

(86) Date de dépôt PCT/PCT Filing Date: 2009/08/27
(87) Date publication PCT/PCT Publication Date: 2010/03/04
(45) Date de délivrance/Issue Date: 2017/07/25
(85) Entrée phase nationale/National Entry: 2011/02/25
(86) N° demande PCT/PCT Application No.: EP 2009/061067
(87) N° publication PCT/PCT Publication No.: 2010/023242
(30) Priorité/Priority: 2008/08/27 (EP08163085.7)

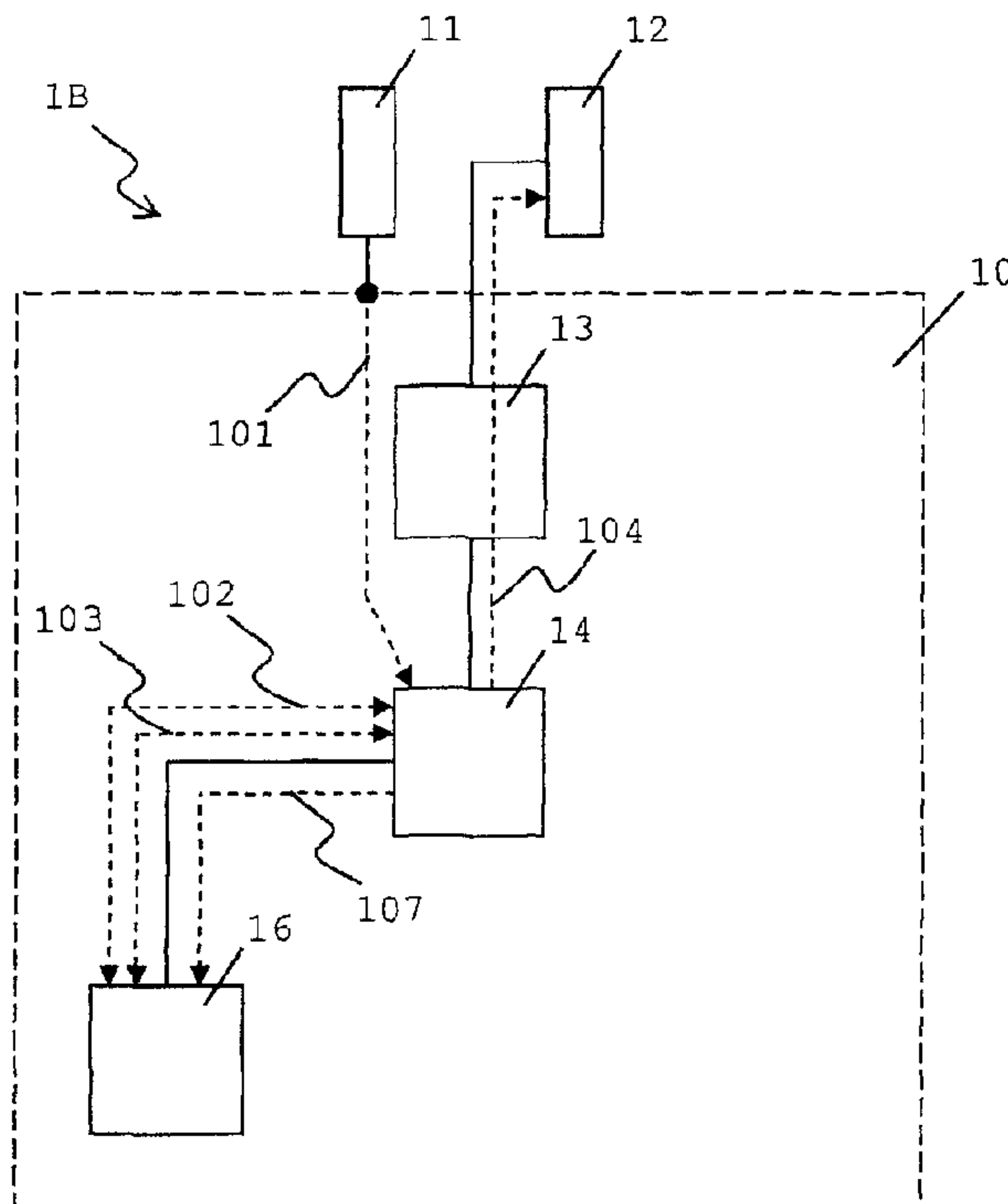
(51) **Cl.Int./Int.Cl.** *H04N 7/167* (2011.01),
H04N 5/00 (2011.01)

(72) **Inventeur/Inventor:**
VAN DE VEN, ANTONIUS JOHANNES PETRUS
MARIA, NL

(73) **Propriétaire/Owner:**
IRDETO B.V., NL

(74) **Agent:** SMART & BIGGAR

(54) Titre : SYSTEME D'ACCES CONDITIONNEL MULTIFOURNISSEUR
(54) Title: MULTI-VENDOR CONDITIONAL ACCESS SYSTEM



(57) **Abrégé/Abstract:**

The invention provides a smartcard, a head-end system and a conditional access system enabling incompatible receivers to be used in a vendor specific conditional access system. Hereto the smartcard stores an operation mode identifier, which is read upon insertion of the smartcard into the receiver and activation of the smartcard. The operation mode identifier is used to select a protocol for communication with the receiver. If the protocol is incompatible with the receiver, the operation mode identifier is changed and another protocol is selected upon reinsertion of the smartcard in the receiver. The head-end system uses data packet encapsulation to enable the receiver to forward EMMs and ECMs to the smartcard.

(10) International Publication Number
WO 2010/023242 A1

- (84) Designated States** (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,

(57) Abstract: The invention provides a smartcard, a head-end system and a conditional access system enabling incompatible receivers to be used in a vendor specific conditional access system. Hereto the smartcard stores an operation mode identifier, which is read upon insertion of the smartcard into the receiver and activation of the smartcard. The operation mode identifier is used to select a protocol for communication with the receiver. If the protocol is incompatible with the receiver, the operation mode identifier is changed and another protocol is selected upon reinsertion of the smartcard in the receiver. The head-end system uses data packet encapsulation to enable the receiver to forward EMMs and ECMs to the smartcard.

Fig. 4

WO 2010/023242 A1



MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, **Published:**
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, — *with international search report (Art. 21(3))*
ML, MR, NE, SN, TD, TG).

Multi-vendor conditional access system

FIELD OF THE INVENTION

The present invention relates to a smartcard for use in a receiver of a conditional access system, a head-end system for use in a conditional access system and a
5 conditional access system. More specifically the invention relates to enabling a multi-vendor conditional access system.

BACKGROUND

Conditional access systems are well known and widely
10 used in conjunction with currently available pay television systems. At present, such systems are based on the transmission of services encrypted with control words (also referred to as service encryption keys) that are received by subscribers having a set-top box (also referred to as a
15 receiver) and a smartcard for each subscription package. Typically these services are transmitted by a head-end system in a broadcast stream. Implementations are known wherein set-top box functionality is integrated into a device like a television, a personal video recorder, a mobile phone, a smart
20 phone or a computer appliance. A smartcard is typically a separate card that is manually inserted into the set-top box before operation. The smartcard for a subscription package from a particular service provider allows the encrypted services within the package to be decrypted and viewed. The
25 broadcast stream further contains entitlement management messages (EMMs), also referred to as key management messages (KMMs), and entitlement control messages (ECMs), which are necessary for the smartcard to decrypt the service. ECMs are used to carry the control word in encrypted form. EMMs are
30 used to convey the secret keys used to decrypt the ECMs to extract the control word, to decrypt other data related to the addition or removal of viewing/usage rights, and/or to decrypt other user-specific data.

