



(22) Date de dépôt/Filing Date: 1998/06/30

(41) Mise à la disp. pub./Open to Public Insp.: 1999/06/30

(45) Date de délivrance/Issue Date: 2001/09/04

(30) Priorité/Priority: 1997/12/30 (09/000,624) US

(51) Cl.Int.⁶/Int.Cl.⁶ G06F 1/00, G06F 12/14, G06F 3/02

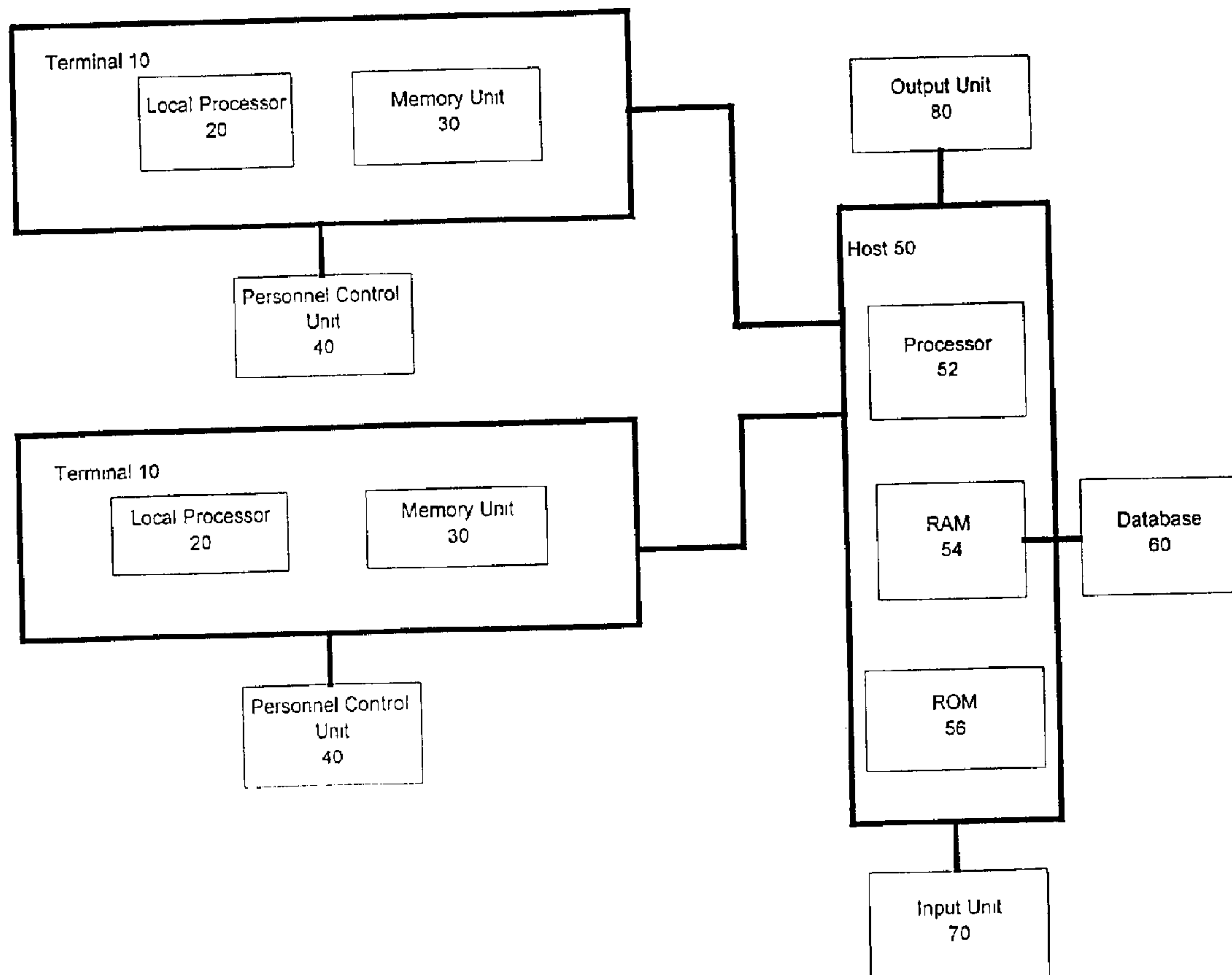
(72) Inventeur/Inventor:
DiMARIA, Peter C., US

(73) Propriétaire/Owner:
ACCU-TIME SYSTEMS, INC., US

(74) Agent: KIRBY EADES GALE BAKER

(54) Titre : INTERFACE BIOMETRIQUE AMELIORANT DES DISPOSITIFS DE CONTROLE D'ACCES EXISTANTS

(54) Title: BIOMETRIC INTERFACE DEVICE FOR UPGRADING EXISTING ACCESS CONTROL UNITS



(57) Abrégé/Abstract:

A method and an apparatus for upgrading an existing personal control system. The upgrade is achieved by replacing the personnel data input unit of an existing personal control system with a biometric interface device capable of reading physical characteristic and an access control signal in the format of the existing personnel control system.



ABSTRACT

A method and an apparatus for upgrading an existing personal control system. The upgrade is achieved by replacing the personnel data input unit of an existing personal control system with a biometric interface device capable of reading physical characteristic and an access control signal in the
5 format of the existing personnel control system.

**BIOMETRIC INTERFACE DEVICE FOR UPGRADING
EXISTING ACCESS CONTROL UNITS**

BACKGROUND OF THE INVENTION

Field of the Invention

5 The present invention relates to a method and apparatus
for upgrading existing personnel control systems. More
particularly, the present invention relates to replacing the
interface units of existing personnel control units with a
biometric interface capable of outputting a signal compatible
10 with the format of the currently installed personnel control
system.

Description of the Prior Art

 Increasingly, security problems are becoming a more
noticeable part of modern life. Security was once primarily
15 the preserve of classified government installations, but
increasing losses and calamity have forced the review of
security equipment and procedures for government and industry.
Cargo losses and the theft of corporate secrets cost industry
billions of dollars annually. Public safety is endangered by
20 the ability of intruders to access secured places, such as
aircraft and airport buildings.

 Personnel control and personal identification are daily
problems, and continue to be the object of significant
expenditures by organizations needing to identify employees,
25 vendors, etc., who are to be allowed access to the secured
areas. Typical personnel control applications include:
computer center; radioactive or biological danger areas;
controlled experiments; information storage areas; airport

5 maintenance and freight areas; hospital closed areas and drug storage areas; apartment houses and office buildings; manufacturing facilities and construction sites; safety deposit boxes and vaults; and computer terminal entry and access to information.

10 Obtaining an individual's identity is a common problem in any access control application. Many existing personnel control applications establish a person's identity using a personal identification code or a card having encoded identification information. More recently, in order to increase security, some organizations are installing biometric devices with personnel control capabilities. These devices electronically scan a personal physical characteristic of an individual, such as a portion of the epidermis or human eye. 15 After scanning a personal physical characteristic, these devices generate a pattern which is compared against a library of patterns that identifies the individuals permitted access to a controlled area.

20 For example, U.S. Patent No. 3,581,282 discloses a palm print identification system. In one example, a number code, encoded on an I.D. card, uniquely identifies a palm of an individual. The system reads the I.D. card and the actual palm of the individual. The number code is used as an index to retrieve a stored palm print pattern. Then, the stored 25 palm print pattern is compared to the fresh palm print pattern to verify the identity of the individual.

U.S. Patent No. 4,210,899 discloses a fingerprint-based personnel control and identification apparatus. The apparatus

reads a human fingerprint and transmits an electronic representation of the fingerprint to a centralized image processing unit. The centralized image processing unit determines access to certain areas, terminals or doors based
5 on the specific fingerprint read.

U.S. Patent No. 5,337,043 discloses a personnel control system using data stored in the form of a barcode. A fingerprint pattern of the keyholder is stored in the form of a barcode on the key. After the key is placed on the keyway
10 of a terminal at a personnel control point and read, the keyholder may then be prompted to place a finger against the fingerprint reader. The fingerprint is scanned and compared at the access control point terminal with the key encoded information. If a match is made, the personnel control point
15 decision and the keyholder identifying code are sent to a remote central processor or host computer. The central processor determines whether a keyholder is permitted to access a particular area at the particular time that the card is read. A signal indicating that access is granted or denied
20 is sent to the terminal.

U.S. Patent No. 5,195,145 provides an apparatus which scans a fingerprint and provides positive confirmation of an individual's identity at a particular location at a particular
time. The terminal utilizes fingerprint scanners with
25 magnetic cardreaders to reduce fraud in credit card transactions by sending the scanned card and fingerprint to a credit verification company.

All these new biometric devices are not compatible with the presently installed personnel control devices which establish a person's identity utilizing a personal identification code or encoded card. Often, presently
5 installed devices must be deactivated or removed, which adds to the expense of installing a new control access system. Therefore, there is a need for an inexpensive biometric interface device to upgrade existing personnel control units.

SUMMARY OF THE INVENTION

10 The present invention provides a biometric interface device for interfacing with an existing personnel control system of a type that utilize individualized stored data for the purpose of determining access authorization.

In one embodiment, the biometric interface device
15 associates a library of personal physical characteristic topographical patterns, such as epidermal topographical patterns, with identification information stored in a memory. When a topographical pattern is read by the biometric interface device, it is compared against the entries of
20 associated identification information stored in a memory unit. If there is a match, the identification information may be transmitted to a host computer in the format of the currently installed system. The host computer may use the identification information as an index to ascertain whether
25 the individual is authorized to access a controlled area. For added security, the subject individual may also be required to input a personal code and present an identification

document containing machine readable data to be scanned or read. If access is authorized, the host transmits an authorization signal in the format of the currently installed system.

5 Alternatively, the personal characteristic topographical pattern is stored on an identification document in a machine readable code. The terminal reads the document, scans the personal characteristic and performs a comparison. If there is a match, the identification information may be transmitted
10 to a host computer in the format of the currently installed system. The host computer accesses the data base to obtain authorization information. If the individual is authorized, the host transmits an authorization signal.

