

(51) International Patent Classification:
G06F 21/32 (2013.01)(21) International Application Number:
PCT/GB2016/052363(22) International Filing Date:
29 July 2016 (29.07.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1509478.2 2 June 2015 (02.06.2015) GB

(72) Inventor; and

(71) Applicant : AYRES, Stuart [GB/GB]; Jacaranda, La Grande Cloture, Portinfer Road, Vale, Vale, Guernsey GY6 8LJ (GB).

(74) Agent: STANLEY, David; Gainsborough House, 2 Sheen Road, Richmond, Surrey TW9 1AE (GB).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR,

KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

- with international search report (Art. 21(3))
- 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))
- with information concerning request for restoration of the right of priority in respect of one or more priority claims (Rules 26bis.3 and 48.2(b)(vii))

(54) Title: IMPROVEMENTS IN OR RELATING TO THE VERIFICATION OF PERSONAL IDENTITY

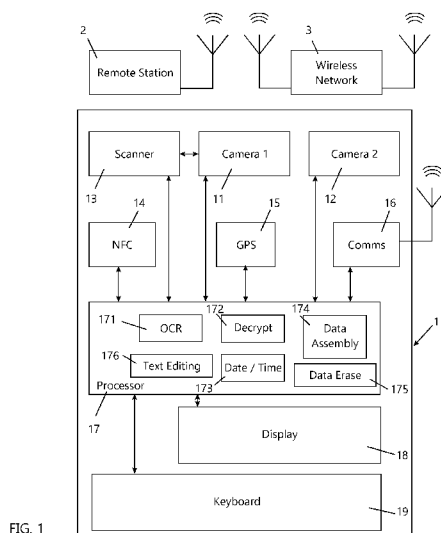


FIG. 1

(57) **Abstract:** A device comprises means for entering unique identifying text from a personal ID document and an NFC reader that reads encrypted biometric data from the document. A decryption application decrypts the biometric data, utilising the unique identifying text. A camera captures an image of the face of a user. A date and time application records the date and time when a user uses the device to capture data. A data assembly application assembles together the unique identifying text, decrypted biometric data, captured image, and recorded date and time data. The device communicates with a remote station via a communication system. For a verification task, a user enters the unique identifying text; places the device adjacent the ID document such that the NFC reader reads the biometric data; activates the camera to capture an image of the face of the user; and activates the communication system to transmit to a remote station all of the assembled data.

- 1 -

IMPROVEMENTS IN OR RELATING TO THE VERIFICATION OF PERSONAL IDENTITY

The present invention relates to methods of and devices for use in verifying personal identity.

5 The current state of the art in the field of regulating financial services relies upon a number of factors. One such factor is jurisdiction. For example, companies registered in Guernsey are required to abide by the regulations and rules administered by the Guernsey Financial Services Commission. Other regulatory bodies may have different rules and regulations. However, in all of the
10 rules and regulations of all regulatory bodies, there is a fundamental requirement to verify the identity of an individual.

 This typically requires sight of original documentation (usually a list of acceptable documents is available, but these typically need to include a photograph). If original documentation as proof of ID is supplied, a copy is
15 taken and filed as evidence that regulatory requirements were fulfilled. However, the moment a customer departs with an original document, there is no persisting evidence that the original document was ever witnessed - other than a claim made by an organisation that it saw the original document – and that organisation may find itself being investigated for not adhering to the rules.

20 A photocopy of a document does not demonstrate that an employee of a regulated company actually viewed an original document. In many cases, the customer in question is not available "locally" and current processes are likely to require them to photocopy their passport before having it certified by a third party who is a member of a professional body. This creates further problems as
25 CDD (Customer Due Diligence) then needs to be carried out on the certifier

- 2 -

who met the individual and certified that the photocopy was a true representation of the original document that they confirm they had sight of. The CDD on this third party certifier often amounts to no more than contacting the professional body to which they claim to belong in order to verify that they are in fact a member. It does not however prove that the person who certified the document was who they said they were. Furthermore, further research may be required to ensure that the certifier was appropriate e.g. that they are not closely related to the individual.

By way of one example only, it is possible to view information supplied by the Guernsey Financial Services Commission that includes CDD and verification guidelines at the following URL:

http://www.gfsc.gg/Documents/AML_Handbook%20-%20November_08.pdf.

Should this URL not be available at the time of reading this specification, suffice it to say that the document is entitled "Handbook for Financial Services Businesses on Countering Financial Crime and Terrorist Financing" and runs to 217 pages. Similar publications are doubtless available from similar regulatory bodies.

Preferred embodiments of the present invention aim to overcome many of the issues with current CDD and KYC (Know Your Customer) processes (in terms of speed and complexity of satisfying regulatory requirements, and also with regards the "quality of the proof" with which those regulatory requirements are satisfied) by uniquely combining several elements of technology for a specific purpose. Much of the technology that exists in many mobile phone devices can be adapted to this purpose. Preferred embodiments of the invention aim to provide a more verifiable proof that the original identification documents were used in a CDD process and to allow a potential customer on whom CDD is

- 3 -

being conducted, potentially in a remote geographic location, to complete a large portion of the due diligence process using their own device, and to the same satisfactory standard in terms of ID proofing as if they were "there in person".

According to one aspect of the present invention, there is provided a
5 device for use in verifying personal identity from a personal ID document that contains unique identifying text and encrypted biometric data, the device comprising:

- a. text entry means for entering said unique identifying text;
- b. an NFC reader that reads said biometric data;
- 10 c. a decryption application that decrypts said biometric data, utilising said unique identifying text;
- d. a camera to capture an image of the face of a user;
- e. a date and time application that records the date and time when a user uses the device to capture data; and
- 15 f. a communication system by which the device communicates with a remote station:

wherein, in use, for a given verification task, a user:

enters said unique identifying text;

places the device adjacent the ID document such that the NFC reader
20 reads said biometric data;

activates said camera to capture an image of the face of the user; and

activates said communication system to transmit to a remote station
data captured by the device relating to said unique identifying text, said
decrypted biometric data, said captured image, and recorded date and
25 time.

- 4 -

Preferably, said text entry means comprises:

- a. a scanner for scanning said unique identifying text;
- b. an OCR application that receives output data from the scanner and recognises text characters from that data;
- 5 c. a display that displays the text characters recognised by the OCR application; and
- d. a text editing application that allows a user to edit text displayed on said display, to provide final text data corresponding to said unique identifying text:

10 and, in use, for a given verification task:

a user scans said identifying text; and checks and edits if necessary the text displayed on said display to provide said final text data; and
said decryption application decrypts said biometric data utilising said final text data.

