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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 July 2015 (02.07.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/097432 A1

(51) International Patent Classification:
G06F 21/34 (2013.01) *G06F 21/35* (2013.01)

(21) International Application Number:
PCT/GB2014/053655

(22) International Filing Date:
10 December 2014 (10.12.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1322879.6 23 December 2013 (23.12.2013) GB

(71) Applicant: **ARM IP LIMITED** [GB/GB]; 110 Fulbourn Road, Cherry Hinton, Cambridge CB1 9NJ (GB).

(72) Inventors: **PRITCHARD, Andrew**; 110 Fulbourn Road, Cherry Hinton, Cambridge CB1 9NJ (GB). **BALINT, Gabor**; 110 Fulbourn Road, Cherry Hinton, Cambridge CB1 9NJ (GB).

(74) Agent: **TLIP LTD**; Label Media Offices, 3rd Floor, Broderick House, 43-51 Cookridge Street, Leeds, Yorkshire LS2 3AW (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))*

(54) **Title**: CONTROL OF DATA PROVISION WITH A PERSONAL COMPUTING DEVICE

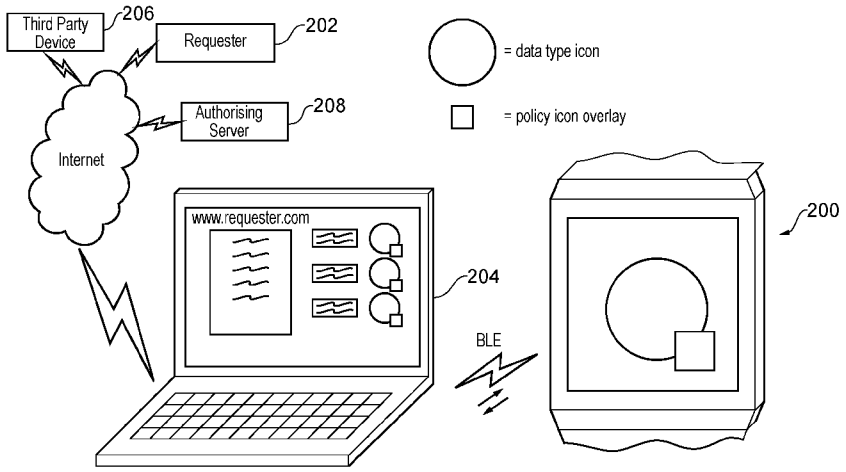

FIG. 16

(57) **Abstract**: A personal computing device (200) receives a request for data from a requester (202). The personal computing device determines whether or not that request is to be permitted or not permitted. The personal computing device indicates to the user both a data indication of what data has been requested by the requester and a policy indication of what policy (e.g. retention policy) is associated with that data. The personal computing device may take the form of a smart watch. The data indication may take the form of an icon and the policy indication may take the form of an icon overlaid upon the data icon.

WO 2015/097432 A1

CONTROL OF DATA PROVISION WITH A PERSONAL COMPUTING DEVICE

This technology relates to the field of data processing systems. More particularly, this technology relates to the control of the provision of data within data processing systems.

It is known to provide data processing systems in which a request for data is sent from a requester to a personal computing device. The personal computing device may permit the request and authorise the provision of data or may not permit the request in which case the provision of data is not authorised.

As the number of different types of data which may be provided by a personal computing device to a requester increases, and the user sensitivity to the release of such data also increases, there is a need to better inform the user of the nature of the data provision they are authorising in order that the user grow in confidence in the automated provision of such data. Furthermore, by better understanding the nature of the data provision being made, the user can make better decisions about whether or not such data provision should be authorised.

Viewed from one aspect there is provided a method of controlling provision of data, said method comprising the steps of:

sending a request for said data from a requester to a personal computing device, said request identifying said data and a policy to be associated with said data;

receiving said request at said personal computing device;

determining with said personal computing device if said request is a permitted request and

(i) if said request is a permitted request, then authorising said provision of said data to said requester; AND

(ii) if said request is not a permitted request, then not authorising said provision of said data to said requester.

The present techniques recognise that when data is being authorised for provision by a personal computing device, the provision may be better understood by considering it in two aspects. The first aspect is what data has been requested for provision. The second aspect is a policy associated with that data. In some embodiments there is provided combined data indications and policy

indications and in this way, a wide variety of different combinations may be represented and yet readily understood by the user.

While it will be appreciated that the policy associated with the data could have a wide variety of different forms, one important form of policy it may be desired to represent is a retention policy to be applied by the requester to the data which is being requested. The retention policy may be, for example, selected from a predetermined group of retention policies which includes one or more of that the data should be permanently retained by the requester, the data is retained until completion of a transaction associated with the data, the data is retained for use by the requester to perform a predetermined processing task and thereafter will not be retained, the data is retained by the requester for a predetermined period of time, and the data is retained for use by the requester a predetermined number of times and thereafter will not be retained.

While it is possible that the indication device could take a number of different forms, one form which works well is when the indication device is a display screen of the personal computing device as such a display screen is well suited to displaying indications of both data type and policy type.

The user understanding of the nature of the provision of data being requested may be increased in embodiments in which the data indication includes a data icon which identifies a data type of the data concerned and where the policy indication includes a policy icon identifying a policy type of a policy to be applied to the data. In this context, the policy icon may be overlaid on the data icon in a way so as to form a combined icon which is then more readily understood by the user, even though it represents one of a wide range of different combinations of data type and policy type.

In addition to indicating with an indication device of the personal computing device the data type and the policy type, in some embodiments there may be additionally provided a display screen associated with the requester and which also displays to the user the data indication and the policy indication. For example, the requester may be a remote server communicating with the personal computing device via a local terminal and a display screen on the local terminal may be associated with a session with the requester within which the data request has been made. Thus, a window in a web browser may be representing a request made from a remote server and that window may display the data indication and the policy indication in addition to the data indication and policy indication

being displayed upon the personal computing device. A user may view both the display on their personal computing device and the display upon the local terminal to check that they match thereby improving their confidence and their control over authorising the provision of their data.

In some embodiments, the step of determining whether or not a request is to be authorised may include the personal computing device communicating with an authorising server via a telecommunications link (such as the internet). With such embodiments, the authorising server may generate the data indication and the policy indication for displaying on the screen associated with the requester thereby improving security by making it more difficult for another party to spoof the data indication and the policy indication presented to a user.

It will be appreciated that in some embodiments the personal computing device may itself directly provide the data being requested. However, in other embodiments, the processing load upon personal computing device may be reduced when the provision of the data is by a third party device to the requester. In such embodiments the personal computing device may authorise the third party device to provide the data to the requester by, for example, issuing a token to the requester using which token the requester can obtain the data they seek from the third party device.

Whether or not a request is to be permitted may be validated by the personal computing device using permission data stored on the personal computing device. Such permission data may indicate that a request is automatically permitted and authorise such a request without requiring any user input. Automatic requests may be ones associated with data of little sensitivity or with requesters in which the user of the personal computing device has already indicated that they have a high degree of trust. Other forms of permission data may indicate that a request is optionally authorised, in which case the user will be presented with a prompt to which they can respond by either authorising or not authorising the request. The permission data may additionally specify that certain requests are unauthorised requests, such as requests originating from requesters known to be untrustworthy or for types of data which the user does not wish to authorise using their personal computing device.

While the personal computing device could take a variety of different forms, one form for which the present techniques are particularly useful is when the personal computing device is a wearable computing device.

Viewed from another aspect there is provided a personal computing device for controlling provision of data, said personal computing device comprising:

receiving circuitry configured to receive a request for said data from a requester, said request identifying said data and a policy to be associated with said data;

determining circuitry configured to determine if said request is a permitted request and

(i) if said request is a permitted request, then authorising said provision of said data to said requester; and

(ii) if said request is not a permitted request, then not authorising said provision of said data to said requester; and

an indicating device configured to provide a data indication of what data has been requested by said requester and a policy indication of what policy is associated with said data.

Viewed from a further aspect there is provided a personal computing device for controlling provision of data, said personal computing device comprising:

receiving means for receiving a request for said data from a requester, said request identifying said data and a policy to be associated with said data;

determining means for determining if said request is a permitted request and

(i) if said request is a permitted request, then authorising said provision of said data to said requester; and

(ii) if said request is not a permitted request, then not authorising said provision of said data to said requester; and

indicating means for providing a data indication of what data has been requested by said requester and a policy indication of what policy is associated with said data.

Embodiments will now be described, by way of example only, with reference to the accompanying drawings in which

Figure 1 schematically illustrates a computer system including a personal computing device, a local device, a requester, a third party device and a token issuing device;

Figure 2 schematically illustrates an example of communication between the various entities in Figure 1;

Figure 3 is a flow diagram schematically illustrating request processing by the local device;

Figure 4 is a flow diagram schematically illustrating request processing by the requester;

Figure 5 is a flow diagram schematically illustrating request processing by the personal computing device;

Figure 6 is a flow diagram schematically illustrating request processing by the third party device;

Figure 7 is a flow diagram schematically illustrating request processing by the token issuing device;

Figure 8 schematically illustrates interaction between the personal computing device and the local device;

Figure 9 is a flow diagram schematically illustrating lock control of a login data store;

Figure 10 is a flow diagram schematically illustrating login data provision by the terminal device (local device);

Figure 11 is a flow diagram schematically illustrating authorised state switching by a personal computing device;

Figures 12 and 13 schematically illustrate icons displayed on a personal computing device to indicate the type of data being authorised and/or requested;

Figure 14 is a diagram schematically illustrating an icon indicating that a request has been refused;

Figure 15 is a diagram schematically illustrating a wearable computing device in the form of a watch on which a user input is required in order to confirm authorisation of a request for data;

Figure 16 schematically illustrates the use of a data type icon and a policy icon associated with a request for the provision of data;

Figure 17 schematically illustrates different types of policy icon; and

Figures 18, 19 and 20 schematically illustrate different combinations of data icons and policy icons with the policy icons overlaid upon the data icons.

Figure 1 schematically illustrates a computer system 2 including a requester 4, which provides a web service, a third party device 6, which provides, for example, driving records, a token issuing device 8 and a local device 10 all communicating via the internet 11 which serves as both a token-issuing telecommunications connection and a third-party telecommunications connection. A personal computing device 12 in the form of a smart watch having a watch body 14, a strap 16 and a clasp 18

is in two-way wireless communication with the local device 10 when proximal thereto. The closure of the clasp 18 is monitored by the smart watch 12 such that if the clasp 18 is opened so that the watch may be removed from a user's arm, then this is detected by the smart watch 12 and serves to switch the smart watch 12 from an authorised state to an unauthorised state.

The local device 10 may be a desktop personal computer, a laptop computer, a workstation or some other form of device. The local device 10 includes a login data store 20 which stores a plurality of items of login data. The login data includes user identifiers and associated passwords for different websites and web services as well as other associated data as may be necessary. The login data store serves as a "keyring" for the login data and the login data store may be in either a locked state or an unlocked state. When the login data store is in an unlocked state, then login data is automatically provided from the login data store to the requester 4. This behaviour using the login data store 20 will be described further below.

The personal computing device 12 is in two-way wireless communication with the local device 10. The communication may use low energy Bluetooth radio connections (BLE). The radio connections may be adapted so as to detect the proximity of the personal computing device 12 to the local device 10. This proximity may be compared with a threshold level of proximity so as to control aspects of the operation of a local device 10 as will be described further below. The proximity may be determined based upon a proximity metric which is determined based upon the wireless signal.

