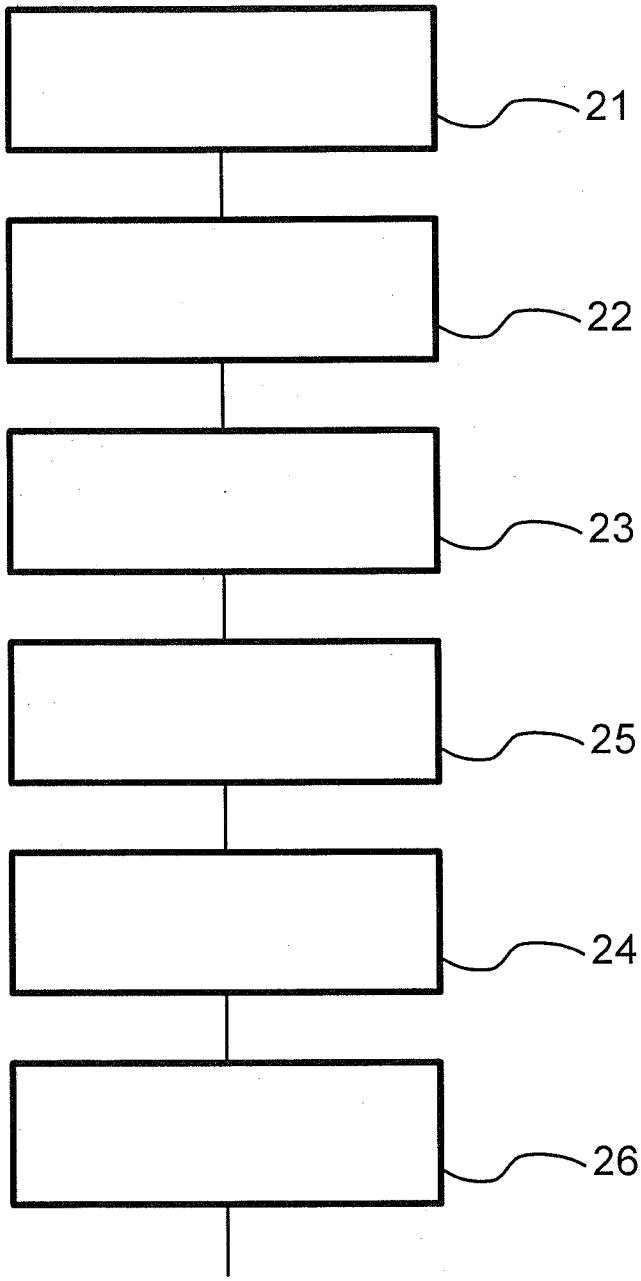


Fig.2

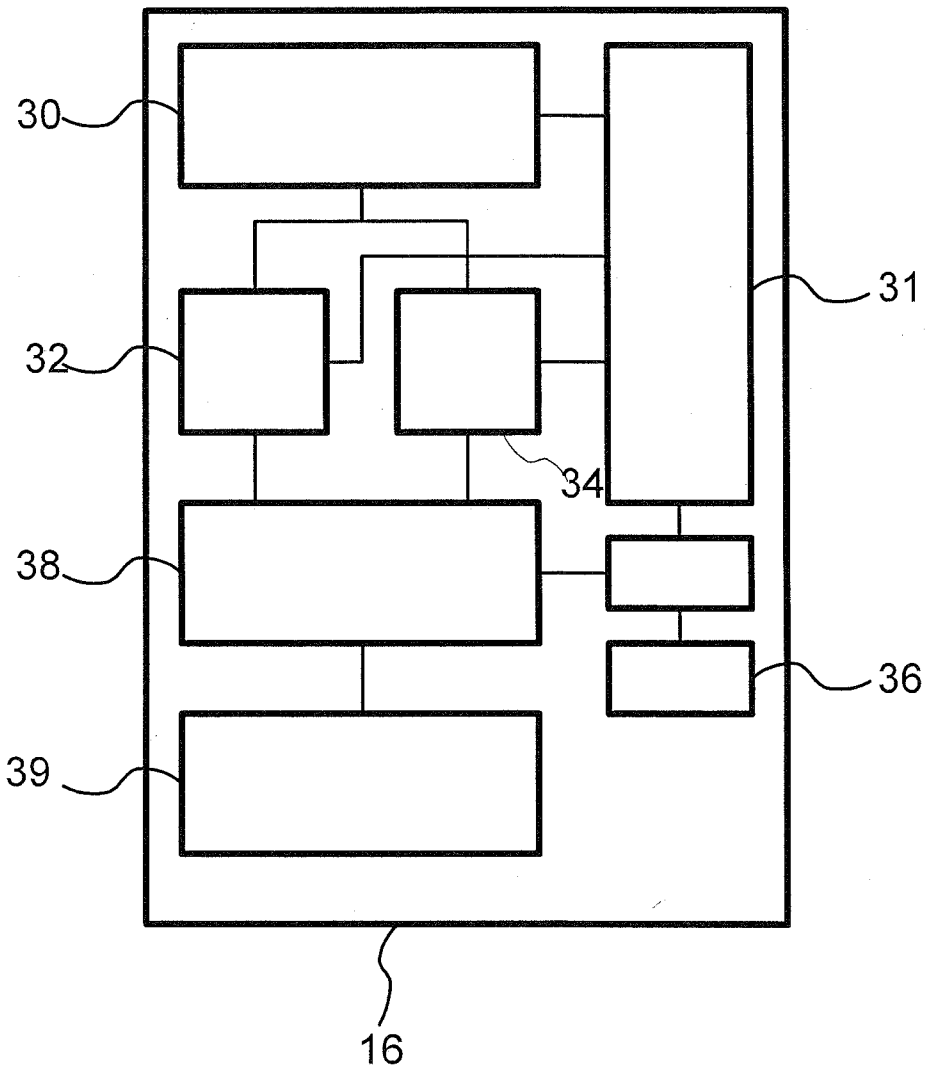


Fig.3

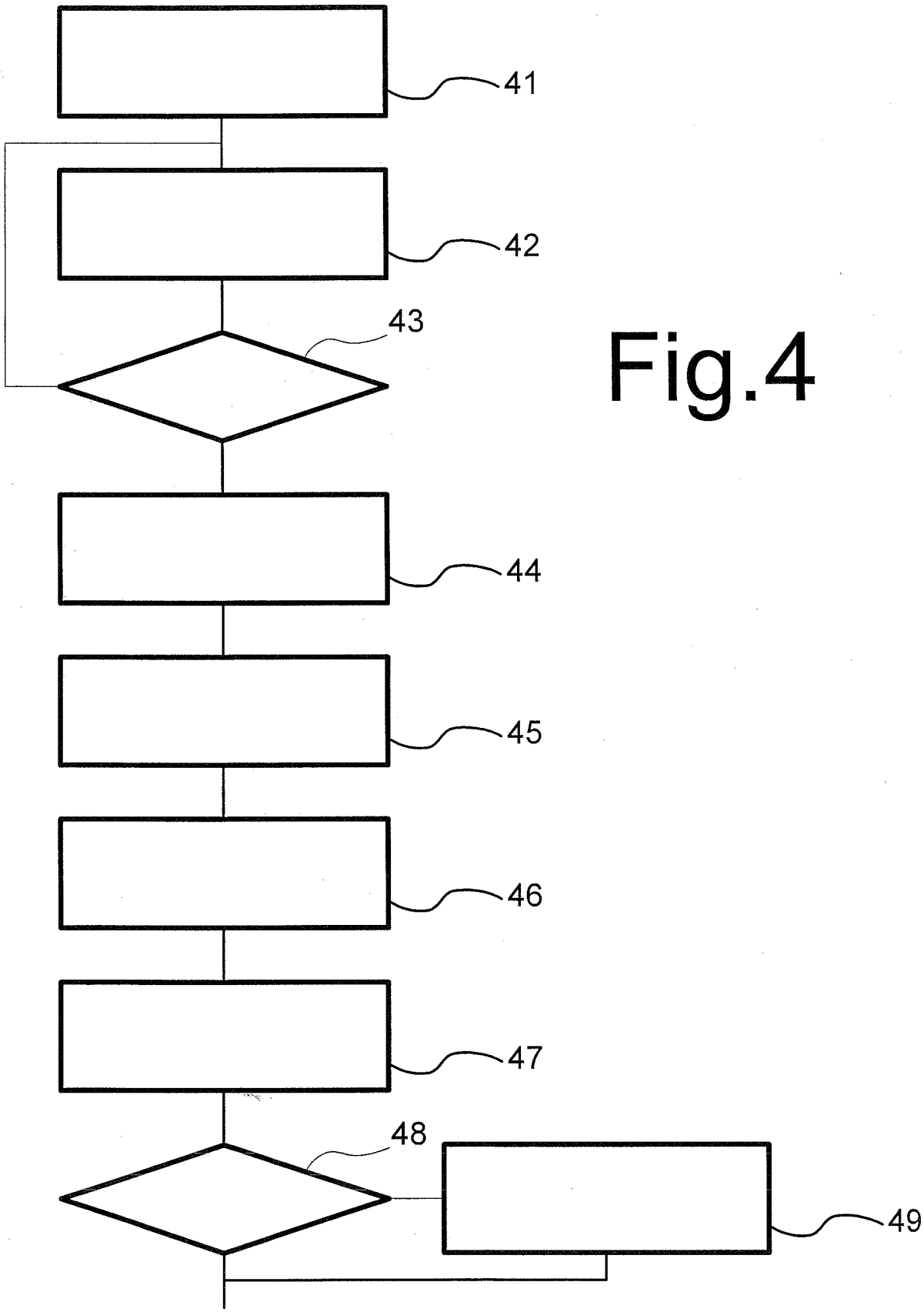


Fig.4

# INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2014/067595

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q20/32 G06Q20/38
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)
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. |
|---|---|---|
| Y | US 2012/308003 A1 (MUKHERJEE ANIRBAN [IN])<br>6 December 2012 (2012-12-06)<br>abstract; claims 1,8,11-17; figures 1, 7<br>paragraph [0051] - paragraph [0057]<br>----- | 1-12 |
| Y | EP 2 424 282 A1 (ALTER CORE S L [ES])<br>29 February 2012 (2012-02-29)<br>paragraph [0037]; claim 1; figures 1-15<br>----- | 1-12 |