15 A device as above preferably comprises dual cameras that capture images at opposite sides of the device simultaneously to show the face of a user and the personal ID document held by the user: and, in use, captured image data of both of the simultaneous images is transmitted to the remote station by said communications system.

20 A device as above preferably further comprises a GPS system that records the global position of a user when using the device to capture data and, in use, the recorded GPS data is transmitted to the remote station by said communications system.

Preferably, all of the recited functions are integrated within the device.

- 5 -

A device as above may comprise a smartphone adapted to provide all of the recited functions.

A device as above preferably further comprises an authorisation application that requires a user to enter an authorisation code provided by an operator, whereupon the device transmits the authorisation code via the communication system to a remote station and, provided that the remote station receives the transmitted authorisation code within a predetermined time from the authorisation code being provided by the operator, the authorisation application receives from a remote station via the communication system an unlock instruction that allows a validation task to proceed on the device.

A device as above preferably further comprises an erasure application that erases all data collected by the device for a given validation task, once all of the data for the task has been transmitted to the remote station by said communication system.

Said encrypted biometric data may comprise data relating to at least one of fingerprint recognition data and iris recognition data.

Preferably, in use, a user may select one or more steps of a given verification task to be carried out; and the user activates said communication system to transmit to the remote station the data captured by said one or more steps.

Preferably, the device further comprises a data assembly application that assembles together data for a given verification task; and in use, a user activates said communication system to transmit to the remote station the data assembled by the data assembly application.

- 6 -

In another aspect, the invention provides a method of verifying personal identity from a personal ID document that contains unique identifying text and biometric data, the method comprising the steps of:

- a. entering said unique identifying text into a device;
- 5 b. reading said biometric data by means of an NFC reader;
- c. by means of a decryption application and utilising said unique identifying text, decrypting said biometric data;
- d. capturing by means of a camera an image to show the face of a user;
- 10 e. recording by a date and time application current date and time data; and
- f. by means of a communication system, transmitting to a remote station data captured by the device relating to said unique identifying text, said decrypted biometric data, said captured image, and recorded
- 15 date and time.

A method as above preferably further includes the steps of:

- scanning said identifying text by a user;
- by means of an OCR application that receives output data from the scanner, recognising text characters from that data;
- 20 displaying on a display the text characters recognised by the OCR application;
- initiating a text editing application that allows a user to edit text displayed on said display, to provide final text data; and
- utilising said final text data to decrypt said biometric data by means of
- 25 said decryption application.

- 7 -

A method as above preferably further includes the steps of capturing by means of dual cameras simultaneous images to show the face of a user and the personal ID document held by the user; and transmitting captured image data of both of the simultaneous images to the remote station by said communications
5 system.

A method as above preferably further includes the steps of recording a video of a user performing a predetermined action, details of which have been sent to the device, and uploading the video data to the remote station.

A method as above preferably further includes the steps of recording by
10 a GPS system the current global position of a user; and transmitting the recorded GPS data to the remote station by said communications system.

A method as above preferably further includes the step of capturing by means of said camera or one of said cameras an image to show a utility bill or other document to show the address of the user within a predetermined recent
15 date range.

A method as above preferably further includes the further steps, after transmitting the data to the remote station, of manually transcribing the address shown on the document to generate a physical letter containing a code that specifically relates to the device and the user; posting the letter physically to the
20 user through a mail delivery system; after delivery of the letter, scanning the code in the letter; and transmitting data of the scanned code from the device to the remote station or other location for verification.

- 8 -

A method as above preferably further includes the step of transmitting to the device a validation report to validate or otherwise the personal identity the subject of the data captured by the device and transmitted to the remote station.

Preferably, said validation report comprises the data captured by the
5 device and transmitted to the remote station, together with further data that has been assembled subsequent to such transmission to the remote station.

Preferably, a method as above is carried out for regulatory purposes.

A method as above preferably further includes the step of transmitting,
to an issuing authority of the personal ID document for verification, data
10 derived from the personal ID document that has been transmitted to the remote station.

A method as above preferably further includes the steps of selecting one or more steps of a given verification task to be carried out; and activating said communication system to transmit to the remote station the data captured by
15 said one or more steps.

A method as above preferably further includes the step of assembling together data captured for a given verification task; and transmitting the assembled data by said communication system to the remote station.

For a better understanding of the invention, and to show how
20 embodiments of the same may be carried into effect, reference will now be made, by way of example, to the accompanying diagrammatic drawings, in which:

- 9 -

Figure 1 is a block schematic diagram of a device for use in verifying personal identity from a personal ID document;

Figure 2 illustrates a page of a passport containing identifying text in a Machine Readable Zone (MRZ);

5 Figure 3 illustrates MRZ data scanned from the page of Figure 2 and displayed in editable text format;

Figure 4 illustrates biometric information that has been read from an RFID chip on the passport, decrypted and displayed;

Figure 5 illustrates a user taking simultaneous dual photographs;

10 Figure 6 illustrates a display whilst data is uploaded from the device;

Figures 7A to 7C show the content of a personal identity verification report sent to a user; and

Figure 8 illustrates a display that gives options to a user to carry out various verification steps.

15 In the figures, like references denote like or corresponding parts.

It is to be understood that the various features that are described in the following and/or illustrated in the drawings are preferred but not essential. Combinations of features described and/or illustrated are not considered to be the only possible combinations. Unless stated to the contrary, individual
20 features may be omitted, varied or combined in different combinations, where practical.

- 10 -

Figure 1 shows a mobile device 1 that communicates with a remote station 2 over a wireless network 3. The device 1 may be a telephone or smartphone. First and second cameras 11 and 12 face in opposite directions – e.g. away from and towards a user. A scanner 13 is connected to receive images
5 from the first camera 11.

An NFC (Near Field Communication) reader 14 is arranged to receive RF (radio frequency) data from a nearby source. A GPS (Global Positioning System) system detects the global position of the device 1. A communication system 16 allows the device 1 to communicate with the remote station 2 and
10 other devices on the wireless network 3.

A processor 17 performs various data processing functions and includes an OCR (Optical Character Recognition) application 171 that receives image data received from the scanner 13. A decryption application 172 decrypts data received from the NFC reader 14. A date and time application 173 records
15 current date and time. A data assembly application 174 assembles data received by the processor 17. A data erasure application 175 erases specified data collected by the device 1. A text editing application 176 allows a user to edit text displayed on a display 18, by means of a keyboard 19. Although shown separately, the keyboard 19 may be incorporated in the display 18, especially if
20 the display 18 comprises a touch screen.

