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

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2460211 A1 2003/03/20

(21) 2 460 211

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2002/09/10
(87) Date publication PCT/PCT Publication Date: 2003/03/20
(85) Entrée phase nationale/National Entry: 2004/03/10
(86) N° demande PCT/PCT Application No.: IB 2002/003739
(87) N° publication PCT/PCT Publication No.: 2003/024092
(30) Priorité/Priority: 2001/09/12 (1682/01) CH

(51) Cl.Int.$^{7}$/Int.Cl.$^{7}$ H04N 5/00, H04N 7/24

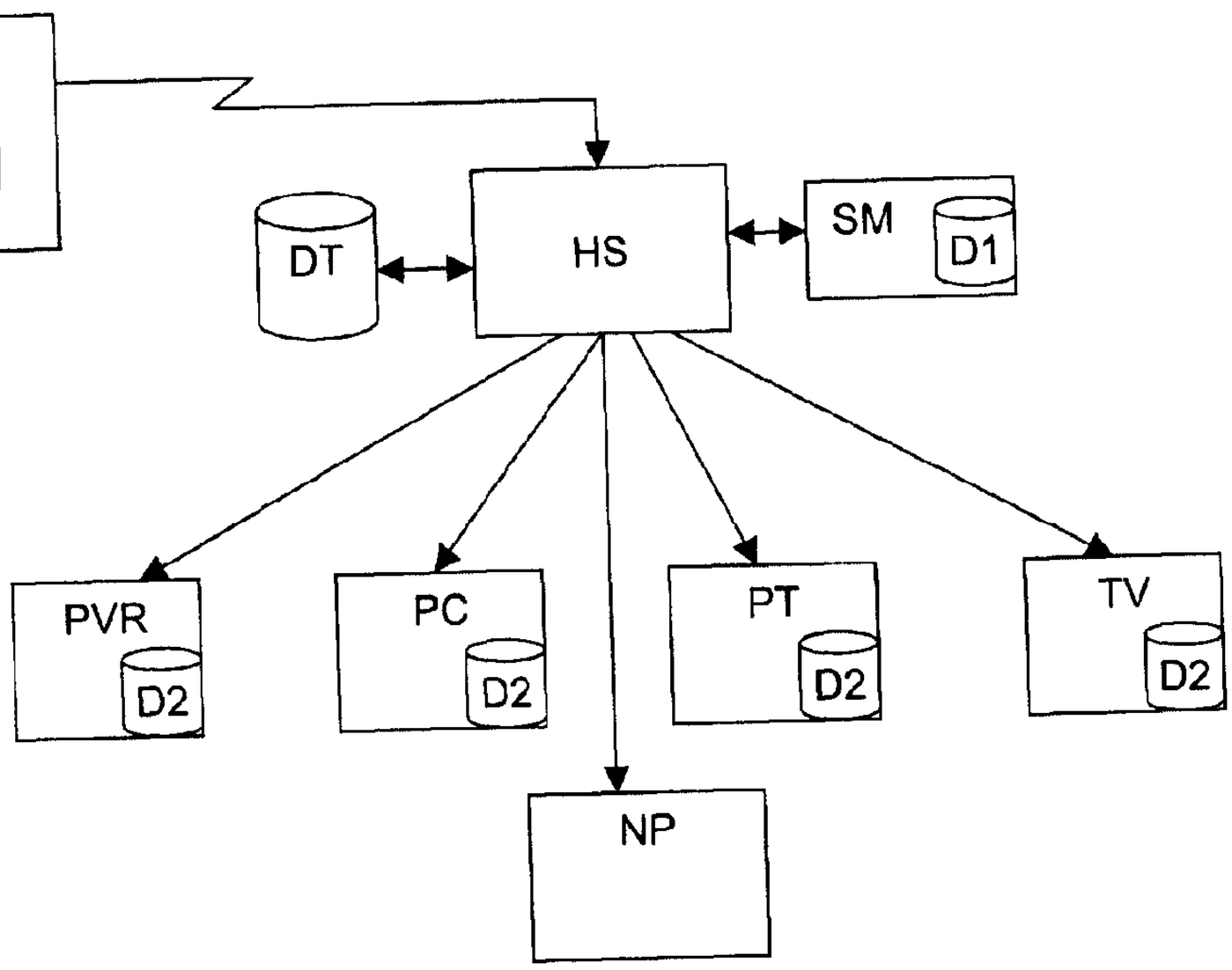
(71) Demandeur/Applicant:
NAGRAVISION SA, CH

