Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2228962 C 2002/04/16

(11)(21) 2 228 962

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(22) Date de dépôt/Filing Date: 1998/02/03

(41) Mise à la disp. pub./Open to Public Insp.: 1998/08/04

(45) Date de délivrance/Issue Date: 2002/04/16

(30) Priorité/Priority: 1997/02/04 (97200305.7) NL

(51) Cl.Int.^{6}/Int.Cl.^{6} H04L 9/32, G06K 19/07

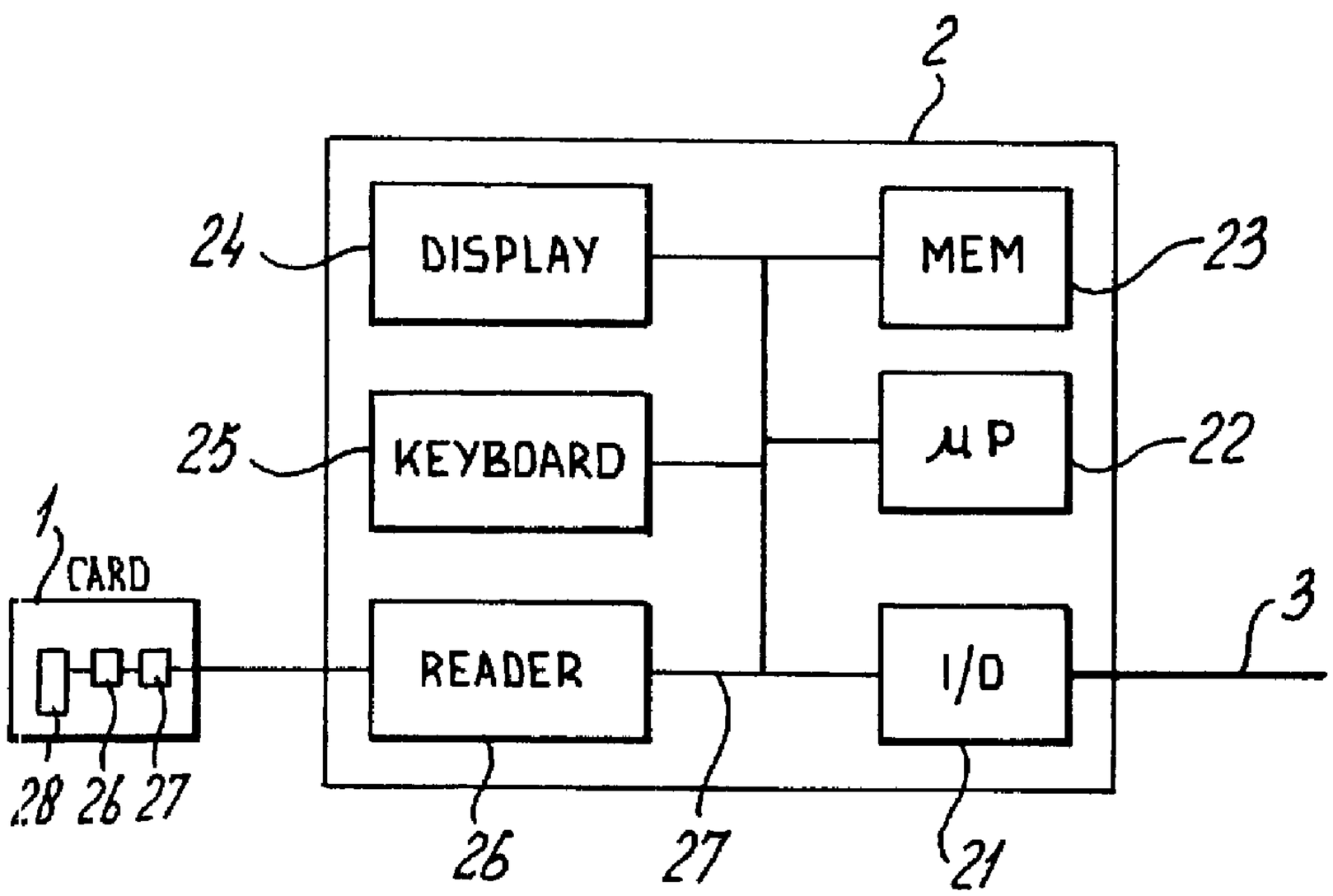
(72) Inventeurs/Inventors:
ROMBAUT, Willem, NL;
VAN BRUCHEM, Dirk J.J., NL

(73) Propriétaire/Owner:
KONINKLIJKE KPN N.V., NL

(74) Agent: FETHERSTONHAUGH & CO.

(54) Titre : SYSTEME DE COMMUNICATION, METHODE ET CARTE A PUCE PERMETTANT D'EXECUTER SUR UNE CARTE A PUCE DES SERVICES FAISANT APPEL A DES NIP

(54) Title: COMMUNICATION SYSTEM FOR CARRYING OUT PIN RELATED SERVICES ON A CHIPCARD, A CHIPCARD SUITABLE FOR SUCH A COMMUNICATION SYSTEM, AND METHOD FOR CARRYING OUT A PIN RELATED SERVICE ON THE CHIPCARD



(57) Abrégé/Abstract:
Communication system provided with at least one server (6) and at least one terminal (2), both the at least one server and the at least one terminal being arranged to communicate with each other, the at least one terminal being provided with input means (25) arranged to allow a user to enter data, e.g. a PIN code, with communication means (26) to communicate with a chipcard (1) and with a processor (22) connected both to the input means and to the communication means, the system being arranged to carry out PIN related and non-PIN related services wherein the control of carrying out a service is transferred from the server to the terminal when the service is PIN related.

