(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 September 2001 (07.09.2001)

PCT

(10) International Publication Number
WO 01/65397 A1

(51) International Patent Classification[7]: G06F 17/00

(21) International Application Number: PCT/US00/05248

(22) International Filing Date: 1 March 2000 (01.03.2000)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **PEKAREK-KOSTKA, Peter** [AT/US]; 2114 Town Place, Middletown, CT 06457 (US).

(74) Agents: **RISTAS, L., James** et al.; Alix, Yale & Ristas, LLP, 750 Main Street, Hartford, CT 06103 (US).

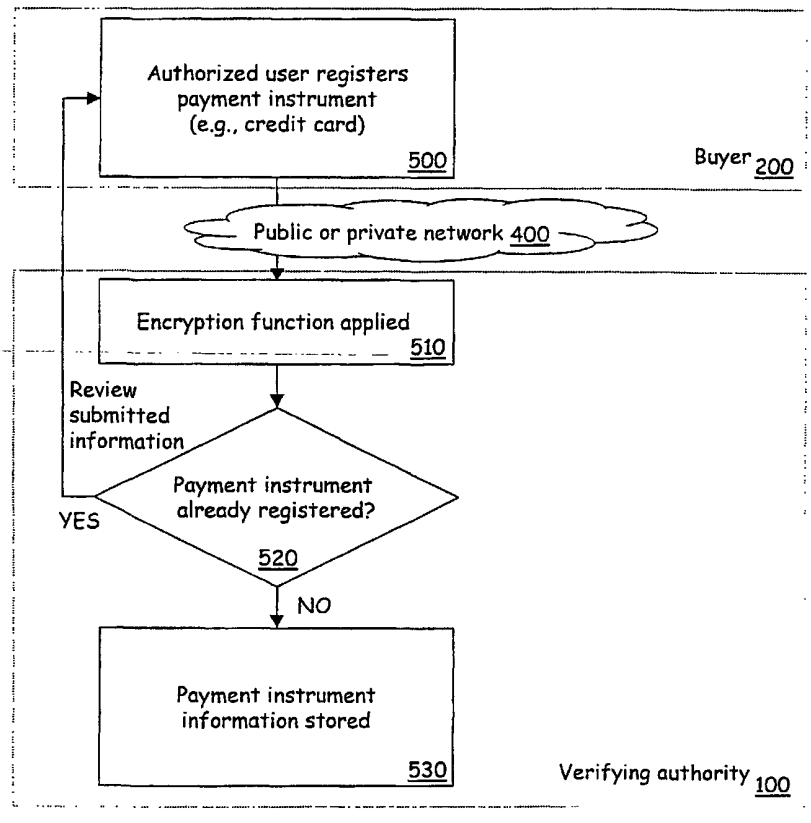
(81) Designated States *(national)*: CA, IL, JP, US.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR PLACING A PURCHASE ORDER BY USING A CREDIT CARD



(57) Abstract: Credit card holders register their credit/debit cards by providing essential information required for a complete purchase order (530), including, but not limited to card number, expiration date, shipping address, preferred shipping method, telephone contact information (see Fig. 2). The verifying authority does not store the credit card number, but only a fingerprint thereof obtained by performing a one-way encryption function (510). The user transmits his credit card number to the merchant at the time of purchase, the merchant submits the credit card information to the card verifying authority and obtains further information required to complete the purchase order (e.g., shipping address) from the card verifying authority. A key feature of the invention is the unique association of encrypted information with unencrypted information pertaining to the proper user of a valid credit card or similar financial instrument. The encrypted information is utilized as much as possible where otherwise sensitive information would be stored or transmitted.

WO 01/65397 A1

METHOD AND SYSTEM FOR PLACING A PURCHASE ORDER BY USING A CREDIT CARD

Background of the Invention

The present invention relates to improving security of placing purchase orders over a publicly accessible communications network, especially the Internet.

The Internet is a network designed to be open and accessible by everyone and has developed as a seemingly ideal medium for all kinds of financial transactions. Ubiquitous access makes it very attractive for consumer-to-business and business-to-business, both domestic and international, transactions. There are many benefits to shopping online, from access to products that might not otherwise be available in the local area to search engines that will find the lowest price for specific items. But the very same accessibility opens up opportunities for unauthorized card uses on the Internet.