If the device 1 comprises an adapted mobile phone or smartphone, it will typically have various other features that are known to the users of such phones and need not be described in any detail here. However, it is to be appreciated that it is not essential to adapt such phones to provide embodiments
25 of the invention. The device 1 may be a custom-made device for the purpose of embodying an example of the invention. Although it is convenient for all local

- 11 -

functions of an embodiment of the invention to be integrated within the device 1, various discrete devices may be interconnected to provide a device similar to the device 1.

The device 1 may be used as follows, to circumvent much of the
5 laborious processes currently followed in order to achieve KYC/CDD which in many respects do not adequately satisfy the regulatory requirements.

A company ("Company") may register as a client with an operator, for the purposes of using the device 1 for personal identity verification. Employees of the Company may be nominated to have individual logins which are
10 additionally IP (Internet Protocol) address restricted for added security. If a potential new Customer wishes to open an account with the Company, there is a requirement for due diligence. In discussion with the Customer, an employee of the Company logs in to his or her account and enters the Customer's email address along with any additional instructions (and potentially specifying a
15 project code that is internal to Company), and simply clicks a button that generates a 16-digit activation code and emails it to the Customer with a standard list of instructions (or sends it to the Customer in any other practical way – e.g. an SMS text message). Any other suitable number of digits could be used in the activation code. The Customer downloads onto the device 1 an app
20 (application) from any source, which may be an open source such as (at the present time) GooglePlay – or it may be made available at a unique, temporary URL. The app will not work until the 16-digit code is entered, and this must be done within a set amount of time from the code having been generated. Once the 16-digit code has been correctly entered into the device 1, the device is
25 registered against the Company's account with the operator. Thus, the app effectively unlocks the device 1 for use in verifying personal ID from regulated and acceptable ID documents. In the present example, the ID document is an

- 12 -

ePassport 5, as shown diagrammatically in Figure 2, i.e. a passport that contains biometric information on an RFID chip 52 as well as textual information in a Machine Readable Zone (MRZ) 51.

5 Firstly, having unlocked the device 1 as above, a user scans the text of the passport 5 in the MRZ 51, using the first camera 11, which feeds image data to the scanner 13. The scanned image data is passed to the OCR application 171, which recognises the text characters in the MRZ 51 and displays the corresponding data on the display 18, as shown in Figure 3.

10 The text data interpreted from the OCR and displayed on display 18 can be manually edited if inaccurate, using the keyboard 19, to ensure that it corresponds to the original text as printed in the MRZ 51. This final text is then used to decrypt the biometric data held in the digital chip 52 in the ID document, which is read by enabling the NFC reader 14 and placing the device 1 sufficiently close to the RFID chip 52. The data read by the NFC reader 14 is
15 passed to the decryption application 172 that decrypts the biometric data, utilising the final text derived from the MRZ text. The method of decrypting such biometric data from a passport, using data from MRZ text, is known per se, and therefore does not need further explanation here.

Figure 4 shows the display 18 on which data derived from both the
20 MRZ 51 text and the RFID chip 52 are displayed to the user. This includes an image 181 of the user, corresponding to the user image 58 as printed on the passport 5 or secured to it.

If the data from the RFID chip 52 cannot be read or decrypted, an error message such as 182 may be displayed, to alert the user to a possible cause and
25 allow the user to repeat the operation. In this example, the error message

- 13 -

“Wrong BAC data” refers to Basic Access Control (BAC) encryption, which is used to encrypt the data on the RFID chip 52. The error message is suggesting that the OCR scanned details are incorrect because the process of decryption using the MRZ text data provided do not appear to be working.

5 Once the biometric information has been read from the RFID chip 52, the user holds the ID document 5 with one hand and the device 1 with the other hand, roughly equidistant between the ID document and the user, as illustrated in Figure 5. Both first and second cameras 11 and 12 are then actuated simultaneously, to take both front and back facing photographs as evidence that
10 the ID document was in the possession of the user at that time, and to provide a "live" image for comparison to the digital image read from the chip 52 on the ID document.

 The user then photographs one or more proofs of residence (such as utility bills) within a recent date range – either using just a single one of the
15 cameras 11, 12 or both simultaneously, as in Figure 5.

 For all of the data captured or generated in the foregoing actions, the date and time application 173 provides associated date and time data. Some of the captured or generated data may be required to be recorded at the same date and time – as in the simultaneous photos described above – or at least within a
20 predetermined time range on the same date. All of the captured or generated data may be required to be recorded within a predetermined time range on the same date. Likewise, all of the captured or generated data may be required to be recorded at the same global location as determined by the GPS system 15, or within a predetermined location range.

- 14 -

All of the captured or generated data is assembled by the data assembly application 174. That is, for a given verification task, the unique identifying text from the MRZ 51, the decrypted biometric data from the chip 52, the captured simultaneous images from the photographs taken by the two cameras 11 and 12, further captured images of proof of residence as taken by the camera 11 and/or 12, recorded GPS and date and time data as to the time of data capture and/or generation.

When all of the data is complete at the device 1, it is uploaded from the data assembly application 174 to the remote station 2, via the communication system of the device 1 and the wireless network 3. This is illustrated in Figure 6. Upon the device 1 receiving confirmation of a successful upload, the erasure application 175 is activated to erase from the device 1 all data collected by the device for the given validation task.

Processing of the data is effected away from the device 1 – at the remote station 2 and/or another location. The erasure application 175 ensures that no sensitive information is retained by the device 1, for security reasons. Processing involves, but is not limited to, two main areas: processing and comparison of uploaded data and its compilation into a report; and scanning other sources of data using the personal details read from the RF ID chip 52. A valuable feature of this is that, when scanning the "other sources of data", the system removes entirely the need for manual data entry to identify the individual concerned and therefore removes the possibility of human error.

In processing the data assembled by the device 1, a comparison is made between the images collected from the device, the results of which are compiled into a report, as illustrated in Figures 7A to 7C, along with the results of electronically matching the name and date of birth details with a number of

- 15 -

other databases including, but not restricted to, the UK/UN/EU and US Financial Sanctions and Investment Ban lists, PEP lists, disqualified directors, restricted individuals and various other Customer Due Diligence data sources. As indicated above, a valuable aspect of scanning against other data sources, using the above described system, is that the details being checked have been read digitally and are therefore a faithful copy of details determined and verified by a passport issuing authority, and they are being scanned against lists that are often produced by government departments. Thus, there is no possibility of human error in transcription. The possibility of failing to properly check, and the risk of failing compliance on this basis, is entirely removed from the Company.