In Figure 2, an example of the communication between the local device 10, the requester 4, the personal computing device 12, the third party device 6 and the token issuing device 8 is illustrated. This communication arises as a consequence of the local device 10 seeking a service from the requester 4, such as seeking to access a web based service, such as car rental. When the local device 10 seeks the service from the requester 4, it may request display of a webpage which indicates that the requester 4 requires some data to be supplied in order that it may provide the web service. As an example, the requester 4 may require personal identity and address details, or driving records, from a user in order to complete an online car rental booking. At step 22 in Figure 2 the local device 10 communicates with the requester 4. At step 24 the requester 4 sends a request to authorise a data access to third party data held by the third party device 6 back to the local device 10. As an example, the third party device 6 may store driving records for the individual seeking to make a car rental. At

step 26, the local device 10 which receives the request from the requester 4 via the internet 12 serves to relay the request to the personal computing device 12 via the short range Bluetooth wireless communication with the personal computing device 12. At step 28, the personal computing device 12 serves to validate the received request and determine whether that request is permitted or not permitted. If the request is permitted, then steps 30 and 32 send a message to the token issuing device 10 that a token for authorising access is to be sent from the token issuing device 8 to the requester 4 at step 34. This token permits the requester 4 to send a request for data to the third party device at step 36. The third party device 6 then forwards the token it has received from the requester 4 to the token issuing device 8 at step 38. The token issuing device at step 40 validates this token and, if valid, sends a reply at step 42 to the third party device 6 indicating that the token is valid. Upon receipt of such a message indicating that the token is valid, the third party device 6 at step 44 sends the data that was requested to the requester 4, e.g. sends the driving records for the owner of the personal computing device 12. At step 46, the requester 4 uses the requested data, such as by checking that the user has a satisfactory driving record, to permit them to rent a car. At step 48 a notification is sent to the local device that the requester 4 has received and used the data from the third party device 6.

Access tokens are used by a client to prove that it has prior authorisation from an authenticating party to a perform actions on a validating party, typically a resource server. Access tokens may take many forms, for example API keys or OAuth tokens, but fall in to one of two categories.

Bearer tokens may contain lists of permissions and describe the conditions under which they are granted, for example until a certain date, these particulars or a digest of them being signed by the issuer using their private key such that the validating party, being in possession of the issuer's public key, can assure itself that the token was indeed issued by said issuing party. Security tokens can be validated directly by the validating party without recourse to any other party.

Security tokens are simply strings of characters, long enough to be difficult to guess correctly. They should only be passed over encrypted connections to authenticated parties. They may be accompanied by further information, such as the identity of the issuer. An API request containing such a key will be accepted by the party receiving the request provided the request is

permitted by the permissions associated with the token. It may change or revoke these permissions at any time. Third parties may issue tokens provided they either apprise the receiving party of each new token before it is first used, or they accept validation requests to validate the keys on behalf of the receiving parties.

Figure 3 is a flow diagram schematically illustrating request processing by the local device 10. At step 50 processing waits until a request for authorisation is received from a requester 4. At step 52 a determination is made by the local device 10 based upon comparing the signal strength for two-way communication with the personal computing device 12 with a threshold level in order to determine whether or not the personal computing device 12 is proximal to the local device 10. If the personal computing device 12 is not proximal to the local device 10, then step 54 serves to notify the requester 4 that the authorisation has failed. If the determination at step 52 is that the personal computing device 12 is proximal to the local device 10, then step 56 serves to send the request from the local device 10 to the personal computing device 12.

At step 58, the local device 10 waits to receive a message from the personal computing device 12 as to whether or not a message is to be sent to the token issuing device 8 indicating that the token issuing device should issue a token to the requester 4. If the message received at step 58 is that the token issuing device 8 should not send a token to the requester 4, then processing proceeds to step 54 and the requester 4 is notified that the authorisation has failed. If the message received at step 58 is that a message is to be sent to the token issuing device 8, then step 60 serves to relay such a message from the personal computing device 12 to the token issuing device 8. Processing then waits at step 62 for notification from the requester 4 that it has received its data following a successful interaction with the token issuing device 8 and the third party device 6. When such a notification is received, then step 64 serves to display on the local device an indication of what data has been supplied.

Figure 4 is a flow diagram schematically illustrating request processing by the requester 4. Processing waits at step 66 until a local device 10 requests a service from the requester 4. At step 68 the requester 4 sends a request for authorisation for data it requires in order to fulfil the service to the local device 10. Processing then proceeds through steps 70 and 72 to identify that either a token has been received from the token issuing device 8 to be used to perform the access or that an authorisation failed notification has been received. If an authorisation failed notification is received, then

processing proceeds to step 66 and the service requested is denied. If a token is received from the token issuing device at step 70, then processing proceeds to step 74 where the requester 4 sends a request for the data being sought to the third party device 6 accompanied with the token it received from the token issuing device 8. The requester 4 then waits at step 76 for the data to be received from the third party device 6. When the data is received, step 78 uses this data, such as ensuring that a driver has an appropriate driving record for the car rental being set up, and processing then proceeds to step 80 where a message is sent to the local device 10 to notify the local device that the data has been received.

Figure 5 is a flow diagram schematically illustrating request processing performed by the personal computing device 12. At step 82 the personal computing device 12 waits for a request to be received from the local device 10. When such a request is received, then step 84 determines whether or not the personal computing device 12 is currently in its authorised state or its unauthorised state. If the personal computing device 12 is in its unauthorised state, then processing proceeds to step 86 where a refused request indication is displayed by the personal computing device 12 and processing returns to step 82.

If the determination at step 84 is that the personal computing device 12 is in its authorised state, then step 88 determines whether or not the request is a permitted request. This may be achieved by comparing the request with permission data stored within the personal computing device 12. This permission data may indicate different types of data which are permitted to be authorised for distribution and/or different requesters who may be authorised in respect of different types of data or individual items of data or combinations of the preceding. It will be appreciated that the permission data could take a wide variety of different forms and the present techniques encompass such forms.

If the determination at step 88 is that the request is not permitted, then processing again proceeds to step 86. If the determination at step 88 is that the request is permitted, then processing proceeds to step 90 where a determination is made as to whether or not the request is one classified as automatically permitted. If the request is automatically permitted, then processing proceeds to step 92 where a message to send an authorisation token is sent to the token issuing device 8 via the local device 10. Step 94 then displays an indication on the personal computing device of the type of data access that has been authorised. This indication may be, for example, in the form of displaying an

associated type of icon indicating the nature of the data for which authorisation has been granted.

If the determination at step 90 is that the request is not an automatically permitted request, then step 96 displays a prompt indication to the user of the personal computing device so as to prompt the user to make a user input to either authorise the request or not authorise the request. The user input may, for example, take the form of pressing a button to indicate that the request is either authorised or not authorised, entering a personal identification number to authorise a request, tapping an icon on a screen to authorise a request or some other predetermined user input. Step 98 determines from the user input whether or not the request is authorised. If the request is not authorised, then processing proceeds to step 86. If the request is authorised, then processing proceeds to step 92.

Figure 6 is a flow diagram schematically illustrating request processing performed by the third party device 6. At step 100 the third party device 6 waits until a request for data and an associated token is received from the requester 4. When such a request and token are received, then step 102 sends the token to the token issuing device 8 associated with that token. Step 104 then waits until a token response is received and determines whether this token response is a token valid response. If the token response was a token valid response, then step 106 sends the data requested to the requester 4. If the token response was not that the token is valid, then processing returns to step 100.

Figure 7 is a flow diagram schematically illustrating request processing by the token issuing device 8. At step 108 processing waits until a message is received from the personal computing device 12, as relayed by the local device 10, that a token authorising access should be sent to the requester 4. When such a message is received at step 108, step 110 sends the associated token from the token issuing device 8 to the requester 4. At step 112, the token issuing device, at least in association with the token that has been issued, waits to receive back from a third party device 6 the token that it sent to the requester 4 in order that it may validate that token. When a candidate token is received, step 114 determines whether or not it is valid. If the token is valid, then processing proceeds to step 116 at which a token valid response is sent to the third party device 6, which will in turn authorise the third party device 6 to send the requested data to the requester 4. If the determination at step 114 is that the token is not valid, then processing proceeds to step 108.

Figure 8 schematically illustrates the interaction between the personal computing device 12

and the local device 10. The personal computing device 12 includes a processor 118, a memory 120, a strap closure monitoring circuit 122, a display 124 and a Bluetooth Low Energy Transmitter/Receiver circuit 126. The memory 120 stores permission data specifying which requests will and will not be authorised, and whether or not those requests are automatically authorised or are optionally authorised requests. Optionally authorised requests require a predetermined user input following display of a prompt indication in order to authorise the data to which they relate to be released. The memory 120 also stores icon data defining icons which are displayed to indicate which types of data are being authorised to be released (or requested) as will be described later. The Bluetooth circuit unit 126 includes signal strength monitoring circuitry which serves to detect the proximity of the local device 10 to the personal computing device 12. This proximity can be compared with a threshold level of proximity in order to determine, at least in part, whether the personal computing device 12 is proximal to the local device 10.

It will be appreciated that the memory 120 stores a computer program that is executed by the processor 118. Such a processor 118 operating under program control can serve as, for example, state determining circuitry for determining whether or not the personal computing device 12 is in an authorised state, permission determining circuitry for comparing a received request with the stored permission data and circuitry serving to either authorise or not authorise provision of data from the third party device 6 to the request 4 in accordance with the above discussions. In general, the processor 118 operating under program control, as well as other processors within the system, may be thought of as providing various forms of circuitry for performing specified functions. As will be familiar to those in this technical field, particular specified functions may be performed either with a program general purpose processor or with dedicated circuitry depending upon the design requirements. Circuitry for performing the various functions described herein may be provided in either manner.

The local device 10, which may be a terminal device in the form of a personal computer, includes a processor 128, a memory 130, a Bluetooth Low Energy Transmitting/Receiver circuit 132 for communicating with the personal computing device 12, and a network interface 134 for communicating with the internet 11. The memory 130 stores a login data store comprising a list of usernames and passwords associated with different websites or web services. This login data store can take the form of a password keyring which is either locked or unlocked. When the login data store is unlocked, then if the local device 10 accesses a webpage or web service that requires a

password to be entered, then if this password is present within the unlocked login data store, the username and password are automatically provided so as to unburden the user from the need to perform this task. The same process may also be applied to logging on to a computer itself. In many embodiments, the process may be seamless such that the login process takes place without any user intervention.

Figure 9 is a flow diagram schematically illustrating lock control of the login data store by the local device 10. At step 136 the login data store is initialised into a locked state. At step 138 a determination is made as to whether or not the personal computing device 12 is proximal to the local device (terminal device) 10. If the personal computing device is not proximal to the terminal device 10, then processing waits at step 138. When the personal computing device 12 becomes proximal to the terminal device 10, then processing proceeds to step 140 where a determination is made as to whether or not the personal computing device is in its authorised state. The personal computing device 12 reports this state to the terminal device 10. If the personal computing device is not in its authorised state, then processing again returns to step 138. If the personal computing device 12 is in its authorised state, then step 142 serves to switch the login data store into its unlocked state. Step 144 then determines whether or not the personal computing device remains proximal to the terminal device 10. If the personal computing device 12 is not proximal to the terminal device 10, then step 146 serves to switch the login data store from its unlocked state to its locked state. If the determination at step 144 is that the personal computing device 12 remains proximal to the terminal device 10, then step 148 also serves to determine that the personal computing device 12 remains in its authorised state before returning to step 144. If the personal computing device 12 is not in its authorised state, then processing again proceeds to step 146. Accordingly, steps 144 and 148 in combination serve to maintain the login data store in the unlocked state providing the personal computing device 12 remains proximal to the terminal device 10 and the personal computing device 12 remains in its authorised state.

Figure 10 is a flow diagram schematically illustrating login data provision by the terminal device 10. At step 150 processing waits until the terminal device 10 receives a request for login data from a requester 4. Step 152 determines whether the login data store is in its unlocked state. If the login data store is not in its unlocked state, then processing proceeds to step 154 where the user is prompted to provide manually the login data requested. If the determination at step 152 is that the

login data store is unlocked, then step 156 accesses this login data and determines whether or not the login data store contains the login data being requested at step 150. If the login data store does not contain the requested login data, then processing again proceeds to step 154. If the determination at step 156 is that the login data store does contain the requested login data, then step 158 serves to return this login data to the requester 4 without requiring user input by the user. An indication that such login data had been automatically provided may be displayed to the user via the terminal device 10 and/or the personal computing device 12.

