PCT

(51) International Patent Classification 6 :		(11) International Publication Number: WO 96/36026
G07F 7/10, 19/00	A1	(43) International Publication Date: 14 November 1996 (14.11.96)

(54) Title: METHOD FOR EFFECTING AN ELECTRONIC PAYMENT TRANSACTION

(57) Abstract

The invention relates to a method for protected payment with electronic payment means, such as "intelligent" payment cards ("smart cards"), in a variable number of steps. In this connection, use is made of a non-reversible function (F), of which successive function values (β_i) are provided by the payment means (1, I) to the payment station (II) in question by way of proof of payment. On the basis of these function values (β_i), there may take place both a verification and a determination of the number of steps. Such method finds application, e.g., in public telephones and in copiers. The invention further relates to a payment means and a payment system for applying the method.

METHOD FOR EFFECTING AN ELECTRONIC PAYMENT TRANSACTION

Method for effecting an electronic payment transaction having a
variable number of payment units, as well as payment means and system
for applying the method.

BACKGROUND OF THE INVENTION

5

10

15

20

25

30

The invention relates to a method for effecting, with an
electronic payment means, a variable number of payments in one payment
transaction. More in particular, the invention relates to a method for
effecting a payment transaction with an electronic payment means and a
payment station, comprising the issuing by the payment means to the
payment station of at least a first payment value, payment values
being representative for one or more payment units to be settled. Such
a method is known, e.g. from European Patent Application EP-A-
0,637,004. There are many types of payment transactions in which a
variable number of payment units must be transferred. Thus, in a
telephone booth, for a single conversation in most cases several
units, corresponding with metering pulses (so-called "ticks"), should
be debited against a payment card. These units are credited to the
telephone set of the telephone booth. In the event of copiers, for a
copying order a certain amount per page should be paid, with such
amount being capable of being debited against a payment card. Within a
single transaction (telephone conversation or copying order),
therefore, a debiting of the payment means (i.e., the payment card)
and a crediting of a payment station (telephone set or copier) must
repeatedly take place.

In the event of modern, protected payment means, such as so-
called "smart cards" or "chip cards", a protocol is applied to each
debiting of the payment means (debit), in which the authenticity of
the payment means and of the electronic money used is verified. An
example of a verification schema using blind signatures is disclosed
in European Patent Application EP-A-0,518,365. Another scheme to
verify electronic money is disclosed in European Patent Application
EP-A-0,507,669, where payment units are provided with random "sequence
numbers". Verification of the electronic money is effected by checking
received sequence numbers against a list of issued sequence numbers.
However, this type of verification still allows the electronic money
to be duplicated and to possibly be spent more than once.

A verification, however, for each payment unit (metering pulse

2

or copying price per page) requires a certain processing time. In the
event of, e.g., international telephone conversations, where the
metering pulses (or ticks) follow each other rapidly, the processing
of the payment units may give rise to problems and obstruct the
5   execution of a protected payment.

In order to solve this problem, prior to the actual transaction
several payment units might already be transferred from the payment
means to the payment station. This has the drawback that restitution
should take place in the event that not all payment units are used up.
10   Payment afterwards, i.e., the transfer of payment values from the
payment means to the payment station following the transaction, has
the drawback that the payment may be sabotaged by removing the payment
means (i.e. the smart card) prematurely.

15   SUMMARY OF THE INVENTION

The object of the invention is to eliminate the above and other
drawbacks of the prior art, and to provide a method which enables the
effecting of a protected payment in a simple and rapid manner with a
variable number of payment units, i.e. a number of payment units to be
20   determined during the transaction.

Another object of the invention is to provide a method which
allows a secure payment involving a minimal amount of processing time.

For this purpose, a method of the type referred to in the
preamble is characterised in that the payment values are mutually
25   related by a one-way function, in such a manner that the first payment
value may be obtained from a further payment value by repeatedly
applying the function. By applying a one-way function, i.e., a
function of which the inverse cannot viably be determined, a very
suitable check on the progress of the payment transaction may be
30   obtained without the need to repeatedly execute a complicated and
therefore time-consuming verification process.

After receiving a payment value, the payment station preferably
checks, by applying the function, whether the payment value received
is correct. This is possible since repeated application of the
35   function produces the first payment value.