Conditional access systems typically deploy proprietary technology, whereby the smartcard, set-top box and head-end system communicate according to a vendor specific protocol. The implementation of the conditional access system requires a vendor specific firmware installed in the set-top box that can search the broadcast stream for cryptograms addressed to the smartcard. As the addressing methods and cryptogram message formats are vendor specific, the receiver infrastructure - i.e. the set-top boxes in the conditional access system - is suitable for only a single vendor's conditional access system. Thus a set-top box operating according to a vendor 'A' specific technology cannot communicate with a smartcard operating according to a vendor 'B' specific technology or a head-end system operating according to a vendor 'B' specific technology. This is potentially problematic in case of for example broadcaster mergers, conditional access vendor mergers, changes of ownership, large scale security breaches or a broadcaster deciding to stop using a particular vendor specific conditional access system. In these cases the existing receiver infrastructure become useless as it is only compatible with the original conditional access system. Writing off an existing receiver infrastructure can be a significant destruction of capital. Moreover, an end-user can be reluctant to buy a new set-top box.

It is known that new firmware can be uploaded to the receiver infrastructure to allow operation according to another vendor specific technology, but lack of commercial incentives for a receiver manufacturer makes this a non-preferred solution.

Digital Video Broadcasting (DVB) protocols are known to allow an existing receiver infrastructure to operate with a smartcard and head-end system operating according to another vendor specific technology. The SimulCrypt DVB protocol uses multiple set-top boxes, each using a different conditional access system, to authorize broadcasted programs for display. The different ECMs and EMMs required by each conditional access system are transmitted simultaneously. Each set-top box

recognizes and uses the appropriate ECM and EMM needed for authorization. The MultiCrypt DVB protocol allows multiple conditional access systems to be used with one set-top box by using a PC card with an embedded smart card for each

5 conditional access system used. Each card is then plugged into a slot in the set-top box. Each card recognizes the ECM and EMM needed for authorization.

SUMMARY OF THE INVENTION

10 It is an object of the invention to provide an improved conditional access system wherein it is possible to change from one (typically vendor specific) technology to another (typically vendor specific) technology without modifying the existing receiver infrastructure.

15 According to an aspect of the invention a smartcard is proposed for use in a receiver of a conditional access system. The smartcard comprises one or more contacts for detachably connecting the smartcard to the receiver. The smartcard further comprises an electrical circuit comprising

20 an input/output module for communication with the receiver. The smartcard further comprises a processor and a memory. The electrical circuit is connected to the one or more contacts and is configured to be activated after connection with the receiver through the contacts. The processor is configured for

25 detecting activation of the electrical circuit and reading a first operation mode identifier for identifying a first protocol from the memory in response to detecting the activation. The processor is further configured for transmitting a first signal to the receiver in accordance with

30 the first protocol. The processor is further configured for detecting a failed attempt to communicate with the receiver and subsequently changing in the memory the first operation mode identifier into a second operation mode identifier for identifying a second protocol when the smartcard is reconnected

35 to the receiver.

According to an aspect of the invention a method is proposed for use in a smartcard. The method comprises the step of detecting activation of an electrical circuit. The method further comprises the step of reading a first operation mode

identifier for identifying a first protocol from a memory in response to detecting the activation. The method further comprises the step of transmitting a first signal to a receiver in accordance with the first protocol. The method
5 further comprises the step of detecting a failed attempt to communicate with the receiver and subsequently changing in the memory the first operation mode identifier into a second operation mode identifier for identifying a second protocol when the smartcard is reconnected to the receiver.

Thus the smartcard of the invention advantageously
10 enables operation with a receiver that uses a particular protocol for communication with the smartcard, by switching to the particular protocol after a failed attempt to communicate with the receiver and reinserting the smartcard into the receiver. Preferably the smartcard supports multiple protocols
15 enabling the smartcard to operate with receivers of different technologies after a number of reinsertions - but possibly after the first insertion - into the receiver.

Some embodiments advantageously enable the smartcard to receive a response signal from the receiver within a predefined timeframe before deciding that
20 communication with the receiver failed.

Some embodiments advantageously enable switching to another protocol only after a predefined number of reinsertions. This ensures that the smartcard does
25 not change the operation mode identifier immediately in case the receiver is temporary unable to send the response signal for whatever reason.

Some embodiments advantageously enable the smartcard to operate with ISO 7816-3 compliant
30 receivers.

Some embodiments advantageously enable translation of vendor specific instructions to allow the receiver to operate according to its original proprietary technology.

35 Some embodiments advantageously enable receiving EMMs and/or ECMs from a head-end system through a receiver of a different proprietary technology.

55876-3

5

According to an aspect of the invention a conditional access system is proposed comprising a head-end system, a receiver and a smartcard having one or more of the above mentioned features. This advantageously enables the head-end
5 system and the smartcard to operation with a receiver of a different proprietary technology.

Some embodiments advantageously enable an incompatible receiver to become operational in the conditional access system.

10 According to an aspect of the invention a computer program product is proposed. The computer program product comprises software code portions configured for, when run in a memory of a smartcard, executing one or more of the above mentioned method steps. This advantageously enables the
15 smartcard to be manufactured separately from the computer program product.

According to an aspect of the invention, there is provided a computer readable medium storing a computer program comprising executable software code portions configured for,
20 when run in a memory of a smartcard, executing a method as described above or detailed below.

Hereinafter, embodiments of the invention will be described in further detail. It should be appreciated, however, that these embodiments may not be construed as limiting the
25 scope of protection for the present invention.

55876-3

5a

BRIEF DESCRIPTION OF THE DRAWINGS

Aspects of the invention will be explained in greater detail by reference to exemplary embodiments shown in the drawings, in which:

- 5 Fig.1 shows an architecture of a conditional access network of an exemplary embodiment of the invention;
- Fig.2 shows a time-sequence diagram for signals between a smartcard and a receiver of an exemplary embodiment of the invention;
- 10 Fig.3 shows a head-end system of an exemplary embodiment of the invention;
- Fig.4 shows a smartcard of an exemplary embodiment of the invention;
- Fig.5 shows a smartcard of an exemplary embodiment of
- 15 the invention;
- Fig.6 shows a schematic view of a method of an exemplary embodiment of the invention;

Fig.7 shows a schematic view of a part of method of an exemplary embodiment of the invention;

Fig.8 shows a schematic view of a method of an exemplary embodiment of the invention;

5 Fig.9 shows a state machine of smartcard of an exemplary embodiment of the invention.

DETAILED DESCRIPTION OF THE DRAWINGS

A simplified overview of an architecture of a conditional access system 5 is shown in Fig.1. The conditional access system 5 comprises a head-end system 2, receivers 3A,3B, smartcards 1A,1B for use in the receivers 1A,1B and a broadcast network 4 for transmission of signals from the head-end system 2 to a receiver 3A,3B and smartcard 1A,1B.

15 Typically a conditional access network comprises many receivers and smartcards, e.g. in the order of hundreds or thousands or even more. The head-end system 2 broadcasts encrypted television programs, or other encrypted services, to the receiver 3A,3B. To enable decryption of the encrypted television programs in the receiver 3A,3B the head-end system 2 further broadcasts EMMs and/or ECMs, which are received in the receiver 3A,3B and forwarded to the smartcard 1A,1B for processing. The head-end system 2 uses a vendor specific, typically proprietary, technology for communication with the smartcard 1A,1B. This means that EMMs and ECMs are formatted according to a vendor specific protocol. If the smartcard 1A,1B is of the same vendor as the head-end system 2, the smartcard 1A,1B understands the format of the EMMs and ECMs and is able to process the EMMs and ECMs. The smartcard 1A,1B and the receiver 3A,3B use a conditional access system specific command set to exchange information such as descrambling keys, conditional access filter parameters and entitlement information.