Abstract

COMMUNICATION SYSTEM FOR CARRYING OUT PIN RELATED SERVICES ON A CHIPCARD, A CHIPCARD SUITABLE FOR SUCH A COMMUNICATION SYSTEM, AND METHOD FOR CARRYING OUT A PIN RELATED SERVICE ON THE CHIPCARD

Communication system provided with at least one server (6) and at least one terminal (2), both the at least one server and the at least one terminal being arranged to communicate with each other, the at least one terminal being provided with input means (25) arranged to allow a user to enter data, e.g. a PIN code, with communication means (26) to communicate with a chipcard (1) and with a processor (22) connected both to the input means and to the communication means, the system being arranged to carry out PIN related and non-PIN related services wherein the control of carrying out a service is transferred from the server to the terminal when the service is PIN related.

[figure 2]

Title

COMMUNICATION SYSTEM FOR CARRYING OUT PIN RELATED SERVICES ON A CHIPCARD, A CHIPCARD SUITABLE FOR SUCH A COMMUNICATION SYSTEM, AND METHOD FOR CARRYING OUT A PIN RELATED SERVICE ON THE CHIPCARD

Background of the Invention

The present invention relates to a communication system provided with at least one server and at least one terminal, both the at least one server and the at least one terminal being arranged to communicate with each other, the at least one terminal being provided with input means arranged to allow a user to enter data, e.g. a PIN code, with communication means to communicate with a chipcard and with a processor connected both to the input means and to the communication means, the system being arranged to carry out at least one PIN related service and at least one non-PIN related service and the at least one server is arranged to control carrying out said at least one non-PIN related service via said at least one terminal.

Such communications systems are now used, e.g., for carrying out banking operations.

In the communication system according to the prior art the at least one server has full control over any of the actions carried out by the terminal on the chipcard to complete the service concerned. When the service to be carried out is PIN related, i.e. the user is requested to enter his PIN code (PIN = Personal Identification Number) before the service can be carried out, the server requests the terminal to have the entered PIN code checked by the chipcard. If the entered PIN code is correct, the data related to any PIN related service available on the chipcard are freely available to the server. Then it is possible for the server to access data files on the chipcard even those to which it may not be allowed to do so. Moreover, unauthorized servers may take over control of the authorized server and carry out PIN related services. Such situations need to be avoided.

Summary of the Invention

Therefore, it is a primary object of the present invention to provide a communication system in which the problems mentioned above are overcome.

It is a further object of the present invention to provide a chipcard able to check software downloaded from the server to the terminal by using Message Authentication Codes (MAC's).

Moreover, it is an object of the present invention to provide a method of carrying out PIN related services without giving unauthorized servers the opportunity to control this.

In order to obtain the primary object the communication system according to the invention as defined above is characterized in that said at least one server is arranged to transfer control to said at least one terminal as soon as a PIN related service has to be carried out, and said terminal is arranged to control carrying out said PIN related service.

By transferring the control of PIN related services from the server to the terminal no unauthorized server can manipulate data flow from and towards the chipcard.

The communication system is able to carry out operations in a PIN validated mode, in which the control of the operations is carried out by the terminal, and a non-PIN validated mode, in which the control of the services concerned is carried out by the server.

Switching between these modes can be done under the control of the server which is, preferably, arranged to control non-PIN related services when the at least one terminal starts a communication with the chipcard, but to transfer control to the at least one terminal as soon as a PIN related service has to be carried out, the terminal being arranged to control carrying out the PIN related service. The discrimination between PIN-related and non-PIN-related services can be done using any suitable method or detection means.

Preferably, any communication between the authorized server and the terminal in the PIN validated mode is carried out by calculating and transmitting message authentication codes.

In order to provide a system in which the terminal is also able to take over the control of future PIN related services from the server, a system as defined above is claimed wherein the at least one server is arranged to download PIN related, service oriented software to the at least one terminal by calculating and

transmitting service related message authentication codes, the at least one terminal being arranged to receive the service related message authentication codes, and to instruct the chipcard to verify the service related message authentication codes.

For the latter communication system the invention also claims a chipcard storing data related to at least one PIN related service and arranged to communicate with a terminal, the latter being arranged to communicate with at least one server characterized in that the data related to at least one PIN related service is provided with a key and an algorithm to calculate message authentication codes and the chipcard is arranged to receive instructions from the terminal to verify software downloaded by the at least one server to the terminal, which software is related to the at least one PIN related service and which downloaded software comprises also message authentication codes.

Moreover, the invention is related to a method of carrying out a service with a chipcard by using a communication system defined above, characterized by the following steps:

a. starting communicating between the at least one terminal and a chipcard and between the at least one terminal and the at least one server;

b. detecting whether the service on the chipcard is PIN related and, if so, transferring control of carrying out the PIN related service from the server to the at least one terminal.

Further methods in accordance with the present invention are defined in the method subclaims.

Brief Description of the Drawings

The invention will now be explained with reference to the drawing which is intended to illustrate and not to limit the present invention.

Figure 1 shows a communication system known from the prior art;

figure 2 shows a card and a schematic block diagram of the terminal of the communication system according to figure 1;

figure 3 shows a flow diagram illustrating the principles of the present invention with respect to changing from a non-PIN validated mode to a PIN-validated mode;

figure 4 shows a flow diagram illustrating the principles of the present invention with respect to downloading application software from a server to a terminal.