After receiving a payment value the payment station, by applying
the function repeatedly, may additionally determine how many payment
units the payment value received represents. Per payment transaction

3

one or more payment values may be transferred, a (last) payment value possibly representing several (previous) payment values. The number of times the function must be applied to obtain the preceding or first payment value, is directly related to the number of payment values generated, but does not have to be equal to the number of issued and thus transferred payment values.

Together with at least the first payment value, authentication data is advantageously transferred from the payment means to the payment station. This authentication data, such as the identification code of the payment means and/or the user, may be contained in the first payment value or precede it.

In a further embodiment of the method according to the invention, the payment station, after receiving a payment value, transfers a debit value to the payment means. The debit values may be used, directly after having been received by the payment means, for debiting a balance, e.g., by lowering a counter reading present in the payment means. It is also possible, however, that after having been received by the payment means the debit values are collected and, at the end of the payment transaction, are used for debiting a balance. In the latter case, the method may progress more rapidly.

In yet a further embodiment of the method according to the invention, together with the debit value a count value is transferred from the payment station to the payment means, which count value represents the number of payment units to be debited. The count value may be one, but may also be greater than one, so that several payment units are debited simultaneously. The count value may furthermore have been determined in advance, or be variable. Preferably, the count value is related to the number of times the one-way function is applied, e.g., to obtain the preceding or the first payment value.

In a yet another embodiment of the method in accordance with the invention the issued payment values are used as proof in a settlement process to be carried out later. In this case, with the issued payment value(s) a payment is laid down while the settlement of payment can take place at another time. Such a settlement can for example result in a summary invoice.

The method according to the invention enables to adjust as needed, during the transaction, the number of payment values and thus the number of payment units to be settled.

4

EXEMPLARY EMBODIMENTS

The invention will be explained in greater detail below with
reference to the Figures.

Fig. 1   shows a smart card as may be used in the method of
5   the present invention.

Fig. 2   schematically shows the integrated circuit of the
             smart card of Fig. 1.

Fig. 3   schematically shows a preferred embodiment of the
             method according to the invention.

10   Fig. 4   schematically shows successive function values of a
             one-way function.

The smart card or IC card 1 shown by way of example in Fig. 1
comprises a substrate 2, in which an integrated circuit is embedded.
The integrated circuit is provided with contacts 3 for contacting a
15   card reader or the like. It should be noted that the present invention
can also be applied in the case of so-called contactless smart cards.

The integrated circuit 10 shown schematically and by way of
example in Fig. 2 comprises a processor 11, a memory 12 and an
input/output circuit 13. The memory may comprise a volatile (RAM)
20   memory part for temporarily storing data and a non-volatile (ROM)
memory part for permanently or semi-permanently storing data. The
latter part is preferably an EEPROM type memory. The data stored in
the non-volatile part may contain both programming data (instructions,
programs) and payment data, i.e. data relating to monetary
25   transactions. It will be understood that a separate memory (not shown)
may be provided to store the instruction set of the processor 11. The
input-output circuit 13 may communicate with external devices via
contacts (not shown in Fig. 2), such as the contacts 3 shown in Fig.
1. The integrated circuit 10 may be contained in the card 1 of Fig. 1.

30   In Fig. 3, there is schematically shown, by way of example, an
embodiment of the method according to the invention. A payment means
(paying party) is referred to by I, and a payment station or terminal
(receiving party) is referred to by II. Between the payment means I
and the payment station II, during a payment transaction an exchange
35   of data takes place. It will be understood that the payment means
(card) I may correspond with the smart card 1 shown in Fig. 1.

At the time t_0, there may take place an exchange of

5

initialisation values I (or Init). This exchange, which inter alia may
relate to the identity of the payment station and/or the payment
means, the type of transaction and the like, is not essential to the
present invention.

5   At the time t_1, the payment means (card) I sends an
authentication value A and a first payment value β_M to the payment
station (terminal) II. The payment value β_M may, like the debit value
R, be contained in the authentication value A or may be determined by
the authentication value A, e.g. when A is constituted by a digital

10   signature on β_M, R and other transaction data. The payment value β_M
need therefore not constitute a separate value.

       After authentication, the payment station provides access to the
desired service or the desired product and saves the authentication
value A and the payment value β_M as proof of payment, e.g. vis-à-vis a

15   banking institution. Alternatively, β_M or one or more possible
subsequent values β_{M-1}, β_{M-2}, ..., may serve as proof to later collect
money from a consumer (compare so-called credit cards). In his context
it should be noted that the settlement of the transaction is, in
principle, independent of the transaction proper and may be carried

20   out at another time and another place.