20
25
30

The receiver must be compatible with the vendor specific technology to be able to receive the EMMs and ECMs from the head-end system 2 and forward the EMMs and ECMs to the smartcard. This means that firstly the receiver and smartcard must be able to communicate and secondly the

35

receiver must be able to recognize the EMMs and ECMs in the
broadcasted signal. If the receiver, e.g. receiver 3A, is
bought specifically for use with the head-end system 2 and the
smartcard 1A, then there should be no compatibility issue. In
5 this case the firmware of the receiver 3A is specifically
programmed according to the vendor specific technology. If the
receiver, e.g. receiver 3B, is not compatible with the head-
end system 2 and the smartcard 1B, then no communication
between the smartcard 1B and the receiver 3B is possible and
10 no EMMs and ECMs are processed by the smartcard 1B.
Consequently the encrypted television program cannot be
decrypted by the receiver 3B.

To enable the initially incompatible receiver 3B to
communicate with the smartcard 1B, the smartcard 1B is capable
15 of changing its operation mode to a protocol that is
compatible with the receiver 3B.

In Fig.4 an exemplary embodiment of smartcard 1B is
shown. The smartcard 1B comprises an electrical circuit 10 and
two contacts 11,12 for detachably connecting the smartcard 1B
20 to the receiver 3B. Contact 11 is used to connect the
electrical circuit 10 to a power supply of the receiver 3B.
Contact 12 is used for communication with the receiver 3B. It
is possible to use more contacts for connecting to the power
supply and for communication with the receiver 3B. The
25 electrical circuit 10 comprises a central processor 14 which
is connected to a memory 16 and an input/output module 13. The
memory 16 is a non-volatile that retains stored information
even when not powered. The memory is, amongst others, used to
store an operation mode identifier and different protocol
30 definitions.

Upon inserting the smartcard 1B into the receiver 3B,
the contact 11 is connected to the power supply of the
receiver 3B and the electrical circuit 10 is activated.
Through electrical elements not shown in Fig.4 the processor
35 14 detects the activation of the electrical circuit 10, which
is indicated by dashed arrow 101. This triggers the processor
14 to read an operation mode identifier from the memory 16,
which is indicated by dashed arrow 102. The operation mode

identifier is used to start the smartcard 1B in a specific operation mode using a particular protocol for communication with the receiver 3B. Dashed arrow 103 indicates the selection of the protocol and reading of the protocol definition from the memory 16 based on the operation mode identifier, which is subsequently used to start the smartcard 1B in the specific operation mode. When started in the specific operation mode, the smartcard 1B communicates with the receiver 3B in accordance with the protocol. Dashed arrow 104 indicates a signal that is transmitted via the input/output module 13 and through contact 12 to the receiver 3B. The receiver 3B is expected to return a response signal, indicating a correct receipt of the signal. If no response signal is received, then it is concluded that the receiver 3B is incompatible with the protocol used. This triggers the processor 14 to change the operation mode identifier in the memory 16 to a value indicating another protocol supported by the smartcard 1B. Dashed arrow 107 indicates the change of the operation mode identifier in the memory 16.

As long as the smartcard 1B remains inserted into the receiver 3B no communication is possible between the smartcard 1B and the receiver 3B as the operation mode and accompanying protocol of the smartcard 1B is incompatible with the receiver 3B. A reinsertion of the smartcard 1B into the receiver 3B will restart the smartcard 1B as described above, only this time the operation mode identifier has a different value resulting in the smartcard 1B starting in another operation mode and thus using another protocol. If this protocol is compatible with the receiver 3B, a return signal will be received. Otherwise, if other operation modes are available on the smartcard, the operation mode identifying is changed again into another value and the smartcard 1B can be reinserted into the receiver 3B again.

The change of the operation mode identifier can optionally be postponed until the smartcard 1B has been reinserted a predefined number of times, e.g. three times. Referring to Fig.5, hereto the processor uses a counter value stored in the memory 16. Initially the counter value has,

55876-3

9

e.g., a value of "0". After the first timeout trigger 106 the counter value is increased by 1, which is indicated by dashed arrow 108. Next the processor 14 reads the counter value from the memory 15 (dashed arrow 109) and only if the counter value equals the predefined value of "3" the operation mode identifier is changed and the counter value is reset to "0". The use of the counter value is not restricted to the given example. The counter may e.g. be a countdown counter or any other counter mechanism.

10 The smartcard of the invention can be used with ISO 7816-3 compliant receivers. An ISO 7816-3 compliant receiver transmits a reset signal to the smartcard after insertion of the smartcard into the receiver. The reset signal is a standardised signal and is independent of the vendor specific technology. In Fig.2 a time-sequence diagram is shown for communication between a smartcard 1B and an ISO 7816-3 compliant receiver 3B. Upon insertion of the smartcard 1B into the receiver 3B the electrical circuit 10 of the smartcard 1B is activated and the processor 14 detects the activation of the electrical circuit 10. This is indicated by dashed arrow 101. Next the receiver 3B transmits the reset signal 301 to the smartcard 1B. Only after having received the reset signal 301, the smartcard 1B transmits an answer-to-reset signal 104 to the receiver 3B. Signal 104 is in accordance with the vendor specific protocol, as described above. If the receiver 3B is compatible with the used protocol, a response signal 302 is transmitted to the smartcard 1B.

 A state machine module can be used to keep track of the current state of the smartcard 1B, e.g. "pending" in case no successful communication has been established with the receiver 3B or "active" in case communication with the receiver 3B is successful. The state machine module keeps track of whether after activation of the electrical circuit 10 a valid message according to the current protocol mode is received or not. It is possible to use the reset signal as a trigger for the state machine module instead of the activation of the electrical circuit 10. In Fig.9 an example of a state machine is shown that can be implemented in the

55876-3

10

state machine module. Two possible operation modes identified by "A" and "B" are shown. After having received a valid message from the receiver 3B, i.e. after a successful communication with the receiver 3B according to the current protocol, the state machine module is put in an "active" state. After a reset signal is received from the receiver 3B, the state machine module is put in a "pending" state. From this "pending" state it either returns to the "active" state of the current operation mode, i.e. when a valid message is received, or to the "pending" state of the next operational mode if the card has been reset a predefined number of times while in the "pending" state. The number of consecutive resets before changing the operation mode identifier to the next operation mode can be operation mode dependent. It can e.g. be dependent on how many times the receiver 3B typically transmits a reset signal to the smartcard 1B after it starts up, i.e. from power-down or when returning from stand-by. In Fig.9 it takes three consecutive resets without valid messages received in-between to switch from operation mode A to B, and four to switch back. After the activation of the electrical circuit 10 or receiving the reset signal, the counter (indicated by cnt in Fig.9) is tested. When the counter equals 0, the operation mode identifier is changed to the next operation mode, an answer-to-reset signal according to the protocol of the new operation mode is returned, and the counter is set to the (possibly mode specific) initial value minus 1. When $cnt > 0$ after a reset, an answer-to-reset signal of the current mode is returned and cnt is decremented by 1. If in the "pending" state a valid message is received from receiver 3B, then the state becomes "active" and the counter is set to the initial value.

The smartcard 1B optionally uses an adaptation module for translating signals from and to the receiver 3B. In Fig.5 the adaptation module is indicated as element 17. The adaptation module 17 operates in-between the processor 14 and the input/output module 13 and is e.g. implemented as an adaptation layer in a protocol stack. When using an adaptation module 17, the adaptation module 17 is started in an operation

mode using a particular protocol as identified by the operation mode identifier. The adaptation module 17 enables the smartcard 1B to operate in a default operation mode, while communication with the receiver 3B is translated into the protocol of the receiver 3B. Hereto the adaptation module 17 translates instruction 104A, also known as commands from a command set, from the processor 14 into instructions understood by the receiver 3B and generates the first signal 104B which is transmitted to the receiver 3B.

