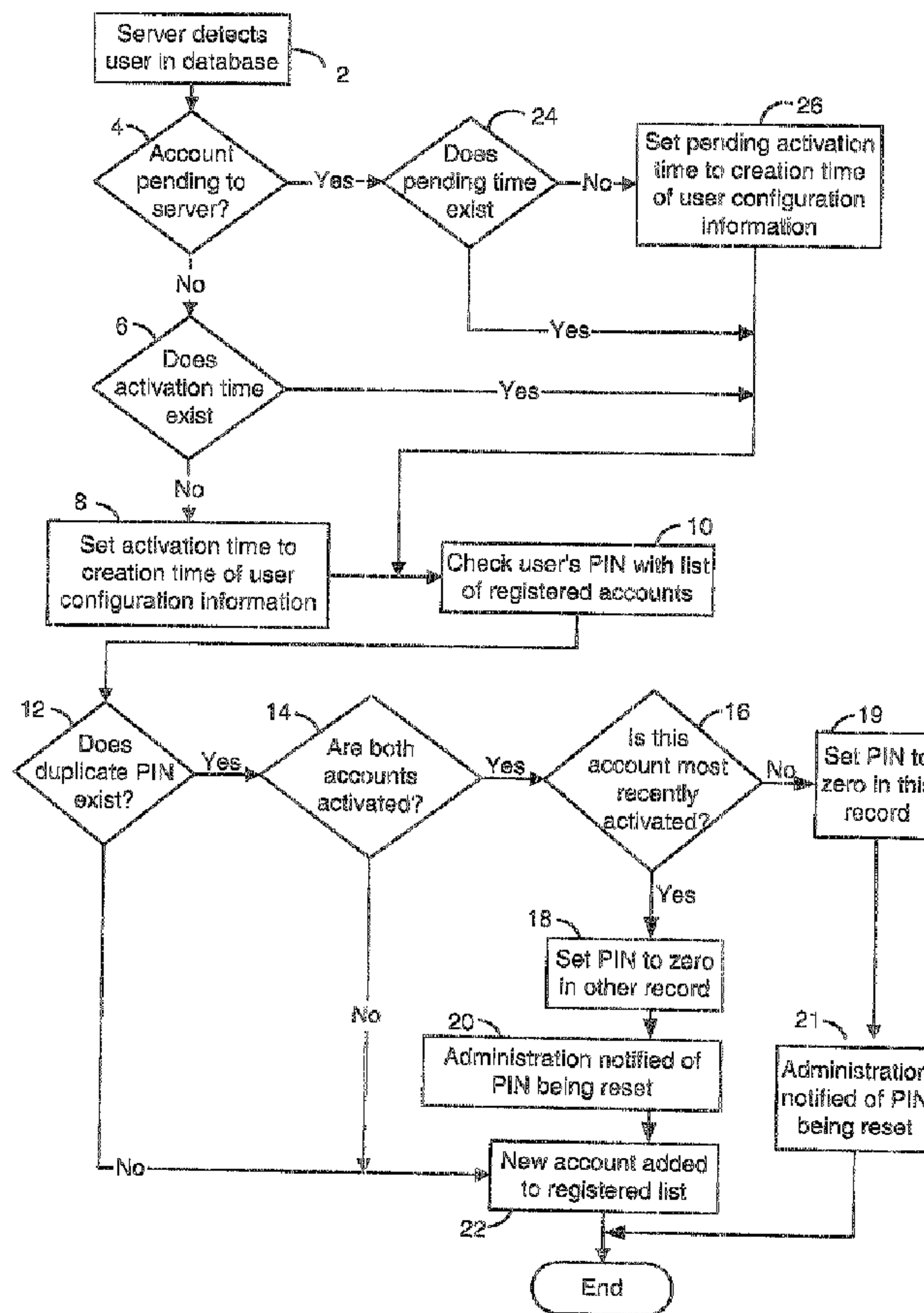




(22) Date de dépôt/Filing Date: 2002/02/20  
(41) Mise à la disp. pub./Open to Public Insp.: 2002/08/20  
(30) Priorité/Priority: 2001/02/20 (60/269,809) US

(51) Cl.Int.<sup>7</sup>/Int.Cl.<sup>7</sup> H04Q 7/36  
(71) Demandeur/Applicant:  
RESEARCH IN MOTION LIMITED, CA  
(72) Inventeur/Inventor:  
FERGUSON, TABITHA K., CA  
(74) Agent: PATHIYAL, KRISHNA K.

(54) Titre : DETECTION ET ELIMINATION DE NIP DOUBLES DE DISPOSITIF DE COMMUNICATION MOBILE  
(54) Title: DUPLICATE MOBILE DEVICE PIN DETECTION AND ELIMINATION



(57) Abrégé/Abstract:

A method and system for detecting and eliminating duplicate wireless mobile communications device Personal Identification Numbers (PINs) stored in user administration records associated with a server system is disclosed. The PIN of a wireless mobile

(57) **Abrégé(suite)/Abstract(continued):**

communications device stored in a user administration record is checked against other existing user administration records, and if a duplicate of the PIN is detected, the PIN in one of the user administration records is reset. Duplicate PIN detection and elimination operations are preferably performed each time a new user administration record is created but may possibly be performed in response to selection of a particular user account, PIN or user administration record.