The report is sent to the registered employee that arranged the activation code for the Customer – e.g. by email, SMS text or a secure communications link. The employee is required to accept or reject the report by logging back in to their account and indicating accordingly. If rejecting the report, reasons have to be given. For example, the Customer's simultaneous forward and back photograph may be blurred or may not adequately match the digital image. A reject will automatically email the Customer at the same address to which the 16-digit code was sent, informing them that the process needs to be repeated, and detailing why the previous attempt had failed. If the Employee indicates that the process has been successful the device 1 is immediately deactivated for further personal identity verification, such that it cannot be used to complete the same process without a further 16-digit activation code being generated and entered.

In the processing of data uploaded from the device, an operator (or other party processing the data) may be able to verify the captured ID details via a direct, secure link to the ID issuing authority. For example, in the case of a passport, an operator may transmit the captured ID details via a direct, secure

- 16 -

link to the respective government passport office, where the details are confirmed or otherwise, preferably in real time.

It may be appreciated that the examples of the invention as illustrated and described above provide devices and methods to confirm or verify a person's identity by accurately relaying relevant information from original biometric identification documents and various other data (including images) and including but not restricted to GPS location, to a company that will scan various other databases and construct a report for a third party for the purposes of satisfying various regulatory requirements related to customer due diligence (CDD) and know your customer (KYC), and to seek to satisfy other regulations e.g. anti-money laundering (AML) and Financial Terrorism (FT).

CDD covers a wide range of circumstances within regulatory guidance and is often an extensive process that requires researching in order to identify the names of people who benefit from or are involved in some way with complex arrangements of businesses and trusts. However, at its most fundamental base, it revolves around correctly identifying, and verifying the identity of, people.

Whilst examples of the invention have been illustrated and described, other options are possible.

Instead of the dual simultaneous photograph feature, illustrated in Figure 5, a user may take two successive photographs, to show the user's face and the ID document, within a short, predetermined time frame. Thus, the device may utilise two cameras as illustrated, or only one.

- 17 -

Instead of the scanner 13 and OCR application 171, a user may enter the MRZ text manually, using the display 18 and keyboard 19.

In another option, a camera of the device may alternatively or additionally be used to record a video of the user quoting a predetermined text or performing another predetermined action, details of which have been sent to the device to inform the user, and uploading the video data to the remote location for processing with the other data. This may provide enhanced security against the possibility of the device being used to capture an image of an image of a person, rather than a direct image of the user.

10 In a further option, where image data of a document establishing proof of residence (such as utility bills) within a recent date range has been uploaded to an operator (or other party processing the data), the address shown on the document may be manually transcribed by the operator and used to generate a physical letter containing a QR (or other) code that specifically relates to a) the device, b) the user and c) the Company client of the operator: the letter is then posted physically to the user through an accredited mail delivery system. When the letter has been received at the address that has been transcribed, the user's device is then used to scan the QR code in order to 'physically' prove the address to which the QR code was sent, and to link that physical location to the user.

15 20 The action of scanning the QR code may be similarly date-stamped, time-stamped and GPS located as in the examples described above. Only the device that was used to collate and upload the original data can be used to scan the QR code, and that device will only be able to scan the QR code relating to the current ID verification task.

25 An alternative to using a QR code is to provide an explicit URL. A further option is for a user to provide a password when initially entering data.

- 18 -

This password can then be required to enter the webpage specified by the QR code or URL, to provide an extra layer of security.

An alternative to manual transcription is to employ an address look-up service where the user selects their address from a pre-populated list (e.g. based
5 on a postcode that the user enters). Thus, the operator does not need to manually enter the address. Another option for an operator is to perform OCR on an image of a utility bill (or other evidence) in order to recognise an address and then compare it to an address entered or selected by a user to indicate a percentage match. That is, the address entered or selected by a user is used to
10 assist in identifying the address on the utility bill etc, as processed by OCR.

In the examples illustrated and described above, the data assembly application 174 assembles all of the data required for the ID verification task, for transmission via the communications application 16 to the remote station 2. This is generally an efficient way to effect the ID verification task. However, it
15 may be desired to carry out only a single step of the overall ID verification task – for instance, in the example given above, where the QR code scan is uploaded as a subsequent step. Also, it may be that a given step has to be repeated – for example, if initially updated data is unsatisfactory, as may happen if a captured image is blurred or a data item does not pass a subsequent check. To this end,
20 the user may be presented with options on the display 18, as illustrated in Figure 8, where the display is a touch-screen display.

On touching button 191, the device is enabled to scan and capture data from an ID document – for example, a passport document, as described above.

- 19 -

On touching button 192, the device is enabled to scan and capture data from a residence document – for example, a recent utility bill, as described above.

On touching button 193, the device is enabled to scan and capture data
5 by way of proof of a user (or presenter of data) – for example, using one or more camera, as described above.

On touching button 194, the device is enabled to scan, for example, a QR code as received on a physical letter, as described above, by way of proof of residence.

10 On touching button 195, the device is enabled to scan an iris of a user and capture the respective data. (Iris recognition is a known process.)

On touching button 196, the device is enabled to scan a fingerprint of a user and capture the respective data. (Fingerprint recognition is a known process.)

15 On touching button 197, the device uploads to the remote station data from one or more of the steps carried out in response to buttons 191 to 196. The button 197 is inactive until at least one of the steps corresponding to buttons 191 to 196 has been performed.

Not all of the steps available in response to buttons 191 to 196 may be
20 required for a given ID verification task.

Different ID documents contain different information. Even passports between countries, and within countries, can vary in the information they hold. For example epassports contain "space" for fingerprint data but the UK does

- 20 -

not currently populate this space in an epassport. If in the future they do it will be uploaded for processing. The same holds true for iris data, which is being increasingly used for identification. As the level of biometric data increases, examples of the invention may be adapted accordingly. Whilst not currently
5 mainstream, many mobile devices are able to, for example, scan a fingerprint and/or an iris. Thus a user's fingerprint and/or iris can be scanned and compared with digital information held on an ID document, for verification before the process is permitted to continue.

Not all passports, and not all countries, adopt the type of biometric
10 ePassport that is used in the above examples, which refer to "passport" for simplicity of explanation. However, examples of the invention can be equally applied to national identity cards that are ICAO9303 compliant (for example those in Netherlands, Brazil and Albania) and may also be adapted to enable the use of selected national ID cards that contain biometric information even where
15 that ID Card may not be ICAO9303 compliant but where it is still considered adequate for a relevant verification purpose. Examples of the invention may in the main utilise interfaces that are in accordance with ISO/IEC 14443, but the invention is not restricted to the use of such interfaces.

Where a personal ID document that contains unique identifying text
20 contains text in a non-Latin language, a translation routine may be applied to translate the text into an English alphabet. This could possibly result in several English variations of the name, all of which may be checked against various sanctions lists.