10 Optionally a timer is used for timing the receipt the response signal. Dashed arrow 105 in Fig.5 indicates an instruction to start the timer at the clock module 15. When a predefined time-out value, e.g. 10 seconds, is reached, the clock module 15 triggers the processor 14 as indicated by
15 dashed arrow 106. The timeout triggers the processor 14 to change the operation mode identifier in the memory 16 to a value indicating another protocol supported by the smartcard 1B.

 To enable the head-end system 2 to communicate with
20 the initially incompatible receiver 3B, the head-end system 2 is capable of encapsulating EMMs and/or ECMs of an incompatible protocol with data packets of a compatible protocol. In Fig.3 a head-end system 2 of an exemplary embodiment of the invention is shown, wherein a signal
25 generator 21 generates the encapsulated data packets and the transmission module 22 transmits the encapsulated data packets to the receiver 3B. The signal carrying the encapsulated data packets is indicated by dashed arrow 201. When the receiver 3B receives the signal 201, it recognizes the encapsulated EMMs
30 and ECMs and transmits the encapsulated EMMs and ECMs to the smartcard 1B. In the smartcard 1B the adaptation module 17 removes the encapsulation and the EMMs and ECMs are obtained. The payload of the EMMs and ECMs is subsequently processed in the smartcard 1B.

35 The head-end system 2 enables e.g. a new conditional access system 5 to operate with an existing and incompatible receiver infrastructure including receiver 3B by including cryptographic messages such as EMMs and ECMs of the new

conditional access system in a message format understood by the existing receiver infrastructure. This allows the receiver 3B to parse the cryptographic message stream in signal 201.

The smartcard 1B of the new conditional access system 5

5 contains the adaptation layer 17 that re-uses the command set from the previously used conditional access system as supported by the receiver 3B. This enables the smartcard 1B to instruct the receiver 3B to search for messages destined for the smartcard 1B. After finding the relevant messages, the
10 receiver 3B sends them to the smartcard 1B using the original command set. The smartcard 1B removes the original message container to end up with a cryptographic message that it can process. The result of the smartcard 1B processing is conveyed to the receiver 3B again using the command set of the older
15 conditional access system.

In Fig.6 a schematic view of a method of an exemplary embodiment of the invention is shown. The steps shown in Fig.6 can e.g. be performed in the smartcard 1B of Fig.4. In step
20 step 1001 activation of the electrical circuit 1 is detected. In step 1002 the first operation mode identifier is read from the memory 16. In step 1003 the first signal is transmitted to the receiver 3B. In step 1004 it is detected that communication with the receiver 3B fails. In step 1005 the first operation mode identifier is changed into the second mode identifier in
25 the memory 16.

In Fig.8 a schematic view of a method of an exemplary embodiment of the invention is shown. The steps shown in Fig.8 can e.g. be performed in the smartcard 1B of Fig.5. In step
30 step 1001 activation of the electrical circuit 1 is detected. In step 1002 the first operation mode identifier is read from the memory 16. In step 1010 the smartcard 1B waits for a reset signal from the receiver 3B. In step 1011 one or more instructions (104A) from the processor (14) are translated into one or more translated instructions. In step 1003 the
35 translated instructions are transmitted to the receiver 3B. Substantially at the same time of transmitting the instructions to the receiver 3B, a timer is started in step 1006 for timing a response signal from the receiver 3B. In

step 1007 the timer runs until a predefined timeout, e.g. 10 seconds, is reached. In step 1008 a counter value is changed. In step 1009 the counter value is compared with a predefined threshold value. If the counter value equals the predefined threshold value, then in step 1005 the first operation mode identifier is changed into the second mode identifier in the memory 16.

Fig.7 shows two sub-steps of a method of an exemplary embodiment of the invention. The steps shown in Fig.7 can e.g. be performed in the smartcard 1B of Fig.5. In step 1012 encapsulated EMMs and ECMs are received from the receiver 3B. In step 1013 the encapsulation is removed and the EMMs and ECMs are obtained to allow its payload to be processed.

A computer program product comprising software code portions can be configured for executing the method steps of the invention, e.g. as shown in Figs.6-8. After installing the computer program product in the memory 16 of a smartcard 1A,1B, the processor 14 of the smartcard 1A,1B can, when the smartcard 1A,1B is inserted into a receiver 3A,3B, execute the software code portions.

In an alternative embodiment of the invention not shown in the figures, the operation mode identifier is changed by a switch that is part of the smartcard. The switch is e.g. a dipswitch that is accessible from the outside of the smartcard (1B). The switch is connected to the electrical circuit (10). A change of the position of the switch results in changing the operation mode identifier in the memory (16). With the switch in a particular position, the smartcard (1B) is to be inserted into the receiver (3B) to activate the electrical circuit (10). The processor (14) acquires the position of the switch and writes a corresponding identifier to the memory location of the operation mode identifier. Further the smartcard (1B) is configured to operate as described above, except for changing the operation mode identifier which is controlled by the switch.

55876-3

14

CLAIMS:

1. Smartcard for use in a receiver of a conditional access system, comprising:

5 one or more contacts for detachably connecting the smartcard to the receiver; and

an electrical circuit comprising an input/output module for communication with the receiver, a processor and a memory, the electrical circuit being connected to the one or more contacts and being configured to be activated after
10 connection with the receiver through the one or more contacts, wherein the processor is configured for:

detecting activation of the electrical circuit and reading a first operation mode identifier for identifying a first protocol from the memory in response to detecting the
15 activation;

transmitting a first signal to the receiver in accordance with the first protocol; and

detecting a failed attempt to communicate with the receiver and subsequently changing in the memory the operation
20 mode identifier into a second operation mode identifier for identifying a second protocol when the smartcard is reconnected to the receiver.

2. Smartcard according to claim 1, wherein said reconnection occurs when the smartcard is reinserted into the
25 receiver.

55876-3

15

3. Smartcard according to claim 1 or 2, further comprising a clock module and wherein the processor is further configured for:

5 substantially at the same time as transmitting the first signal to the receiver, starting a timer for timing a response signal from the receiver in response to the first signal using the clock module; and

detecting that the timer reaches a predefined timeout,

10 and wherein the processor is configured for changing the first operation mode identifier into the second operation mode identifier after detecting the predefined timeout.

4. Smartcard according to any one of the claims 1-3, wherein the processor is further configured for:

15 changing a counter value stored in the memory after detecting the failed attempt to communicate; and

changing the operation mode identifier only if the counter value equals a predefined threshold value.

5. Smartcard according to any one of the claims 1-4,
20 wherein the processor is further configured for receiving a reset signal from the receiver prior to transmitting the first signal to the receiver and wherein the first signal is an answer-to-reset signal.

6. Smartcard according to any one of the claims 1-5,
25 further comprising an adaptation module configured for translating one or more instructions from the processor into

55876-3

16

one or more translated instructions in accordance with the first protocol and wherein the first signal is transmitted from the adaptation module and comprises the one or more translated instructions.

5 7. Smartcard according to claim 6, wherein the adaptation module is further configured for:

receiving a second signal from the receiver, the second signal comprising a first data packet in accordance with a third protocol that is encapsulated by a second data packet
10 in accordance with the first protocol; and

obtaining a payload portion from the first data packet for processing by the processor.

8. Conditional access system comprising a head-end system, a receiver and a smartcard according to any one of the
15 claims 1-7.

9. Conditional access system according to claim 8, wherein the smartcard is initially incompatible with the receiver.

10. Method for use in a smartcard, comprising the steps
20 of:

detecting activation of an electrical circuit and reading a first operation mode identifier for identifying a first protocol from a memory in response to detecting the activation;

25 transmitting a first signal to a receiver in accordance with the first protocol; and

55876-3

17

detecting a failed attempt to communicate with the receiver and subsequently changing in the memory the first operation mode identifier into a second operation mode identifier for identifying a second protocol when the smartcard
5 is reconnected to the receiver.