Figure 11 is a flow diagram schematically illustrating authorised state switching performed by the personal computing device 12. At step 160 the personal computing device 12 is initialised into an authorised state. Step 162 then displays a prompt to the user to make a predetermined input in order to switch the personal computing device 12 from the unauthorised state to the authorised state. Such a predetermined input may take a variety of different forms, such as entering a personal identification number, scanning a fingerprint, scanning of another biometric parameter, or various other ways of validating a user.

Step 164 determines whether the user input at step 162 was valid. If the user input was not valid, processing returns to step 162 and the personal computing device 12 remains in the unauthorised state. If the input received at step 162 was valid, then step 166 serves to switch the personal computing device 12 from the unauthorised state to the authorised state. Processing then passes to step 168. Step 168 serves to continuously monitor that the personal computing device 12 remains under the user's physical possession. This may, for example, be carried out by monitoring the closure of the watch clasp 18 to ensure that this remains closed indicating that the watch strap 16 and the watch body 14 are attached to the user. Other forms of confirmation of physical possession are also possible, such as monitoring biometric parameters of the user, such as heart activity, characteristic motion etc. If the determination at step 168 at any time is that the personal computing device 12 has ceased to be in the continued physical possession of the user, then processing proceeds to step 170 where the personal computing device 12 is switched from the authorised state back to the unauthorised state and processing is returned to step 162.

Figures 12, 13 and 14 schematically illustrate displays which may be presented to the user on the personal computing device 12. Figure 12A illustrates a normal time display when the personal

computing device 12 is being used as a watch. Figure 12B illustrates an icon which is displayed when identity data is being authorised for provision to the requester 4 or, at least requested. The use of a small set of known icons to represent the data being authorised facilitates the user in understanding which actions are being taken by the personal computing device 12 and what data is being released to the requester 4. Figure 12C illustrates an icon which is displayed when key data is being provided. This key data may be, for example, password data and username data of a wide variety of different forms used to control access to an account or service in one of many known ways.

Figures 13 A, B, C respectively indicate icons displayed where the data authorised for provision is insurance data, vehicle related data and health data of the user. The data authorised for provision is stored by the third party device 6. Different types of data may be stored in different third party devices. For example, insurance data may be held within the web server of an insurance company whereas health data may be held within the web server of a health provider.

Figure 14 schematically illustrates an indication which is displayed to the user when a request for authorisation to access data is refused. This icon is in the form of a no entry sign.

Figure 15 schematically illustrates a personal computing device 12 in the form of a smart watch in which an icon is displayed indicating that key data is potentially authorised for release (e.g. in response to an optionally-authorised request). The personal computing device 12 includes a user activated button 172 which the user can press within a predetermined period to authorise the request for release of key data. The button 172 may be illuminated when a user input (or not) using the button is required.

The display of icons as illustrated in Figures 12, 13, 14 and 15 indicating the type of data to be released, provides a back channel of communication to the user of the personal computing device 12 to permit them to more readily understand the nature of the authorisations being requested and made.

Figure 16 schematically illustrates a data processing system including a personal computing device 200, which receives a request to authorise the provision of data from a requester 202. This request is passed via the internet and a local terminal 204 using internet connections and a wireless

two-way communication link between the local terminal 204 and the personal computing device 200. Also communicating via the internet are a third party device 206, which stores the data being requested, and an authorising server 208 which may authorise the requester 202 to retrieve the data from the third party device 206. The authorising server 208 may be instructed by the personal computing device 200 to issue a token to the requester 202. This token may be sent by the requester 202 to the third party device 206 accompanying their request for data and the third party device 206 may validate the authenticity of the token with the authorising server 208 before returning the requested data to the requester 202.

The requester 202 may request the data as a consequence of a request for a web service initiated by a user of the personal computer device 200 using the local terminal 204. For example, the user may access a website associated with the requester 202 and seek to obtain services of the requester 202. The requester 202 may display its webpage, as illustrated in Figure 16, and use icons supplied by the authorising server 208 to indicate the nature of the data that the requester 202 is requesting as well as a policy, such as retention policy, to be associated with the use of that data by the requester 202. In another embodiment, the token is valid for a defined period of time and is accepted by the third part device without being further validated with the authorising server. In such an embodiment the token may be issued by the personal device.

The retention policy may be selected from a group of predetermined retention policies including: the data is permanently retained by the requester, the data is retained until completion of a transaction associated with that data, the data is retained for use by the requester to perform a predetermined processing task and thereafter will not be retained by the requester, the data is retained by the requester for a predetermined period of time, and the data is retained for use by the requester for a predetermined number of times and thereafter will not be retained by the requester.

A set of policy icon overlays, each associated with a different one of these retention policies, may be stored and provided by the authorising server 208 for display on the display of the local terminal 204 as illustrated. The same policy icons may also be displayed as overlays upon a data type icon on the display of the personal computing device, such as in the form of a wearable computing device, e.g. a smart watch. The person computing device 200 may store its own version of the icons as a double-check to indicate that the data type icon and the policy icon overlay displayed upon the

personal computing device 200 match the data type icon and policy icon overlay displayed upon the display of the local terminal 204 and associated with the requester 202. In practice the personal computing device may display the data type icons and the policy icon overlays in sequence as the display of the personal computing device may be too small to display all of these icons simultaneously.

Figure 17 schematically illustrates a variety of different types of policy icon. These icons may include an hour glass indicating a time limited policy whereby the data is retained by the requester for a predetermined period of time. Another example is an icon in the form of a safe indicating that the data will be permanently retained by the requester. Another example is in the form of a pin indicating that the data is retained until completion of the transaction associated with the data. Another icon is in the form of a tool indicating that the data is retained for use by the request to perform a predetermined processing task and thereafter will not be retained by the requester. The final example policy icon overlay is in the form of a sequence of pages indicating that the data is retained for use by the requester a predetermined number of times and thereafter will not be retained by the requester.

Figures 18, 19 and 20 illustrate data icons with policy icons overlaid thereupon. Each of these Figures illustrates a display on the personal computing device 200 serving as a data indication of what data has been requested by the requester 202 and a policy indication of what policy (retention policy) is associated with that data. In the example of Figure 18, personal identification data has been requested and this data will be held permanently by the requester 202. In the example of Figure 19, insurance data has been requested and this data will be held by the requester 202 until the transaction has been completed. In the example of Figure 20 health data has been requested and this data will be held by the requester 202 for a limited period of time. It will be appreciated that these same data icons and policy icons can be displayed upon the display of the local terminal 204 and they can be matched by the user. The use of a relatively small number of icons to represent a wide number of different combinations facilitates user understanding of the nature of the data they are authorising for provision and the policy to be applied to the retention of that data by the requester 202.

CLAIMS

1. A method of controlling provision of data, said method comprising the steps of:

sending a request for said data from a requester to a personal computing device, said request identifying said data and a policy to be associated with said data;

receiving said request at said personal computing device;

determining with said personal computing device if said request is a permitted request and

(i) if said request is a permitted request, then authorising said provision of said data to said requester; and

(ii) if said request is not a permitted request, then not authorising said provision of said data to said requester.

2. A method as claimed in claim 1, further comprising the step of:

indicating with an indication device of said personal computing device a data indication of what data has been requested by said requester and a policy indication of what policy is associated with said data.

3. A method as claimed in any one of claims 1 and 2, wherein said policy is a retention policy for said data applied by said requester.

4. A method as claimed in claim 3, wherein said retention policy is selected from a predetermined group of retention policies.

5. A method as claimed in claim 4, wherein that said predetermined group of retention policies includes one or more of:

said data is retained permanently by said requester;

said data is retained until completion of a transaction associated with said data;

said data is retained for use by said requester to perform a predetermined processing task and thereafter will not be retained;

said data is retained by said requester for a predetermined period of time; and

said data is retained for use by said requester a predetermined number of times and thereafter will not be retained.

6. A method as claimed in any one of the preceding claims, wherein said indication device is a display screen.

7. A method as claimed in claim 6, wherein said data indication includes a data icon identifying a data type of said data.

8. A method as claimed in any one of claims and 7, wherein said policy indication includes a policy icon identifying a policy type of said policy.

9. A method as claimed on claims 7 and 8, wherein said policy icon is overlaid on said data icon.

10. A method as claimed in any one of the preceding claims, comprising displaying on a display screen associated with said requester said data indication of what data has been requested by said requester and said policy indication of what policy is associated with said data.

11. A method as claimed in any one of the preceding claims, wherein said requester is a remote server communicating with said personal computing device via a local terminal device.

12. A method as claimed in any one of the preceding claims, wherein said step of determining includes said personal computing device communicating with an authorising server via a telecommunications connection.

13. A method as claimed in claim 10, claim 11 and claim 12, wherein said authorising server generates said data indication and said policy indication for display on said display screen associated with said requester.

14. A method as claimed in any one of the preceding claims, wherein said provision is by a third party device to said requester.

15. A method as claimed in any one of the preceding claims, wherein said personal computing device generates said data indication and said policy indication for display on said display screen of

said personal computing device in dependence upon a data type and a policy type indicated by said request.

16. A method as claimed in any one of the preceding claims, wherein said personal computing device determines if said request is a permitted request by validating said request with permission data stored in said personal computing device.

17. A method as claimed in claim 16, wherein if said permission data indicates said request is an automatically permitted request, then said personal computing device automatically authorises said provision and at least one of said data indication and said policy indication indicates that said request has been authorised.

18. A method as claimed in and one of claims 16 and 17, wherein if said permission data indicates said request is an optionally authorised request, then at least one of said data indication and said policy indication prompts a user of said personal computing device to provide a user input to one of (i) authorise said request whereupon said personal computing device authorises said provision; and (ii) not authorise said request.

19. A method as claimed in any one of claims 16, 17 and 18, wherein if said permission data indicates said request is an unauthorised request, then said personal computing device does not authorise said provision.

20. A method as claimed in any one of claims 16 to 19, wherein if said permission data indicates said request is an unauthorised request, then at least one of said data indication and said policy indication indicates that said request has not been authorised.

21. A method as claimed in any one of the preceding claims, wherein said personal computing device is a wearable computing device.

22. A personal computing device for controlling provision of data, said personal computing device comprising:

receiving circuitry configured to receive a request for said data from a requester, said request

identifying said data and a policy to be associated with said data;

determining circuitry configured to determine if said request is a permitted request and

(i) if said request is a permitted request, then authorising said provision of said data to said requester; and

(ii) if said request is not a permitted request, then not authorising said provision of said data to said requester.

23. A personal computing device for controlling provision of data, said personal computing device comprising:

receiving means for receiving a request for said data from a requester, said request identifying said data and a policy to be associated with said data;

determining means for determining if said request is a permitted request and

(i) if said request is a permitted request, then authorising said provision of said data to said requester; and

(ii) if said request is not a permitted request, then not authorising said provision of said data to said requester.

24. A method of controlling provision of data substantially as hereinbefore described with reference to the accompanying drawings.