Credit card fraud can generally be classified into two categories. The first one has to do with someone obtaining valid credit card details and using them to purchase goods or services without being authorized by the rightful cardholder. The second category includes fraudulent activity by the rightful cardholder, who first obtains goods or services using his card only to later dispute the charge. Both fraud categories add a significant burden on the online merchant, because all Internet transactions are performed without the merchant having physical access to the customer's card. If the merchant cannot prove that he was properly authorized to charge the card by presenting a card imprint (or magnetic stripe information obtained by physically swiping the card) and a signature, he is most likely in a position where he has to accept a "charge-back", i.e. the bank debiting the merchant's account for the amount in question plus an additional charge-back fee. The merchant not only forgoes the sale, but he may also be left with no merchandise, if he shipped the order already.

When an unauthorized transaction takes place, someone must have obtained at a minimum a valid credit card number and an expiration date.

There are several ways of obtaining these pieces of information: Capture the card number while it is being sent over the Internet, obtain the number from a merchant site, and generate or "guess" a valid credit card number.

Many consumers believe it is extremely dangerous to enter your credit card number on your computer and to send it off over the Internet, passing several different servers around the world. While this is true for so-called un-secure Internet transactions, most of today's e-commerce sites operate in a secure SSL (Secure Sockets Layer) environment. Major browsers have these security features built in. When the browser is sending encrypted information to a server that supports encryption, a closed padlock or key icon appears at the bottom of the browser window. Browsers usually provide two different levels of encryption: standard 56-bit encryption (already hard to crack) and 128-bit encryption, which is even stronger. The 56-bit version was available to everyone around the world; the 128-bit version of the software was only available in the United States due to export restrictions. Legislation recently passed allows for export of 128-bit software, so that most e-commerce sites will now be accessed using strong 128-bit encryption. This secure access provides a channel between the consumer's computer and the merchant's server. The information is sent in encrypted format, and therefore the risk of someone obtaining the information and decrypting it is extremely small. So small, that many experts think it is safer to sent your credit card over SSL than to give it to the waiter in the restaurant in the real world. While many merchants understand the worry of consumers about sending credit card details over the Internet, most of them do not address it in the right way. Instead of explaining the security of SSL, they often provide an option to store the credit card information once and assign a username/password to the customer, so that the customer never has to enter his card information again. This, however, may be completely misleading the consumer. Some merchants may provide this service primarily to establish a relationship with the consumer. Additionally, there is only a limited number of usernames/passwords available: While early adopters may be able to register identical usernames at multiple sites, most consumers will have to

remember many different usernames and associate them with the right merchant.

Once credit card information has been transmitted to the merchant's server, it is used to authorize the purchase. After receiving the authorization/denial code, the information could be filed off-line for records keeping purposes only. Most of times, however, the information is stored online (encrypted or un-encrypted) to be available for the consumer's next purchase. This practice leads to another source of fraud: hacking into the merchant's server and obtaining credit card information together with other valuable data, i.e., name and address. Merchants may claim to take precautions to protect credit card data from being stolen from their servers. But since merchants themselves retrieve card information from their servers every time the customer makes a purchase, it is very possible to obtain that card data.

Another way of getting valid credit card information is to generate it. Credit card numbers are not completely random. In fact, many of the digits are determined by card type, card issuing bank, and country of issuance. This allows hackers to pre-set certain card number digits and to generate the remaining digits using software available on the Internet. This method, however, rarely works, as many of the generated card numbers are not active. Additionally, for card information to be useable, it is essential to have the correct expiration date as well, which would have to be guessed at this time.

A different source of credit card fraud is cardholders disputing transactions which are legitimate. This phenomenon is particularly common in the online adult industry. Cardholders sign up for various services, and once they receive their monthly statement, they call up their bank and dispute the charge. Online merchants can do very little against that type of fraud. They can share their experience with other merchants, but it is unlikely that the cardholder would use the very same card again. Instead he may be using a different card, which makes him look like a new customer, allowing him to commit the fraud again.

Summary of the Invention

The present invention provides a method and system for placing a purchase order by using a credit or debit card in such way that potential financial losses arising out of unauthorized use of credit/debit cards are reduced.