**ABSTRACT OF THE DISCLOSURE**

A method and system for detecting and eliminating duplicate wireless mobile communications device Personal Identification Numbers (PINs) stored in user administration records associated with a server system is disclosed. The PIN of a wireless mobile communications device stored in a user administration record is checked against other existing user administration records, and if a duplicate of the PIN is detected, the PIN in one of the user administration records is reset. Duplicate PIN detection and elimination operations are preferably performed each time a new user administration record is created but may possibly be performed in response to selection of a particular user account, PIN or user administration record.

## **DUPLICATE MOBILE DEVICE PIN DETECTION AND ELIMINATION**

### **Field of the Invention**

This invention relates to user administration in a mobile communication system, and in particular to reconciling duplicate Personal Identification Number (PIN) registrations, i.e. the same device PIN being used by more than one user.

### **Description of the Prior Art**

Personal Identification Numbers (PINs) are used to identify a wireless mobile communications device within a communication network, hereinafter referred to primarily as a "mobile device". The registration of the mobile device in the communication network effectively associates the particular mobile device with a particular user messaging account.

In prior art communication systems, two user accounts with the same PIN could potentially be created within the same system. This could happen, for example, when a new user takes over a mobile device previously used by another user. When the mobile device PIN is associated with an account for the new user, but also remains associated with the previous user's account, this results in communications for the two different user accounts, such as host system mailboxes for example, being sent to a single mobile device, and vice versa. In a messaging system, network resources are therefore expended to deliver messages intended for one user's account to a different user's mobile device. For the intended recipient, this represents a substantial security issue, since another user

may be receiving his or her messages. Furthermore, for the mobile device user, increased message traffic due to messages for the other user account consumes mobile device power and resources, thus shortening battery life, and may also increase airtime costs.

When operating within a secure system, a mobile device and a host system  
5 which communicates with the mobile device sometimes use corresponding encryption keys in order for decryption of secure communications to occur successfully. Therefore, in the above example of a mobile device PIN being associated with two user accounts, associated although messages for both user accounts would be sent to the mobile device, messages for only one of the user accounts could be successfully decrypted at the mobile  
10 device. Since over-the-air protocols do not typically identify a user or user account, a host system would be unable to determine, using the device PIN, which user's account should be associated with the PIN. If the wrong account is chosen, then the associated encryption key will be used to encrypt a message, and attempts to decrypt messages at the mobile device would fail. Similarly, incoming message from a mobile device whose PIN has been  
15 associated with more than one user account might not be properly decrypted at a host system when an incorrect one of the user accounts is chosen.

Therefore, there remains a need for a system and method for detecting duplicate mobile device PIN assignments and reconciling such conflicting mobile device registrations.

20

### **SUMMARY OF THE INVENTION**

It is an object of the invention to detect and eliminate duplicate mobile device

PINs from user administration records.

A related object of the invention is to provide for detection and elimination of duplicate mobile device PINs from existing administration information when a new user or user account is added to a communication network.

5 In one aspect of the invention, a method for detecting and eliminating duplicate wireless mobile communications device PINs stored in user administration records associated with a server system comprises the steps of checking the PIN of a wireless mobile communications device stored in a user administration record against other existing user administration records, and if a duplicate of the PIN is detected in one of the  
10 other existing user administration records, then resetting the PIN in either the user administration record or the one of the other existing user administration records.

According to a related aspect of the invention, a system for detecting and eliminating duplicate wireless mobile communications device PINs in a communication system comprises a data store configured to store user administration records, each user  
15 administration record being adapted to include a PIN, and a server system configured to detect whether or not a PIN stored in a user administration record in the data store occurs in any other user administration record in the data store, and if so, to reset the PIN in either the user administration record or the other user administration record.

Further features of the invention will be described or will become apparent in  
20 the course of the following detailed description.

### **BRIEF DESCRIPTION OF THE DRAWINGS**

In order that the invention may be more clearly understood, the one or more

embodiments thereof will now be described in detail by way of example, with reference to the accompanying drawings, in which:

Fig. 1 is a block diagram of a communication system in which the invention may be implemented;

5 Fig. 2 is flow diagram showing an overview of a method to eliminate duplicate mobile device PINs;

Fig. 3 is a flow diagram depicting a method used when a user's mobile device PIN is changed; and

10 Fig. 4 is a flow diagram depicting a method used to rescan a user's mobile device PIN.

### **DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS**

As used in this description and the appended claims, a PIN refers to an identifier for a particular mobile device. It will be apparent to those skilled in the art to which the present invention pertains that different mobile devices and communications  
15 networks use different types of mobile device identifiers, including not only numbers but also combinations of numbers, letters and other characters. Therefore, the term "PIN" should be interpreted to include numeric as well as other types of mobile device identifiers.