25. A personal computing device substantially as hereinbefore described with reference to the accompanying drawings.

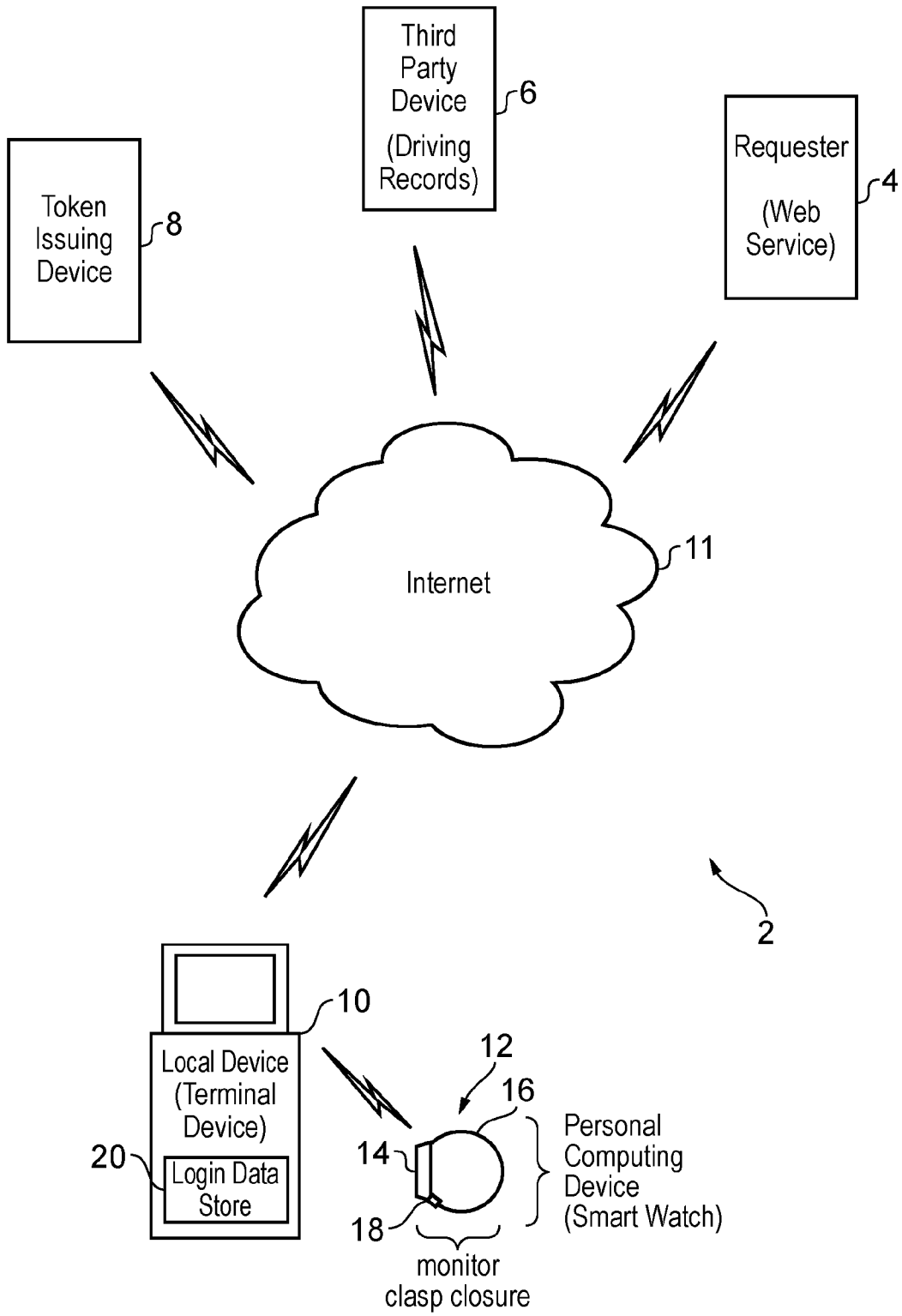
Third Party Device (Driving Records)
6
Requester (Web Service)
4
Token Issuing Device
8
Internet
11
2
10
Local Device (Terminal Device)
Login Data Store
20
12
16
14
18
Personal Computing Device (Smart Watch)
monitor clasp closure

FIG. 1

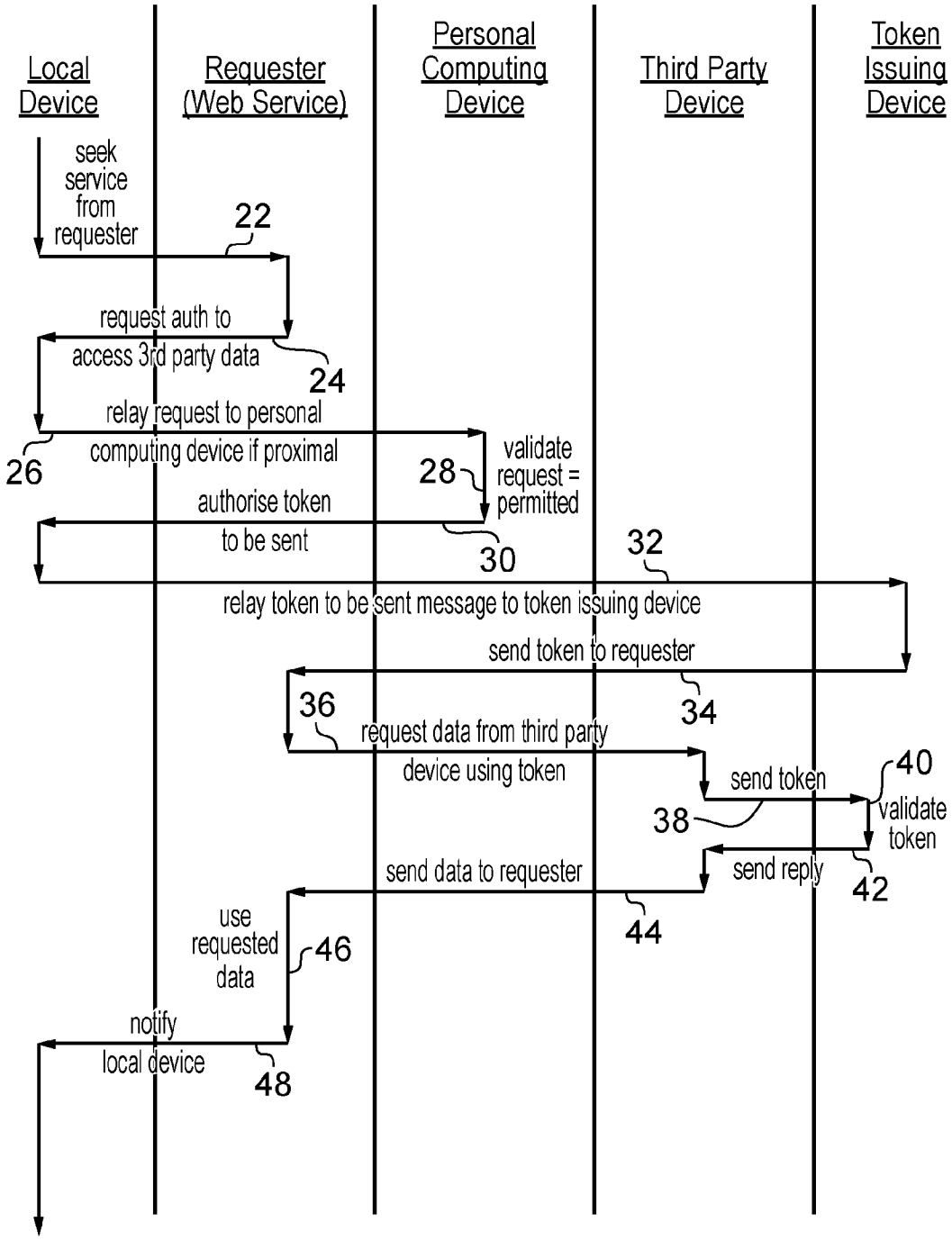
Local Device
Requester (Web Service)
Personal Computing Device
Third Party Device
Token Issuing Device
seek service from requester
22
request auth to access 3rd party data
24
relay request to personal computing device if proximal
26
28
validate request = permitted
authorise token to be sent
30
32
relay token to be sent message to token issuing device
send token to requester
34
36
request data from third party device using token
send token
38
40
validate token
send reply
42
send data to requester
44
use requested data
46
notify local device
48

FIG. 2

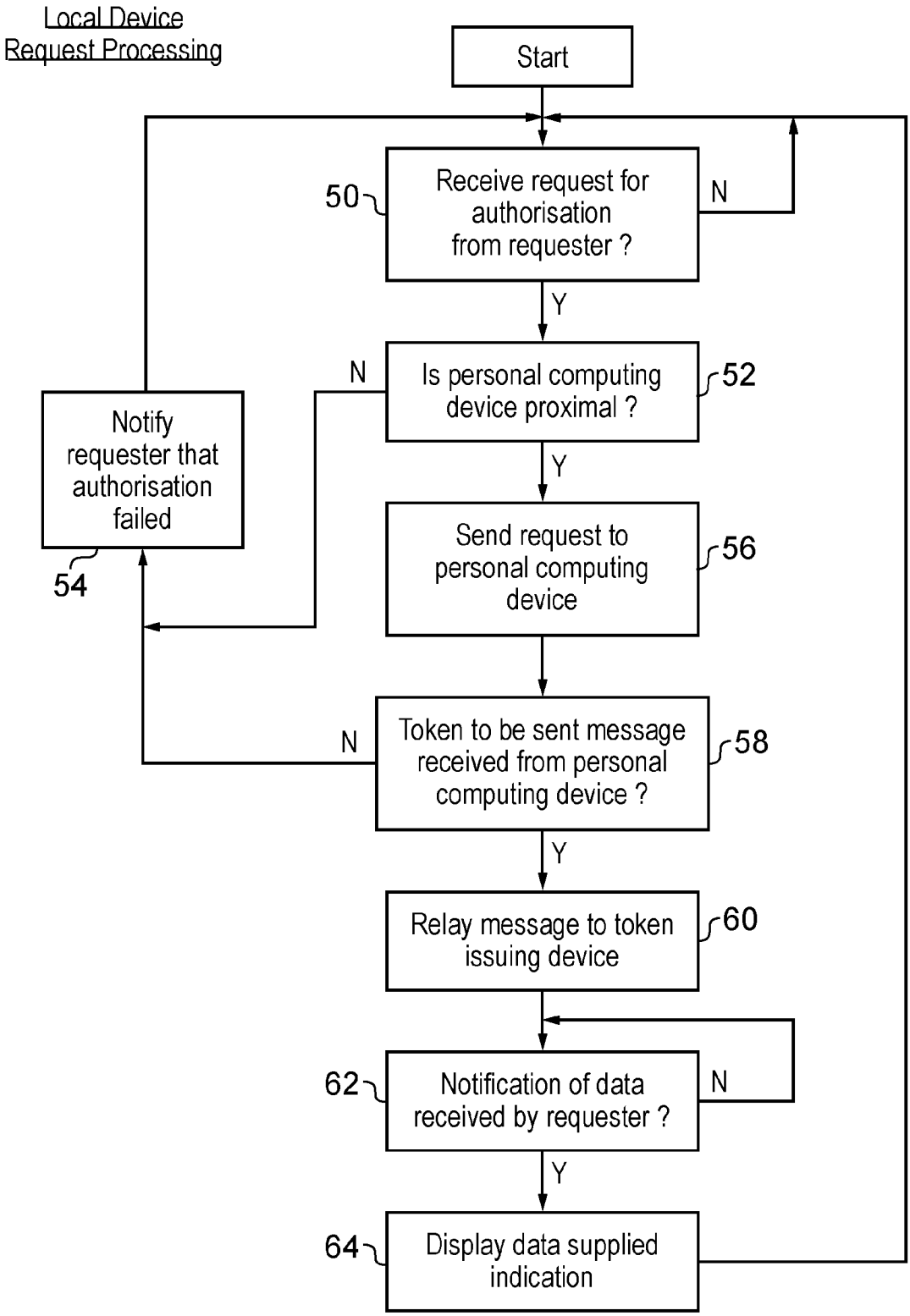
Local Device
Request Processing
Start
Receive request for authorisation from requester ?
50
N
Y
Is personal computing device proximal ?
52
N
Y
Notify requester that authorisation failed
54
Send request to personal computing device
56
Token to be sent message received from personal computing device ?
58
N
Y
Relay message to token issuing device
60
Notification of data received by requester ?
62
N
Y
Display data supplied indication
64