A card verifying authority allows potential buyers to become users of the invention. Credit card holders register their credit/debit cards by providing essential information required for a complete purchase order, including but not limited to card number, expiration date, shipping address, preferred shipping method, telephone contact information. The verifying authority does not store the credit card number, but only a fingerprint thereof obtained by performing a one-way encryption function.

Registration links are established among the user, merchants, an acquiring bank, a card issuer, and the card verifying authority. The acquiring bank can also be the card issuer. In many respects the relationships among these entities are similar to those supporting credit card purchases via conventional telephone ordering. The invention affords protection to the user, in connection with commercial transactions over, e.g., the Internet, through three aspects of the invention which are considered novel relative to conventional purchasing procedures for consumer goods.

According to the invention the card verifying authority provides a first form of protection, in that merchants are not required to store any buyer information on their systems. The user transmits his credit card number to the merchant at the time of purchase, the merchant submits the credit card information to the card verifying authority and obtains further information required to complete the purchase order (e.g., shipping address) from the card verifying authority. The card verifying authority, however, does not need to have access to the unencrypted credit card information at any time and therefore affords to store only a footprint or image of the credit card information after applying a one-way encryption function (such as MD-5 which is generally available). The merchant may submit either the unencrypted card number or the encrypted footprint or image to the card

verifying authority in order to obtain further purchase order information. The card verifying authority may apply this method of data identification not only for credit card numbers, but also for other information (e.g., pass phrase). Moreover, in one embodiment there is no need to store unencrypted information anywhere.

In a second form of protection, which may be an alternative to or additive with the first form of protection, the details provided by the card verifying authority are considered unchangeable without additional verification efforts. Even if a credit card is stolen and used by a buyer who is not a registered user, for purchasing goods, the shipping information could not be easily changed, and goods would be delivered to the rightful card owner's address where they could be easily traced.

In a third form of protection, which may be an alternative to or additive with the first and second forms of protection, the user can register his preferred computer system for shopping with the card verifying authority and indicate a pass phrase for credit card transactions initiated from a different computer system (e.g., public computer terminal at airports). If a particular use of a credit card is not originating from a preferred computer system, which the merchant can determine by checking with the card verifying authority, then the card user will be required to enter an additional pass phrase to confirm his identity. Again, the pass phrase entered will be verified by the card verifying authority with the pass phrase on record.

A key feature of the invention is the unique association of encrypted information with unencrypted information pertaining to the proper user of a valid credit card or similar financial instrument. The encrypted information is utilized as much as possible where otherwise sensitive information would be stored or transmitted. Even if a stranger obtains a part of this combination of information, it is insufficient for the stranger to complete many of the most common forms of fraudulent transactions.

In one embodiment, the invention is a method for a buyer to make a purchase from a merchant using a valid credit card issued to the buyer. Before making a purchase, the buyer transmits the valid credit card number

and at least one other personal information data element to a verifying authority. The verifying authority registers the valid card number as an encrypted output number of a one-way encryption function and associates the additional data element with the encrypted number, and stores the encrypted number and associated data element in a database with encrypted numbers and associated data elements of other registrants. The buyer initiates a purchase order by providing a credit card number and a personal information data element to the merchant. The merchant transmits the credit card number and data element received from the buyer, to the verifying authority. The verifying authority encrypts the credit card number received from the merchant, confirms whether the encrypted number and data element from the merchant matches an encrypted number and associated data element in the database, and informs the merchant of whether a match was made, thereby verifying that the buyer is authorized to use the valid credit card number. Equivalently, the merchant could receive the credit card number as encrypted by the user, and transmit the encrypted number to the verifying authority.

In another embodiment, the invention is a system wherein a merchant verifies that a buyer is authorized to make a credit card purchase of goods or services by transmitting a credit card number and another data element received from the buyer at the time of purchase to a verifying authority over a digital communications network. The verifying authority includes a database of a multiplicity of sets of associated data, each set comprising a valid credit card number in encrypted form and at least another data element. The multiplicity of sets have been registered with the verifying authority by a respective multiplicity of potential buyers. Computer hardware and software define means for comparing a credit card number or encrypted credit card number and another data element transmitted by the merchant in the course of a credit card transaction with a buyer, against the registered encrypted numbers and associated data elements, and means for informing the merchant whether a match was made, thereby verifying that the buyer is authorized to use the valid credit card number.