A typical system in which the invention may be implemented is shown  
20 generally in Fig. 1, in which user workstations **126** and **128** operate within a local area network (LAN) **114** controlled by a server computer **111**. A component **112**, shown as a redirection server **112**, may be implemented for example as software installed and running

on the server computer **111** or may instead possibly be a separate server computer operatively associated with the server computer **111**. The redirection server **112** enables data items, such as email messages, calendar appointments, meeting reminders and the like, to be forwarded from the LAN **114** to a mobile device **124**. Such data items are sent  
5 through a wide area network (WAN) **118** such as the Internet, via a preferably high-bandwidth connection **117**, to a routing system **120**. The routing system **120** then forwards the data items through links **122** and one of a plurality of wireless networks **123** within which the mobile device **124** is adapted to operate. The mobile device **124** may for example be a mobile data communications device, a mobile voice communications device,  
10 a dual-mode communications device having both voice and data communications capabilities, a wireless mobile messaging client, a cellular telephone, a personal digital assistant (PDA) enabled for communications, a wireless modem, a one-way pager or a two-way pager.

Those skilled in the art will appreciate that a communications system may  
15 include many more components than those shown in Fig. 1. For example, although the network server **111** and redirection server **112** are shown as having direct connections **116**, **117** to the WAN **118**, it should be apparent that one or both of these connections may be indirect, possibly through further networks and computer systems which have not been shown in Fig. 1 to avoid congestion in the drawing. It is also contemplated that  
20 connections **116**, **117** may be implemented as a single shared connection which provides both the network server **111** and the redirection server **112** with access to the WAN **118**.

Operation of the system shown in Fig. 1 will now be described in further



detail. For example, an email message **A** destined for a user account on the network server **111**, originating at either a workstation such as **126** within the LAN **114** or arriving at the LAN **114** via its connection **116** to the WAN **118**, may be both received by the network server **111** and redirected by the redirection server **112** to a mobile device **124** associated  
5 with the user account. As shown in Fig. 1, once the message **A** has been received by the network server **111**, it may be accessed using a network workstation such as **128**. Redirection of the message **A** allows an owner of a user account to also receive the message **A** at a mobile device **124**.

The redirection server **112** preferably compresses and possibly encrypts the  
10 message **A**, repackages the compressed and possibly encrypted message **A** in an outer envelope **B**, and sends the repackaged message, **A** in **B**, to the mobile device **124**. The outer envelope **B** provides all the routing information required to deliver the message through the WAN **118**, routing system **120**, links **122** and a wireless network **123** to the mobile device **124**. The mobile device **124** then removes the outer envelope **B** and  
15 decrypts (if necessary) and decompresses the message **A**. Further details of redirection operations are described for example in United States Patent no. 6,219,694, granted on April 17, 2001 and titled "System and Method for Pushing Information from a Host System to a Mobile Data Communication Device Having a Shared Electronic Address". Where the message is encrypted by the redirection server **112**, message decryption problems may  
20 occur at the mobile device **124**, as described above.

In order for such message redirection to occur, a mobile device and user account, such as an email account or mailbox for example, within the LAN **114** must be

registered with the redirection server **112**. This registration is a server administration function that is normally, although not necessarily, performed in two steps, by first adding a new user record at a storage location accessible by the redirection server **112** and then assigning a particular mobile device for the user by adding the mobile device PIN to the user record. Preferably, after a user record has been created, a mobile device user connects the mobile device to a workstation, such as the workstation **128** in the above example, associated with the user account to be enabled for redirection to the mobile device **124** to complete the registration process.

Embodiments of the invention will now be described in reference to Figs. 2-4. Although reference is also made to the system of Fig. 1, the invention is in no way restricted to implementation in that system. The system of Fig. 1 is intended for illustrative purposes only.

Fig. 2 illustrates a method for detecting and eliminating a duplicate mobile device PIN when a new user account and mobile device are registered in a communication system or when a mobile device is first registered for an existing user account. In step **2**, a server with which a user account and mobile device must be registered reads the user's configuration information. In the illustrative example system of Fig. 1, this server is the redirection server **112**. The configuration information, which is normally stored in a new administration record created on the server or on a data store accessible by the server when the user account is registered with the server, represents the user account on the server and includes the PIN of the mobile device to which messages addressed to the user account are to be redirected. In step **4**, the server checks whether a user account is

pending to the server. A user account is pending to the server when a corresponding new administration record has been added to the server, but the user has not yet connected the mobile device to a host system or network workstation to download required routing information and possibly one or more encryption keys to be used by the mobile device for  
5 communication within a system such as shown in Fig. 1.