Detailed Description of the Embodiments

The present invention can best be explained with reference to figure 1 which shows, very schematically, a communication system used in the prior art. The communication system comprises at least one terminal 2 and at least one server 6. The server 6 may be any server known from the prior art and may be implemented by a personal computer provided with a processor, I/O means, memory and software. The terminal 2 is connected to the server 6 by means of a connection 3 and a public switch telephone network PSTN 4 and a connection 5 to the server 6. The connections 3, 5 may be physical connections, like wiring or optical fibres. However, they may also be any known wireless connection. The PSTN 4 may be substituted by any known communication network, like ISDN, X25, Internet.

The terminal 2 is able to communicate with a chipcard 1, as is indicated by a double headed arrow between card 1 and terminal 2. The chipcard is an "intelligent" card, i.e., it is provided with a processor 26, I/O means 27, and a memory 28, as known to persons skilled in the art.

Figure 2 schematically shows some functional blocks within the terminal 2 which are useful for a terminal in accordance with the present invention.

The terminal 2 is provided with an I/O unit 21 for connection to the connection 3.

The terminal 2 further comprises a reading unit 26 arranged for communicating with the chipcard 1.

Moreover, the terminal 2 is provided with input means, for instance a keyboard 25 allowing a user to input data. Also provided are a display 24 and a memory 23.

A microprocessor μP 22 is provided to carry out and to control processing tasks. The microprocessor 22 is connected to the I/O unit 21, the reading unit 26, the input means 25, the display 24, and the memory 23 by means of a data bus 27.

The terminal 2 may, for instance, be a modern telephone apparatus connected to the telephone network. However, the telephone

apparatus 2 may, alternatively, be a wireless telephone apparatus. Such telephones need to be provided with a reading unit 26 for communicating with a chipcard. Such telephones are now available on the market.

The chipcard 1 referred to may be a card known as "Chipper"®.

The chipcard 1 may be provided with a multiple service capacity. One of these services may be an electronic purse. For payments with this electronic purse, no PIN code is used, nowadays. However, for transferring (electronic) money into such a purse, the user of the chipcard has to enter his PIN code.

Moreover, it is envisaged that some of these services may be related to classified data or may relate to large amounts of money. These services may only be used by persons knowing a predetermined PIN code related to the service concerned.

One such service is the service called "girofoon", which gives a user the possibility of transferring money from one of his own accounts to another one of his own accounts.

A new service is planned by the Dutch Postbank to allow a user to transfer money from one's own account to an account of a third party.

For the transfer of money from one account to another account, the server 6 requests a user through the terminal 2 to input his PIN code by means of the input means 25. The microprocessor 22 controls the transfer of the PIN code to the chipcard 1 and requests the chipcard 1 to validate the PIN code. The chipcard's processor 26 checks the PIN code received and sets a PIN flag after it has established that the correct PIN code was entered by the user. The PIN code is not transmitted to the server 6, since that would introduce the risk of tapping the PIN code from the connections 3, 5, by an unauthorized party.

However, as soon as the terminal 2 has identified by checking the value of the PIN flag that the user has entered the correct PIN code the related service is free to be carried out by the server 6. In other words, at that moment, the reading unit 26, the input means 25, the display 24, the microprocessor 22 and the memory 23 of the terminal 2, as shown in figure 2, can be considered to form remote elements of the server 6.

At that moment, the server 6 has full control over any PIN

code related service of the chipcard 1, whereas it may, actually, only be authorized to control, say, one or two PIN related services.

Moreover, it is then principally possible for any unauthorized server to take over the communication between the terminal 2 and the server 6 in order to communicate with the terminal 2 itself. At that moment, the unauthorized server (not shown) will also be able to control PIN related services of the chipcard 1 since permission has been given to carry out those services.

In accordance with the present invention it is proposed to introduce two modes of operation: a PIN validated mode and a non-PIN validated mode. The PIN validated mode is the mode of operation in which PIN related services of the chipcard 1 can be carried out. The non-PIN validated mode is the mode in which the remaining services of a chipcard 1 can be carried out.

In the non-PIN validated mode, the terminal 2 operates as a usual remote terminal to the server 6. In other words, in the non-PIN validated mode the server 6 has complete control over any of the actions carried out by the terminal 2 on the chipcard 1. Only the "verify PIN" command is not allowed to be carried out by the server 6; the "verify PIN" command is always generated by the terminal 2 and sent to the chipcard 1 after the PIN has been entered by the user.

Preferably, when starting a communication between the chipcard 1 and the terminal 2, the non-PIN validated mode is the standard mode with which the system is working.

As soon as the server 6 establishes that a service of the chipcard 1 which a user wishes to be carried out is PIN related, the server 6 transfers overall control to the terminal 2. With modern telephone apparatuses this is possible since they are equipped with a microprocessor 22 and a memory 23 as shown in figure 2. From that moment onwards, the communication system operates in the PIN validated mode. In the PIN validated mode, the microprocessor 22 controls carrying out the service concerned by means of full control of the reader unit 26, the keyboard 25, the display 24, and the memory 23. Of course, in the PIN validated mode there are still some communications to be made between the terminal 2 and the server 6. However, these communications are related to "high

level commands". Here, "high level commands" refer to commands that are received by microprocessor 22 of terminal 2 and are translated by the microprocessor 22 in predetermined instructions for the reader 26, the keyboard 25, the display 24, and the memory 23. The microprocessor 22 has full control over these instructions. The server 6 is not allowed to have direct access to these components in the terminal 2 or the chipcard 1 itself. In other words, "low level commands" sent by the server 6 to the terminal 2, which would give the server 6 direct access to the components in the terminal 2, are not accepted by the microprocessor 22. Thus, the server 6 can only carry out those PIN related services which it is authorize to carry out under the control of the terminal 2. The server 6 does not have access to PIN related services to which it is not authorized.