(72) Inventeur/Inventor:
ROBERT, ARNAUD, CH

(74) Agent: GOWLING LAFLEUR HENDERSON LLP

(54) Titre : METHODE DE DIFFUSION DE DONNEES ENTRE UN SERVEUR LOCAL ET DES PERIPHERIQUES LOCAUX

(54) Title: METHOD FOR DATA BROADCAST BETWEEN A LOCAL SERVER AND LOCAL PERIPHERALS




(57) Abrégé/Abstract:
The invention aims at providing domestic broadcasting of conditional access encrypted data without limitation concerning the type of terminal used while guaranteeing that said broadcast will not exceed said limit. This is achieved by a method for encrypted data broadcasting between a local server connected to one or more local peripherals, said local server comprising security means responsible for acquiring a first right of use of said data, characterized in that it consists in: transmitting the encrypted data from the local server to a peripheral; extracting from the first right a second right corresponding to the part required for decrypting the data in the peripherals; encrypting by the security module the second right with a matching key particular to the couple formed by the local server security module and the peripheral security module; transmitting said encrypted second right to the local peripheral; decrypting with the matching key the second right with the peripheral security means; decrypting by the peripheral the data encrypted with the second right.

# ABSTRACT

The objective of the present invention is to allow the domestic transmission of encrypted data with conditional access without limitation of the type of terminal used, at the same time guaranteeing that this transmission will not be able to go beyond this limit.

This objective is achieved by a transmission method of encrypted data between a local server connected to one or several local peripherals, said local server comprising security means in charge of acquiring a first right of use of these data, characterised in that it consists in:

- transmitting the encrypted data from the local server towards a peripheral,
- extracting from the first right a second right corresponding to the part necessary for the decryption of the data in the peripherals,
- encrypting by the security module the second right by means of a pairing key specific to the couple formed by the security module of the local server and the security module of the peripheral,
- transmitting this encrypted second right to the local peripheral,
- decrypting with the help of the pairing key the second right by the security means of the peripheral,
- decrypting by the peripheral the data encrypted by the second right.

# METHOD FOR DATA BROADCAST BETWEEN A LOCAL SERVER AND LOCAL PERIPHERALS

The present invention belongs to the field of information distribution in electronic form, particularly in the case where this information is sent with conditions of use.

The information can be of several types, such as the audio/video, musical, programme, or game type.

This information is transmitted in encrypted form in order to control the transmission. It can also be downloaded from the Internet or be available on a portable support such as CD-ROM or DVD.

The problem that the present invention examines concerns the transmission of a decryption key or keys of this information.

According to a known way, particularly in the field of transmission of video contents, the key or keys are encrypted by a secret key contained in a security unit reputed inviolable. Thus, the information is received by the multimedia unit that wants to use it, to which is connected the security unit. The multimedia unit transfers to the security unit the message containing the key related to the information. The latter verifies that the owner of the security unit has the rights for decrypting the information.

If this is the case, this security unit decrypts the key and returns it to the multimedia unit so that the latter decrypts the information.

This method satisfies a use of the information or data in the multimedia unit such as in a pay television receiver. Once in plaintext, the data are viewed by the television.