| Y | WO 2011/147433 A1 (SWISS TECHNICAL ELECTRONICS STE HOLDING AG [LI]; LOCHER JOHANN KASPAR)<br>1 December 2011 (2011-12-01)<br>page 23, line 15 - page 26, line 22; figure 3<br>----- | 1-12 |

-/--

[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 |
|---|---|
| 7 January 2015 | 14/01/2015 |

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

1

Form PCT/ISA/210 (second sheet) (April 2005)

# INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2014/067595

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | US 2012/087551 A1 (BHAGWAN VARUN [US] ET AL) 12 April 2012 (2012-04-12) abstract | 1-12 |
| Y | GB 2 392 291 A (NEC CORP [JP]) 25 February 2004 (2004-02-25) abstract | 1-12 |
| Y | WO 2008/129373 A2 (NOKIA CORP [FI]; SCHLOTER C PHILIPP [US]; GAO JIANG [US]) 30 October 2008 (2008-10-30) abstract | 1-12 |
| A | US 2011/108622 A1 (DAS PRADEEP K [US] ET AL) 12 May 2011 (2011-05-12) paragraph [0076] - paragraph [0084]; claims 1,2; figures 1-17 | 1-12 |
| A | KR 2012 0109424 A (INHA IND PARTNERSHIP INST [KR]) 8 October 2012 (2012-10-08) paragraph [0001] - paragraph [0120] | 1-12 |
| A | WO 2012/142740 A1 (EGONEXUS LTD [CN]; MAEVSKY DMITRY [JP]) 26 October 2012 (2012-10-26) page 7 - page 19; figures 2-4a | 1-12 |
| A | WO 2013/050738 A2 (BARCLAYS BANK PLC [GB]) 11 April 2013 (2013-04-11) abstract | 1-12 |
| A | WO 03/049007 A1 (INT BARCODE CORP [US]; LUBOW ALLEN [US]) 12 June 2003 (2003-06-12) claims 1-20 | 1-12 |
| A | EP 2 506 204 A1 (RESEARCH IN MOTION LTD [CA]) 3 October 2012 (2012-10-03) abstract | 1 |