If the user account is not pending to the server, then the process continues at step 6, in which the server determines whether or not an activation time exists for the user account. If an activation time does not exist, then in step 8, the server sets the activation time for the user account to the time of the creation of the user's configuration information  
10 in the new record. This may be the time at which the user account was first registered with the server, or possibly a later time at which particular settings or information were specified, such as a new mobile device PIN. In step 10, the server checks the PIN of the mobile device associated with the user account against the existing user records for all other user accounts currently registered on the server. The server preferably maintains a list of PINs  
15 for existing registered user accounts to facilitate the checking function at step 10. Using such a list, only the list, not entire user records, must be accessed to check for the new PIN.

In step 12, the server determines whether or not a duplicate of the mobile device PIN has been stored in an existing user record or a list of registered mobile device  
20 PINs. If a duplicate of that PIN exists, then in step 14, the server determines if both of the user accounts are currently activated, i.e. if both user accounts have been registered on the server and have connected a mobile device to download the required routing

information. In step **16**, the server determines which user account was most recently activated on the server and allows the most recently activated user account to keep the PIN by setting the PIN in the administration record associated with the older user account to zero, or alternatively to some other default or null value, in step **18**. In step **20**, the server  
5 notifies its associated administration arrangement or sub-system that the PIN in the older record has been reset. In step **22**, the server adds the new user account to the registered user account list.

When the new user account is not the most recently activated user account, resulting in a negative determination at step **16**, then the mobile device PIN in the record  
10 for the new user account is set to zero or a default or null value at step **19**. Then, at step **21**, server administration is notified that the mobile device PIN in the administration record for the new account has been reset. Since a PIN is typically programmed into a memory on a mobile device by a manufacturer, a redirection or other communication service provider or possibly a server administrator, a user may then either obtain a new mobile  
15 device or have a different PIN programmed into the mobile device in order to register an account and mobile device with the server.

If the user account is pending to the server, as determined at step **4**, then in step **24**, the server determines whether a pending time exists. In step **26**, if no pending time exists for the user, the server sets a pending activation time to the time when the  
20 configuration information for the user account was created. When a user connects the device to a host system as described above, the activation time will be set to the pending activation time.

Fig. 3 shows a similar duplicate PIN detection and elimination method used when the PIN in a user's administration record is changed. In step 30, the user connects a different mobile device to a host system, such as workstation 128 in Fig. 1. In step 32, the server detects the different PIN for the different mobile device by accessing an existing record for the registered user account. In step 34, the server checks the PIN of the different mobile device against the list of user accounts currently registered on the server. In step 36, the server determines whether or not a duplicate of the PIN exists. If a duplicate PIN does not exist, then the method ends. In step 38, if the server determines that a duplicate PIN exists, the server determines whether both user accounts with the duplicate PIN have been activated. In step 40, if both accounts have been activated, the server allows the most recently activated account to retain the PIN. In step 42, the server sets the PIN in the record associated with the older user account to zero or another predetermined null value. In step 44, the server notifies administration that the PIN has been reset. The method then ends.

In some circumstances or at certain times, network owners or operators may wish to verify that the same mobile device PIN has not been assigned to different user accounts. Such a verification or "rescan" method is shown in Fig. 4. At step 50, the server retrieves information for a user account, such as an administration record for a particular specified user for example, from a database or list of activated user accounts which may be stored at the server or a data store accessible to the server. In step 52, the server checks the mobile device PIN against the list of user accounts, records or PINs that are currently registered. In step 54, the server determines if a duplicate PIN exists. If so, then

in step 56, the server determines whether or not both user accounts with the duplicate PIN are currently activated. In step 58, if both accounts have been activated, the server allows the most recently activated user account to keep the PIN. In step 60, the server sets the PIN in a record associated with the other account to a null value such as zero. In step 62,  
5 the server notifies its administration system that the PIN has been reset. If desired, an owner of a user account could be notified of a PIN reset by some means, although typically a previous user would have stopped using a mobile device or is using a new mobile device with a new PIN and therefore has no need of that particular PIN any more.

It will be appreciated that the above description relates to preferred  
10 embodiments by way of example only. Many variations on the invention will be obvious to those knowledgeable in the field, and such obvious variations are within the scope of the invention as described and claimed, whether or not expressly described.

For example, although the invention has been described primarily in the context of a messaging system, it is no way restricted thereto. Detection and elimination of  
15 duplicate mobile device PINs in accordance with aspects of the invention may also be implemented in other mobile communication systems such as cellular telephone networks and the like.

It should be appreciated that instead of resetting the PIN in a older user administration record, an alternative which might be desirable in certain organizations or  
20 under certain conditions would be to reset a PIN in a new user record or when the PIN is added to an existing administration record. The new user would then be forced to either obtain a new mobile device or contact a server administrator, mobile device manufacturer

or service provider for assignment of a new PIN to the mobile device, as described briefly above. The frequency of such administrator action being required is likely to be significantly higher in most organizations, however, than when the PIN in an older record is reset. Nevertheless, the invention contemplates that either PIN could be reset, as desired.

5           The invention also contemplates that from time to time, a "master" scan could be conducted, to check across the system for duplicate PINs assigned to different user accounts. However, such a master scan should only be needed once, if at all, i.e. at the time of implementing a duplicate PIN detection and elimination scheme according to aspects of this invention, since thereafter any duplicate PINs would be detected as they  
10 occur.