This method is not adapted to the use of these same data by domestic peripherals. By domestic peripherals we understand all the peripherals connected to the multimedia unit in a restricted geographical limit such as a home. These peripherals can be a personal computer, a digital video recorder, a palmtop, or another MP3 recorder, a mobile phone or another mobile multimedia reading system.

In this configuration, the multimedia unit works as a local server for the different peripherals, and the problem arises when we have to transfer the encrypted or decrypted data from this unit to one of the peripherals.

According to the example described above, this function is simply not allowed as it opens the path to a transmission to other users without the supplier of the data being able to control the access.

According to another layout adopted in the frame of the DRM (Digital Rights Management) concept, the transmission between peripherals is carried out in encrypted form and a programme is in charge of the decryption. The documents WO01/50225 and WO00/13412 describe such a process: to obtain the right to decrypt the data, the user must request the supplier for a licence, which licence is accompanied by a decryption key. With this licence, the user accesses a right of use according to the modalities defined in the licence, generally a right of access at wish for a private use on the different domestic peripherals.

Of these two approaches, one allows abusive transmissions of a content out of the domestic environment, and the other is too restrictive because it prevents any use outside of the central multimedia unit.

The objective of the present invention is to allow the domestic transmission of conditional access data without limitation of the type of terminal that is used, and at the same time guaranteeing that this transmission will not be able to go beyond the limit of the using or the belonging place of the peripherals.

This objective is achieved by a transmission method of encrypted data between a local server connected to one or several local peripherals, this local server comprising security means in charge of acquiring a first right of use of these data, characterised in that it consists in:

- transmitting the encrypted data from the local server to a peripheral,

- extracting from the first right a second right corresponding to the part necessary for the decryption of the data in the peripherals,

- encrypting by the security module the second right by means of a pairing key specific to the couple formed by the security module of the local server and the security module of the peripheral,

- transmitting this second right encrypted to the local peripheral,

- decrypting with the help of the pairing key the second right with the security means of the peripheral,

- decrypting by the peripheral of the encrypted data by the second right.

This method takes place in two steps. In a first step, the local server accesses the service of the supplier of the data to obtain the right of use of the data. There exist numerous solutions in this objective, for example, the purchase on the Internet by means of a credit card or the pay television. In return, the supplier sends a message in encrypted form containing the decryption key of the data. The right of decryption can also be supplied in the form of a decryption and viewing programme. This exchange is carried out advantageously by a protocol using an asymmetric key, allowing to ensure that we transmit the message only to this single user.

This message is transmitted to the security module (for example a smart card) in charge of decrypting this message and of extracting the key (or the decryption programme). This key will be used to decrypt the data for their use on the local server.

The concept of key can be replaced by the concept of operating software. In fact, the data are useless without the programme capable of starting them up. In the case where the data would represent a video, the operating software will be the viewing programme.

During the use of the data in a local peripheral, the encrypted data are transferred to this peripheral. According to the method of the invention, this peripheral also comprises a security module that may have several forms: it can consist of a smart card or a chip directly integrated inside the peripheral or of a software solution.

The control information such as the decryption key or the decryption programme are transmitted in encrypted form to the several peripherals connected to the local server. This encryption is carried out by a pairing key, that is, a key that is unique

and specific to the couple formed by the security module of the local server and the security module of the peripheral.

Thus, only the considered peripheral will be able to recognise the control information necessary for the operating of the data. This information is processed by the security module of the peripheral that allows the viewing of the video emission or of the game previously acquired from the supplier.

A characteristic of the invention is hence to allow the secured purchase of data and their operation without limit of the type of peripheral considered as long as they are included in the definition of “domestic”. The right acquired in a classical way is thus transferred to these peripherals, at the same time controlling their transmission thanks to the pairing. The pairing method is described in the document WO 99/57901 and consists in generating a unique encryption key between the security module of the local server and the security module of the peripheral during an initialisation phase. This key is memorised on both sides and is used for the transfers of data.