FIG. 3

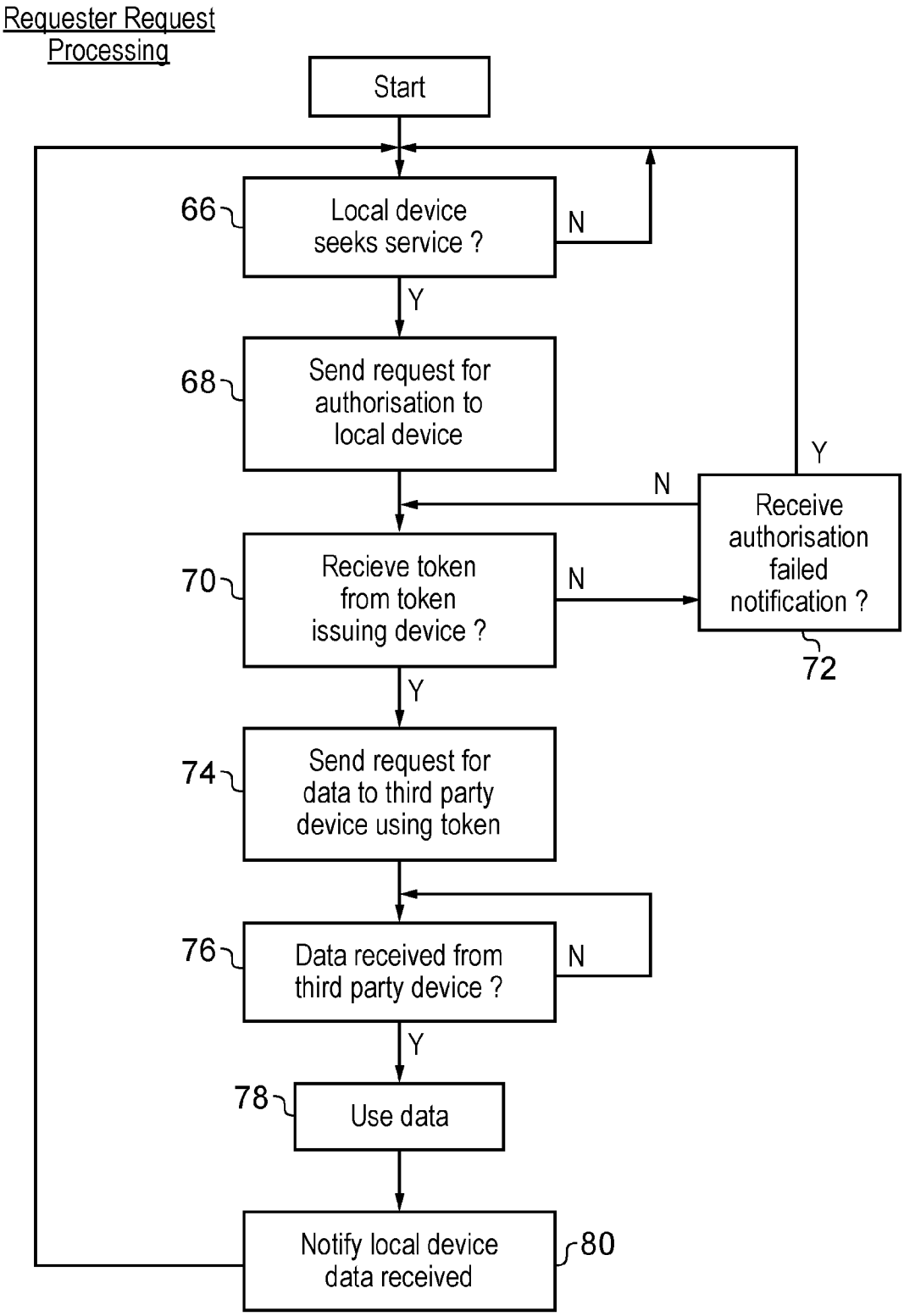
Requester Request Processing
Start
66
Local device seeks service ?
N
Y
68
Send request for authorisation to local device
Y
N
Receive authorisation failed notification ?
72
70
Recieve token from token issuing device ?
N
Y
74
Send request for data to third party device using token
76
Data received from third party device ?
N
Y
78
Use data
Notify local device data received
80

FIG. 4

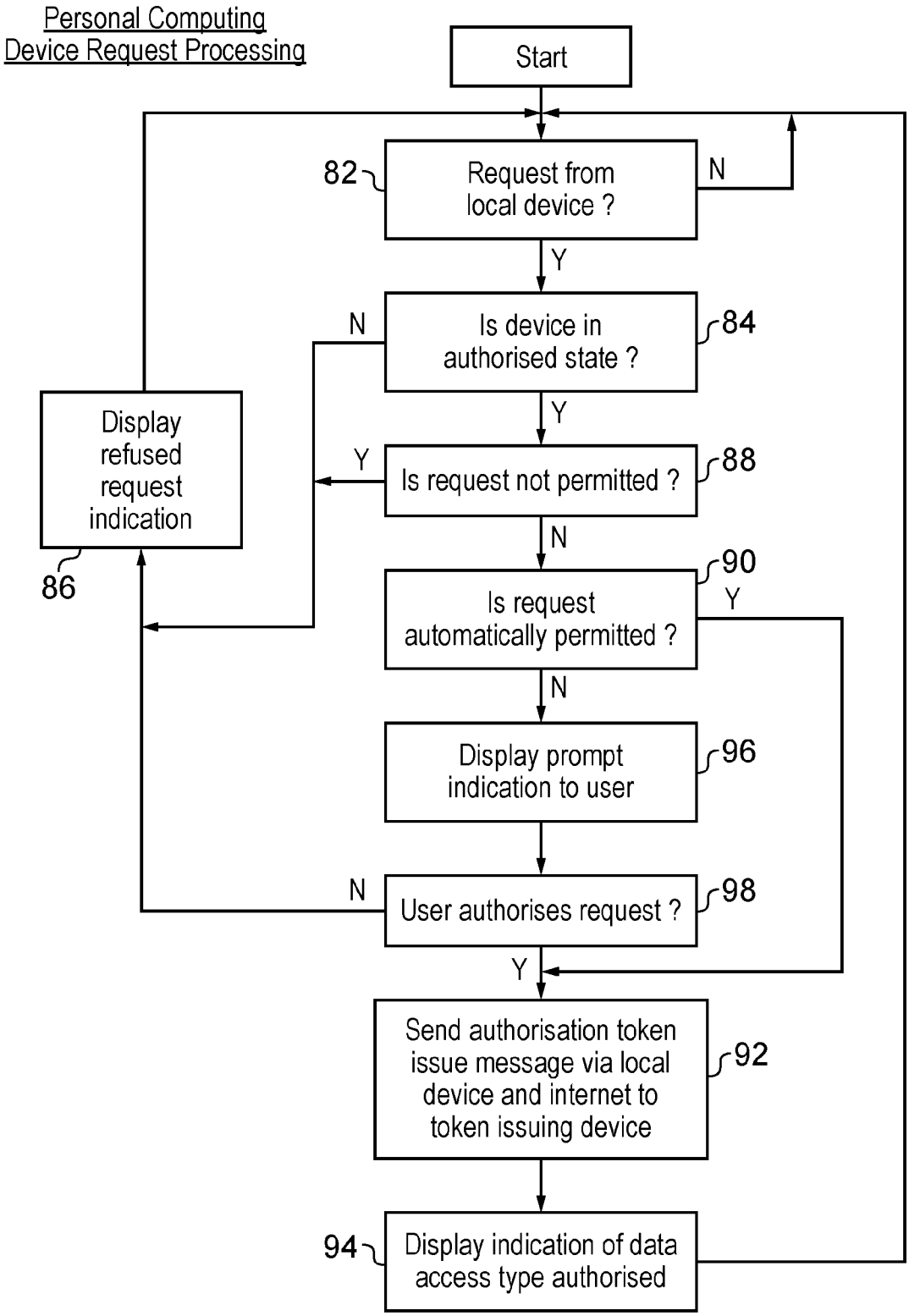
Personal Computing Device Request Processing
Start
82
Request from local device ?
N
Y
N
Is device in authorised state ?
84
Y
Display refused request indication
Y
Is request not permitted ?
88
N
86
90
Is request automatically permitted ?
Y
N
Display prompt indication to user
96
N
User authorises request ?
98
Y
Send authorisation token issue message via local device and internet to token issuing device
92
94
Display indication of data access type authorised