**CLAIMS:**

1. A method for detecting and eliminating duplicate wireless mobile communications device Personal Identification Numbers (PINs) stored in user administration records associated with a server system, the method comprising the steps of:  
5  
checking the PIN of a wireless mobile communications device stored in a user administration record against other existing user administration records; and  
if a duplicate of the PIN is detected in one of the other existing user administration records, then resetting the PIN in either the user administration record or the one of the  
10 other existing user administration records.
2. A method as recited in claim 1, wherein the step of resetting the PIN comprises resetting the PIN of the one of the other existing user administration records to a null value.
- 15 3. A method as recited in claim 1, wherein:  
the server system maintains a separate list of PINs for existing user records; and  
the step of checking the PIN against other existing user records comprises checking the PIN against the list.
- 20 4. A method as recited in claim 1, wherein:  
each of the user administration records includes a wireless mobile communications device activation time; and  
the step of resetting comprises the steps of:



comparing the activation time in the user administration record with the activation time in the one of the other existing user administration records; and resetting the PIN in the user administration record or the one of the other existing user administration records based on a result of the step of comparing.

5

5. A method as recited in claim 4, wherein the step of resetting the PIN based on a result of the step of comparing comprises resetting the PIN in the user record having an earlier activation time.

10 6. A method as recited in claim 1, further comprising the step, before the step of checking, of storing a new PIN in the user administration record, wherein the new PIN is checked against other existing user administration records.

15 7. A method as recited in claim 6, further comprising the step, before the step of storing, of creating a new user administration record, wherein the new PIN is stored to the new user administration record and checked against other existing user administration records.

20 8. A method as recited in claim 6, wherein the new PIN replaces a PIN previously stored in the user administration record.

9. A method as recited in claim 1, further comprising the step, before the step of checking, of selecting a particular user account for a duplicate PIN detection operation,

wherein the PIN stored in an existing user information record for the particular user account is checked against other existing user administration records.

10. A system for detecting and eliminating duplicate wireless mobile communications  
5 device Personal Identification Numbers (PINs) in a communication system, comprising:  
a data store configured to store user administration records, each user  
administration record being adapted to include a PIN; and  
a server system configured to detect whether or not a PIN stored in a user  
administration record in the data store occurs in any other user administration record in the  
10 data store, and if so, to reset the PIN in either the user administration record or the other  
user administration record.
11. A system as recited in claim 10, wherein the server system resets a PIN by storing a  
null value to a user information record.
- 15 12. A system as recited in claim 11, wherein the server system resets the PIN in the  
other user administration record.
13. A system as recited in claim 11, wherein the server system provides a message  
20 redirection service and is further configured to redirect messages from a host system to  
wireless mobile communication devices.
14. A system as recited in claim 13, wherein a wireless mobile communications device

is registered for the message redirection service by adding a new user administration record to the data store and storing a PIN in the new administration record.

15. A system as recited in claim 14, wherein the server system is further configured to  
5 detect and if necessary to reset a PIN each time a PIN is stored in a new administration record.

16. A system as recited in claim 14, wherein the wireless mobile communications device  
is selected from the group consisting of: a mobile data communications device, a mobile  
10 voice communications device, a dual-mode communications device having both voice and data communications capabilities, a wireless mobile messaging client, a cellular telephone, a personal digital assistant (PDA) enabled for communications, a wireless modem, a one-way pager and a two-way pager.

15 17. A system as recited in claim 10, wherein the server system is further configured to detect and if necessary to reset a PIN each time a PIN is stored in a new user administration record.

18. A system as recited in claim 10, wherein the server system is further configured to  
20 detect and if necessary to reset a PIN each time a PIN is stored in a user administration record.

19. A system as recited in claim 10, wherein the server system is responsive to a

selection of a particular user account for a PIN detection operation, whereby the server system detects whether or not a PIN stored in a user administration record for the particular user account occurs in any other user administration record in the data store, and if so, resets the PIN in either the user administration record for the particular user account  
5 or the other user administration record.