The use of a PIN validated mode is shown in figure 3 which shows a flow diagram of steps taken in the system.

In step 301 the system waits for the user of the chipcard 1 to enter his PIN.

As soon as the user has entered his PIN the terminal 2 transmits a "verify PIN" command to the chipcard 1. The chipcard 1 then checks the entered PIN and sends a corresponding message to the terminal 2. Then, the chipcard 1 may set a PIN flag if it has established that the correct PIN was entered. Also the terminal 2 will notice that the PIN validated mode is entered, e.g., by setting a PIN flag.

In step 303 the terminal 2 establishes whether the entered PIN was correct or not. If the PIN was incorrect the system steps to step 304 in which a message is shown to the user indicating that an incorrect PIN was entered.

Step 304 may be followed by a step 305 which allows the user, for instance, at maximum two additional attempts for entering a correct PIN code.

If the terminal 2 establishes that the correct PIN was entered (step 303), it takes over full control of any activity to be carried out on the chipcard 1, step 306.

In step 307, the terminal 2 controls carrying out the PIN related service.

After terminating the PIN related service, the chipcard 1

will be automatically reset by the terminal 2. A message corresponding to this reset state is transmitted to the terminal 2. The terminal 2, then, transfers control to the server 6, step 309. After step 309, the system returns to step 301.

Transferring the control of PIN related services from the server 6 to the terminal 2 presupposes that the microprocessor 22 and the memory 23 of the terminal 2 are provided with suitable software to carry out the PIN related service concerned. However, at this moment only the PIN related service of "girofoon" mentioned above, has been fully developed. Therefore, terminals such as terminal 2 now available on the market, can only be provided with suitable software related to the "girofoon" service.

New PIN related services will certainly become available in the near future. However, a problem will then arise, since the software necessary to carry out local control of these new PIN related services in the terminal 2 has not been developed. Selling new software related to these new PIN related services, e.g. on a floppy disk, may be a problem since modern telephone apparatuses are not provided with a floppy disk reader. Therefore, it is proposed to solve this problem by downloading software related to new PIN related services from the server 6 to the terminal 2.

However, downloading software from a server 6 to the terminal 2 introduces the risk of software being downloaded by an unauthorized server through connections 3, 5, to the terminal 2. The latter problem can be solved by only allowing downloading of software data to the terminal by using the concept of message authentication codes (MAC's). However, to do so, the terminal 2 must be able to verify MAC's. In order

to verify MAC's, the terminal 2 must be provided with predetermined algorithms and keys. However, neither these algorithms nor these keys are stored on the terminals 2 which are now sold to the public.

To solve the latter problem, it is proposed to store the algorithms and keys necessary to calculate the MAC's on the chipcard 1. Each service, thus, has its own set of service data coupled to a predetermined algorithm and key on the chipcard 1.

Since the chipcard 1 is itself provided with a microprocessor (not shown) the chipcard 1 is able to calculate and verify the MAC concerned. The terminal 2 only has to instruct the chipcard 1 to do

so during a download session.

After completing any PIN related service the chipcard 1 is automatically reset by the terminal 2. Then, the terminal 2 transfers overall control to the server 6, which means that it accepts low level commands transmitted by the server 6 again. Only as soon as a new PIN related service with the chipcard 1 has to be carried out, control of the service concerned is transferred to the terminal 2.

Figure 4 schematically shows a flow diagram for an embodiment of the method according to the invention for downloading application software from the server 6 to the terminal 2.

In step 401 the terminal 2 waits until a download application command has been received. If so, a download mode is started, step 402, and the server 6 starts downloading software related to the new application to the terminal 2. In step 403 the terminal 2 receives the downloaded application software and the MAC calculated by the server 6.

After step 403 has been completed, the MAC has to be checked. As indicated above, this check will be made by the microprocessor of the chipcard 1 upon request of the terminal 2. This check is carried out in step 404.

If it turns out that the MAC is incorrect, in step 405 the terminal 2 erases the downloaded application software and may send an error message to the server 6. Then, the terminal 2 switches to the non-PIN validated mode, step 406.

If the check of the MAC gives the result that the MAC is correct, the terminal 2 switches back to the former mode, which may either be a PIN-validated mode or a non-PIN validated mode and sends the result to the server 6, step 407.

It is observed that the terminal 2 may either be in the non-PIN validated mode, or in the PIN validated mode, when starting the routine shown in figure 4.

Preferably, as soon as the PIN validated mode is entered any communication between the terminal 2 and the server 6 can only be carried out by transmitting data and commands obtained by MAC operations. This further reduces the risk of manipulating data and commands.

It is to be understood that the description of the present

invention given above is only meant to illustrate the present invention and not to limit its scope. The scope of the present invention is only limited by the annexed claims.