BRIEF DESCRIPTION OF THE DRAWINGS

15 **Figure 1** is a block diagram of an embodiment of the present invention;

Figure 2 is a block diagram of a front face of a first embodiment of a terminal of the present invention;

20 **Figures 3A and 3B** are diagrams of the steps of controlling access utilizing the terminal of the first embodiment of the present invention;

Figure 4 is a block diagram of a front face of a second embodiment of a terminal of the present invention;

25 **Figures 5A and 5B** are diagrams of the steps of controlling access utilizing the terminal of the second embodiment of the present invention;

Figure 6 is a block diagram of a typical card;

Figure 7 is a block diagram of the rear face of the typical card;

Figure 8 is a block diagram of a front face of a third embodiment of a terminal of the present invention;

5 **Figures 9A** through **9C** are diagrams of the steps of controlling access utilizing the terminal of the third embodiment of the present invention; and

10 **Figures 10A** and **10B** are diagrams of alternative steps of controlling access utilizing the terminal of the third embodiment of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

The preferred embodiments are described with reference to drawing figures wherein like numerals represent like elements throughout.

15 **Figure 1** shows a plurality of terminals **10** having a local processor **20** and memory unit **30**. Each terminal **10** is substituted for an existing terminal and is preferably connected to an existing personnel control unit **40**. The personnel control unit **40** controls access based upon a signal
20 from the terminal **10**. Each terminal **10** is also preferably connected to an existing host **50** which includes a processor **52**, RAM **54** and a ROM **56**. The host **50** is preferably programmed to permit access, entry and/or egress, for certain personnel based upon authorization information. Authorization
25 information preferably includes a list of personnel controlled areas and times during which an individual is to be permitted access. For example, an individual may be permitted access

only during a specified work shift. The authorization information would include the permitted area(s) and the permitted time(s) for that individual. Since the authorization information is under the employer's control, the permitted access area(s) and time(s) can be changed easily without the need for the issuance of a new individual identification card or a manual check of updated access information by security personnel. The host 50 has a database 60 for storing the authorization information and is connected to an input unit 70, such as a keyboard, and an output unit 80, such as a liquid crystal display.

Figure 2 is a diagram of a first embodiment of the terminal of the present invention. The terminal 10 includes a display 12 and a personal characteristic scanner 14 as well as the local processor 20 and memory unit 30. Examples of the personal characteristic scanner 14 include an epidermal topographical scanner and an eye scanner. Examples of epidermal topographical scanners include fingerprint scanners, knuckleprint scanners, handprint scanners and palmprint scanners. Examples of eye scanners include iris scanners and retina scanners. The personal characteristic scanner reads an individual's personal characteristic and generates a personal characteristic pattern which is compared to stored personal characteristic patterns.

The operational flow of a first embodiment of the terminal 10 is shown in **Figure 3**. After the terminal 10 is activated, the program is started (S1) and the system is initialized, preferably automatically (S2). When a personal

characteristic is detected (S3), the personal characteristic scanner 14 scans the personal characteristic (S4) and a personal characteristic topographical pattern is generated (S5). The local processor 20 compares the generated pattern to a library of patterns stored in memory unit 30 (S6). If there is no match, access is denied (S6A). The terminal 10 may transmit the time of attempted access and the generated personal characteristic topographical pattern to the host 50 for storage in the database 60 (S6B). Alternatively, the terminal 10 may store the time of attempted access and the generated personal characteristic topographical pattern in the memory unit 30. The host 50 or terminal 10 may generate a report of the attempted access (S6C). Thereafter, the system returns to step S3.

15 If there is a match, identification information associated with the stored personal characteristic topographical pattern is transmitted to the host 50 (S7). The host 50 accesses the database 60 to obtain authorization information regarding the individual seeking access (S8). If the authorization information associated with the identification information in the database 60 permits access (S9), the host 50 transmits a signal to the terminal 10 and stores the access time (S10). The terminal 10 instructs the personal control unit 40 to grant access (S11) and the host 25 50 generates a report (S12), and the system returns to step S3.

 If the authorization information does not permit access (S9A), the host 50 stores the time of attempted access with

the generated physical characteristic topographical pattern in the data base 60 (S9B). The host 50 may also generate a report of the attempted access (S9C). Thereafter, the system returns to step S3.

5 It will be recognized that a principal advantage of the present invention is the ability to replace an existing access control device, such as a barcode scanner, with a personal characteristic identification control apparatus without the need for modifying the existing system. Since the present
10 invention provides an output that is compatible with the existing system, the change will appear seamless to the current host. The ability to avoid the need for changes in software or hardware provides an economic advantage that greatly enhances the added feature of a physical
15 characteristic identification system.

Figure 4 is a diagram of a second embodiment of a terminal of the present invention. The terminal 100 preferably includes the same apparatus as terminal 10. In addition to the local processor 20, memory unit 30, display
20 12 and personal physical characteristic topographical scanner 14, the terminal 100 also includes a keypad 16 for receiving a personalized code, such as a PIN, which is required to gain access.

 The operational flow of a second embodiment of the present invention utilizing terminal 100, is shown in **Figures**
25 **5A-5B**. After the terminal 100 is activated, the program is started (S1) and the system is initialized, preferably automatically (S2). When a personal code is detected (S3),

the terminal 100 requests a personal characteristic (S4).
When a personal characteristic is detected (S5), the personal
characteristic is scanned (S6) by the scanner 14 and a
personal characteristic pattern is generated (S7). The local
5 processor 20 compares the newly generated personal
characteristic pattern and personal code with the library of
corresponding data stored in memory unit 30 (S8).

If there is no match, access is denied (S8A), and the
host 50 or terminal 100 stores the time of attempted access
10 with the generated physical characteristic topographical
pattern in the data base 60 or memory unit 30 (S8B). The host
50 or terminal 100 may also generate a report of the attempted
access (S8C). Preferably, the terminal 100 stores the
information and generates the report. Thereafter, the system
15 returns to step S3.

If there is a match, the identification information
associated with the stored personal characteristic
topographical pattern is transmitted to the host 50 in a
format compatible with the existing system (S9). The host 50
20 accesses database 60 to obtain authorization information
regarding the individual seeking access (S10). If the
authorization information does not permit entry or exit,
access is denied (S11A) and the host 50 stores the time of
attempted access with the identification information (S11B).
25 Subsequently, the host 50 generates a report (S11C) and the
system returns to step S3.

If there is a match, the host 50 transmits a signal to
the terminal 100 in the existing format and stores the time

access is granted. The terminal 100 instructs the personal control unit 40 in the existing format to grant access (S13) and the host 50 generates a report (S14). Thereafter, the system returns to step S3.

5 **Figures 6 and 7** show an example of an identification document 90, which is read by a terminal 200 (**Figure 8**) in a third embodiment of the present invention. In order to gain access, an individual is required to present an identification document 90 having at least one machine readable medium.

10 **Figure 6** shows the front face of an identification document 90 having a photograph 92 and a visible machine readable code 94. The identification document 90 may also contain personal identification information such as the bearer's name, eye color, personal characteristic information, etc. The same

15 personal identification information may be encoded in a visible machine readable code 94. **Figure 5** shows the rear face of the identification document 90 which includes a magnetic stripe 96. Personal identification information from a front face of the identification document 90 and personal

20 characteristic information are preferably encoded on the magnetic stripe 96.

Referring to **Figure 8**, a block diagram of a third embodiment of the present invention is shown. The terminal 200 is substituted for the terminal 10 in **Figure 1**. In

25 addition to the local processor 20, memory unit 30, display 12, and personal topographical scanner 14, the terminal 200 further includes a keypad 16 for receiving a personal code, such as a PIN, and a card reader 210 for reading either

visible machine readable code 94 or encoded data on a magnetic stripe 96. The reader 210 may be configured to read both 94 and 96. The personal characteristic topographical scanner 14 reads a personal characteristic and generates a personal characteristic pattern.

Operation of the third embodiment of the present invention is shown in the flowchart in **Figure 9**. After the terminal 200 is activated, the program is started (S1) and the system is initialized, preferably automatically (S2). Once the identification document 90 is detected (S3), the identification document 90 is read to obtain encoded identification information (S4). A personal code is requested (S5). If a code is not entered, the system returns to step S3. If a code is detected, the system requests a personal characteristic (S7). If a personal characteristic is not detected by scanner 14, the system returns to step S3. If a personal characteristic is detected, it is scanned (S9) by scanner 14 and a personal characteristic pattern (S10) is generated.

If the encoded identification information, personal code, and generated personal characteristic pattern does not match the identification information, code, and personal characteristic information retrieved from memory unit 30, access is denied. The host 50 or terminal 200 stores the newly presented encoded identification information, code and generated personal characteristic information in database 60 or memory unit 30. The host 50 or terminal 200 generates a report (S11A-S11C), and the system returns to S3.

If the encoded identification information, code and generated personal characteristic pattern matches stored identification information, code and personal characteristic pattern retrieved from the memory unit 30, an identification information signal is transmitted to the host 50 (S12).

Once the host 50 receives the identification information signal, the host 50 accesses the database 60 to obtain authorization information (S13). If the authorization information does not permit entry, access is denied (S14A) and the host 50 stores time of attempted access with the identification information (S14B). The host 50 generates a report (S14C) and returns to step S3. If the authorization information permits entry, the host 50 transmits a signal in the existing format to the terminal 200 and stores the time access is granted. The terminal 200 instructs the personal control unit 40 in the existing format to grant access (S16). The host 50 generates a report (S17), and the system returns to step S3.