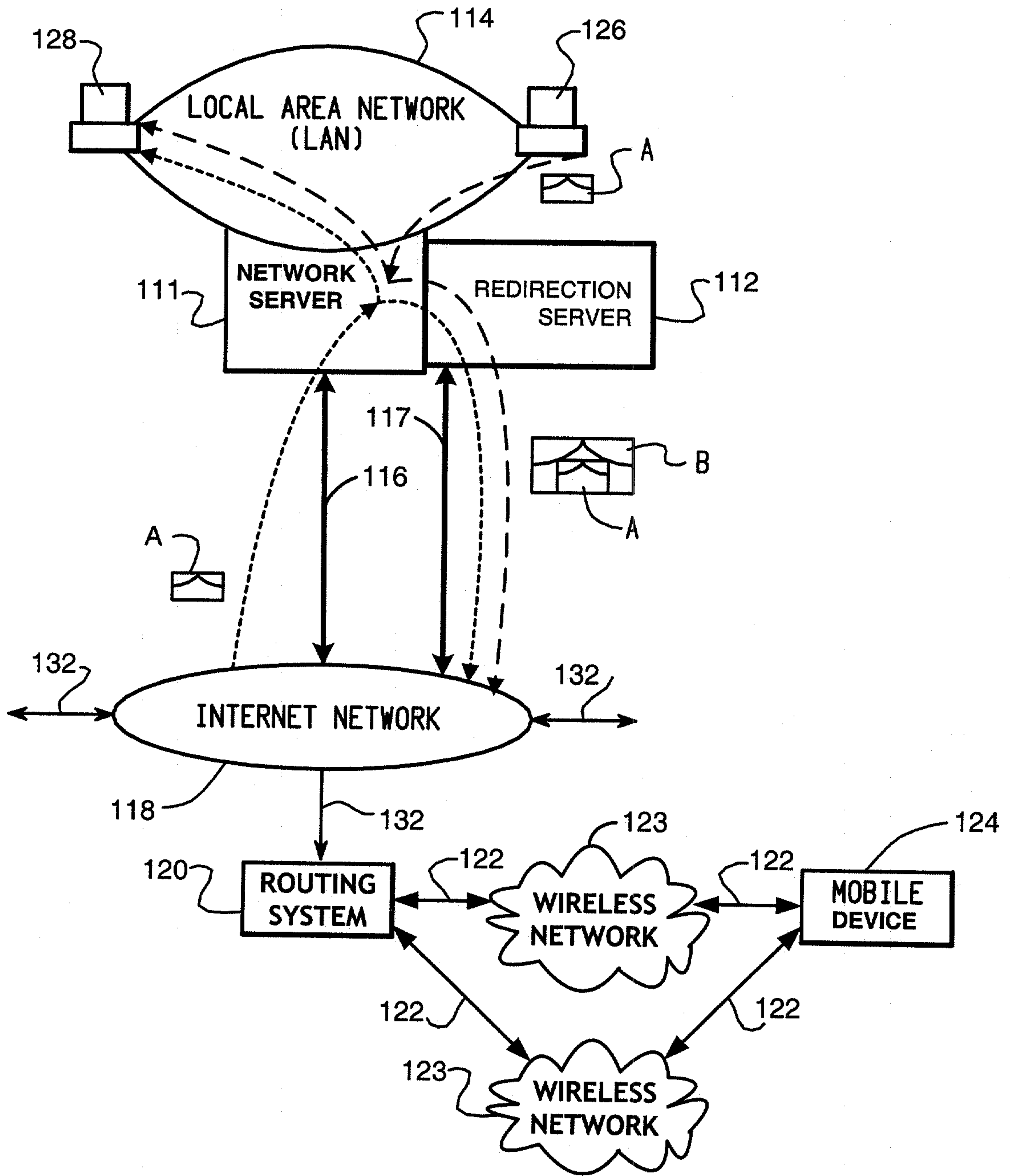


FIG. 1