The present invention is particularly well suited for incorporation into the type of credit card transaction verification system and method as are described in International Application PCT/US99/20693, entitled "Detection of Unauthorized Use of Payment Instruments Over Commercial Network Systems", the disclosure of which is hereby incorporated by reference. The present invention can be implemented using similar system and application programming and communications software and hardware.

Brief Description of the Drawings

Fig. 1 is an overview of the minimum components of the inventive system;

Fig. 2 shows how the card holder can register his card by having the card information encrypted by the verifying authority;

Fig. 3 shows what information is preferably encrypted;

Fig. 4 shows an alternative embodiment whereby the card holder can register his card information by applying the encryption function before sensitive information is transmitted to the verifying authority; and

Fig. 5 shows a simple purchase authorization process in another embodiment whereby sensitive information is encrypted by the purchaser before transmission to the merchant.

Description of the Preferred Embodiments

As shown in Figure 1, a verifying authority 100 is accessible to a large pool of buyers 200 who desire to make purchases from a large pool of merchants 300, via a public or private communications network 400, preferably a global communications network such as the Internet. Such purchase transactions according to the invention require communications between a particular buyer from among the pool of buyers 200 and the authority 100; between the particular buyer and a particular merchant; and between the particular merchant and the authority 100. However, the particular means of communication need not be the same (e.g., one may be on a public network and another on a private network).

The remainder of this description will focus on the invention as implemented between a particular buyer 200 and a particular merchant 300, but it should be appreciated that when the system is fully operational, it includes one authority 100 and a multiplicity of buyers and merchants. The authority can be an independent entity which handles one or more types of credit cards, or an agency affiliated with one card issuer or an acquiring bank.

Figure 2 shows the simplest form of the invention, whereby a particular one of the potential buyers 200 who possesses a valid credit card is deemed a user of the invention 500 who first registers the card with the verifying authority 100 via the network 400. The credit card number and at least one additional personal information element of data, as shown in Figure 3, are transmitted to the authority 100, where at least the credit card number is subjected to an encryption function 510. Typically, the name, expiration date, and mailing address are not encrypted. The information as received by the authority is confirmed to the user via logic 520. Also, the user can at a later time change the registration, via logic 520. The information associated with the user (after encryption) is stored in a database 110, 530 at the authority 100. Preferably, the original form of the encrypted information is not stored in the database. Thus, even if a hacker were to access the database 110,530, he could not obtain the combination of original card number and expiration date for any of the registered users. The only vulnerability is during the transmission of the original information over the network to the authority.

The user initiates a purchase transaction when he transmits his credit card number (and usually other information such as expiration date) to the merchant 300 at the time of purchase. The merchant submits the credit card number and other information to the card verifying authority 100 and obtains further information required to complete the purchase order (e.g., shipping address) from the card verifying authority. The card verifying authority, however, does not need to have access to the unencrypted credit card information at any time. The card verifying authority may apply this method

of data identification not only for credit card numbers, but also for other information (e.g., pass phrase).

The particular merchant is among the plurality of merchants who have also registered with the authority 100. Optionally, the registered merchants have been given the encryption function so that after receiving the original number from the user making a purchase, the merchant transmits the encrypted number and expiration date to the verifying authority.

As another alternative, shown in Figure 4, the user 500 can apply the encryption function 510 before transmission via the network 400 to register with the verifying authority 100.

Figure 5 illustrates yet another embodiment of the process by which a purchase order is handled according to the invention. The user 600 submits the encrypted card number 510 and expiration date via the network 400, to a particular merchant 610. The merchant 300 merely forwards the encrypted information to the verifying authority 100. Under current commercial procedures, the merchant must have the original credit card number so that he can transmit it to his acquiring bank and the bank can transmit the information to the user's card issuing bank. However, another possible implementation would include such banks having access to the encryption function such that processing can be made on that basis.