Alternatively, the same terminal 200 may be programmed to provide a fourth embodiment of the present invention. Operation of the fourth embodiment of the present invention is shown in **Figure 10**. After the terminal 200 is activated, the program is started (S1) and the system is initialized, preferably automatically (S2). After the card is detected, the machine readable code is read or scanned to obtain the encoded personal characteristic information (S4). A personal code is requested (S5). If a code is detected, a personal characteristic is requested (S7). If the personal

characteristic is detected (S8), a personal characteristic pattern is generated by scanner 14 (S10).

5 If there is no match, access is denied (S11A), and the host 50 or terminal 200 stores the time of attempted access with the generated physical characteristic topographical pattern in the data base 60 (S11B). The host 50 or terminal 200 may also generate a report of the attempted access (S11C). Thereafter, the system returns to step S3.

10 If the generated personal characteristic pattern matches the encoded information and personal identification number (S11), the identification information associated with the stored personal characteristic topographical pattern is transmitted to the host 50 (S8). The host 50 accesses the database 60 to obtain authorization information (S12). If the
15 authorization information permits entry then the host 50 transmits a signal in the existing format to a terminal 200 and stores the time access is granted (S13-S14). The terminal 200 instructs the personnel control unit 40 to grant access (S15) in the existing format and the host 50 generates a
20 report (S16). If authorization is not permitted, access is denied, the host 50 stores the time of attempted access and the host 50 generates a report (13A-13C). The system then returns to step S3.

*

*

*

CLAIMS

1. An apparatus for interfacing with an existing personnel control system that utilizes stored data in a predetermined format for the purpose of determining whether
5 a presented individual is authorized to have access to a controlled area, the apparatus comprising:

means for storing physical characteristic information for a plurality of individuals;

10 means for storing for each individual, an access signal associated with the existing personnel control system;

means for scanning a physical characteristic of a presented individual;

means for generating a scanned physical characteristic signal for the presented individual;

15 means for comparing the stored physical characteristics information to the scanned physical characteristic signal to determine if a match is found;

means for outputting the access signal associated with the presented individual when a match is found; and

20 means for communicating the outputted access signal to the existing control system in a format that is compatible with the predetermined format of the stored data so that the existing personnel control system will recognize the outputted access signal as a match for the presented
25 individual stored data and authorize access to the controlled area.

2. The apparatus of claim 1 wherein the predetermined format of the existing personnel control system is
30 compatible with information stored on a card.

3. The apparatus of claim 2 wherein the card has a magnetic stripe and the stored information is encoded thereon.

5 4. The apparatus of claim 2 wherein the stored information is encoded on the card in machine readable code.

10 5. The apparatus of claim 1 wherein the predetermined format of the existing personnel control system is compatible with a PIN.

6. The apparatus of claim 1 further comprising means for denying access when a match is not found.

15 7. The apparatus of claim 1 further comprising means for storing a time of attempted access and the scanned physical characteristic when a match is not found.

20 8. A biometric apparatus for interfacing with an existing personnel control system that utilizes stored data, in addition to biometric data, for the purpose of determining whether a presented individual is authorized to have access to a controlled area, the apparatus comprising:

25 means for storing biometric information for a plurality of individuals;

means for obtaining biometric information on a presented individual;

means for storing for each individual, an access signal associated with the existing personnel control system;

30 means for generating an obtained biometric information signal for the presented individual;

means for comparing the stored biometric information to the obtained signal to determine if a match is found;

means for outputting the access signal associated with the presented individual when a match is found; and

5 means for communicating the outputted access signal to the existing control system in a format that is compatible with the stored data so that the existing personnel control system will recognize the outputted access signal as a match for the presented individual stored data and authorize
10 access to the controlled area.