CLAIMS:

1. Communication system provided with at least one server and at least one terminal, both said at least one server and said at least one terminal comprising means to communicate with each other via communication network, said at least one terminal being provided with input means for allowing a user to enter data, e.g., a PIN-code, with communication means to communicate with a chipcard and with a processor connected both to said input means and to said communication means, the system comprising means for carrying out at least one PIN-related service and at least one non-PIN related service, the at least one server comprising means for controlling the carrying out of said at least one non-PIN-related service via said at least one terminal and detection means for detecting whether a PIN-related service is requested from the at least one terminal, the at least one server further comprising means to transfer control to said at least one terminal in response to a signal from the detection means that a PIN-related service is requested, after which control transfer said terminal controls carrying out said PIN-related service.

2. System according to claim 1 wherein, in use, after said at least one terminal has taken over control of carrying out a PIN-related service any communication between said at least one server and said at least one terminal is carried out by calculating message authentication codes.

3. System according to claim 1 or 2 wherein, in use, after said PIN-related service has been completed said at least one terminal automatically resets the chipcard and then transfers control of carrying out services to said at least one server.

4. System according to any of one of claims 1 to 3 wherein said at least one server is arranged to download PIN-related, service oriented software to said at least one terminal by calculating and transmitting service related message authentication codes, said at least one terminal being arranged to receive said service related message authentication codes, and to instruct chipcard to verify said service related message authentication.

5. Chipcard storing data related to at least one PIN-related service and arranged to communicate with a terminal, the latter being arranged to communicate with at least one server characterized in that said data related to at least one PIN related service is provided with a key and an algorithm to calculate message authentication codes and said chipcard is arranged to receive instructions from said terminal to verify software downloaded by said at least one server to said terminal, which software is related to said at least one PIN-related service and which downloaded software comprises also message authentication codes.

6. Method of carrying out a service with a chipcard by using a system according to any of the claims 1 through 4 characterized by the following steps:

a. starting communicating between said at least one terminal and a chipcard and between said at least one terminal and said at least one server;

b. said detection means detecting whether said service on said chipcard is PIN-related and, if so, transferring control of carrying out said PIN-related service from said server to said at least one terminal.

7. Method according to claim 6 also including the steps of:

- carrying out at least one non-PIN-related service and

- controlling carrying out said at least one non-PIN-related service by said at least one server via said at least one terminal.

8. Method according to claim 7 including the steps of:

- controlling any non-PIN-related service by said at least one server when said at least one terminal starts a communication with said chipcard but

- transferring control from said at least one server to said at least one terminal as soon as a PIN-related service has to be carried out.

9. Method according to claim 8 including the step of:

- communicating between said at least one server and said at least one terminal by calculating message authentication codes after said at least one terminal has taken over control of carrying out a PIN-related service.

10. Method according to any of the claims 6 to 9 including the step of:

- automatically resetting said chipcard and transferring control of carrying out services to said at least one server after said PIN-related service has been completed.

11. Method according to any of the claims 6 through 10 including the steps of:

- downloading PIN-related, service oriented software from said at least one server to said at least one terminal by calculating and transmitting service related message authentication codes;

- receiving said service related message authentication codes by said at least one terminal, and

- instructing said chipcard to verify said service related message authentication codes by using a key and an algorithm stored on said chipcard.

FETHERSTONHAUGH & CO.