11. Method according to claim 10, wherein said reconnection occurs when the smartcard is reinserted into the receiver.

12. Method according to claim 10 or 11, further
10 comprising the steps of:

substantially at the same time as transmitting the first signal to the receiver, starting a timer for timing a response signal from the receiver in response to the first signal using a clock module; and

15 detecting that the timer reaches a predefined timeout,

and wherein the first operation mode identifier is changed into the second operation mode identifier after detecting the predefined timeout.

20 13. Method according to any one of the claims 10-12, further comprising the steps of:

changing a counter value stored in the memory after detecting that the timer reaches the predefined timeout; and

changing the operation mode identifier only if the
25 counter value equals a predefined threshold value.

55876-3

18

14. Method according to any one of the claims 10-13,
further comprising the steps of receiving a reset signal from
the receiver prior to transmitting the first signal to the
receiver and wherein the first signal is an answer-to-reset
5 signal.

15. Method according to any one of the claims 10-14,
further comprising the steps of translating one or more
instructions from the processor into one or more translated
instructions in accordance with the first protocol and wherein
10 the first signal comprises the one or more translated
instructions.

16. Method according to claim 15, further comprising the
steps of:

receiving a second signal from the receiver, the
15 second signal comprising a first data packet in accordance with
a third protocol that is encapsulated by a second data packet
in accordance with the first protocol; and

obtaining a payload portion from the first data
packet for processing by the processor.

20 17. A computer readable medium storing a computer program
comprising executable software code portions configured for,
when run in a memory of a smartcard, executing the method steps
according to any of claims 10 to 16.

1/6

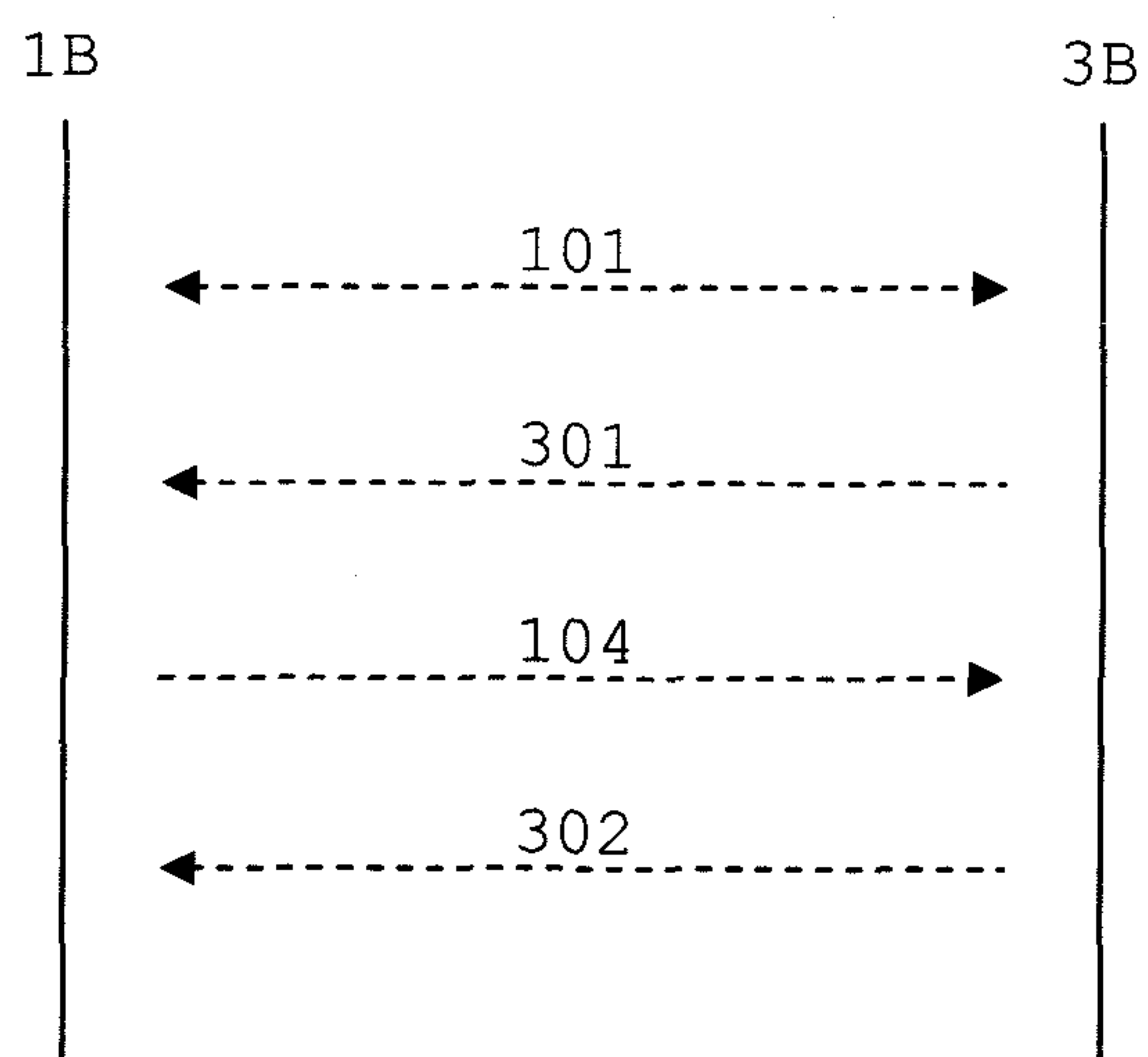
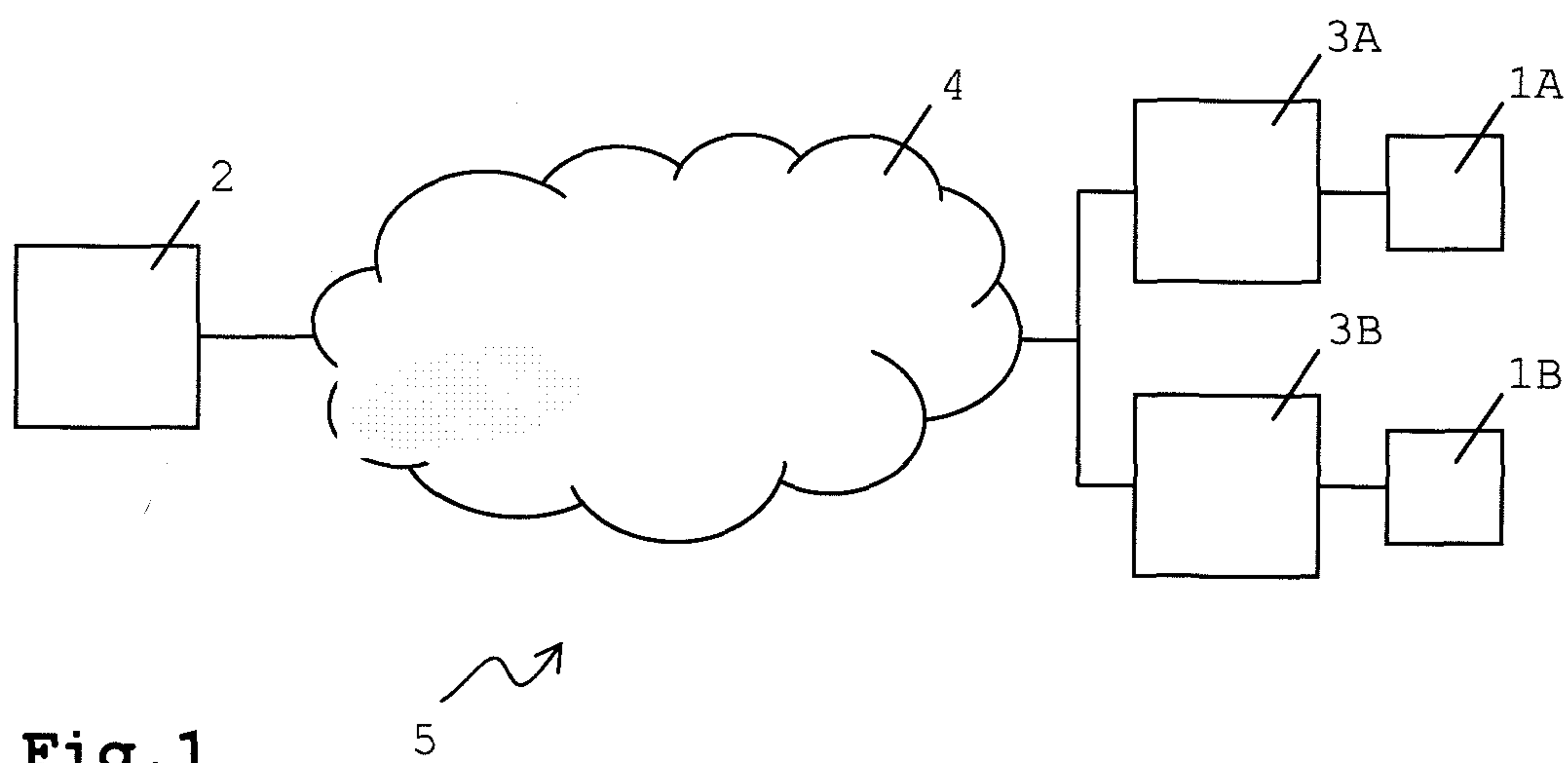