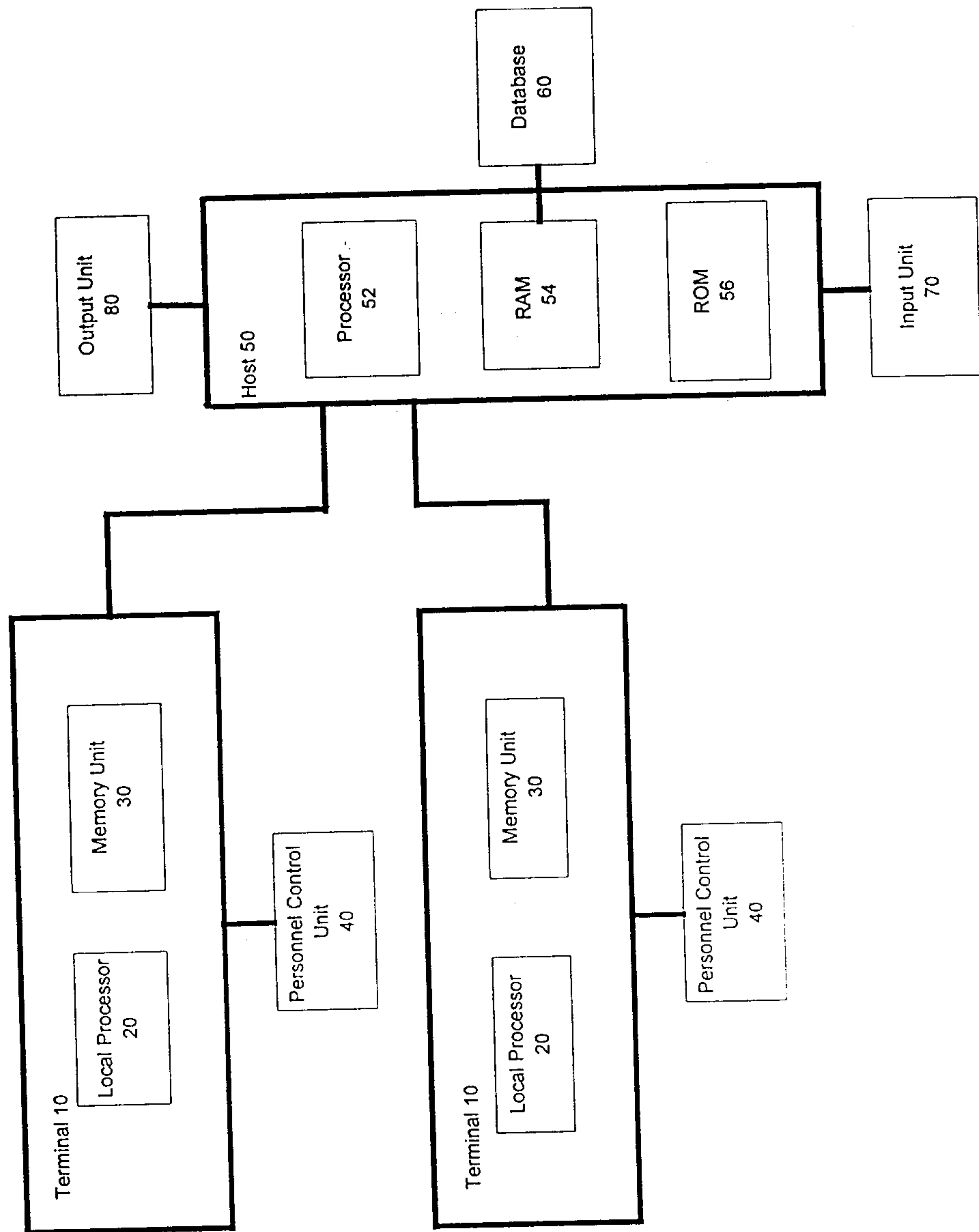


Fig. 1

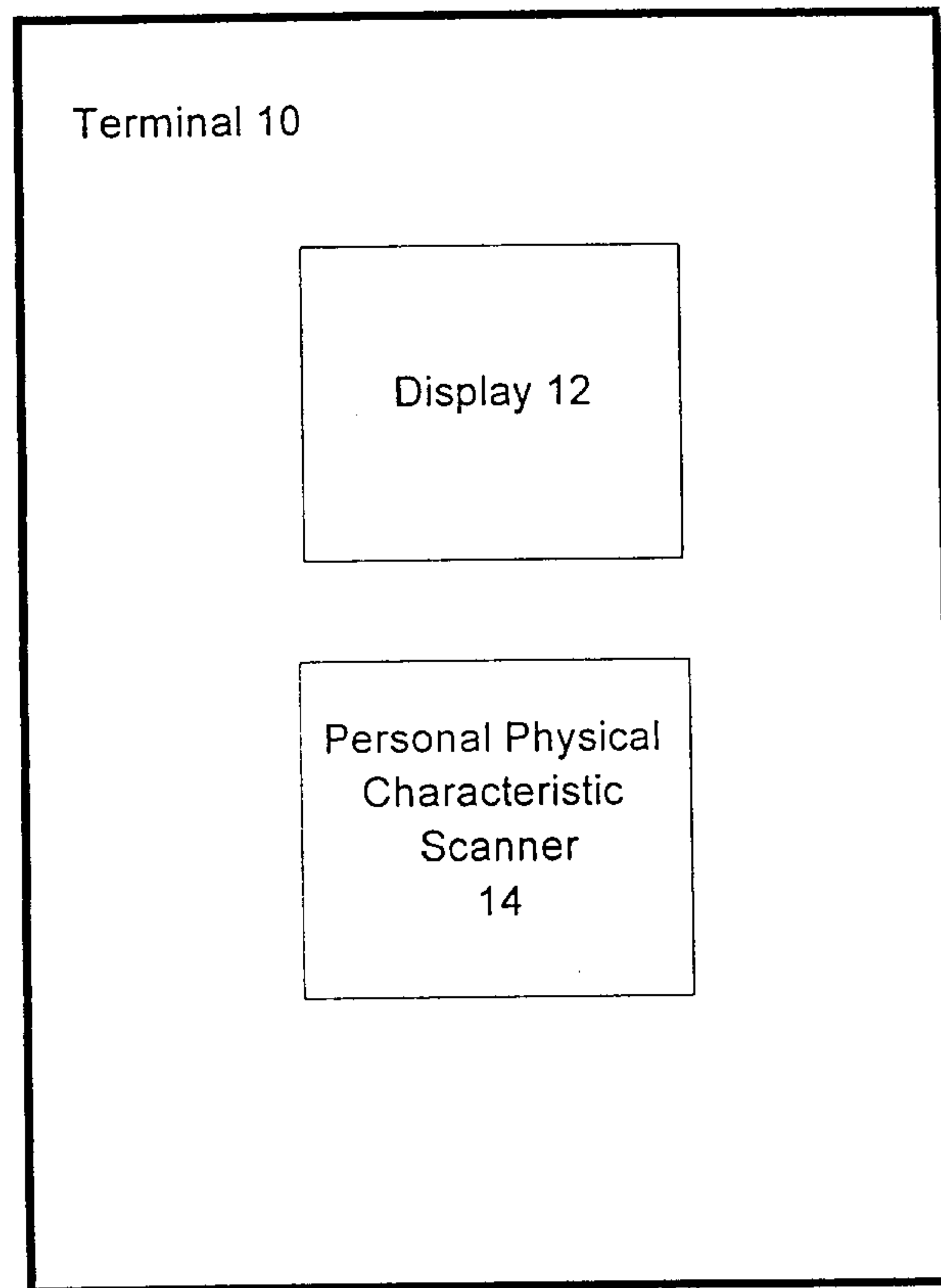
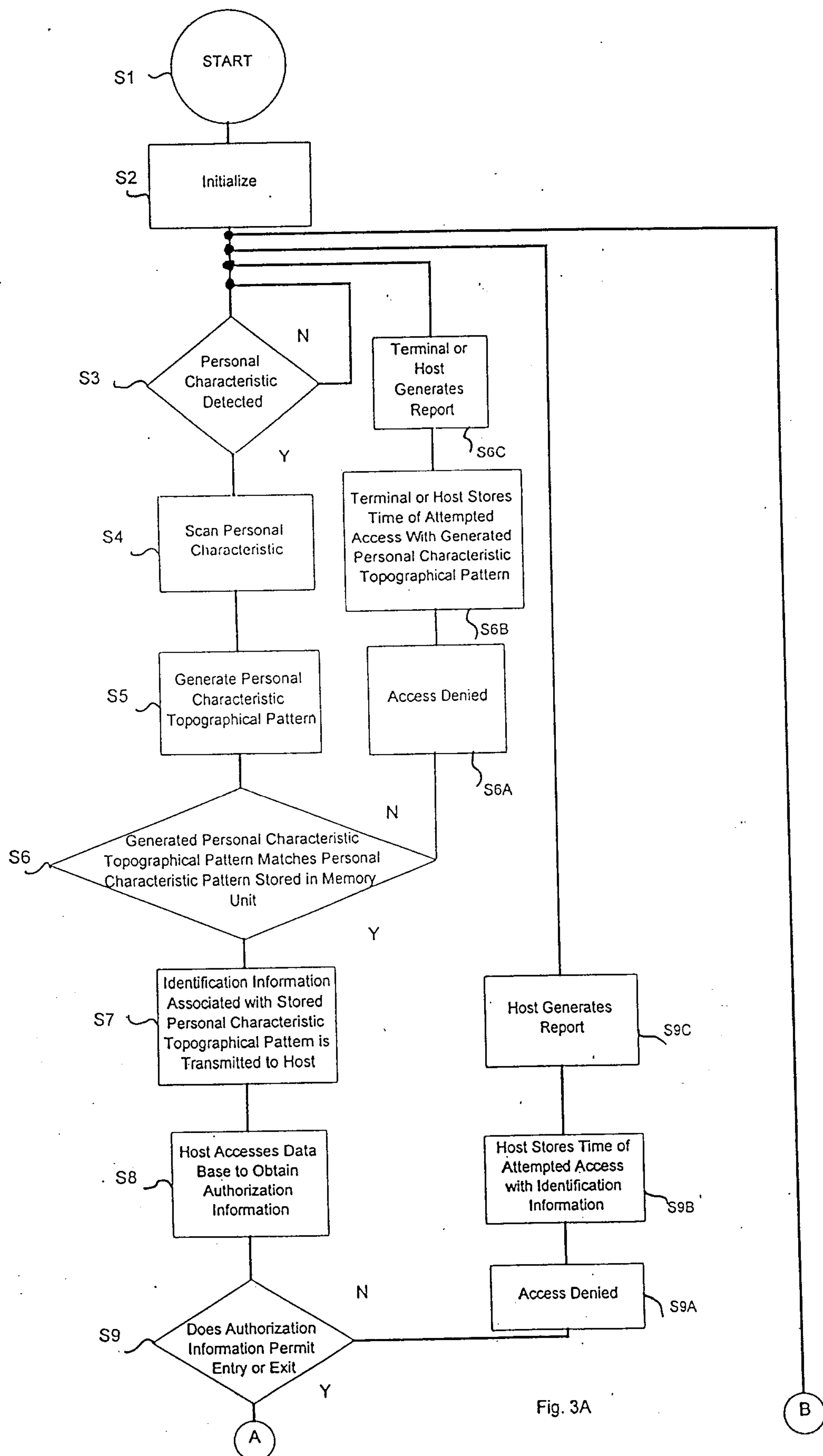