FIG. 5

Third Party Device
Request Processing

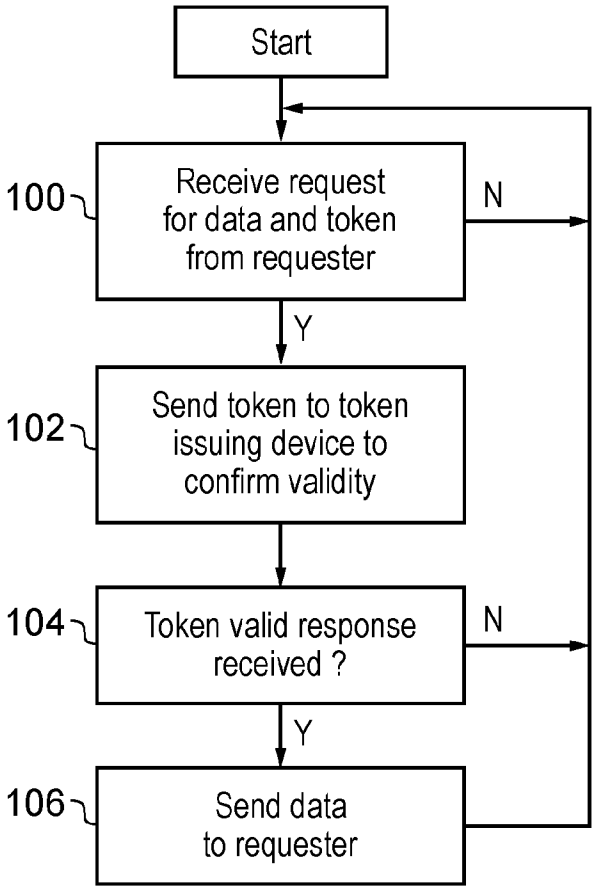

FIG. 6

Token Issuing Device
Request Processing

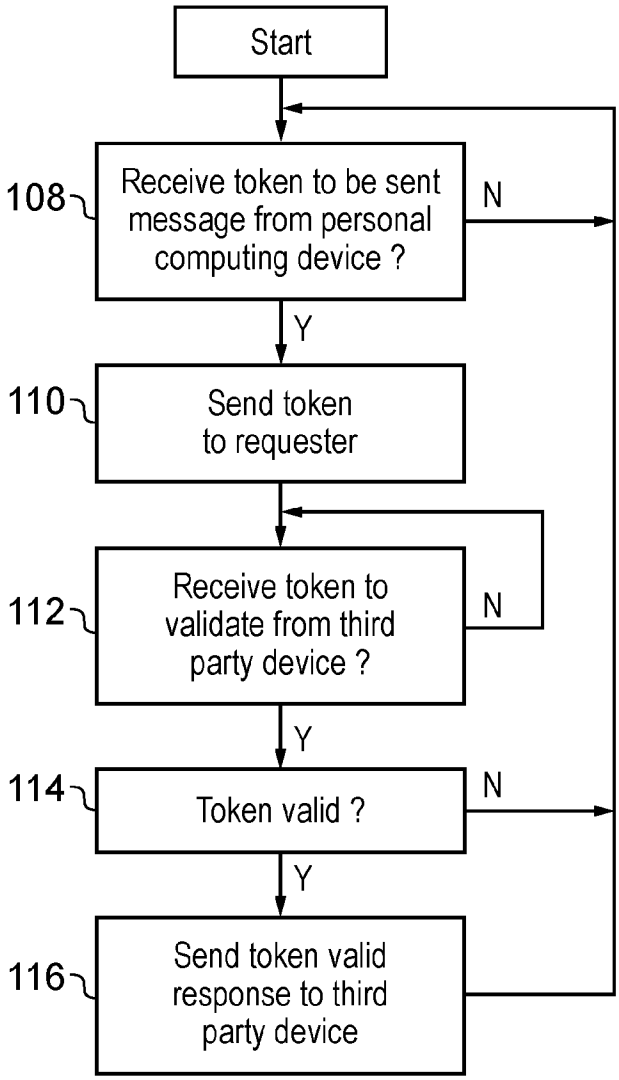

FIG. 7

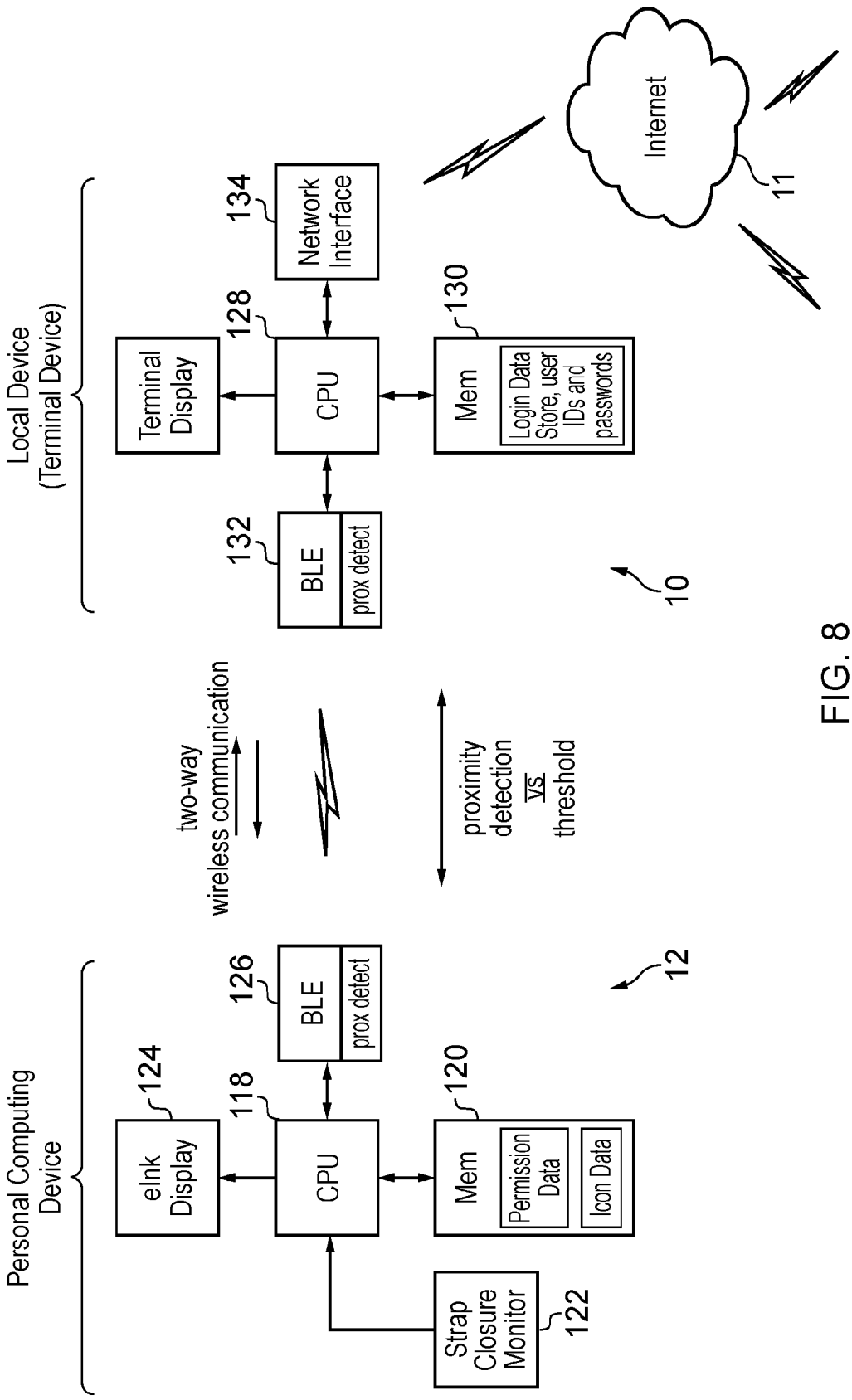
Internet
11
Local Device
(Terminal Device)
Network Interface
134
Terminal Display
CPU
128
Mem
130
Login Data Store, user IDs and passwords
BLE
prox detect
132
10
two-way wireless communication
proximity detection
vs.
threshold
12
Personal Computing Device
eInk Display
124
CPU
118
BLE
prox detect
126
Mem
120
Permission Data
Icon Data
Strap Closure Monitor
122

FIG. 8

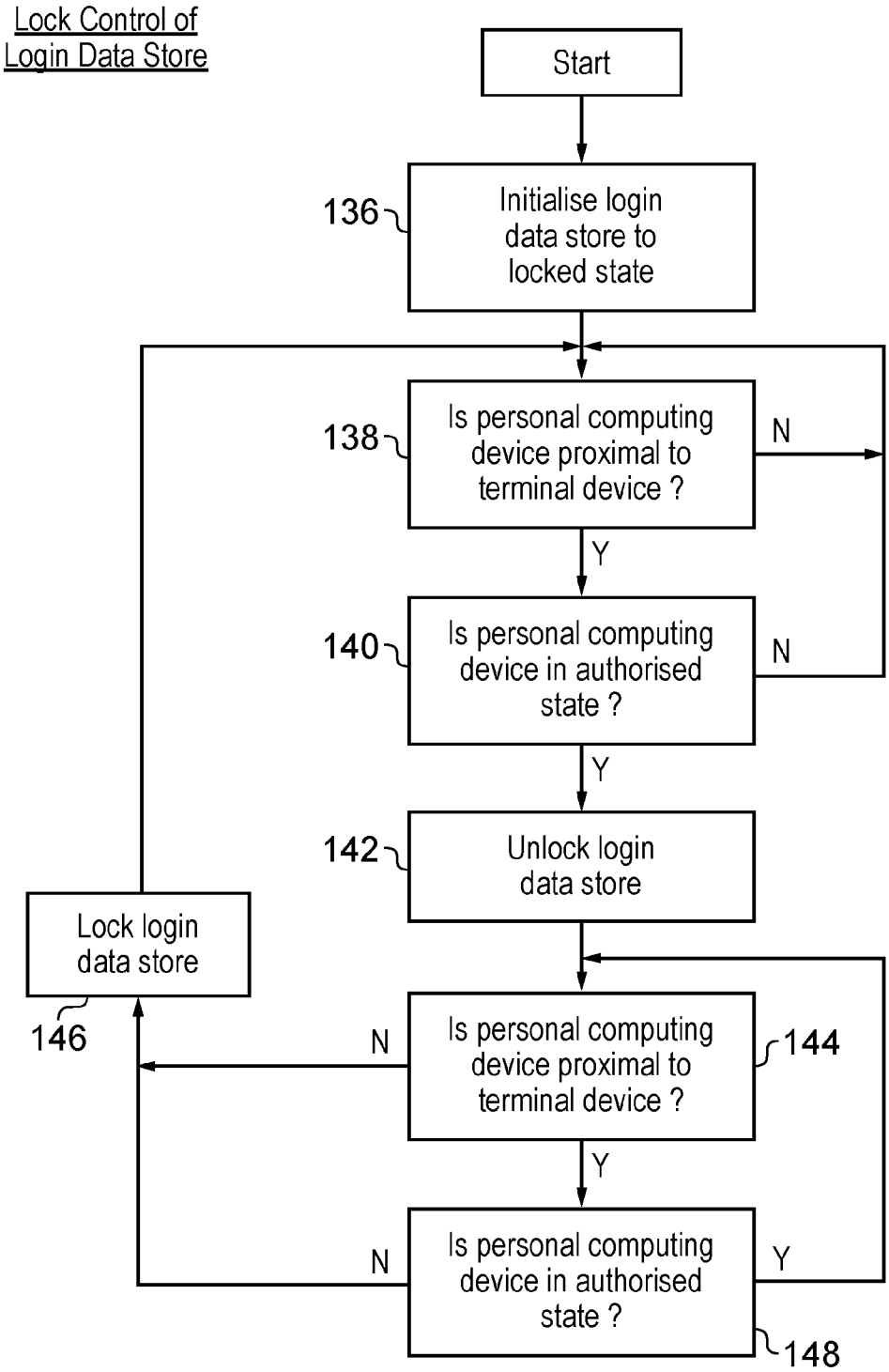
Lock Control of Login Data Store
Start
136
Initialise login data store to locked state
138
Is personal computing device proximal to terminal device ?
N
Y
140
Is personal computing device in authorised state ?
N
Y
142
Unlock login data store
144
Is personal computing device proximal to terminal device ?
N
Y
148
Is personal computing device in authorised state ?
N
Y
146
Lock login data store

FIG. 9

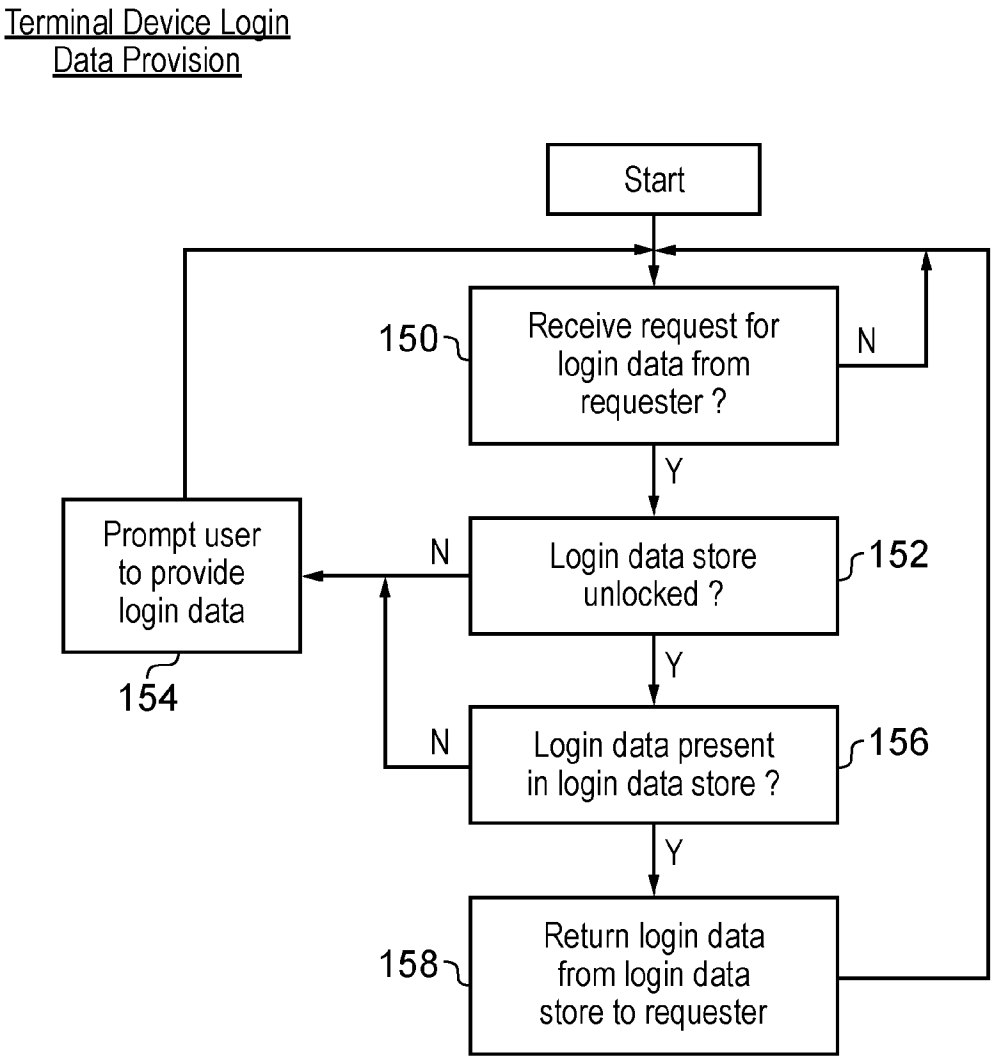
Terminal Device Login Data Provision
Start
150
Receive request for login data from requester ?
N
Y
Prompt user to provide login data
N
Login data store unlocked ?
152
154
Y
N
Login data present in login data store ?
156
Y
158
Return login data from login data store to requester