Fig. 2

2/6

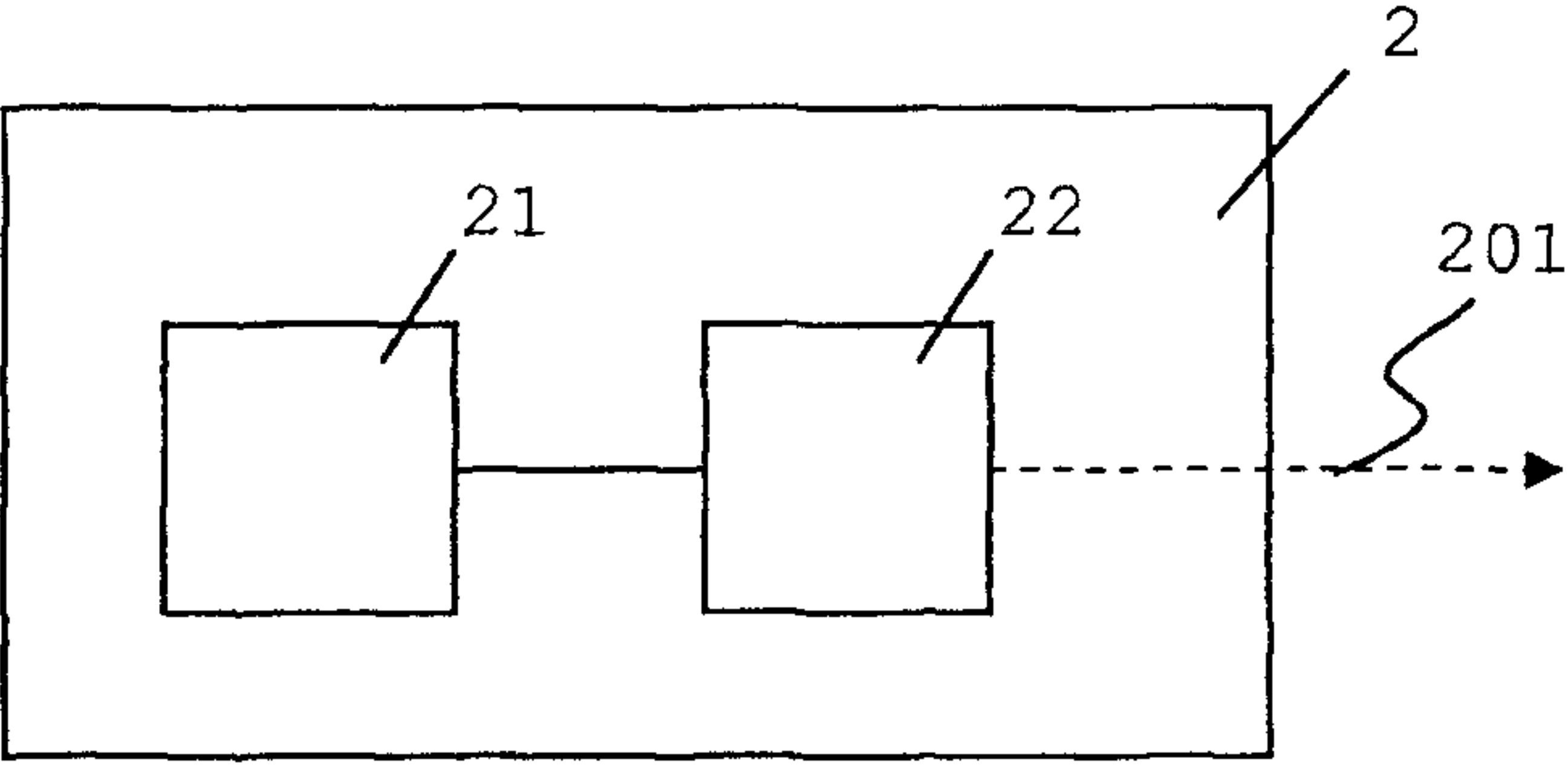


Fig. 3

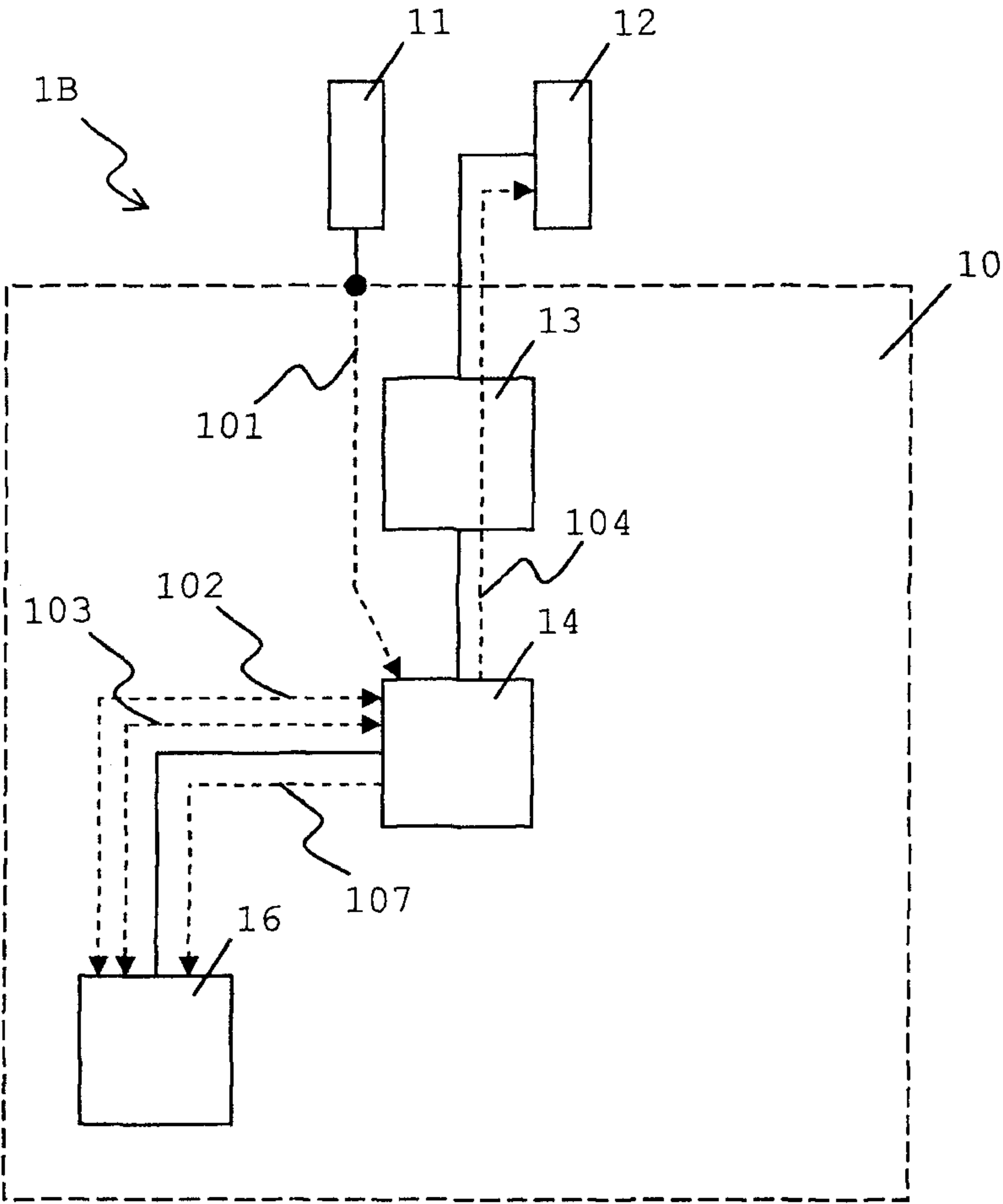


Fig. 4

3/6

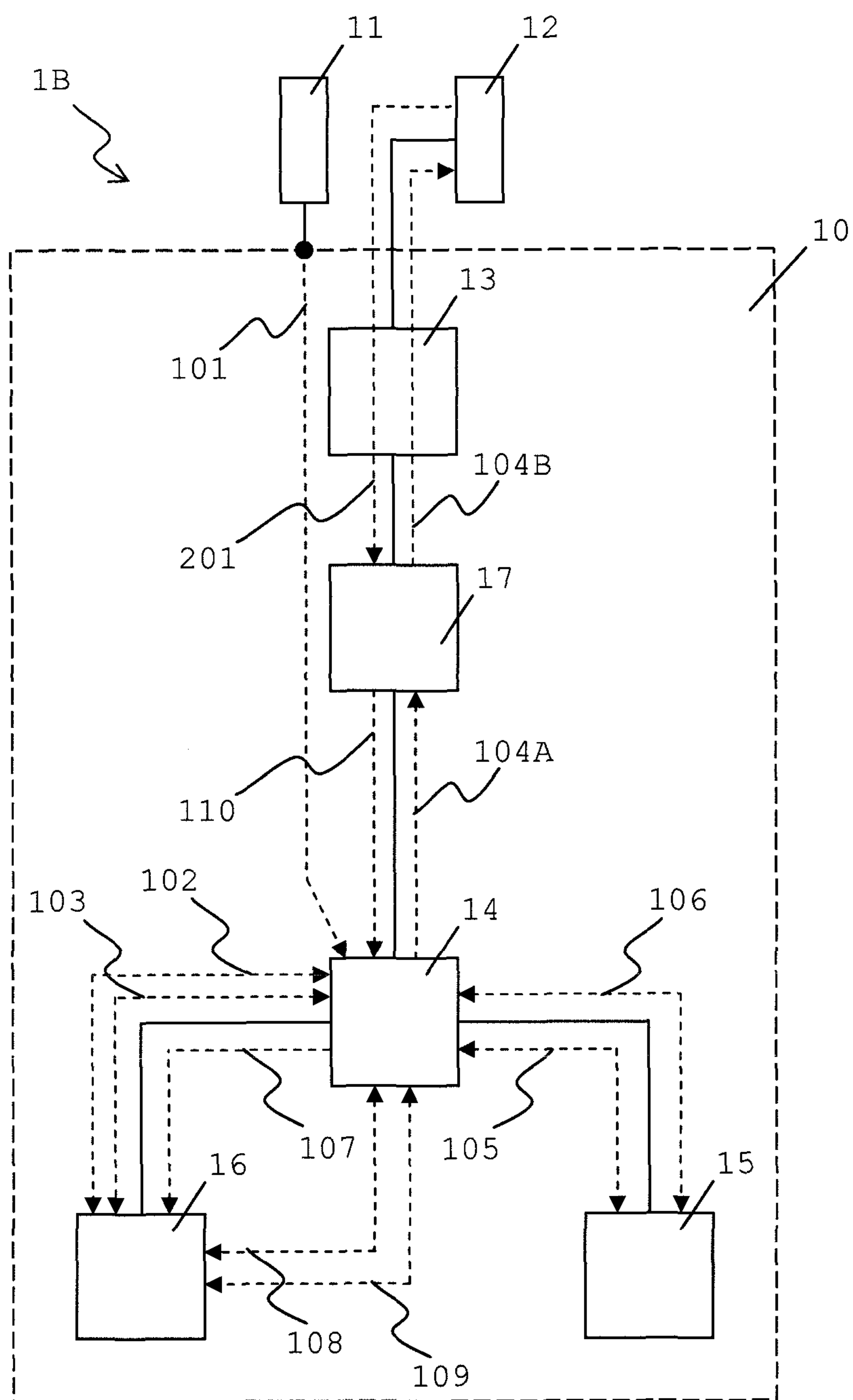