Fig. 2



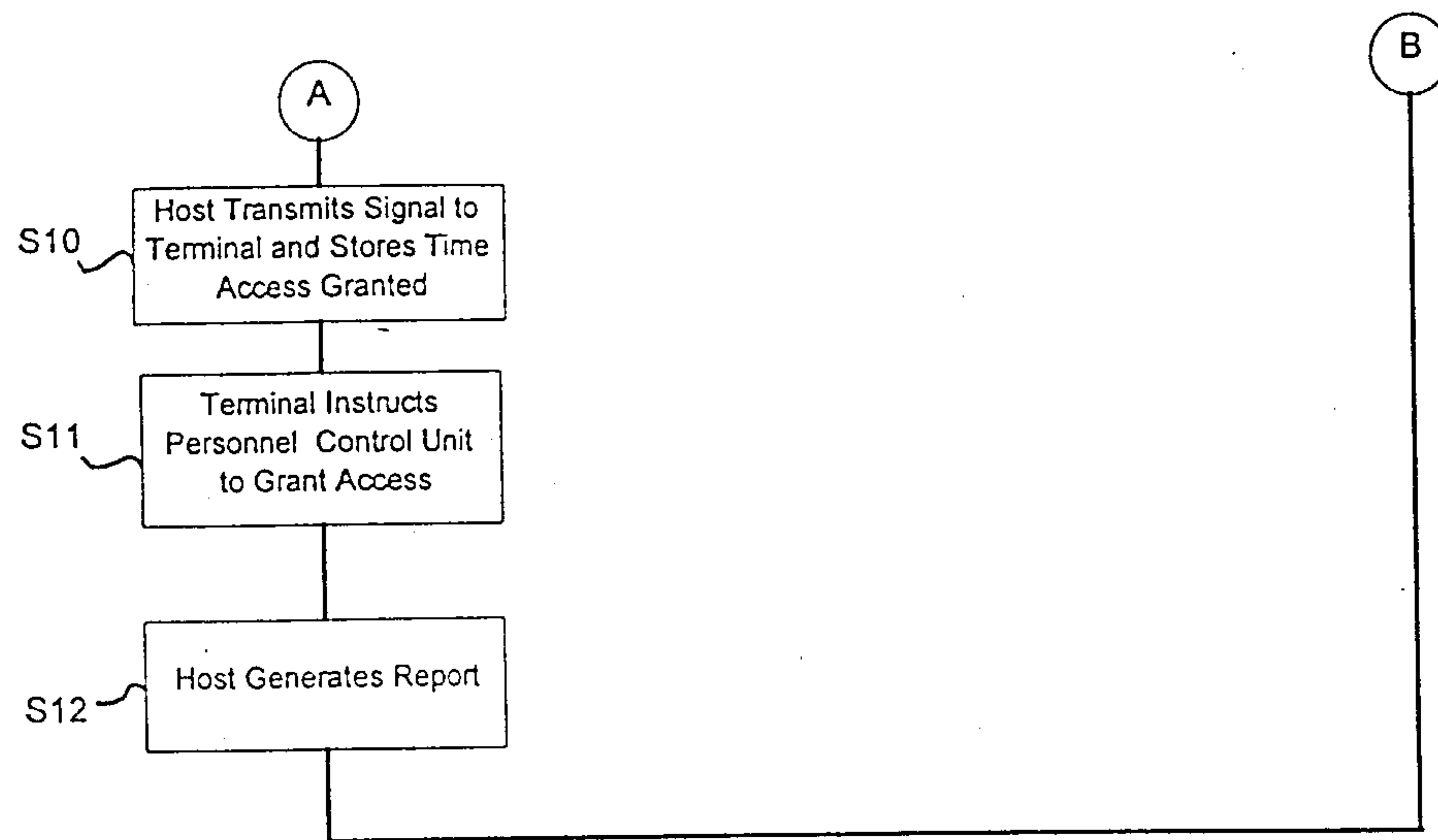


Fig. 3B

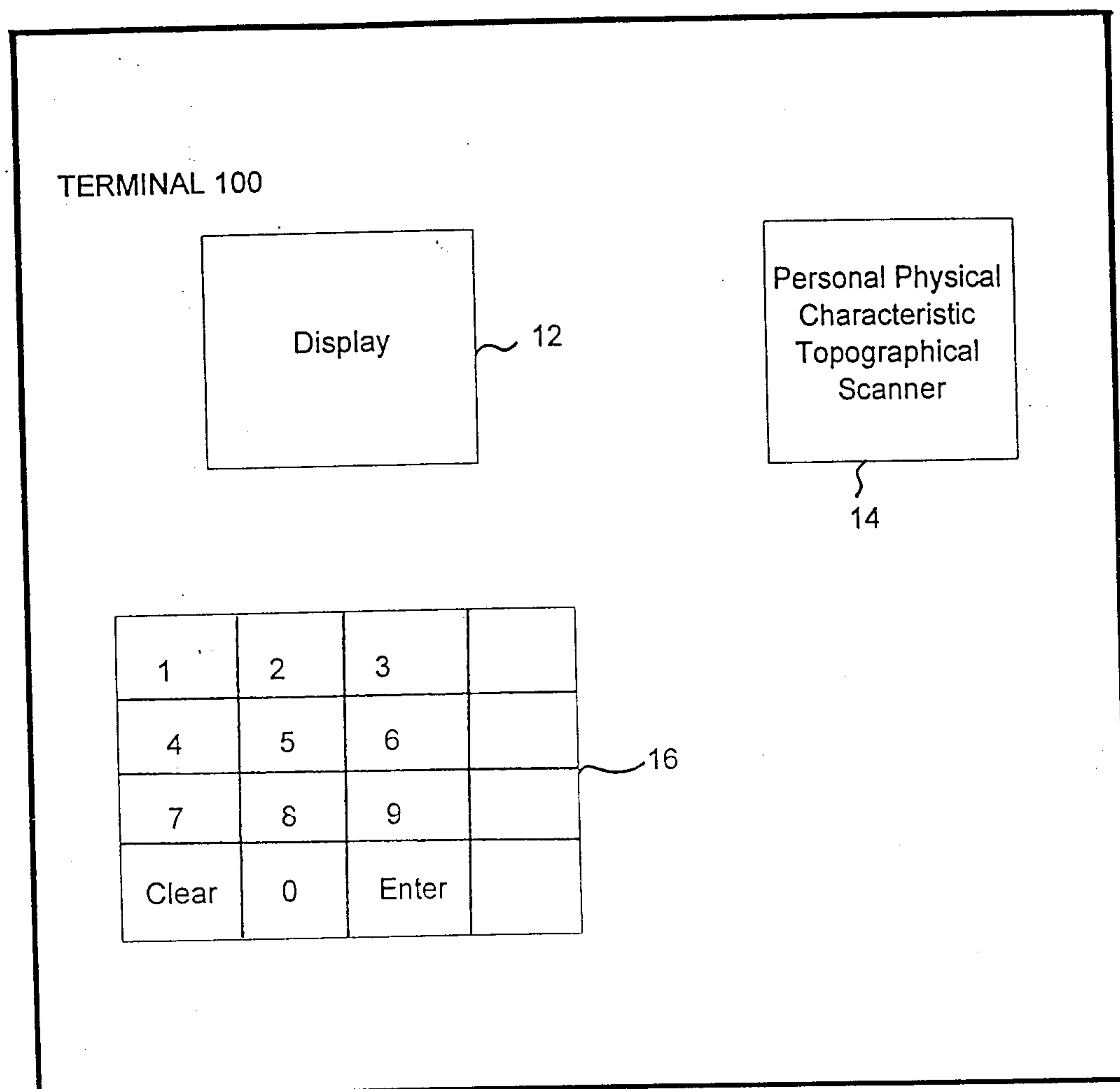


Fig. 4

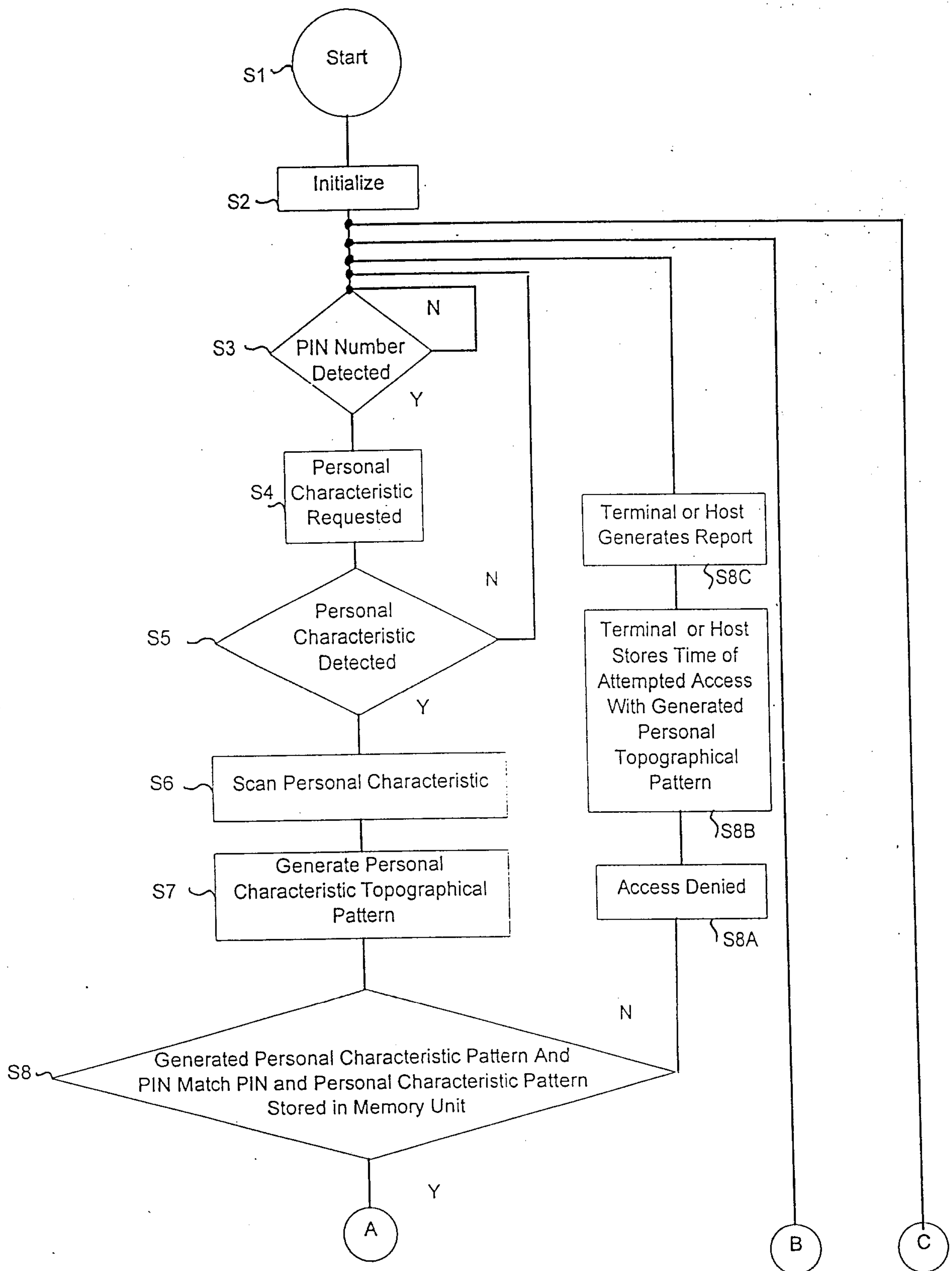