This pairing key could also be a session key, which is generated on request based on stored pairing key (symmetric), or key pair (asymmetric). These pairing keys are unique and constant for the set formed by the security module of the local server and the security module of the peripheral. When the communication between the local server and a peripheral is initiated, the pairing key (or keys) is used either to encrypt and decrypt the data flow or to generate a session key which is unique for the set connected together but not constant.

If one apparatus wants to communicate with the local server, it must necessarily pass through an initialisation phase, during which are carried out controls in terms of quantity and of type of apparatus.

The security means of the local server are in charge of administering the pairing with each peripheral. To avoid that all the neighbourhood of a user is considered as “domestic”, the number of paired peripherals will be limited. We can also imagine a limitation of the type of peripheral, for example authorising only one personal computer.

It may occur that one of the peripherals does not contain a security module and that the exchange of rights in encrypted form cannot be performed. This is the case for example of a portable terminal having a small sized screen. In this case, the local server is authorised to transmit in plain text the data in a degraded form. For example, a video transmission will see its resolution reduced, but enough to allow the portable terminal to view it with its screen in a low resolution mode. The interception of such a transmission by a third person does not represent a great danger of broadcasting because the content has not a high added value.

In the case of a musical or video content, this degradation can be carried out either qualitatively or quantitatively, for example by only transmitting a part of the content.

According to a mode of realisation of this embodiment, the right of use of these data is different than in the case where the data are transmitted in encrypted form. This right can be in the form of another decryption key (or another decryption software) that only authorises the partial decryption of the data, for example one frame of every two for a video signal.

In another case, the peripheral does not contain a security module such as defined above, but carries out the security operations (decryption, storage of the rights and keys) in a software way. This type of peripheral can be a mobile telephone for example and will be classified in a different category whose use of the transmitted data may know certain restrictions.

According to a particular embodiment of the invention, the supplier of the content associates a condition of transmission to the transmitted right. This condition determines in what measure this right can be transmitted to the peripherals.

According to one example of use of this condition, the following categories are foreseen:

A category: no transmission of the right is authorised,

B category: the transmission of the right is only authorised if the number of paired peripherals is less than a threshold b (5 for example),

C category: the transmission of the right is only authorised if the number of paired peripherals is less than a threshold c (10 for example)

D category: the transmission of the right is only authorised as long as there is only one peripheral per type of peripheral (thus we prevent for example the transmission to several MP3 readers or to several numerical video recorders)

E category: the transmission in plain text, even in degraded form, is not authorised,

F category: the transmission is only authorised to peripherals containing a security module (cryptographic processor).

This list of categories is not comprehensive and can also be combined. It is possible to integrate the notion of a maximum number of transmissions to the peripherals.

This allows the supplier to determine the policy he/she desires to follow regarding domestic transmission, even to practice different prices according to the chosen category.

The invention will be better understood with the help of the following detailed description which makes reference to the annexed figure, which is given as a non-limiting example, and that describes the structure in which the method of the invention is implemented:

In this Figure, a supplier of content FC offers the data DT. According to the example represented here, the transmission is carried out by Internet to a local server HS. The latter stores locally the data DT for their use.

The acquisition of the right of use D1 of the data DT can be done at the same time as the downloading of the data. It can also be done in a second step, even from another supplier. In fact, the supplier of the data DT can merely be an intermediary and it is necessary to address the holder of the rights for the acquisition of the right of use.

Once the purchase procedures are carried out, the right D1 is kept in the security module SM of the local server HS. This right contains the indications of the origin of the data, the conditions of use such as described above. In order to prevent any

movement from the security module SM towards another local server HS, a pairing mechanism between the security module SM and the local server HS is applied. The considered security module SM can now only communicate with one local server, the one that has been initialised with the module SM.

According to the illustrated example, the local server HS is connected with a digital video recorder DVR, a personal computer PC, a pocket computer (PALM-TOP), and a television TV. Each of these peripherals is paired with the local server HS and thus has a specific encryption key. The electronic notepad NP does not have such a module and the transmission of data DT is only carried out in plain text, but in a degraded quality mode.