FIG. 10

Personal Computing Device Authorised State Switching

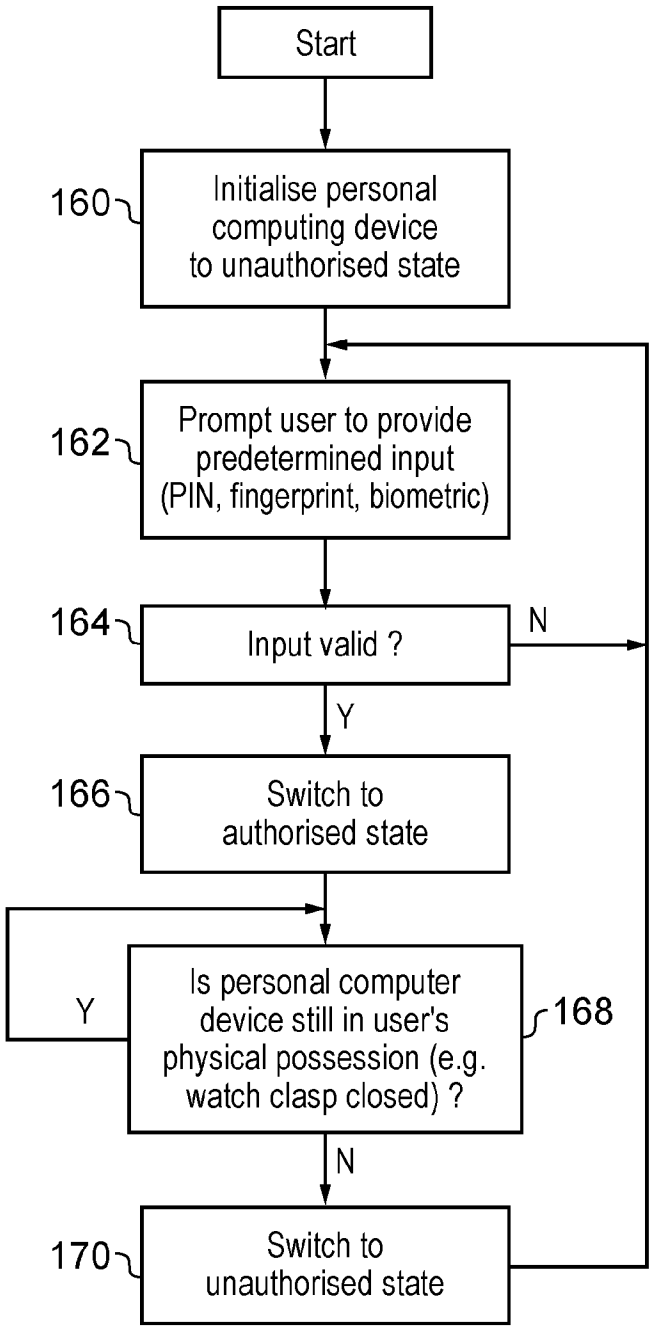

FIG. 11

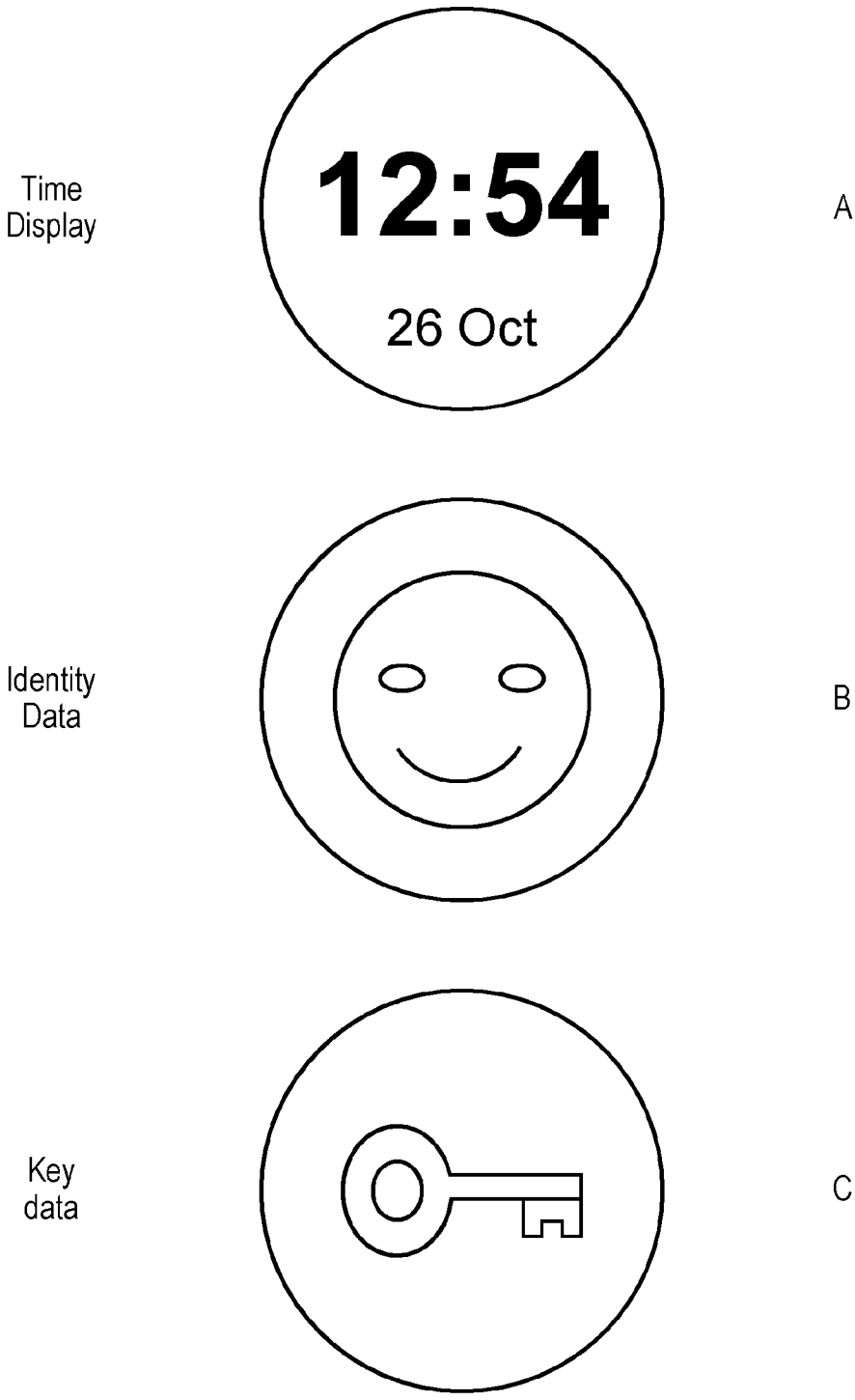

FIG. 12

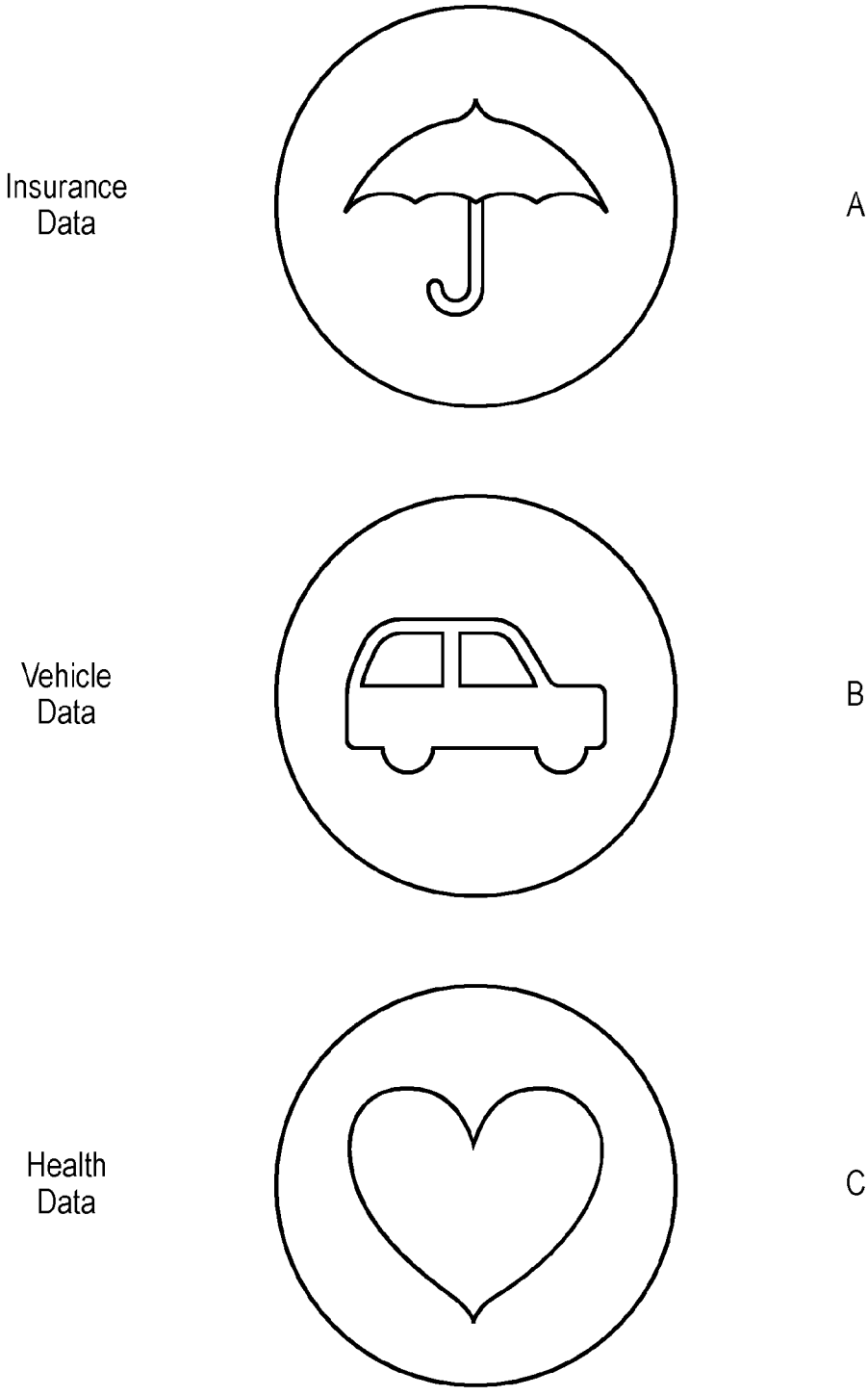

FIG. 13

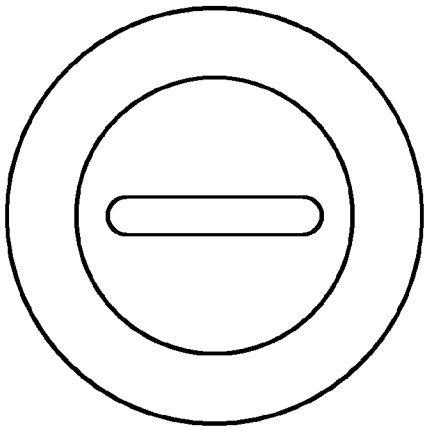

FIG. 14

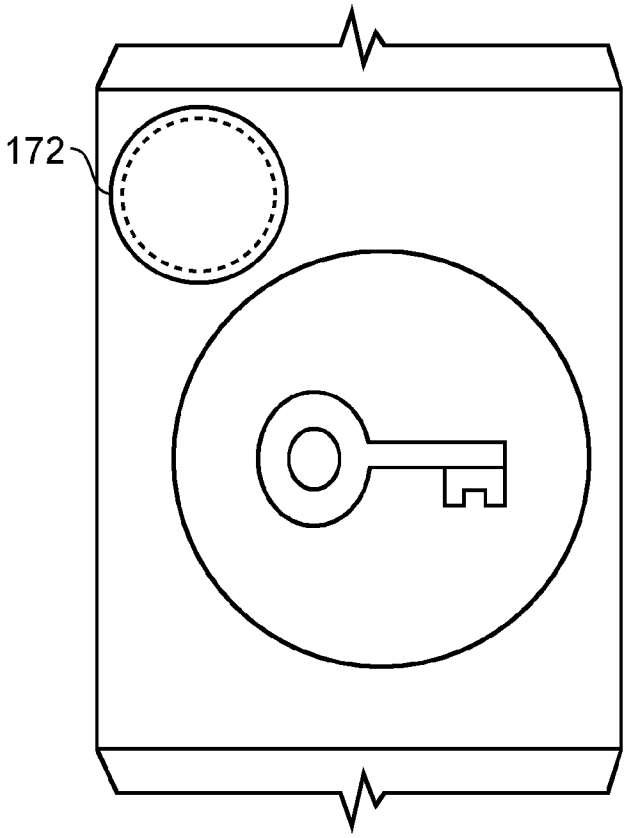

FIG. 15

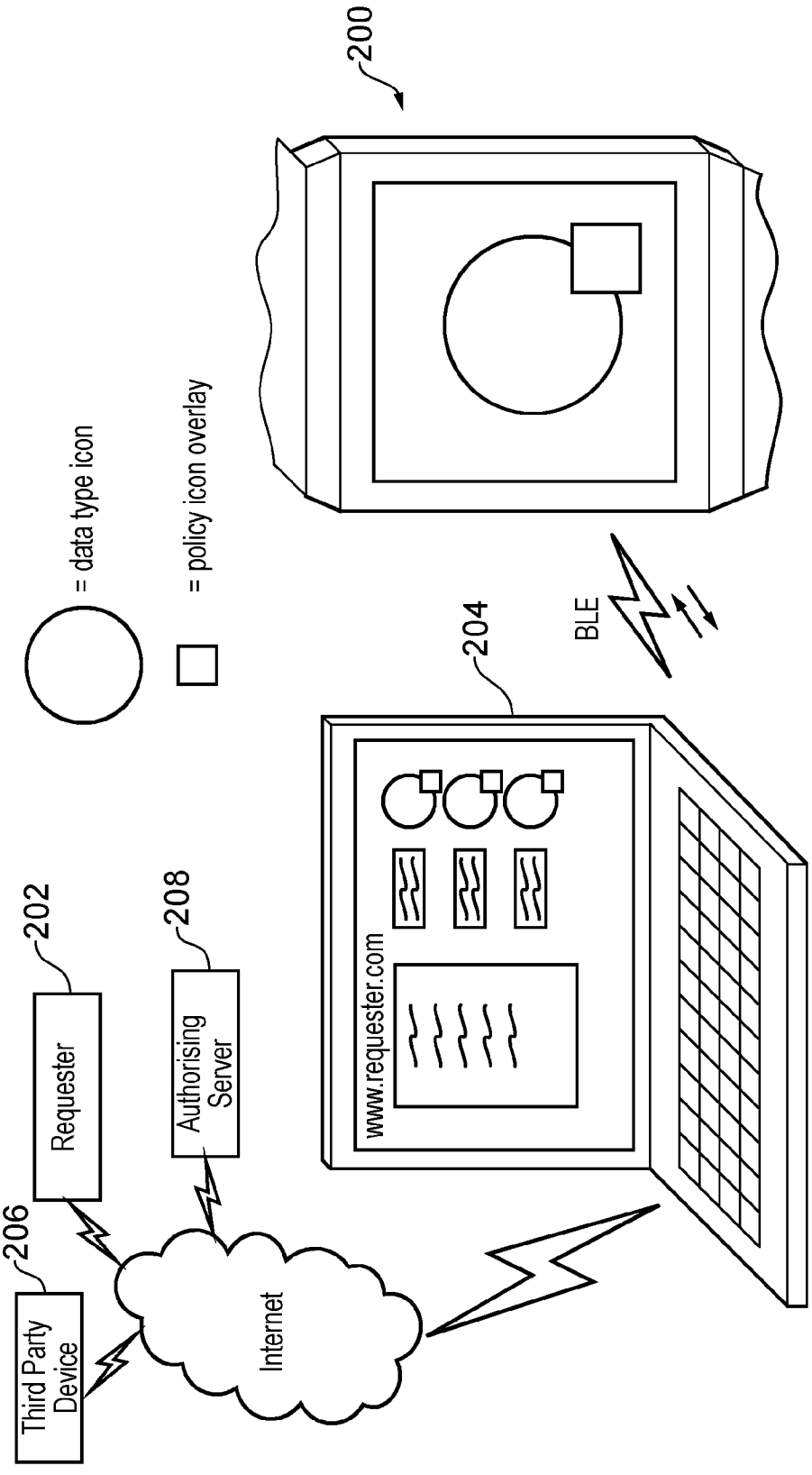
200
= data type icon
= policy icon overlay
BLE
204
www.requester.com
202
Requester
208
Authorising Server
206
Third Party Device
Internet

FIG. 16

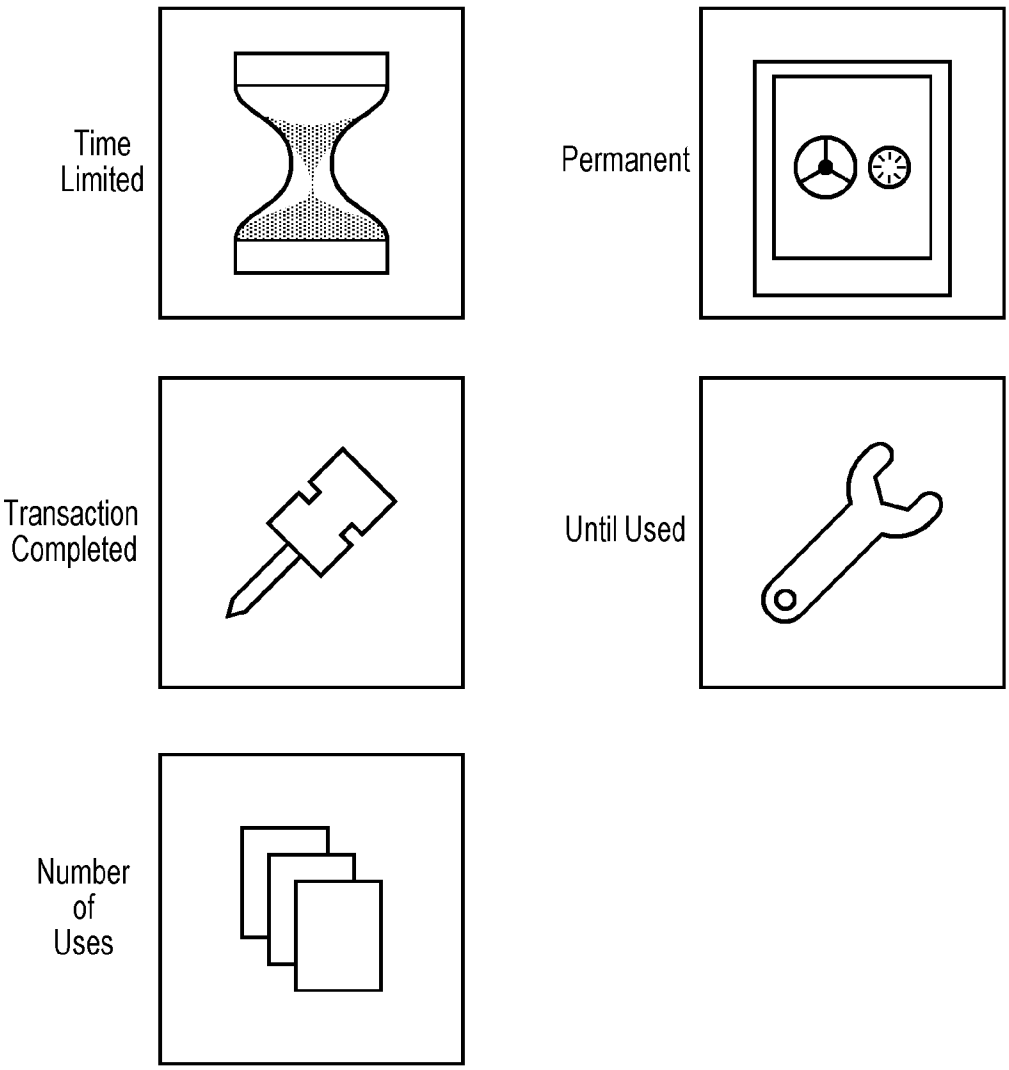
Time Limited
Permanent
Transaction Completed
Until Used
Number of Uses

FIG. 17

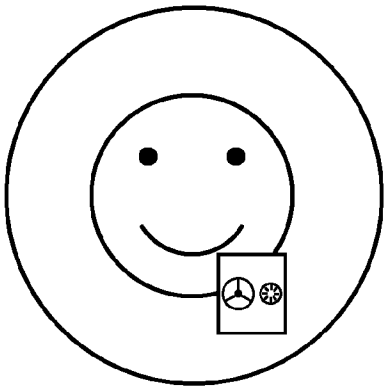

FIG. 18

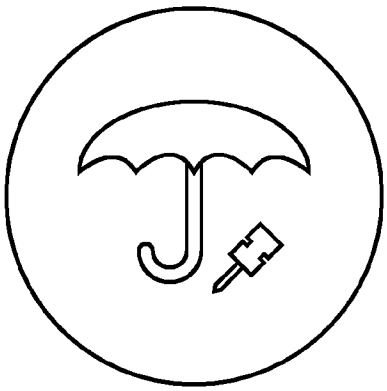

FIG. 19

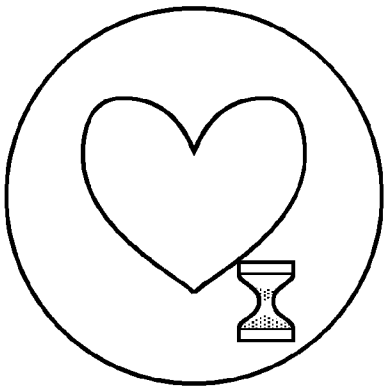

FIG. 20

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2014/053655

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/34 G06F21/35
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 H04L