Fig. 5A

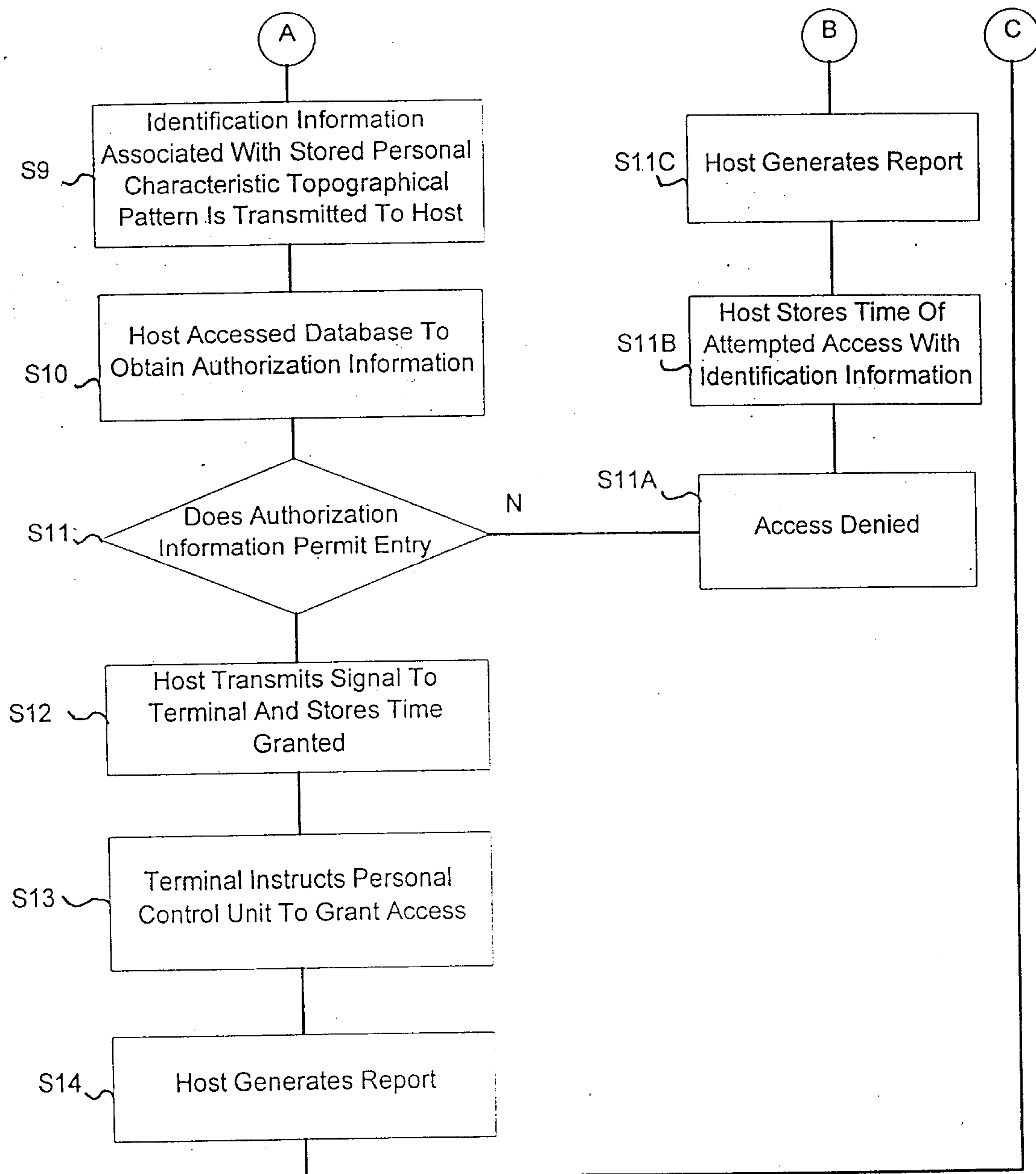


Fig. 5B

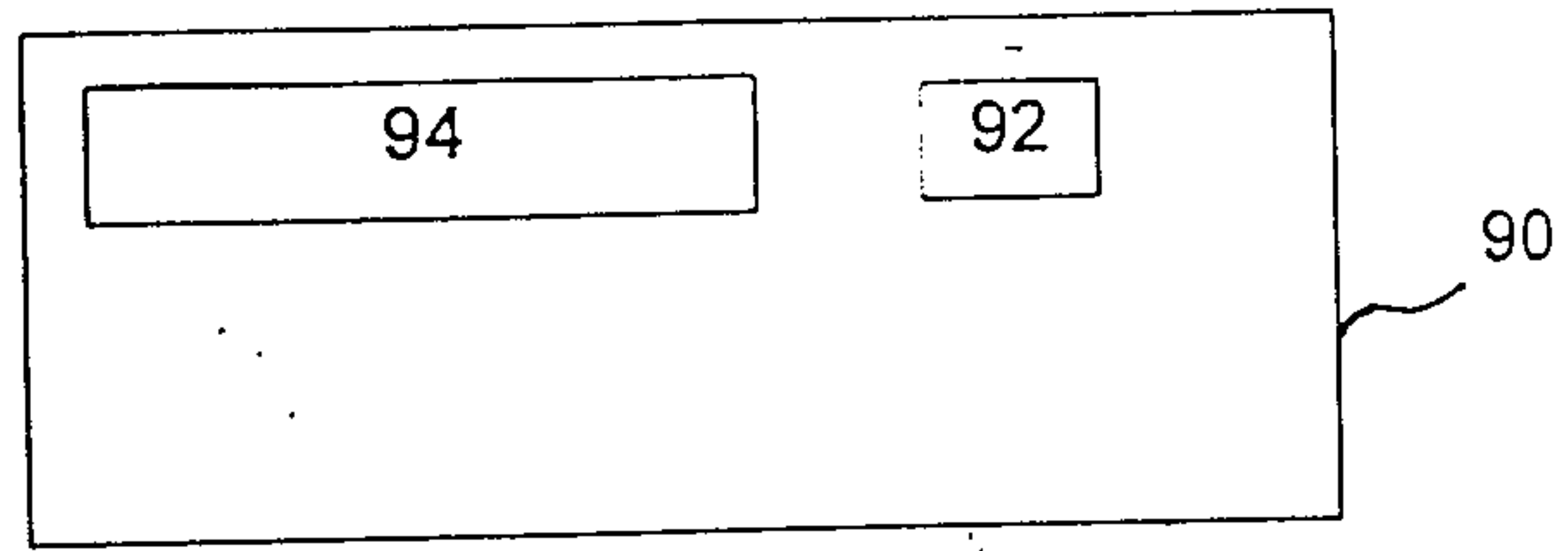


Fig. 6