OTTAWA, CANADA

PATENT AGENTS

fig-1

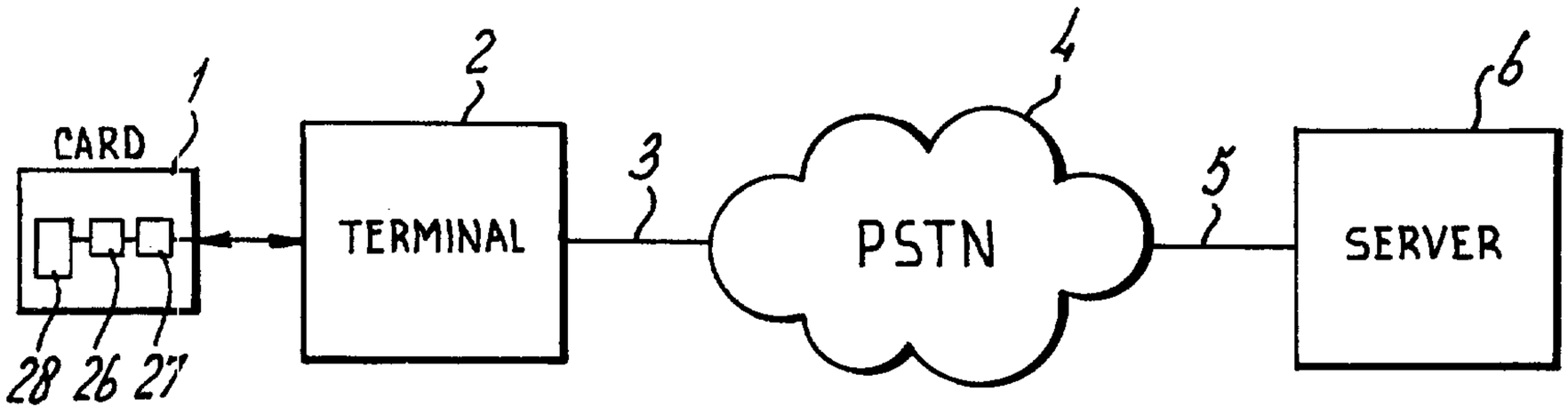
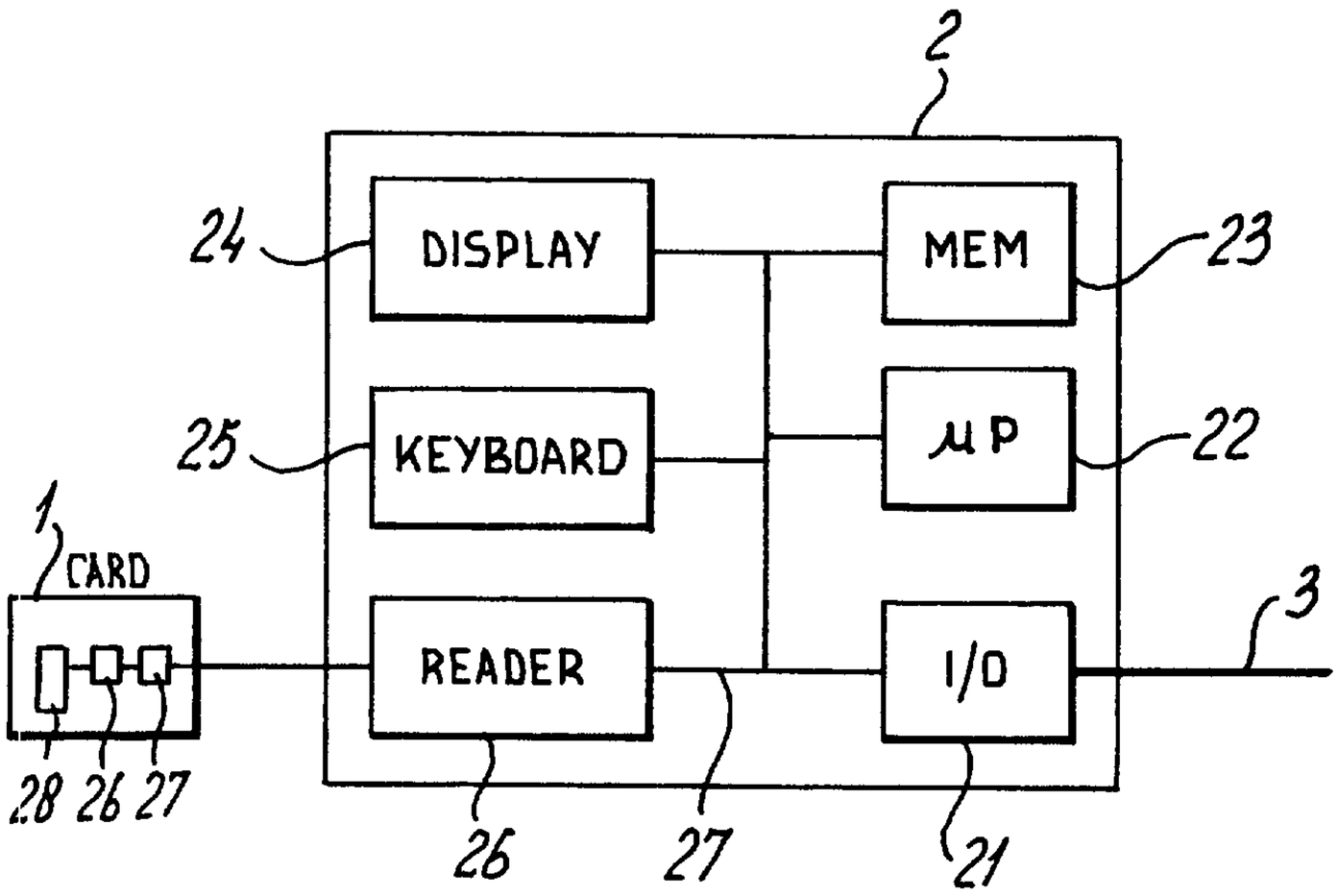


Fig-2



Patent Agents
Fetherstonhaugh & Co.