       At the time t_2, the payment station II sends a debit value R to
the payment means, possibly accompanied by a count value N. The count
value N may have a previously determined fixed value, e.g., one. In
this case, the transfer of the count value N may be dispensed with, or

25   may be effected only once (time t_2).

       On the basis of the debit value R, one or more payment units are
debited against a balance on the card, e.g., by lowering a counter
reading (see also e.g. EP-A-0,637,004). This number of payment units
to be debited may be predetermined, or may be referred to by the count

30   value N. Also the debit value R may be predetermined, because of which
R is redundant and may be dispensed with. Instead of R_1, or R and N, a
generic debit signal may be transferred. The debiting may take place
directly or shortly after the time t_2, or may be postponed till the end
of the transaction. In the latter case, the payment means will be

35   constructed in such a manner that this debiting takes place even if
the transaction is prematurely interrupted.

       As a reaction to the receipt of the debit value R, or as a

6

reaction to the receipt of an interim request (not shown in Fig. 3)
from the payment station, at the time t_3 the payment means I sends a
further payment value, β_{M-1}, to the payment station II. In the payment
station II, A and β_{M-1} are now saved as proof of payment. In addition,

5     $F(\beta_{M-1})$ is calculated; in other words, β_{M-1} is subjected to the function
F. If the result of this operation indeed produces β_M, not only has a
check on the authenticity of β_{M-1} been effected, but the number of
payment values is also determined: the total number of payment values
is equal to the number of operations required to obtain β_M plus one. It

10   follows that in the event of receiving a payment value β_{M-x} the value
of x may be determined by applying the function F x times. Thus, the
count value N may be adjusted on the basis of the value of x found.
This will be explained later with reference to Fig. 4.

      At the time t_4, a further debit value R is transferred from the

15   payment station II to the payment means I, possibly together with a
count value N. The payment means carries out similar operations as at
the time t_2.

      After the time t_4, further similar steps may be carried out, or
the transaction may be terminated. The transaction will be terminated

20   anyway after the last payment value β_0 has been transferred. Possibly,
an acknowledgement of the termination of the transaction may be
transferred from the payment station II to the payment means I. This
is not further indicated in Fig. 3.

      As is explained above, the number of payment units to be debited

25   is variable and may depend on the duration of the transaction, inter
alia.

      In summary, the method according to the invention, at any rate
if use is made of debit values, comprises the following steps:

1.   The payment means sends a value β to the payment station.

30   2.   The payment station sends a debit value to the payment means.

3.   The payment means sends a value of (β') derived from β,
      determined with the help of the one-way function, to the payment
      station.

4.   The payment station checks whether the received value β' is

35   indeed a value derived from β.

5.   If the transaction has not been terminated, β is replaced by its
      derived value β', and the process continues at step 2.
The derived value referred to here is always the value β' for which:

7

$F(\beta') = \beta$, i.e. the value "preceding" β.

It should be noted that the method described above may also be
terminated after step 2, that is in case only one payment unit, such
as a telephone tick (metering pulse), is to be transferred.

5   The payment values β referred to above may each represent one
payment unit, such as a telephone tick, currency unit or calculation
unit. It is also possible, however, that each payment value represents
several payment units, or that different payment values represent
different numbers of payment units. This may be recorded in the
10   authentication value A. The first payment value may e.g. represent a
base rate of several (e.g., two or three) payment units, while further
payment values always represent one payment unit. In this manner, a
differentiation may be made between, e.g., the set-up costs and the
duration costs of a telephone connection. The payment values consist
15   of numbers which are transferred in the form of electrical, optical or
acoustical signals.

The so-called one-way function F per se is simple to calculate,
but the inverse (F^{-1}) cannot viably be determined. This is understood
to mean that in practice it is extremely unlikely that a value β_{M-1} may
20   be determined from a value β_M. Such a one-way function, known per se
from cryptography, may be constructed, e.g., by involution modulo a
certain number, in which that specific number may be a so-called "Blum
integer", i.e. a product of two large prime numbers in a special form.
A so-called "hash" function may also be applied.

25   In Fig. 4, the application of the one-way function is further
illustrated with reference to an example. In this example, M is equal
to 5 (see also Fig. 3), so that the first payment value is β_5. In
practice, M will have a much greater value, e.g., 255.