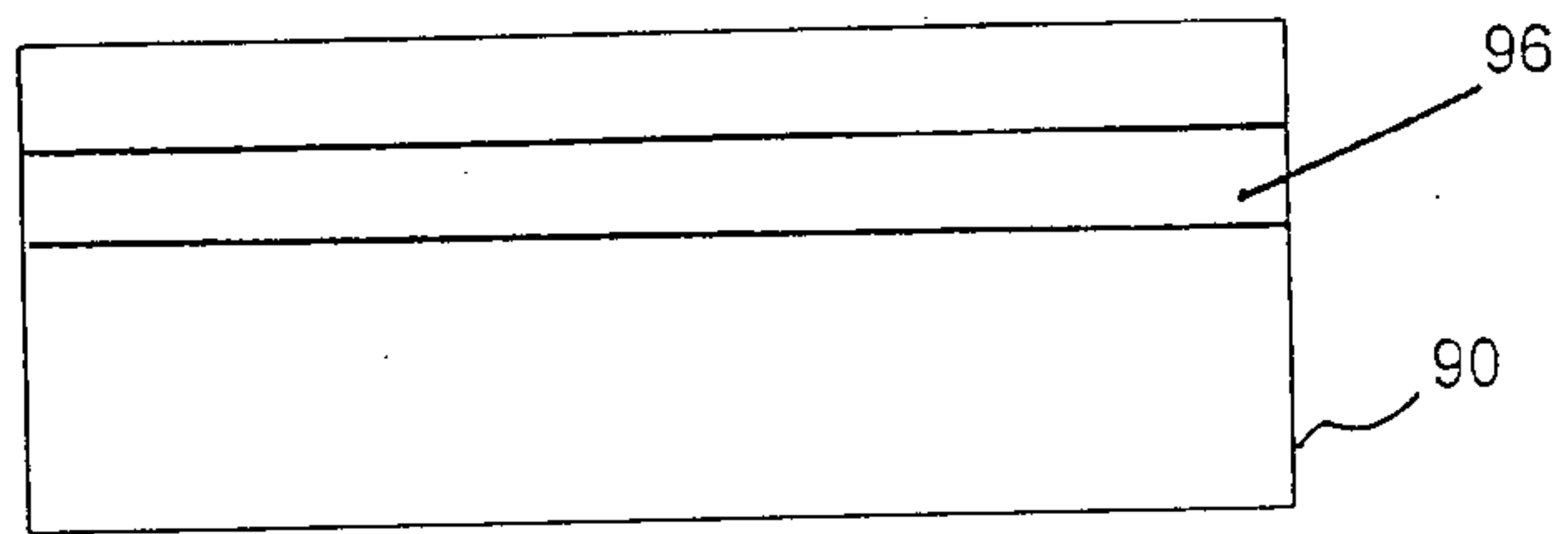


Fig. 7

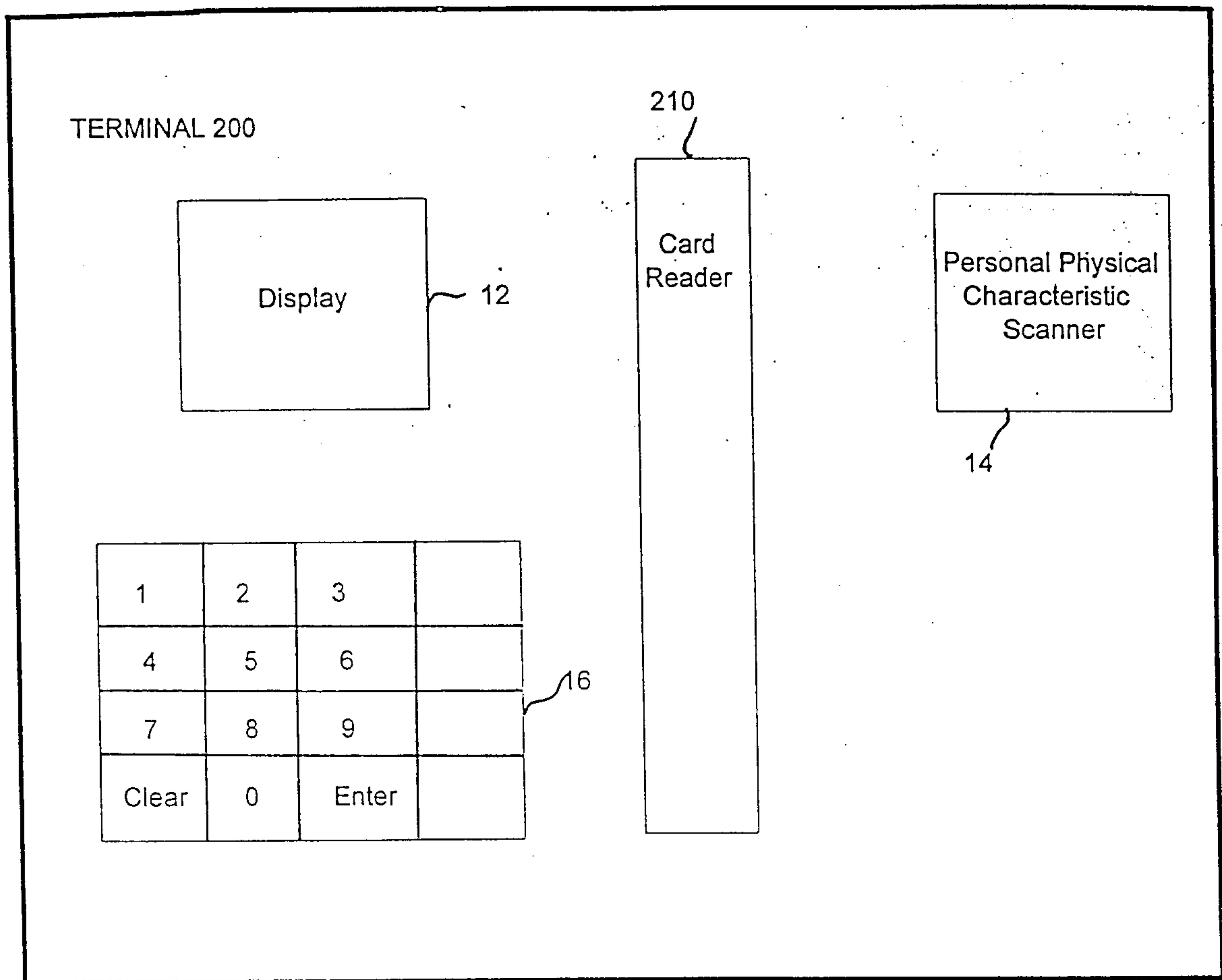
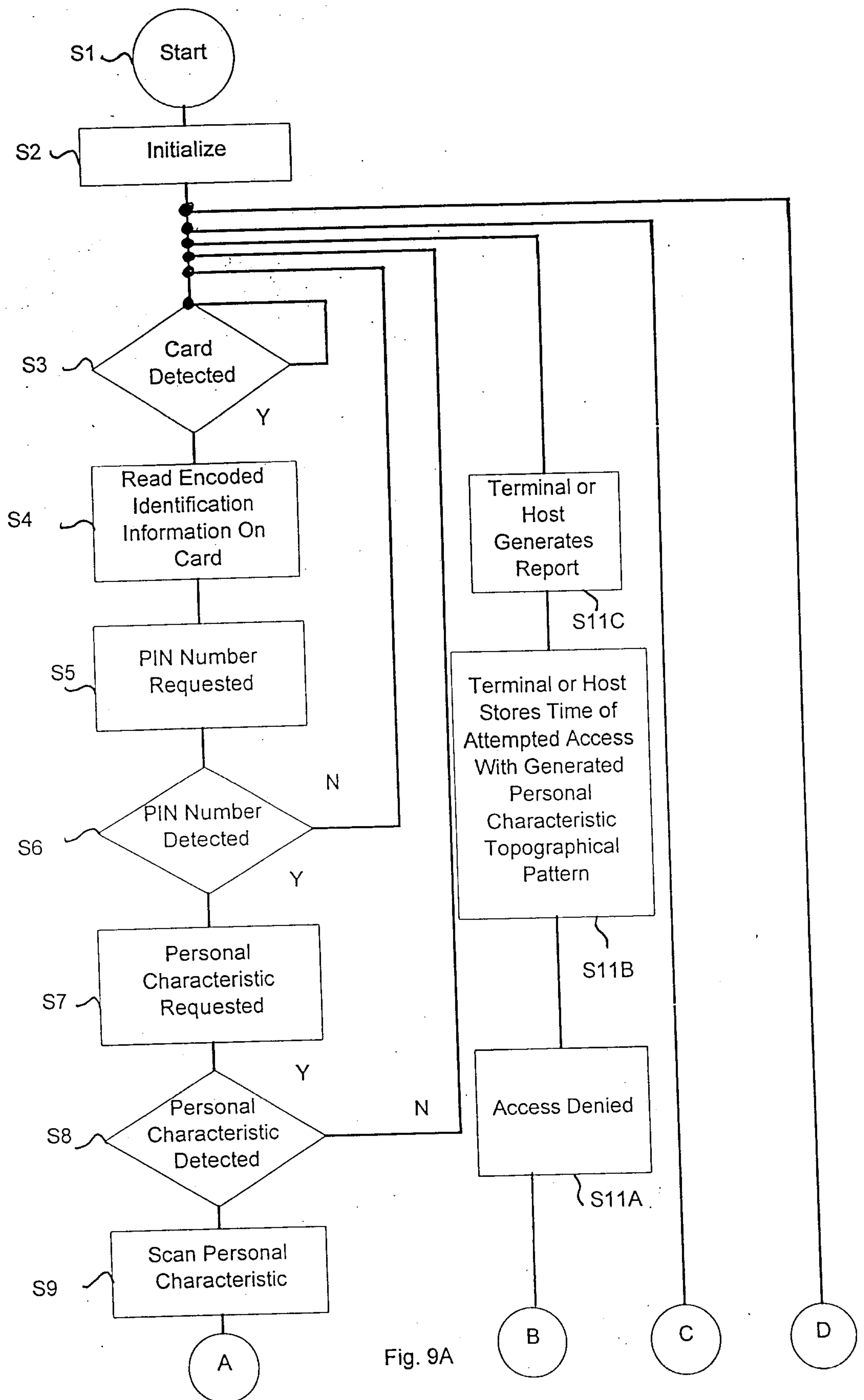