Fig-3

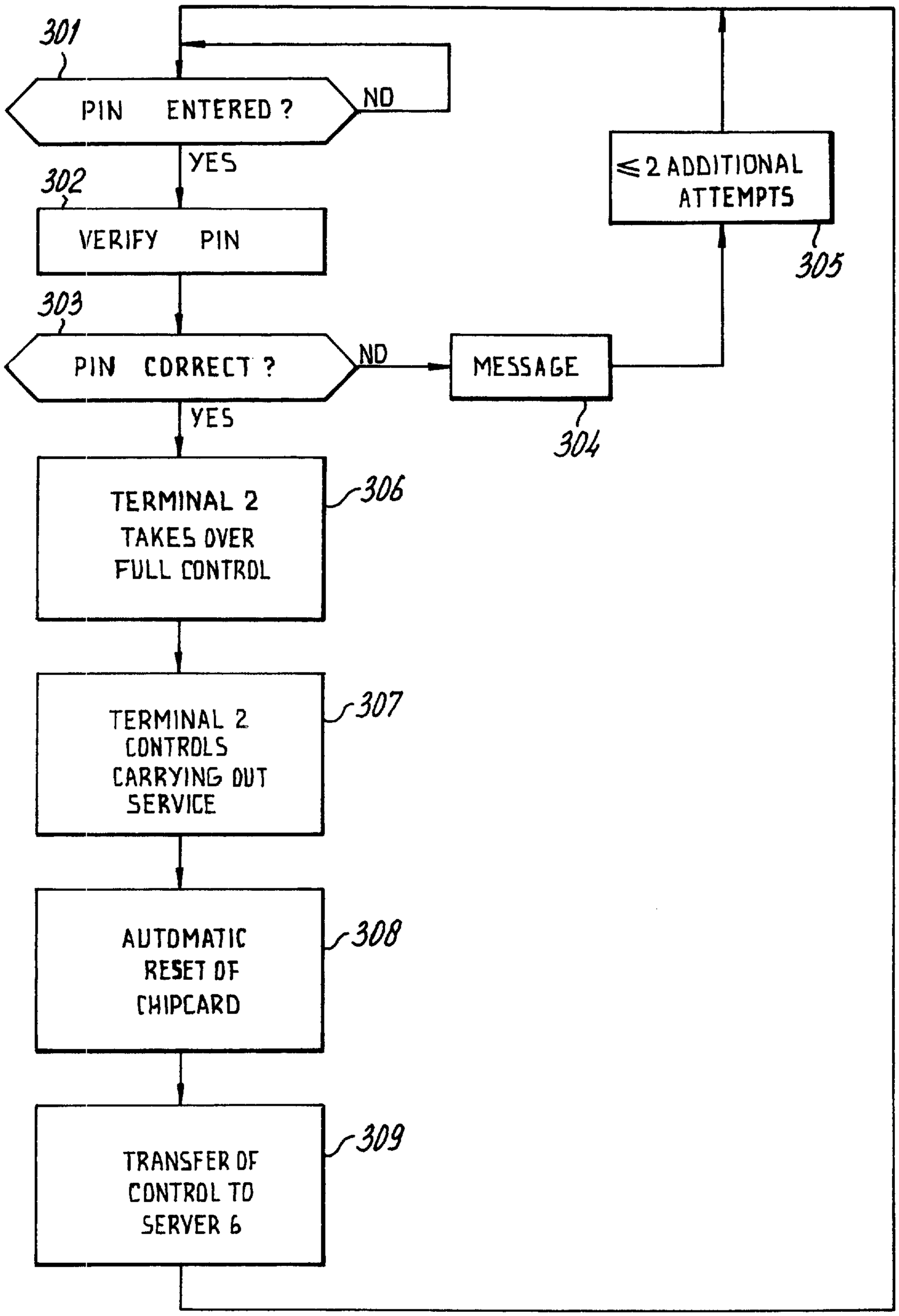
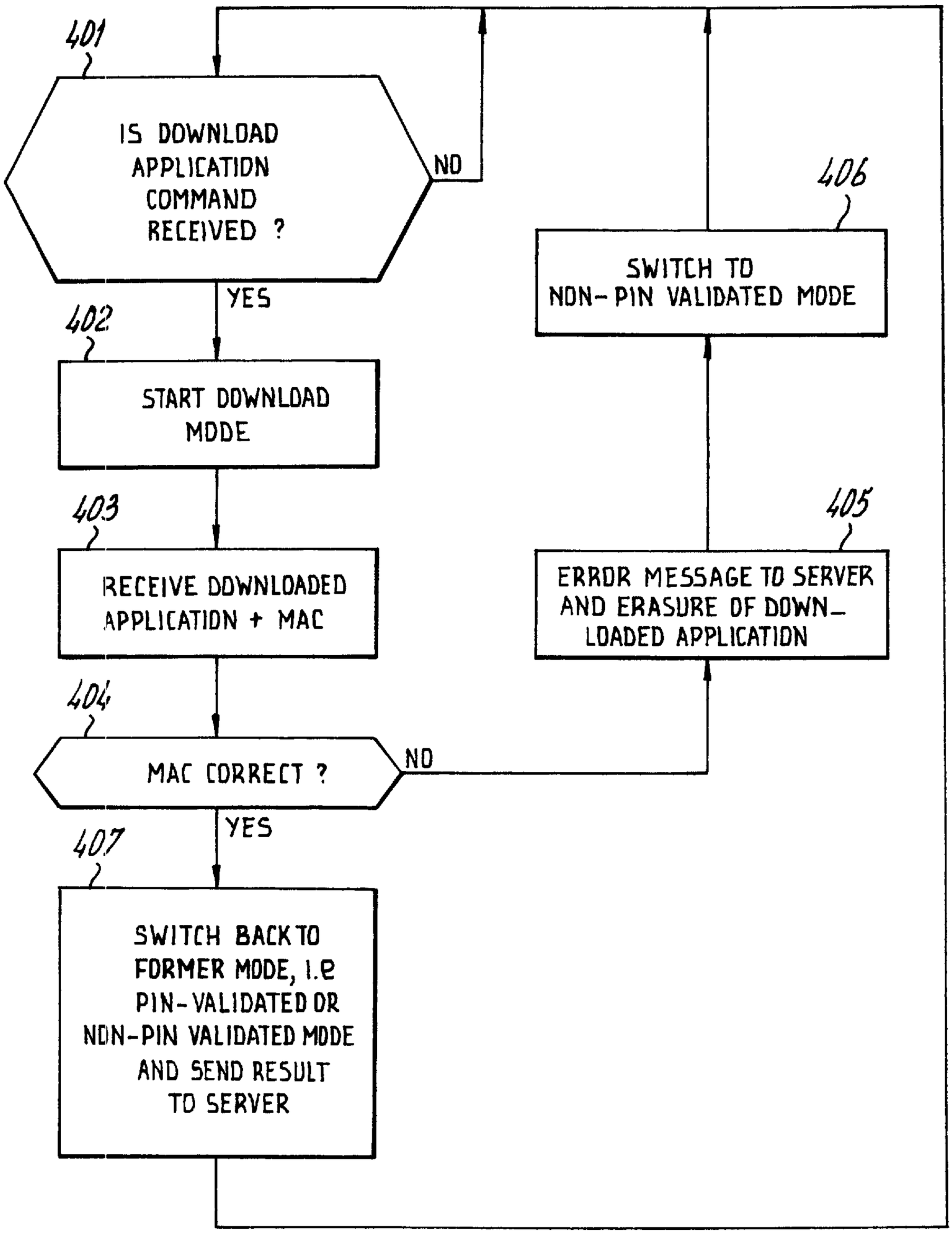
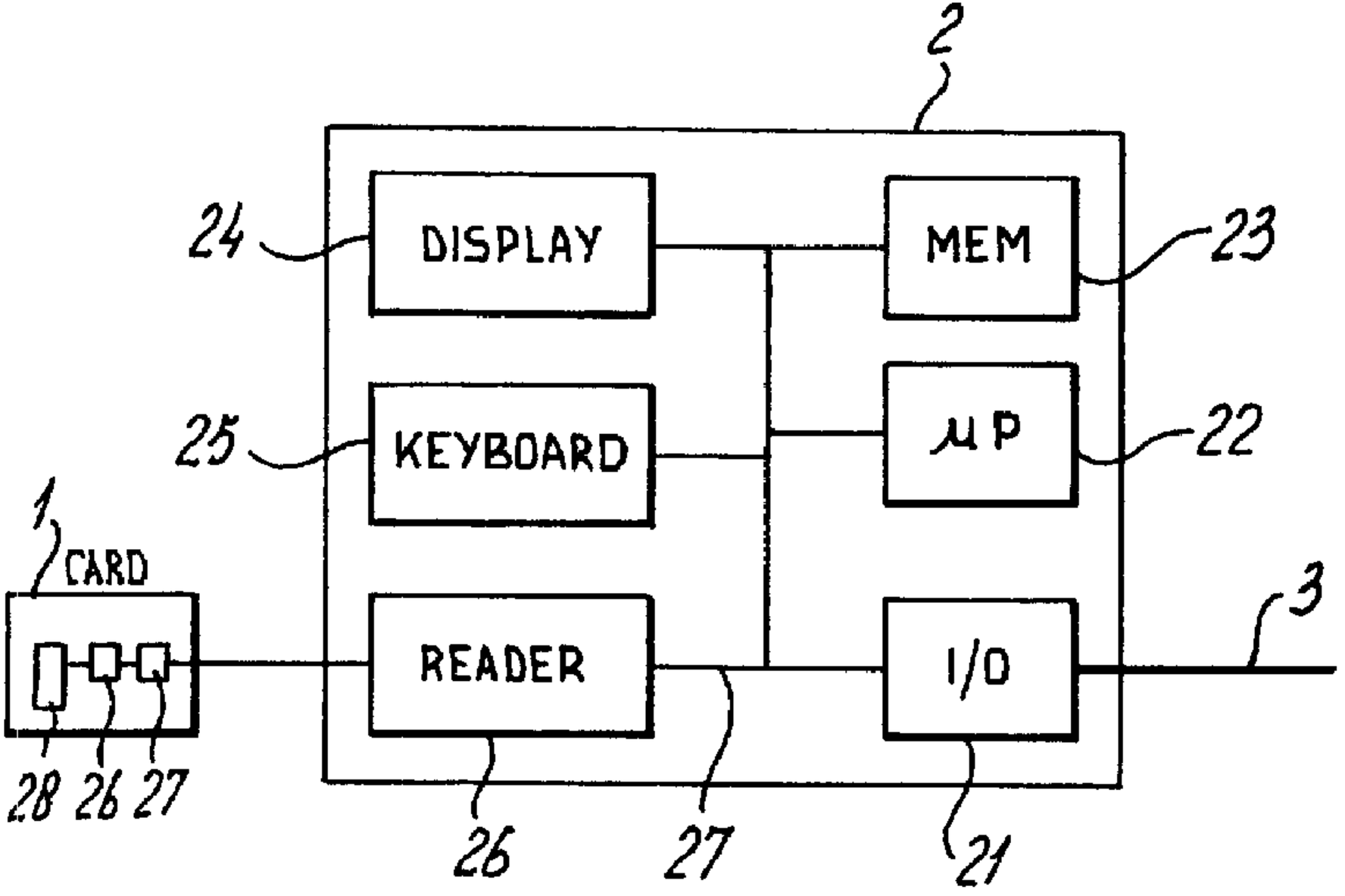

301
PIN ENTERED ?
NO
YES
302
VERIFY PIN
303
PIN CORRECT ?
ND
YES
MESSAGE
304
≤2 ADDITIONAL ATTEMPTS
305
TERMINAL 2 TAKES OVER FULL CONTROL
306
TERMINAL 2 CONTROLS CARRYING OUT SERVICE
307
AUTOMATIC RESET OF CHIPCARD
308
TRANSFER OF CONTROL TO SERVER 6
309

Fig-4


401
IS DOWNLOAD APPLICATION COMMAND RECEIVED ?
NO
YES
402
START DOWNLOAD MODE
403
RECEIVE DOWNLOADED APPLICATION + MAC
404
MAC CORRECT ?
NO
YES
405
ERROR MESSAGE TO SERVER AND ERASURE OF DOWN-LOADED APPLICATION
406
SWITCH TO NON-PIN VALIDATED MODE
407
SWITCH BACK TO FORMER MODE, I.E PIN-VALIDATED OR NON-PIN VALIDATED MODE AND SEND RESULT TO SERVER


2
24
DISPLAY
MEM
23
25
KEYBOARD
μP
22
1
CARD
READER
I/O
3
28
26
27
26
27
21