A value β_i (i=0...5) may simply be calculated from the value β_{i-1}
30   by applying the one-way function F: $F(\beta_{i-1})=\beta_i$. Conversely, it is very
difficult to determine the inverse of F, so that in practice it is not
viable to determine the value β_{i-1} from β_i. In the method according to
the invention, this provides a form of guarantee: the payment station
is able to check whether the value β_i is correct and what is the
35   (relative) value thereof by applying the function F several times.
Conversely, the payment station itself is not able to calculate the
next payment value, which represents a greater number of payment
units.

8

   As may be seen from Fig. 4, the value β_5 may be obtained from β_2
by applying the function F three times. If the payment station first
receives β_5 and then β_2, it may therefore be determined that β_2 is the
fourth payment value (relative to β_5) and, e.g., represents four

5 payment units (i.e. the units associated with β_5 plus β_4 plus β_3 plus
β_2). In response thereto, e.g., a count value N=4 may be transferred to
the payment means in order to debit four payment units at once. If no
value β_5 results after the function F has been applied at most M (in
this case 5) times to β_2, it may be concluded that the most recently

10 received value (i.c. β_2) is invalid, as the values β_5 and β_2 are
apparently not related by F.

   The possession of a valid β_2 therefore demonstrates that the
receiver (the payment station) is entitled to payment units
corresponding to four payment values: β_2 through β_5. These may be four

15 payment units but, e.g., also four times C payment units, where C is a
conversion factor.

   As explained above, the use of a one-way function provides a
simple and rapid method for effecting payments with a variable number
of payment units. This may not only be advantageous in the case of

20 telephony, but for example also in the case of vending machines, taxi-
meters, and other devices where the amount to be settled can be
dependent on the time duration.

   The payment values issued need not be settled, for example by
means of debit values, during or immediately afterwards a transaction

25 with a payment means, but may be used as proof in a settlement process
to be carried out at a later time. In this case a payment is laid down
with the issued payment means, while the settlement of the payment can
take place at a later time (incontestable charging). Such a settlement
may for example result in a summary invoice with several transactions

30 being settled in one settlement process. Using payment values as proof
for settlements afterwards, can for example be used with mobile
telephone and video distribution services (video-on-demand).

   The invention may be applied with or without so-called
electronic "cheques" comprising an electronic "signature" (e.g., a

35 cryptographic operation with a specific key on certain data) of the
bank and/or the user.

   It will be understood by those skilled in the art that the
invention is not limited to the embodiments shown, and that many

9

modifications and amendments are possible without departing from the scope of the invention.

10

CLAIMS

1.   Method for effecting a payment transaction with an electronic
payment means (1, I) and a payment station (II), comprising the
issuing by the payment means to the payment station of at least a

5   first payment value (β_M), payment values being representative for one
or more payment units to be settled, <u>characterised in that</u> each
subsequent payment value $(\beta_{M-1}, \beta_{M-2}, \ldots)$ is related to the first
payment value (β_M) by a one-way function (F) in such a manner that the
first payment value (β_M) may be obtained from a further payment value

10   (β_{M-x}) by repeatedly applying the function (F).

2.   Method according to claim 1, wherein the payment station (II),
after receipt of a payment value (β_i), checks by applying the function
(F) whether the payment value received is correct.

3.   Method according to claim 1 or 2, wherein the payment station

15   (II), after receipt of a payment value (β_i), determines by applying the
function (F) how many payment units the payment value received
represents.

4.   Method according to any of the preceding claims, wherein
authentication data (A) is transferred together with at least the

20   first payment value (β_M) from the payment means (I) to the payment
station (II).

5.   Method according to any of the preceding claims, wherein the
payment station (II), after receipt of a payment value (β_i), transfers
a debit value (R) to the payment means.

25   6.   Method according to claim 5, wherein debit values (R) are used,
directly after receipt by the payment means (I), for debiting a
balance.

7.   Method according to claim 5, wherein debit values (R), after
receipt by the payment means (I), are collected and, at the end of the

30   payment transaction, are used for debiting a balance.

8.   Method according to any of the claims 5 up to and including 7,
wherein a count value (N) is transferred, together with the debit
value (R), from the payment station (II) to the payment means (I),
which count value (N) represents the number of payment units to be

35   debited.

9.   Method according to claim 8, wherein the count value (N) is
related to the number of times the one-way function (F) has been
applied.