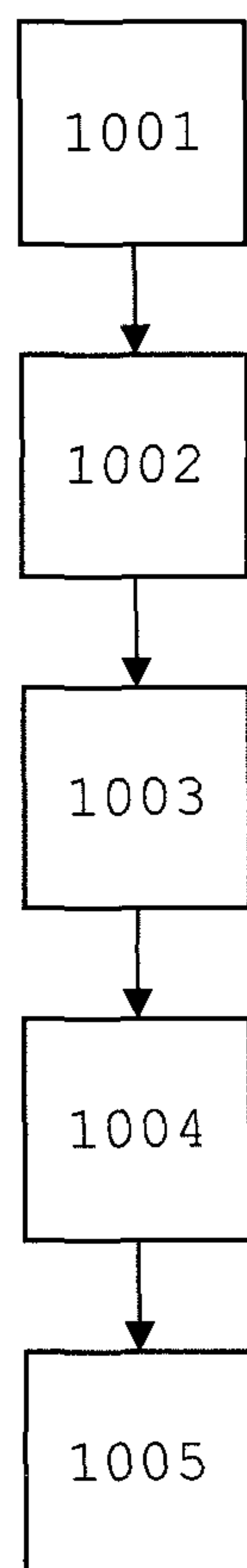
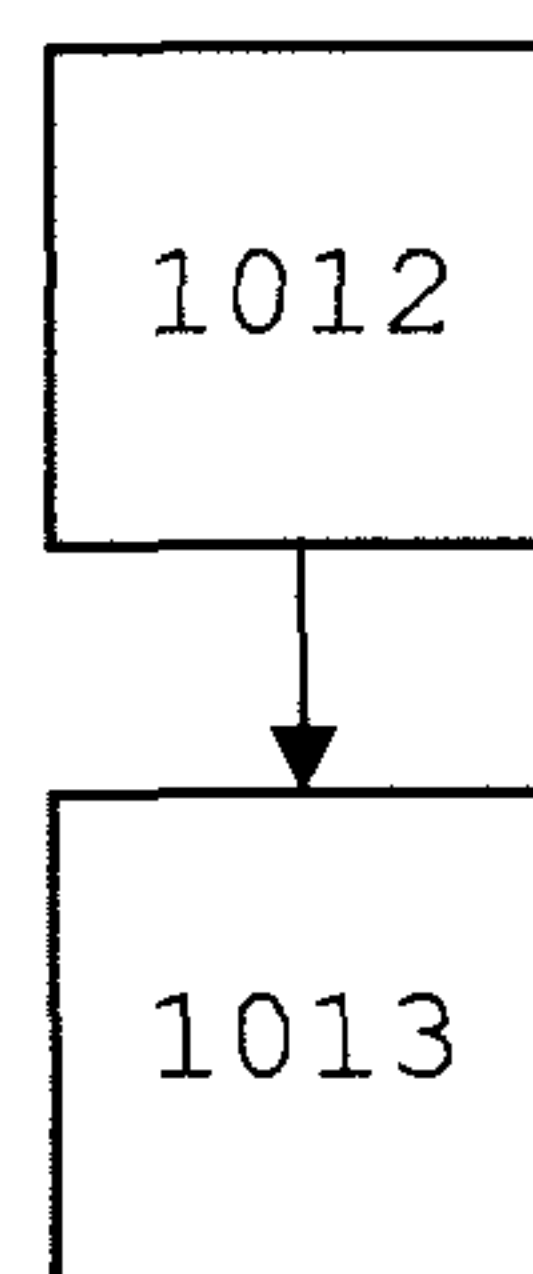
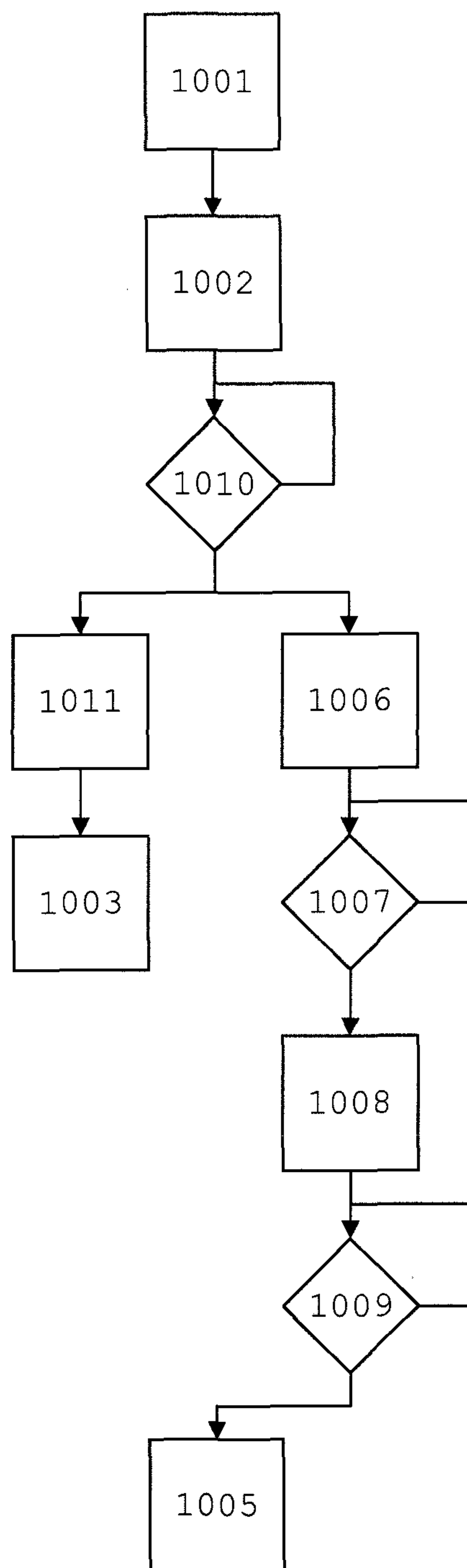