In all embodiments, the authority 100 attempts to match the encrypted information with the information stored in the database 110. In essence, the authority registers the card number as an encrypted output number of a one-way encryption function and associates at least one additional personal data element with the encrypted number, and stores the encrypted number and associated data element in a database with encrypted numbers and associated data elements of other registrants. Preferably, a credit limit for a particular purchase or a sequence of purchases within a given time period is registered and is checked by the authority during the verification logic 620, 630, and 640. The authority 100 then communicates to the merchant 300, whether the transaction is approved or denied.

It should thus be appreciated that a variety of possibilities and

associated scenarios for implementing the invention are possible. Registration can be over the network 400, by postal service or by facsimile transmission. Each registrant would pay a registration fee and optionally an annual service fee. Alternatively, if the verifying authority is affiliated with a card issuer or an acquiring bank, the credit card holder may be automatically registered at no apparent charge, upon issuance of the card. The number and type of personal information data elements can vary considerably, but as shown in Figure 3, options include a personal ID corresponding to the authorized user's personal computer or other digital signal generating device, and pass phrase or other such code, which can be used for verification if an authorized user initiates a purchase transaction from another computer. These can be encrypted to the same extent as the credit card number. Other personal information, such as the credit card holder's mailing address and the holder's choice of a transaction or cumulative monetary limit, need not be encrypted. Sensitive information may be handled in at least three ways. Encryption can be made by the card holder, whereby only encrypted information travels on the network; the merchant can encrypt the sensitive information; or the sensitive information can be encrypted by the verifying authority. Preferably, the merchant does not store any credit card information.

The foregoing functional features, data elements and other options of the inventive system and method, can be implemented in a variety of combinations.

CLAIMS:

1. In a method for a buyer to make a purchase from a merchant, using a valid credit card issued to the buyer, the improvement comprising:

before making a purchase, the buyer transmits the valid credit card number and at least one other personal information data element to a verifying authority;

the verifying authority

registers the valid card number as an encrypted output number of a one-way encryption function and associates said additional data element with said encrypted number, and

stores the encrypted number and associated data element in a database with encrypted numbers and associated data elements of other registrants;

the buyer initiates a purchase order by providing a credit card number and a personal information data element to the merchant;

the merchant transmits the credit card number and data element received from the buyer, to the verifying authority; and

the verifying authority

encrypts the credit card number received from the merchant,

confirms whether the encrypted number and data element from the merchant matches an encrypted number and associated data element in the database, and

informs the merchant of whether a match was made, thereby verifying that the buyer is authorized to use the valid credit card number.

2. The method of claim 1, wherein at least some of the buyers who register, transmit a respective valid credit card number to the verifying authority as an encrypted number resulting from application of a one-way encryption function on the valid credit card number and this encrypted number is the encrypted number stored in the database.

3. The method of claim 1 or 2, wherein one of the at least one other personal information data element is the credit card expiration date.

4. The method of any of claims 1 through 3, wherein one of the at least one other personal information data element is the valid credit card owner's mailing address.

5. The method of any of claims 1 through 4, wherein one of the at least one other personal information data element is a personal identification number stored in the database as an encrypted number resulting from application of a one-way encryption function on an original personal identification number.

6. The method of claim 5, wherein the personal identification number is uniquely associated with a particular digital signal generating device by which the authorized credit card holder initiates purchase orders.

7. The method of any of claims 1 through 4, wherein one of the at least one other personal information data element is a password.

8. The method of claim 1, wherein the buyer registers with the verifying authority over a publicly accessible digital communications network.

9. The method of claim 1, wherein the verifying authority is the financial institution that issued the credit card to the buyer.

10. The method of any of claims 1 through 9, wherein

the buyer initiates a purchase order by providing an encrypted credit card number and a personal information data element to the merchant; and

the merchant transmits the encrypted credit card number and said data element received from the buyer, to the verifying authority.

11. The method of any of claims 1 through 9, wherein at the time of a purchase order the merchant applies said one way encryption function to the credit card number received from the buyer and transmits said encrypted number with the personal information data element to the verifying authority.

12. The method of claim 4 wherein after the verifying authority confirms a match, the credit card authority transmits the valid credit card owner's mailing address to the merchant.