Fig. 8



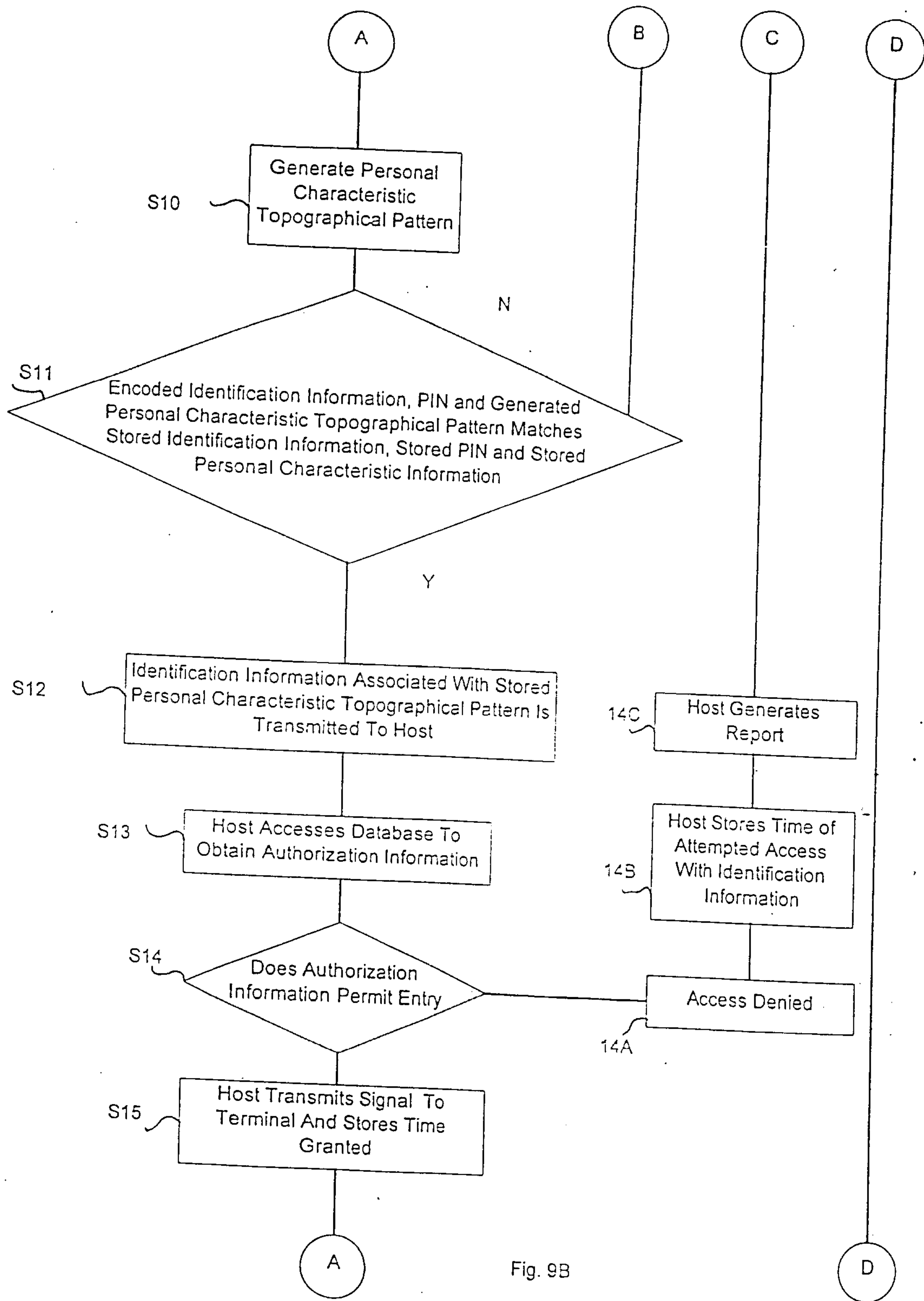


Fig. 9B

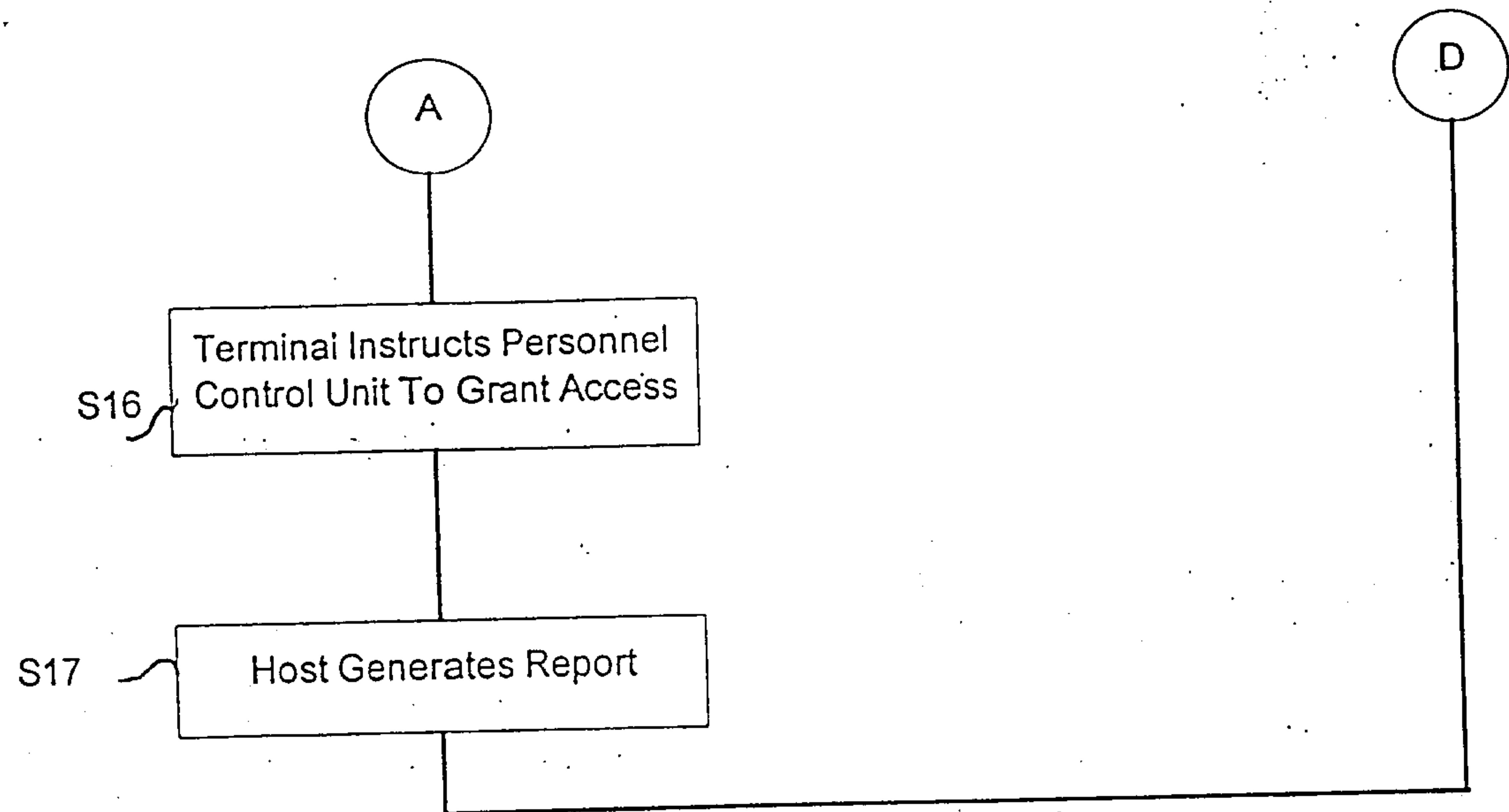
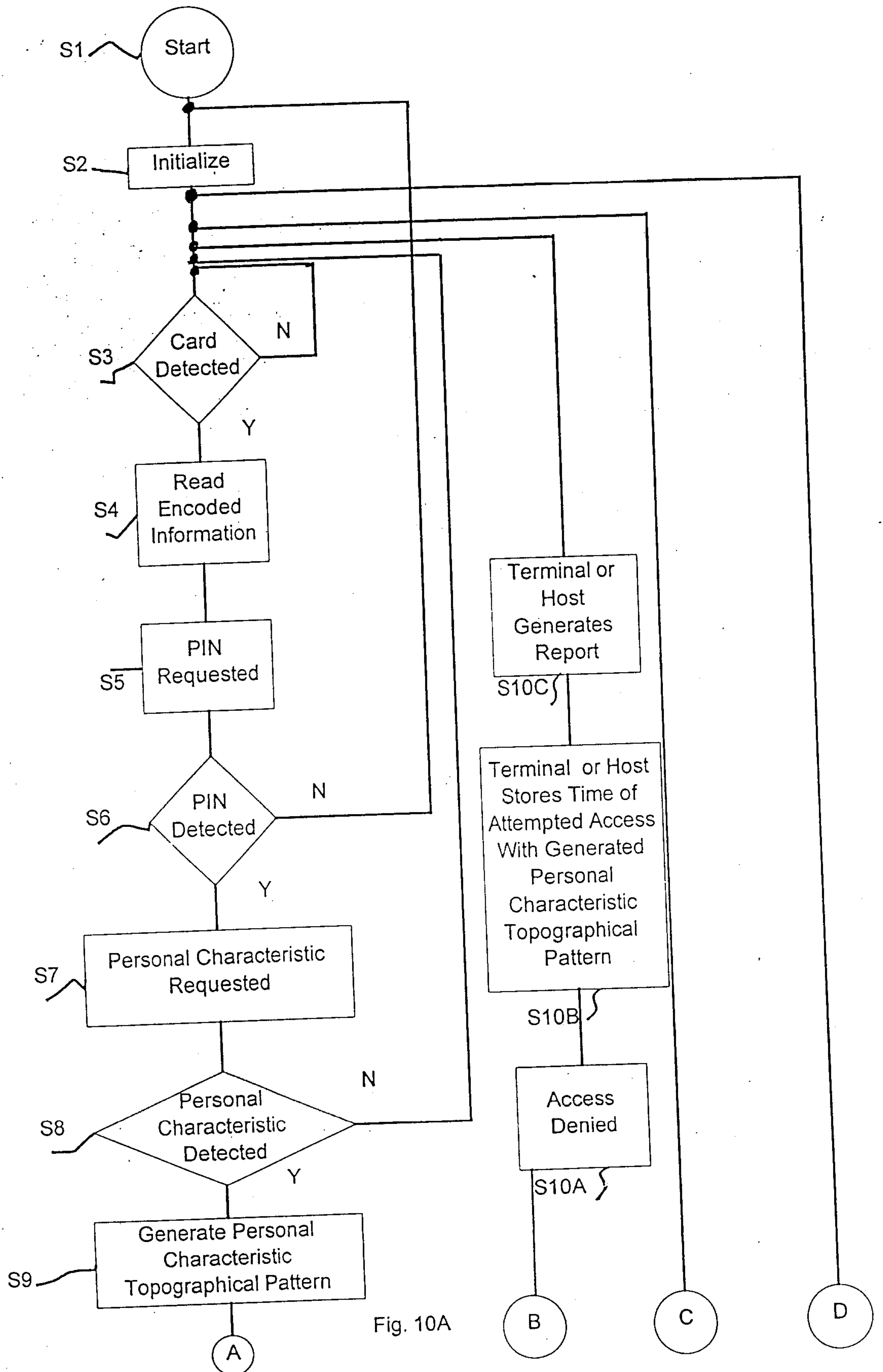


Fig. 9C



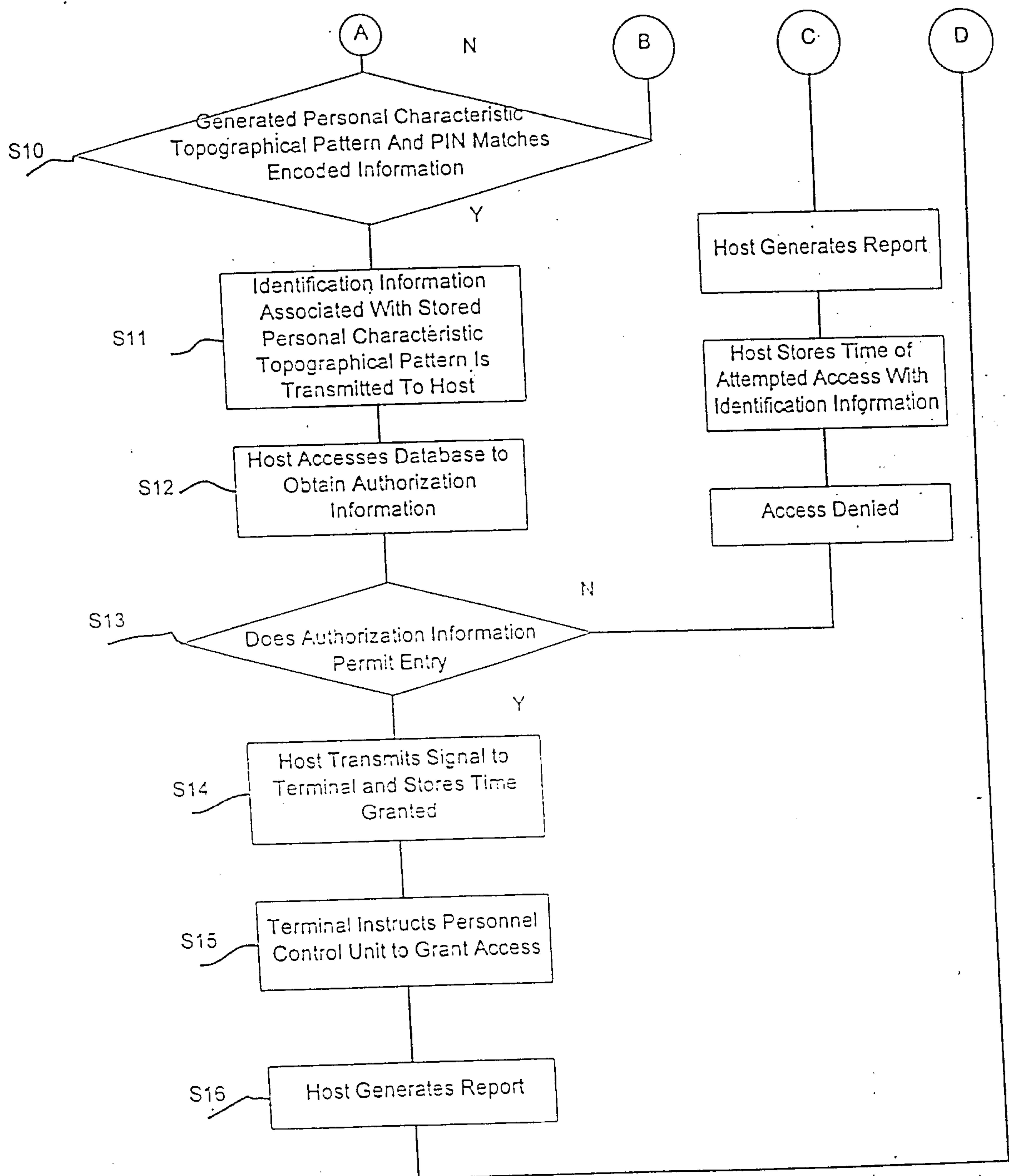


Fig. 10B