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/010780 A1 (KANE JOHN RICHARD [US] ET AL) 13 January 2005 (2005-01-13) paragraphs [0001], [0008] - [0017], [0019], [0027] - [0029], [0042] - [0044] figures 1-4	1-4,6-25
X	WO 2004/047398 A1 (NOKIA CORP [FI]; AARTS ROBERT [FI]; BJORKSTEN MARGARETA [FI]; SKYTTA T) 3 June 2004 (2004-06-03) page 1, line 7 - page 1, line 24 page 2, line 25 - page 3, line 18 page 4, line 20 - page 8, line 33 figures 1, 4	1-25
A	US 2005/221798 A1 (SENGUPTA UTTAM K [US] ET AL) 6 October 2005 (2005-10-06) paragraphs [0001], [0008], [0018] - [0021] figures 1, 5	1-25

☐ 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	Date of mailing of the international search report
5 February 2015	12/02/2015

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

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/GB2014/053655

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005010780 A1	13-01-2005	US 2005010780 A1	13-01-2005
		WO 2005006147 A2	20-01-2005
WO 2004047398 A1	03-06-2004	AT 453277 T	15-01-2010
		AU 2003276287 A1	15-06-2004
		EP 1561322 A1	10-08-2005
		US 2005076233 A1	07-04-2005
		WO 2004047398 A1	03-06-2004
US 2005221798 A1	06-10-2005	NONE	