13. In a system wherein a merchant verifies that a buyer is authorized to make a credit card purchase of goods or services by transmitting a credit card number and another data element received from the buyer at the time of purchase to a verifying authority over a digital communications network, the improvement wherein the verifying authority includes:

a database of a multiplicity of sets of associated data, each set comprising a valid credit card number in encrypted form and at least one other data element, said multiplicity of sets having been registered with the verifying authority by a respective multiplicity of potential buyers;

means for comparing a credit card number or encrypted credit card number and another data element transmitted by the merchant in the course of a credit card transaction with a buyer, against the registered encrypted numbers and associated data elements; and

means for informing the merchant whether a match was made, thereby verifying that the buyer is authorized to use the valid credit card number.

14. The system of claim 13, wherein the least one other data element is the credit card expiration date.

15. The system of claims 13 or 14, wherein the at least one other

data element is the valid credit card owner's mailing address.

16. The system of claim 15, wherein the at least one other data element is a personal identification number stored in the database as an encrypted number resulting from application of a one-way encryption function on an original personal identification number.

17. The system of claim 16, wherein the personal identification number is uniquely associated with a particular digital signal generating device by which the authorized credit card holder initiates purchase orders.

18. The system of claim 17, wherein another data element is a pass phrase stored in the database as an encrypted number resulting from application of a one-way encryption function on an original pass phrase.

19. The system of claim 13, wherein the verifying authority is the financial institution that issued the credit card to the buyer.