Whilst the examples of the invention as illustrated and described above
25 provide for circumstances where an individual is required to prove their identity to a particular level of satisfaction, examples of the invention can be extended to,

- 21 -

for example, companies that at least want to ensure that personal details of remote applicants are transcribed accurately, or for example pre-flight remote check-in for airlines.

As regards reports generated in respect of individuals, report
5 information may be arranged for the respective employee of the Company, in their online account, such that they are easily able to group and review the results for all of the individuals associated with a particular project, with management information detailing progress of a project as a whole. Failure to verify the identity of all individuals can lead to compliance failure for the entire project and
10 it is therefore possible for an employee to add individuals' details to their account even if they are not having their identity verified, in order to manage the progress of the entire project.

A method of verifying personal identity as disclosed herein may be a self-contained method or form part of a more extensive method or application.
15 For example, it may be provided as part of an online gaming application.

In this specification, the verb "comprise" has its normal dictionary meaning, to denote non-exclusive inclusion. That is, use of the word "comprise" (or any of its derivatives) to include one feature or more, does not exclude the possibility of also including further features. The word "preferable" (or any of
20 its derivatives) indicates one feature or more that is preferred but not essential.

All or any of the features disclosed in this specification (including any accompanying claims, abstract and drawings), and/or all or any of the steps of any method or process so disclosed, may be combined in any combination, except combinations where at least some of such features and/or steps are
25 mutually exclusive.

- 22 -

Each feature disclosed in this specification (including any accompanying claims, abstract and drawings), may be replaced by alternative features serving the same, equivalent or similar purpose, unless expressly stated otherwise. Thus, unless expressly stated otherwise, each feature disclosed is one example only of a
5 generic series of equivalent or similar features.

The invention is not restricted to the details of the foregoing embodiment(s). The invention extends to any novel one, or any novel combination, of the features disclosed in this specification (including any accompanying claims, abstract and drawings), or to any novel one, or any novel
10 combination, of the steps of any method or process so disclosed.

CLAIMS

1. A device for use in verifying personal identity from a personal ID document that contains unique identifying text and encrypted biometric data, the device comprising:
 - 5 a. text entry means for entering said unique identifying text;
 - b. an NFC reader that reads said biometric data;
 - c. a decryption application that decrypts said biometric data, utilising said unique identifying text;
 - d. a camera to capture an image of the face of a user;
 - 10 e. a date and time application that records the date and time when a user uses the device to capture data; and
 - f. a communication system by which the device communicates with a remote station:wherein, in use, for a given verification task, a user:
 - 15 enters said unique identifying text;
 - places the device adjacent the ID document such that the NFC reader reads said biometric data;
 - activates said camera to capture an image of the face of the user; and
 - activates said communication system to transmit to a remote station
 - 20 data captured by the device relating to said unique identifying text, said decrypted biometric data, said captured image, and recorded date and time.
2. A device according to claim 1, wherein said text entry means comprises:
 - a. a scanner for scanning said unique identifying text;

- 24 -

- b. an OCR application that receives output data from the scanner and recognises text characters from that data;
- c. a display that displays the text characters recognised by the OCR application; and
- 5 d. a text editing application that allows a user to edit text displayed on said display, to provide final text data corresponding to said unique identifying text:

and wherein, in use, for a given verification task:

- a user scans said identifying text; and checks and edits if necessary the
- 10 text displayed on said display to provide said final text data; and
- said decryption application decrypts said biometric data utilising said final text data.

- 3. A device according to claim 1 or 2, comprising dual cameras that capture images at opposite sides of the device simultaneously to show the face of a user
- 15 and the personal ID document held by the user: and wherein, in use, captured image data of both of the simultaneous images is transmitted to the remote station by said communications system.

- 4. A device according to claim 1, 2 or 3, further comprising a GPS system that records the global position of a user when using the device to capture data and,
- 20 in use, the recorded GPS data is transmitted to the remote station by said communications system.

- 5. A device according to any of the preceding claims, wherein all of the recited functions are integrated within the device.

- 25 -

6. A device according to claim 5, being a smartphone adapted to provide all of the recited functions.

7. A device according to any of the preceding claims, further comprising an authorisation application that requires a user to enter an authorisation code
5 provided by an operator, whereupon the device transmits the authorisation code via the communication system to a remote station and, provided that the remote station receives the transmitted authorisation code within a predetermined time from the authorisation code being provided by the operator, the authorisation application receives from a remote station via the communication system an
10 unlock instruction that allows a validation task to proceed on the device.

8. A device according to any of the preceding claims, further comprising an erasure application that erases all data collected by the device for a given validation task, once all of the data for the task has been transmitted to the remote station by said communication system.

15 9. A device according to any of the preceding claims, wherein said encrypted biometric data comprises data relating to at least one of fingerprint recognition data and iris recognition data.

10. A device according to any of the preceding claims wherein, in use, a user may select one or more steps of a given verification task to be carried out; and
20 the user activates said communication system to transmit to the remote station the data captured by said one or more steps.

11. A device according to any of the preceding claims, wherein the device further comprises a data assembly application that assembles together data for a given verification task; and in use, a user activates said communication system to

- 26 -

transmit to the remote station the data assembled by the data assembly application.

12. A method of verifying personal identity from a personal ID document that contains unique identifying text and biometric data, the method comprising the
5 steps of:

- a. entering said unique identifying text into a device;
- b. reading said biometric data by means of an NFC reader;
- c. by means of a decryption application and utilising said unique identifying text, decrypting said biometric data;
- 10 d. capturing by means of a camera an image to show the face of a user;
- e. recording by a date and time application current date and time data; and
- f. by means of a communication system, transmitting to a remote
15 station data captured by the device relating to said unique identifying text, said decrypted biometric data, said captured image, and recorded date and time.

13. A method according to claim 12, including the steps of:

- scanning said identifying text by a user;
- 20 by means of an OCR application that receives output data from the scanner, recognising text characters from that data;
- displaying on a display the text characters recognised by the OCR application;

- 27 -

initiating a text editing application that allows a user to edit text displayed on said display, to provide final text data; and
utilising said final text data to decrypt said biometric data by means of said decryption application.