1

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2014/067595

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 2012308003 A1 | 06-12-2012 | NONE | |
| EP 2424282 A1 | 29-02-2012 | AR 076339 A1 | 01-06-2011 |
| | | AU 2010240822 A1 | 08-12-2011 |
| | | CA 2759414 A1 | 28-10-2010 |
| | | CN 102461229 A | 16-05-2012 |
| | | EP 2424282 A1 | 29-02-2012 |
| | | ES 2381293 A1 | 24-05-2012 |
| | | JP 5592477 B2 | 17-09-2014 |
| | | JP 2012524493 A | 11-10-2012 |
| | | KR 20120017044 A | 27-02-2012 |
| | | RU 2011147154 A | 27-05-2013 |
| | | US 2012096277 A1 | 19-04-2012 |
| | | UY 32564 A | 29-10-2010 |
| | | WO 2010122190 A1 | 28-10-2010 |
| WO 2011147433 A1 | 01-12-2011 | SG 186863 A1 | 28-02-2013 |
| | | US 2013087612 A1 | 11-04-2013 |
| | | WO 2011147433 A1 | 01-12-2011 |
| US 2012087551 A1 | 12-04-2012 | US 2012087551 A1 | 12-04-2012 |
| | | US 2014226878 A1 | 14-08-2014 |
| GB 2392291 A | 25-02-2004 | CN 1486115 A | 31-03-2004 |
| | | GB 2392291 A | 25-02-2004 |
| | | JP 4123473 B2 | 23-07-2008 |
| | | JP 2004080442 A | 11-03-2004 |
| | | US 2004046745 A1 | 11-03-2004 |
| WO 2008129373 A2 | 30-10-2008 | CN 101743541 A | 16-06-2010 |
| | | EP 2156334 A2 | 24-02-2010 |
| | | KR 20100007895 A | 22-01-2010 |
| | | US 2008267504 A1 | 30-10-2008 |
| | | US 2012027301 A1 | 02-02-2012 |
| | | WO 2008129373 A2 | 30-10-2008 |
| US 2011108622 A1 | 12-05-2011 | NONE | |
| KR 20120109424 A | 08-10-2012 | NONE | |
| WO 2012142740 A1 | 26-10-2012 | CN 103477372 A | 25-12-2013 |
| | | JP 2014512058 A | 19-05-2014 |
| | | US 2014025582 A1 | 23-01-2014 |
| | | WO 2012142740 A1 | 26-10-2012 |
| WO 2013050738 A2 | 11-04-2013 | AU 2012320281 A1 | 22-05-2014 |
| | | CA 2850942 A1 | 11-04-2013 |
| | | EP 2774344 A2 | 10-09-2014 |
| | | GB 2495474 A | 17-04-2013 |
| | | GB 2495571 A | 17-04-2013 |
| | | US 2014250512 A1 | 04-09-2014 |
| | | WO 2013050738 A2 | 11-04-2013 |
| WO 03049007 A1 | 12-06-2003 | AT 440337 T | 15-09-2009 |
| | | AU 2002351216 A1 | 17-06-2003 |
| | | CN 1618077 A | 18-05-2005 |
| | | EC SP045170 A | 26-11-2004 |
| | | EC SP085170 A | 28-04-2008 |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2014/067595

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| | | EP 1461760 A1 | 29-09-2004 |
| | | HK 1067215 A1 | 30-10-2009 |
| | | JP 2005512371 A | 28-04-2005 |
| | | KR 20040085137 A | 07-10-2004 |
| | | MX PA04005216 A | 01-07-2005 |
| | | US 2005072846 A1 | 07-04-2005 |
| | | WO 03049007 A1 | 12-06-2003 |
| EP 2506204 A1 | 03-10-2012 | CA 2772821 A1 | 29-09-2012 |
| | | EP 2506204 A1 | 03-10-2012 |