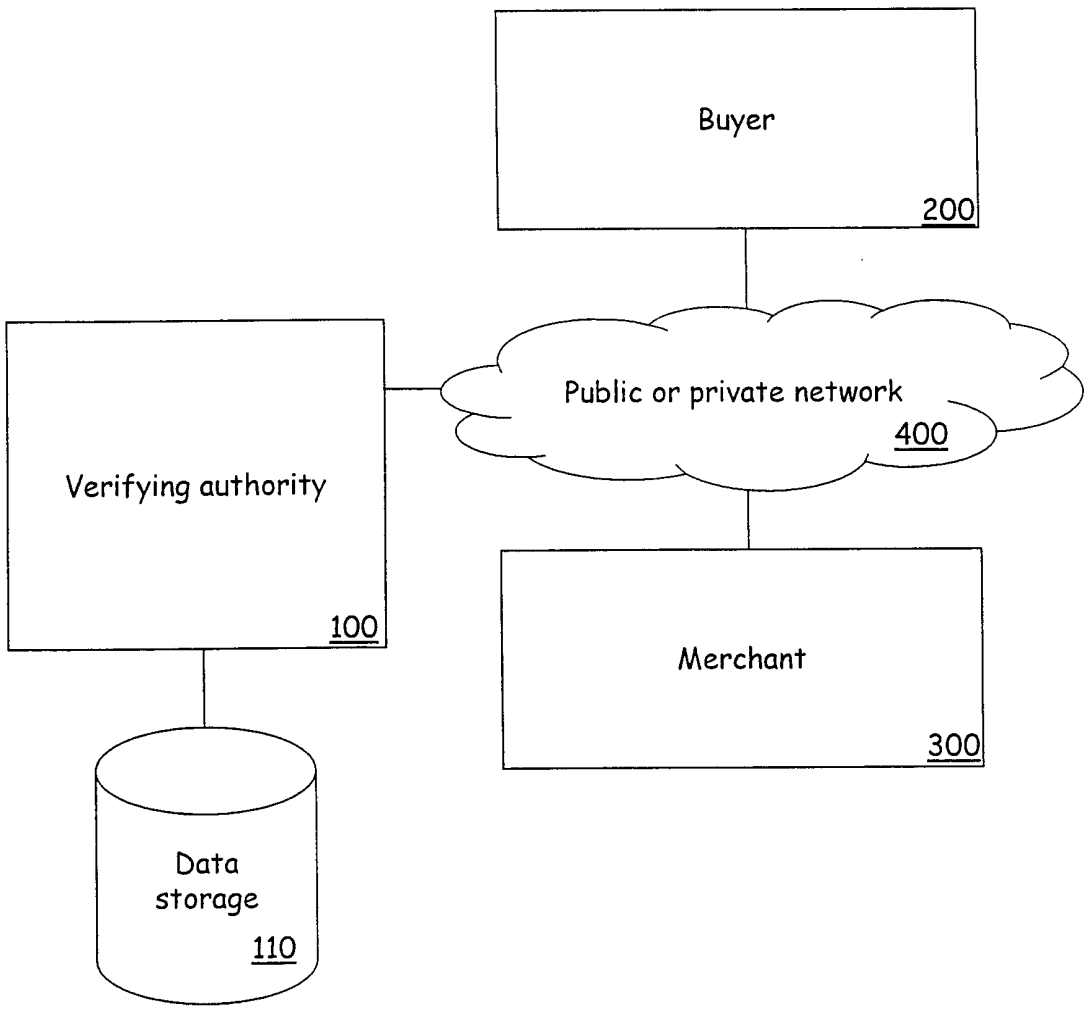

Buyer
200
Public or private network
400
Verifying authority
100
Merchant
300
Data
storage
110