- 5 14. A method according to claim 12 or 13, including the steps of capturing by means of dual cameras simultaneous images to show the face of a user and the personal ID document held by the user; and transmitting captured image data of both of the simultaneous images to the remote station by said communications system.
- 10 15. A method according to claim 12, 13 or 14, including the steps of recording a video of a user performing a predetermined action, details of which have been sent to the device, and uploading the video data to the remote station.
16. A method according to any of claims 12 to 15, including the steps of recording by a GPS system the current global position of a user; and transmitting
15 the recorded GPS data to the remote station by said communications system.
17. A method according to any of claims 12 to 16, including the further step of capturing by means of said camera or one of said cameras an image to show a utility bill or other document to show the address of the user within a predetermined recent date range.
- 20 18. A method according to claim 17, including the further steps, after transmitting the data to the remote station, of manually transcribing the address shown on the document to generate a physical letter containing a code that specifically relates to the device and the user; posting the letter physically to the user through a mail delivery system; after delivery of the letter, scanning the code

- 28 -

in the letter; and transmitting data of the scanned code from the device to the remote station or other location for verification.

19. A method according to any of claims 12 to 18, including the further step of transmitting to the device a validation report to validate or otherwise the
5 personal identity the subject of the data captured by the device and transmitted to the remote station.

20. A method according to claim 19, wherein said validation report comprises the data captured by the device and transmitted to the remote station, together with further data that has been assembled subsequent to such transmission to
10 the remote station.

21. A method according to any of claims 12 to 20, carried out for regulatory purposes.

22. A method according to any of claims 12 to 21, including the step of transmitting, to an issuing authority of the personal ID document for
15 verification, data derived from the personal ID document that has been transmitted to the remote station.

23. A method according to any of claims 12 to 22, comprising the steps of selecting one or more steps of a given verification task to be carried out; and activating said communication system to transmit to the remote station the data
20 captured by said one or more steps.

24. A method according to any of claims 12 to 23, comprising the step of assembling together data captured for a given verification task; and transmitting the assembled data by said communication system to the remote station.

- 29 -

25. A device for use in verifying personal identity from a personal ID document, the device being substantially as hereinbefore described with reference to the accompanying drawings.

26. A method of verifying personal identity from a personal ID document, the
5 method being substantially as hereinbefore described with reference to the accompanying drawings.