11

10.   Method according to claim 8, wherein the count value (N) amounts to one.

11.   Method according to any of the claims 1 up to and including 4, wherein the payment values (β_i) issued are used as proof in a settlement process to be carried out later.

12.   Financial transaction, effected by means of the method according to any of the preceding claims.

13.   Payment means (1, I) provided with an integrated circuit (10), such as a so-called smart card, designed for applying the method according to any of the claims 1 up to and including 11.

14.   System for electronic payments, comprising a payment station (II) and a settlement station, designed for applying the method according to one of the claims 1 up to and including 11.
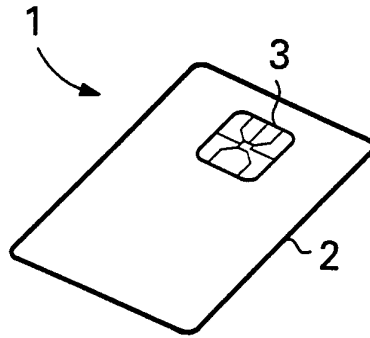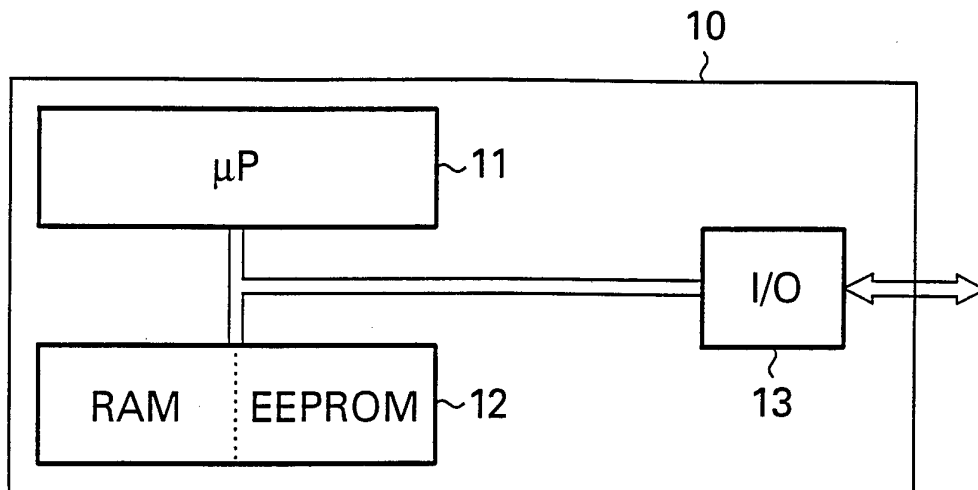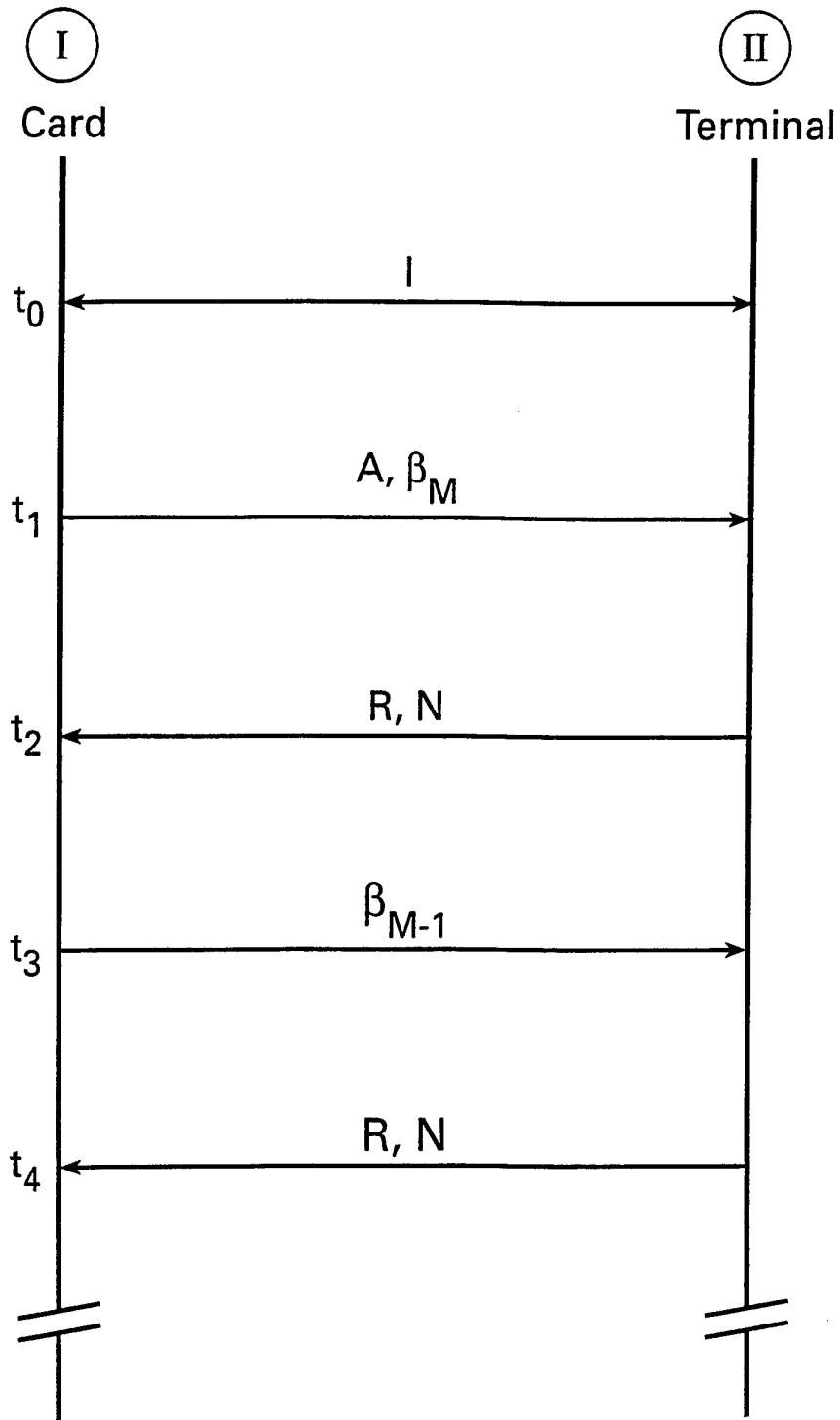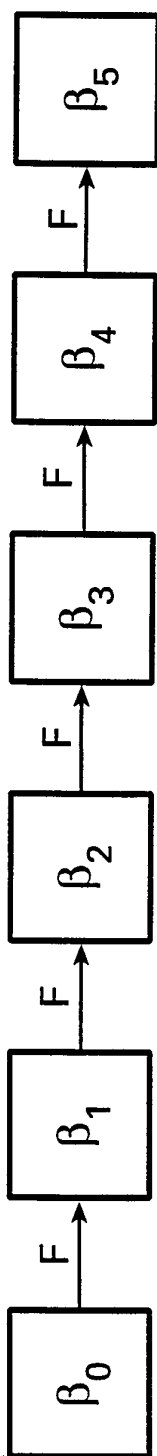
Fig. 1