During the use of the data in a peripheral, the local server HS, more precisely the security module SM, transmits the right D2 that represents the part necessary for the decryption of the data DT on the peripheral. This right is stored in the security means of the peripherals.

When the data DT and the right D2 are inside the peripheral, it is possible for the latter to use said data inside the limits depending on the content and the using rules. For example, a program paid once can be watched three times. The right received and recorded allows that a purchase of a program involves a maximal number of visualisations fixed at three. The operation of decryption of the data DT by the peripheral can be performed by the peripheral itself or by the security means of the peripheral, according to the chosen implementation.

According to an embodiment of the invention, the limits of use transmitted by the supplier FC to the local server HS, are reported to the peripheral.

When the case is a number of uses by the peripheral, this information contained in the right D2 is processed by the security module of the peripheral.

If the number of uses is defined, whichever the type of peripheral, the right D2 contains the right of one use, each new use having necessarily to be requested to the security module SM of the local server HS that is in charge of the global registration, that is, all the peripherals involved.

According to an embodiment of the invention, the pairing between the local server and the peripherals is performed by a unique key that is common to all the peripherals. The unique pairing key contained in the local server is transmitted during each initialisation with a new peripheral.

5

# CLAIMS

1. A transmission method of encrypted data (DT) between a local server (HS) connected to one or several local peripherals, comprising security means, said local server (HS) comprising security means (SM) in charge of acquiring a first right (D1) of use of these data (DT), characterised in that it consists in:

- transmitting the encrypted data (DT) of the local server (HS) towards a peripheral,

- extracting from the first right (D1) a second right (D2) corresponding to the part necessary for the decryption of the data (DT) in the peripherals,

- encrypting by the security module (SM) the second right (D2) by means of a pairing key specific to the couple formed by the security module of the local server and the security module of the peripheral,

- transmitting this encrypted second right (D2) to the local peripheral,

- decrypting with the help of the pairing key the second right (D2) with the security means of the peripheral,

- decrypting the encrypted data (DT) received by the peripheral by means of the second right (D2) with the intention of operating them.

2. A transmission method of encrypted data (DT) according to Claim 1, characterised in that the right (D1, D2) is an operating software of these data (DT).

3. A transmission method of encrypted data (DT) according to Claim 1, characterised in that the right (D1, D2) is a decryption key.

4. A transmission method of encrypted data (DT) according to Claims 1 to 3, characterised in that the first right (D1) comprises conditions of transmission towards the peripherals, and in that the security module of the local server restrains the transmission of the second right (D2) depending on these transmission conditions.

5. A transmission method of encrypted data (DT) according to Claim 4, characterised in that these conditions contain indications of the type of accepted peripherals.

6. A transmission method of encrypted data (DT) according to Claim 4, characterised in that these conditions contain indications of the level of security of the accepted peripherals.

7. A transmission method of encrypted data (DT) according to Claim 4, characterised in that these conditions contain indications of the maximum number of uses of the data (DT).

8. A transmission method of encrypted data (DT) between a local server (HS) connected to one or several local peripherals, said local server (HS) comprising security means (SM) in charge of acquiring a right (D1) of use of these data (DT), characterised in that it consists in:

- decrypting by the local server (HS) the data (DT) and degrading the quality,

- transmitting these degraded data in plain text from the local server (HS) towards a peripheral,

- operating these degraded data by the local peripheral.

9. A transmission method of encrypted data (DT) according to Claim 8, characterised in that the right (D1) is a decryption key allowing to decrypt only partially the data (DT).

10. A transmission method of encrypted data (DT) according to Claim 8, characterised in that the right (D1) is an operating programme of the data reducing the quality of output of said programme.