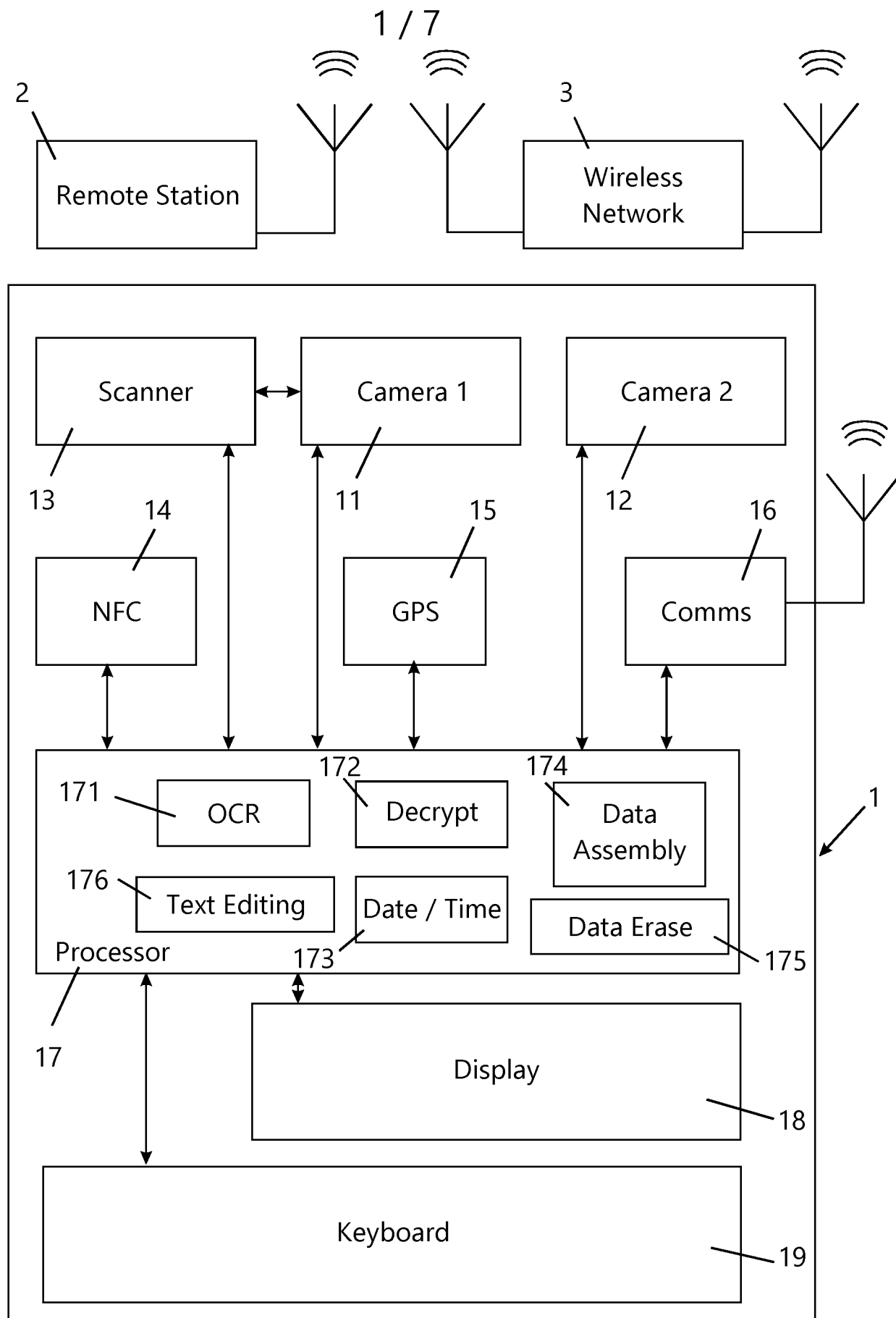


FIG. 1

2 / 7

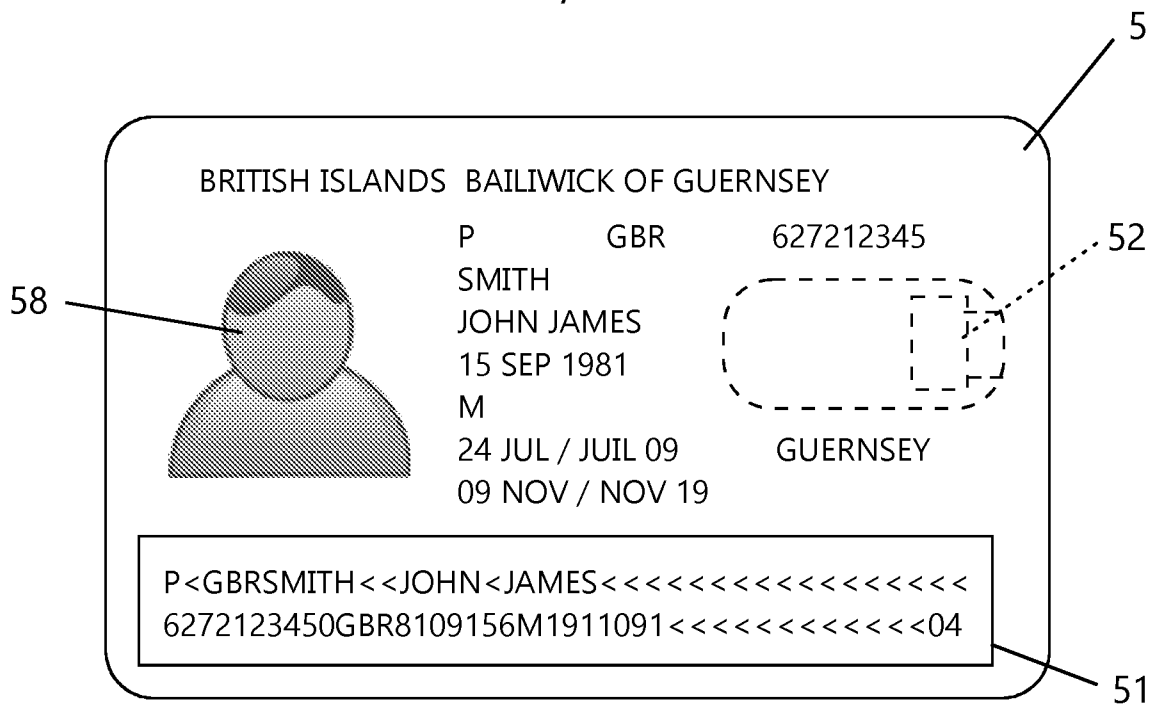


FIG. 2

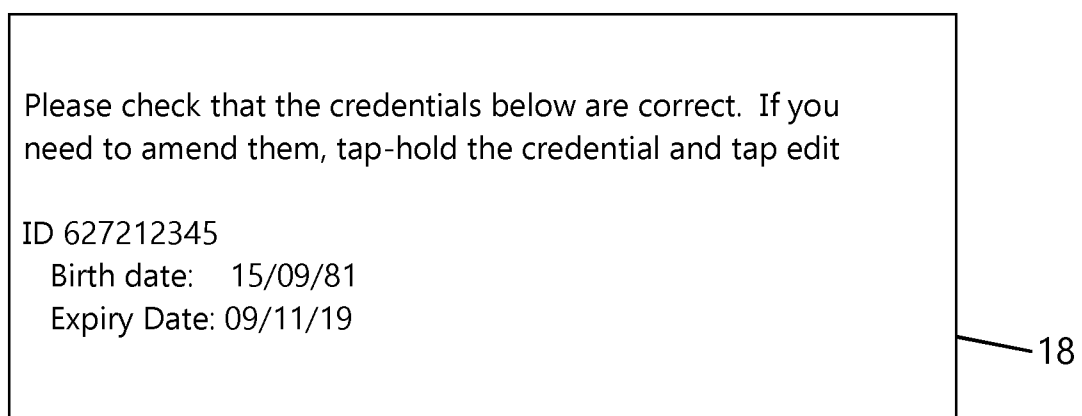
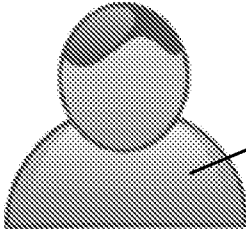


FIG. 3

3 / 7

PHOTO



PERSONAL INFO

NAMES	JOHN JAMES
SURNAME	SMITH
DATE OF BIRTH	15/09/1981
GENDER	MALE
NATIONALITY	GBR

PASSPORT INFO

PASSPORT NUMBER	627212345
EXPIRATION DATE	19/11/2019

**Can not read the ePassport data.
Wrong BAC Data?**

181

18

182

FIG. 4

4 / 7

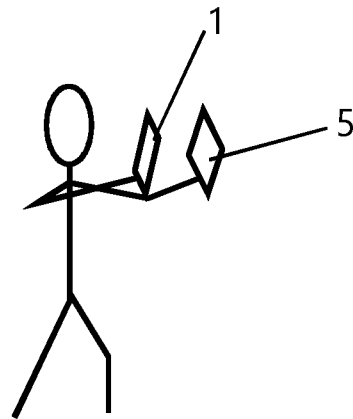


FIG. 5

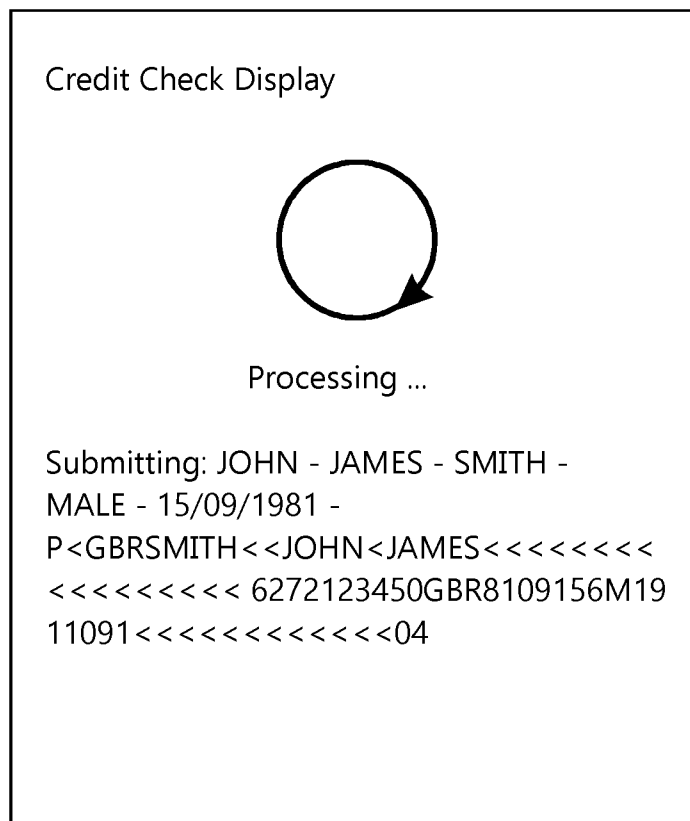


FIG. 6

5 / 7

CDD/KYC Report

Search conducted on:



Mr John Smith [43720] (dob: 15 September 1981)

UK Financial Sanctions : CLEAR

Currently at address:

14 Acacia Avenue, Vale, GY6 9DL

ID Checks:

Passport:

Passport image ... Datestamp: 30 April 2015 12:28



Simultaneous front: 30 April 2015 12:29

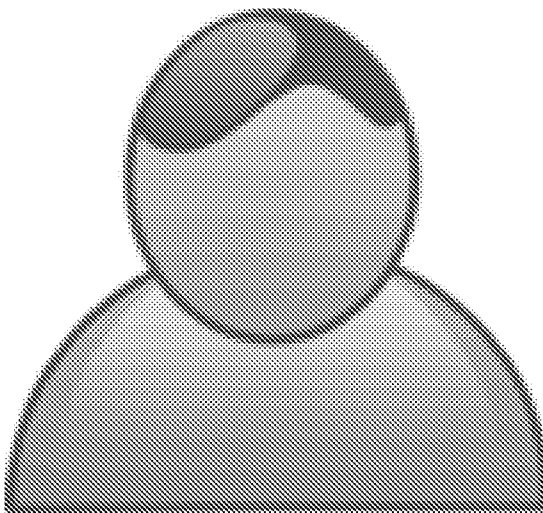


FIG. 7A

Residency Proof: 30 April 2015 12:30

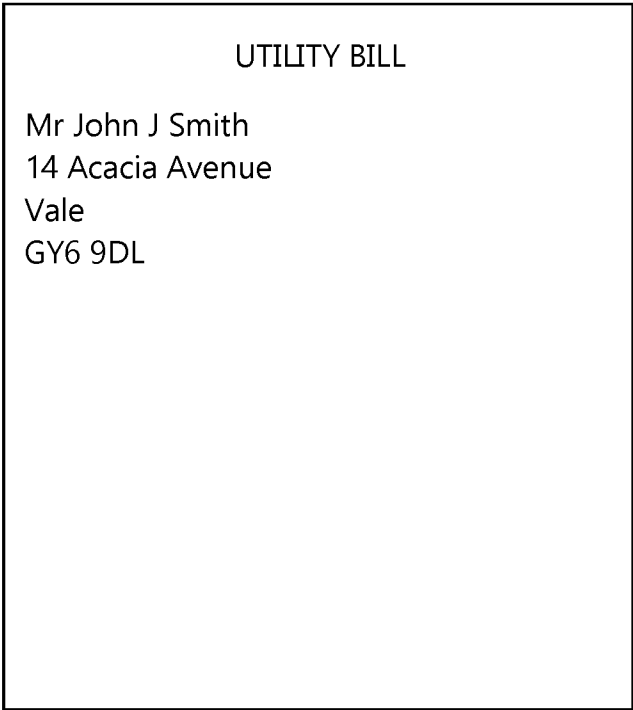


FIG. 7C

Judgements:

Searches:

Debts:

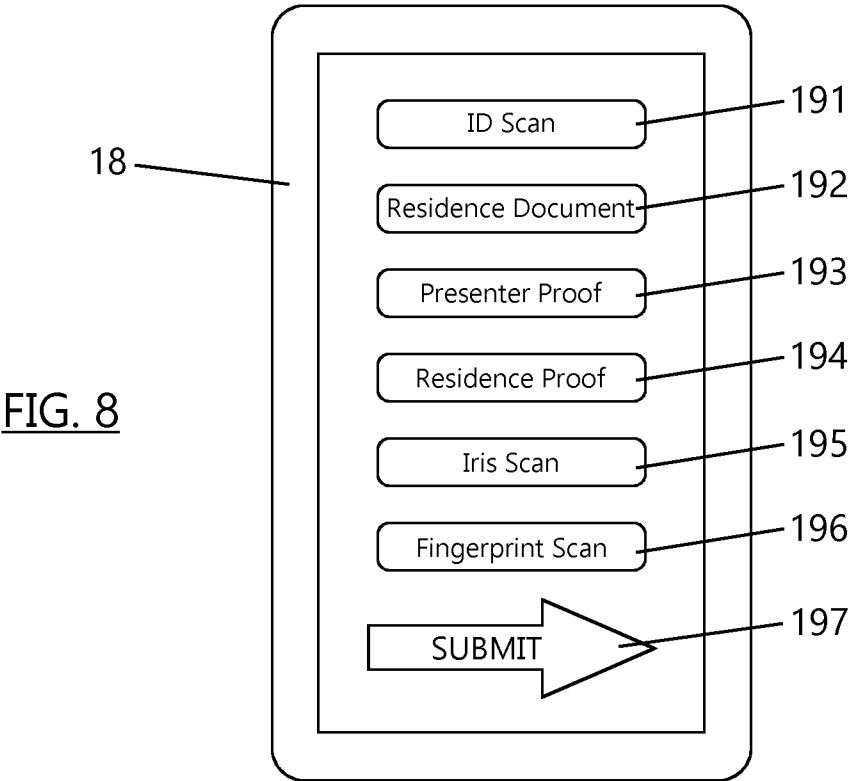


FIG. 8

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2016/052363

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/32
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 G07C G07D 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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2 704 077 A1 (NXP BV [NL]) 5 March 2014 (2014-03-05) paragraphs [0017] - [0030] figure 1	1-24
A	----- US 2013/305059 A1 (GORMLEY MICHAEL JOHN [US] ET AL) 14 November 2013 (2013-11-14) paragraphs [0004] - [0008] paragraphs [0048] - [0053] paragraphs [0061] - [0065] -----	1-24

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

☒ See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

8 November 2016

Date of mailing of the international search report

16/11/2016

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

Segura, Gustavo

INTERNATIONAL SEARCH REPORT

International application No.
PCT/GB2016/052363

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.: 25, 26
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.: 25, 26

Independent claims 25 and 26 claim a device and a method "substantially as hereinbefore described with reference to the accompanying drawings", respectively. However, from the above expression it is not possible to determine which are the features of the claimed device and method. As a consequence, a meaningful search cannot be made for these claims.

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/GB2016/052363

Patent document cited in search report		Publication date		Patent family member(s)		Publication date
EP 2704077	A1	05-03-2014	CN	103684775	A	26-03-2014
			EP	2704077	A1	05-03-2014
			US	2014062658	A1	06-03-2014

US 2013305059	A1	14-11-2013	AU	2013246898	A1	27-11-2014
			CA	2869515	A1	17-10-2013
			DE	202013011992	U1	22-04-2015
			SG	10201509815W	A	30-12-2015
			SG	11201406418S	A	27-11-2014
			US	2013305059	A1	14-11-2013
			US	2015281232	A1	01-10-2015
			WO	2013153118	A1	17-10-2013