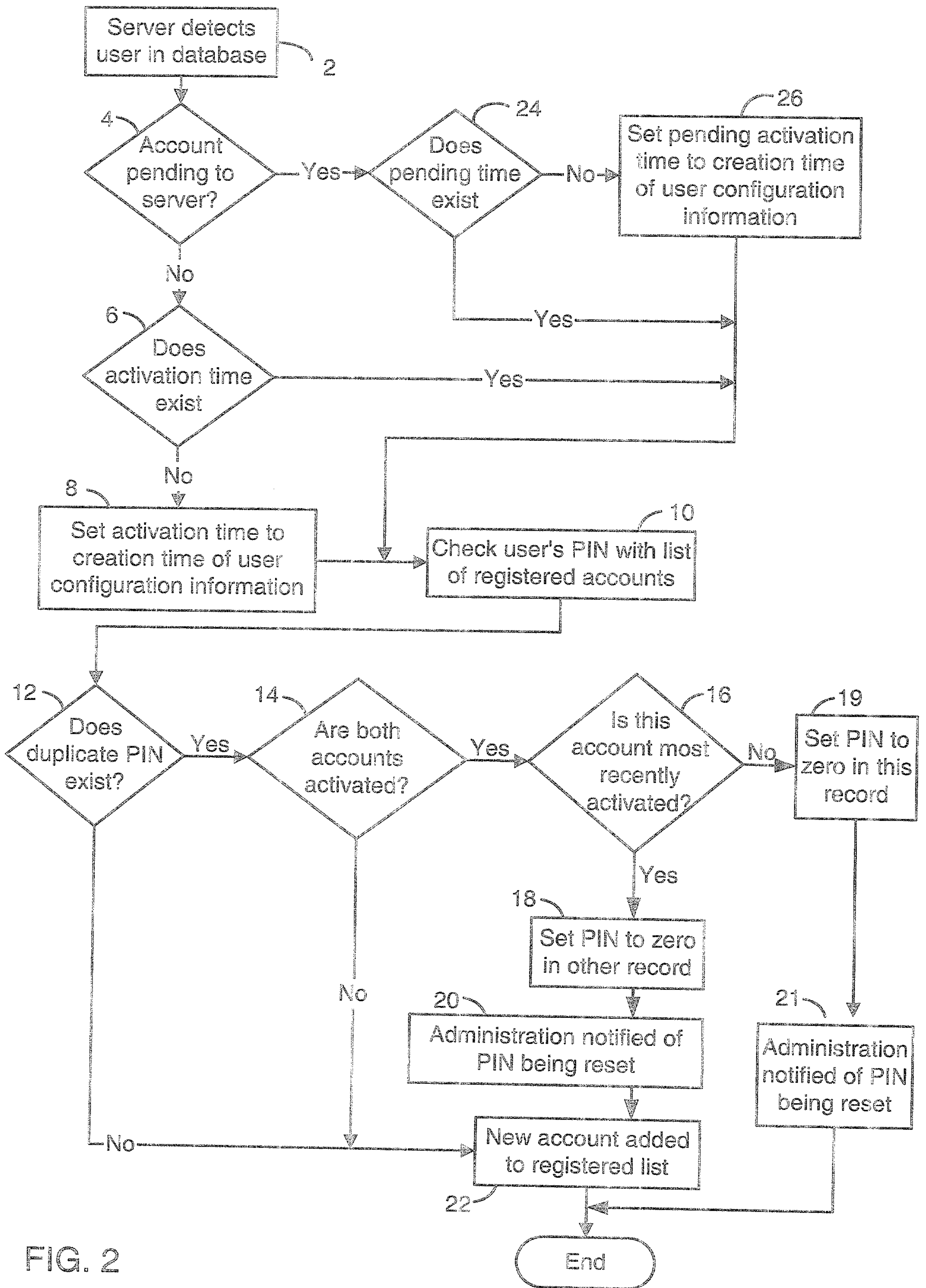


FIG. 2

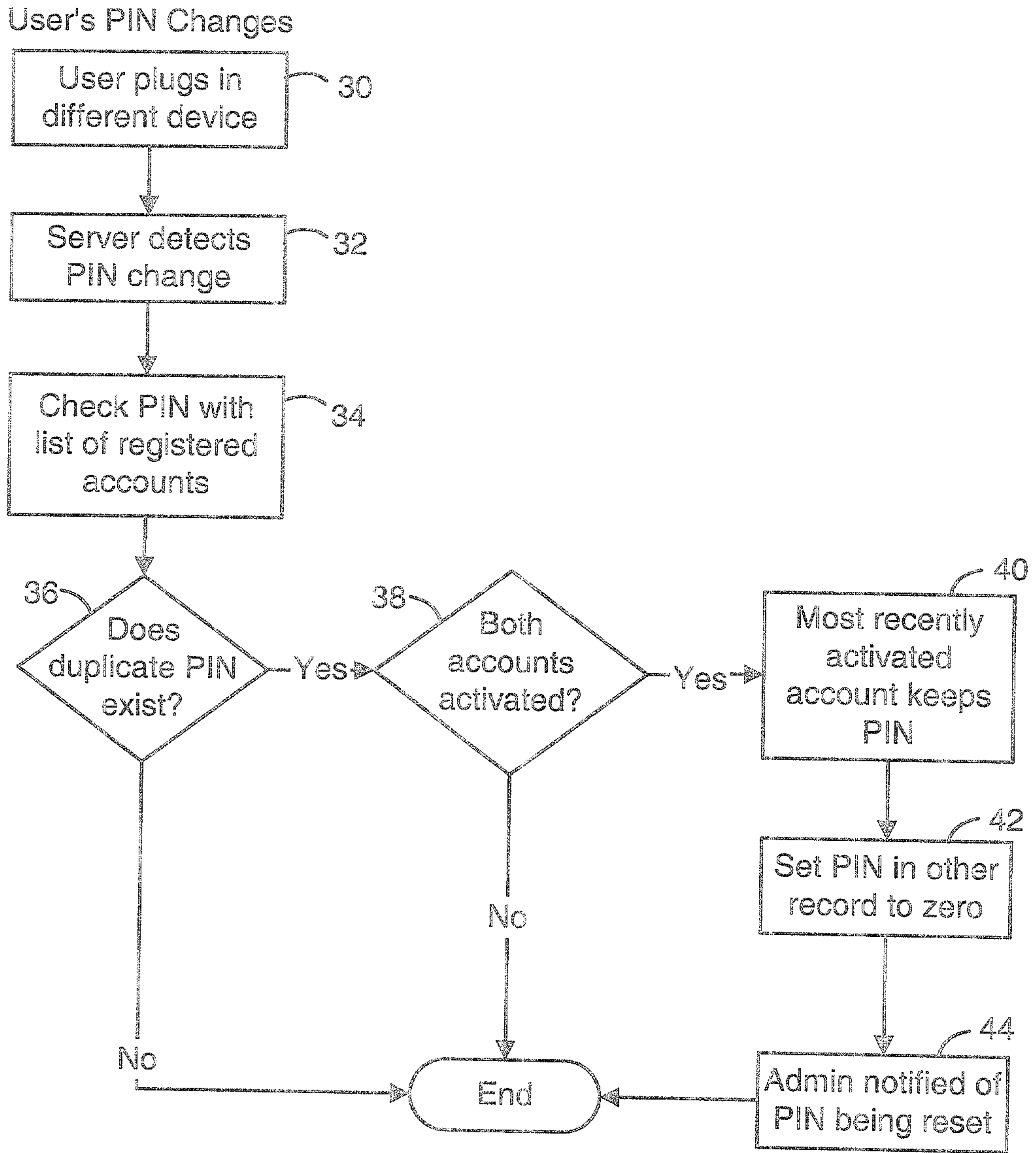