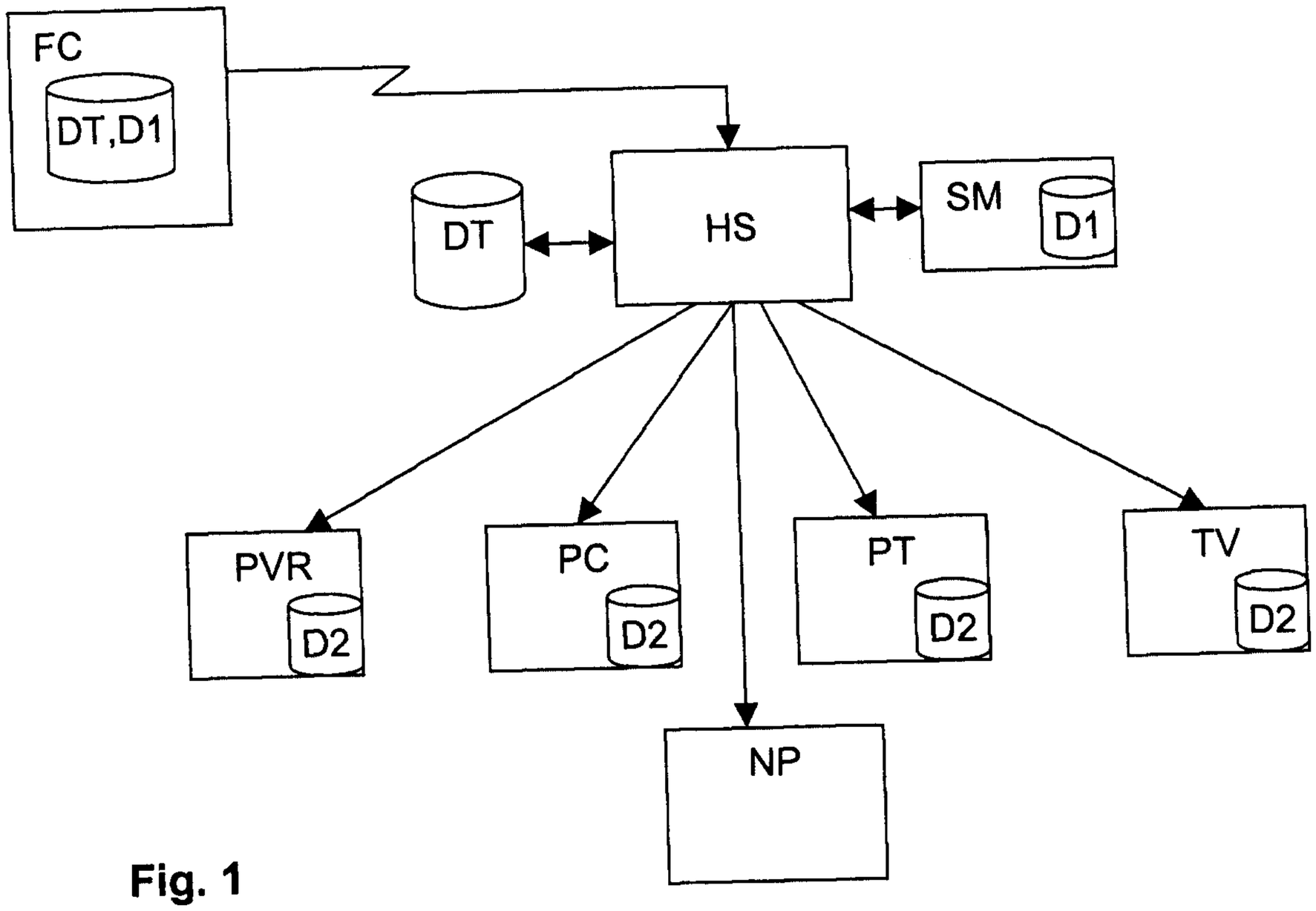
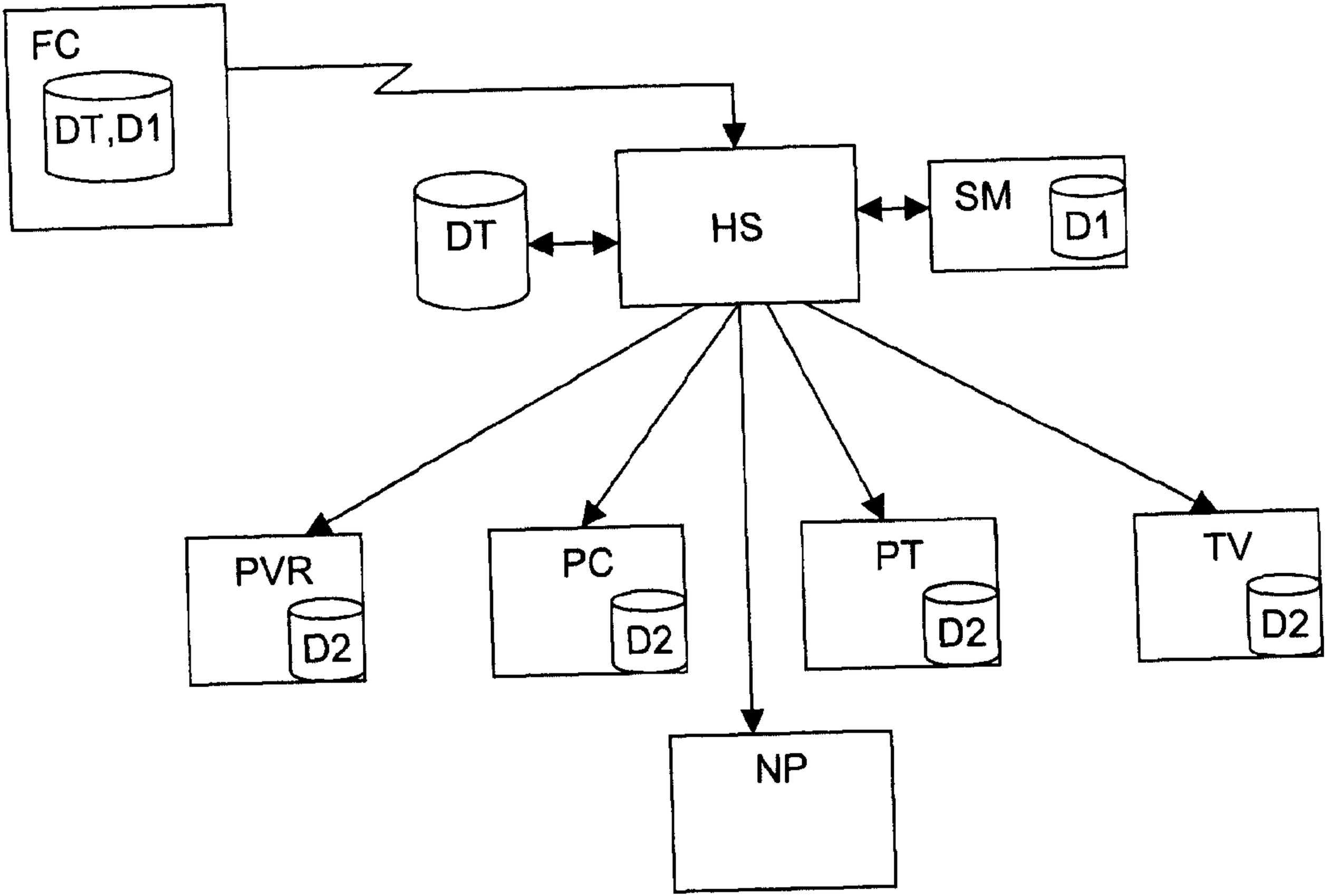



Fig. 1


FC
DT,D1
DT
HS
SM
D1
PVR
D2
PC
D2
PT
D2
TV
D2
NP