Fig. 5

4/6

**Fig. 6****Fig. 7**

5/6

**Fig. 8**

6/6

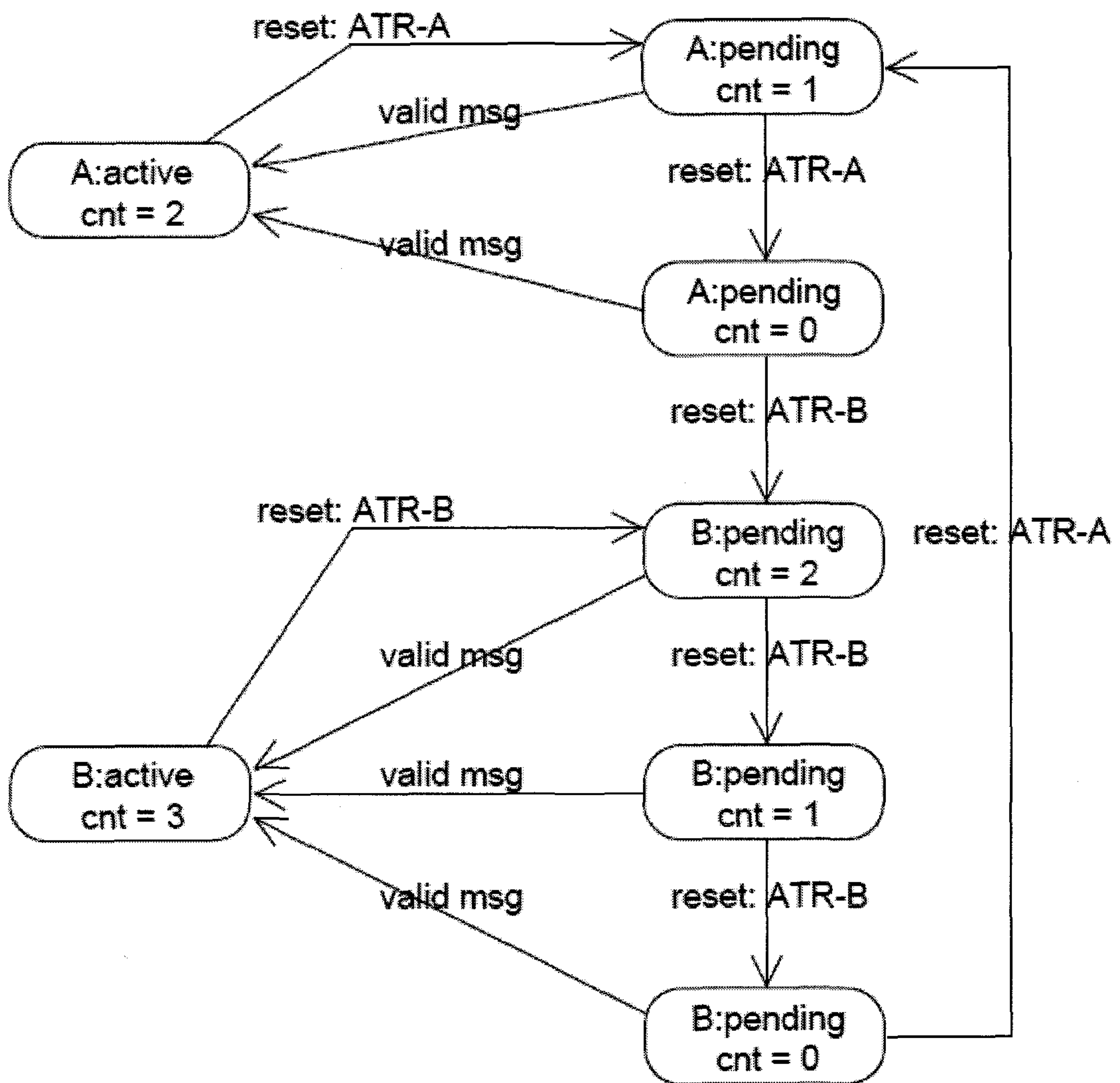


Fig. 9