FIG. 3

Rescan

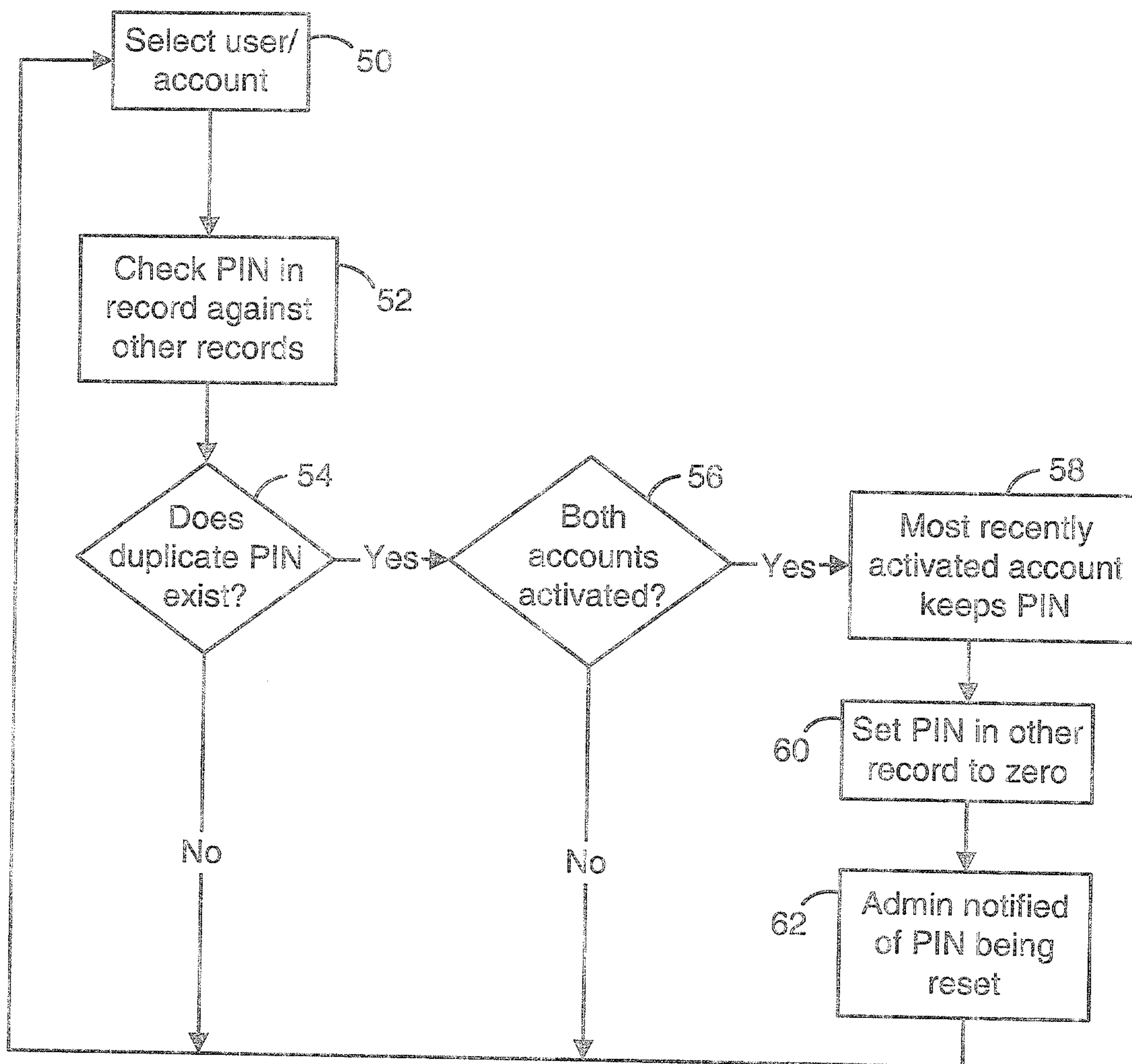


FIG. 4