Fig. 2

2/3

Fig. 3

Fig. 4

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6   G07F7/10   G07F19/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6   G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP,A,0 507 669 (FRANCE TELECOM) 7 October 1992 cited in the application see abstract; claims; figures	1,12-14
A	EP,A,0 265 728 (WILHELM RUF) 4 May 1988 see abstract; claims; figures 1,2	1-4,9
A	EP,A,0 496 656 (FRANCE TELECOM) 29 July 1992	
A	EP,A,0 459 781 (NANOTEQ) 4 December 1991	

☐ Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 September 1996	20.09.96

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	David, J

Form PCT/ISA/210 (second sheet) (July 1992)

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP-A-0507669	07-10-92	FR-A-	2674976	09-10-92
		DE-D-	69211407	18-07-96
		JP-A-	6325055	25-11-94
		US-A-	5305383	19-04-94
EP-A-0265728	04-05-88	DE-C-	3636822	23-12-93
		US-A-	4847614	11-07-89
EP-A-0496656	29-07-92	FR-A-	2671889	24-07-92
		DE-D-	69204696	19-10-95
		DE-T-	69204696	02-05-96
		JP-A-	6203226	22-07-94
		US-A-	5247578	21-09-93
EP-A-0459781	04-12-91	AT-T-	136975	15-05-96
		DE-D-	69118748	23-05-96
		ES-T-	2085425	01-06-96
		US-A-	5517187	14-05-96