Fig. 1

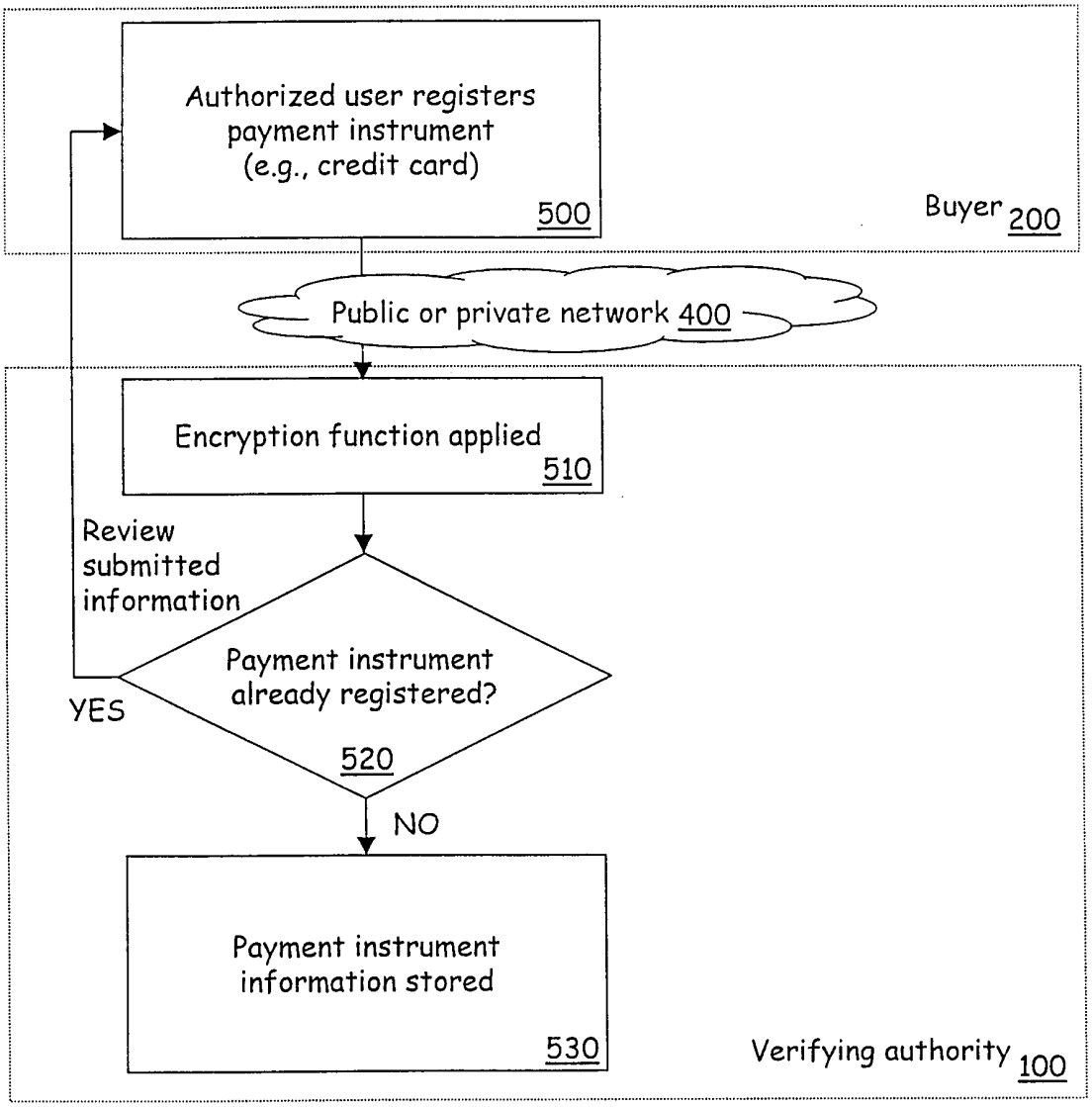

Authorized user registers payment instrument (e.g., credit card)
500
Buyer 200
Public or private network 400
Encryption function applied
510
Review submitted information
Payment instrument already registered?
520
YES
NO
Payment instrument information stored
530
Verifying authority 100

Fig. 2

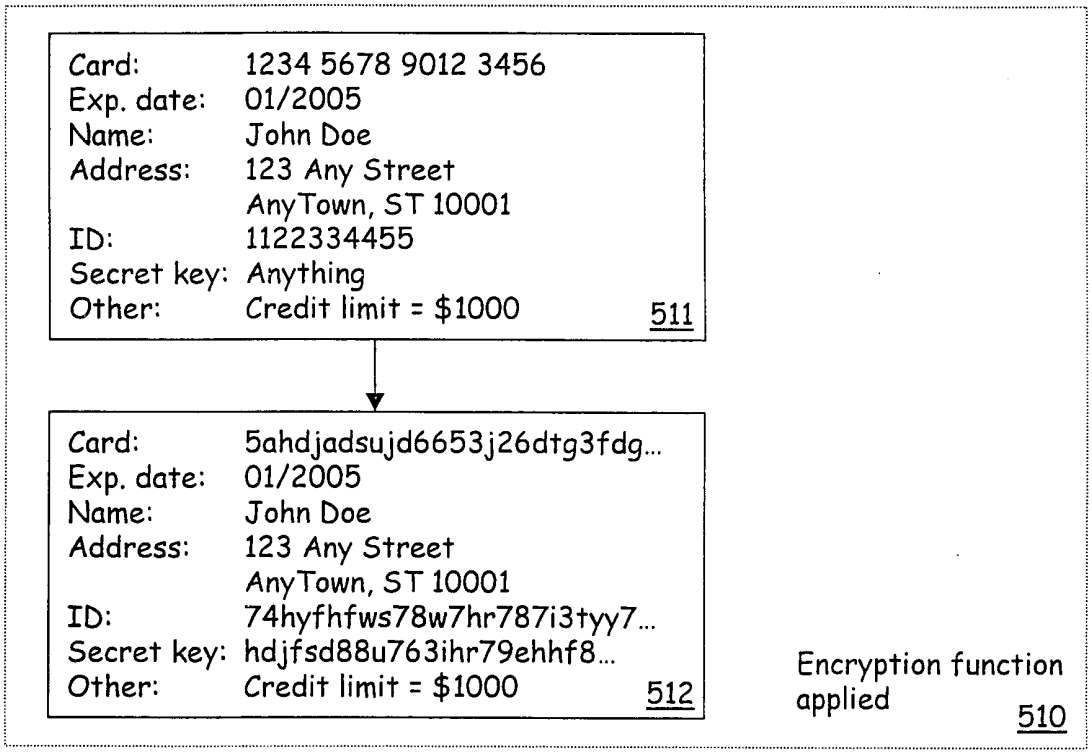

Card: 1234 5678 9012 3456
Exp. date: 01/2005
Name: John Doe
Address: 123 Any Street
AnyTown, ST 10001
ID: 1122334455
Secret key: Anything
Other: Credit limit = $1000
511
Card: 5ahdjadsujd6653j26dtg3fdg...
Exp. date: 01/2005
Name: John Doe
Address: 123 Any Street
AnyTown, ST 10001
ID: 74hyfhfws78w7hr787i3tyy7...
Secret key: hdjfsd88u763ihr79ehhf8...
Other: Credit limit = $1000
512
Encryption function applied
510

Fig. 3

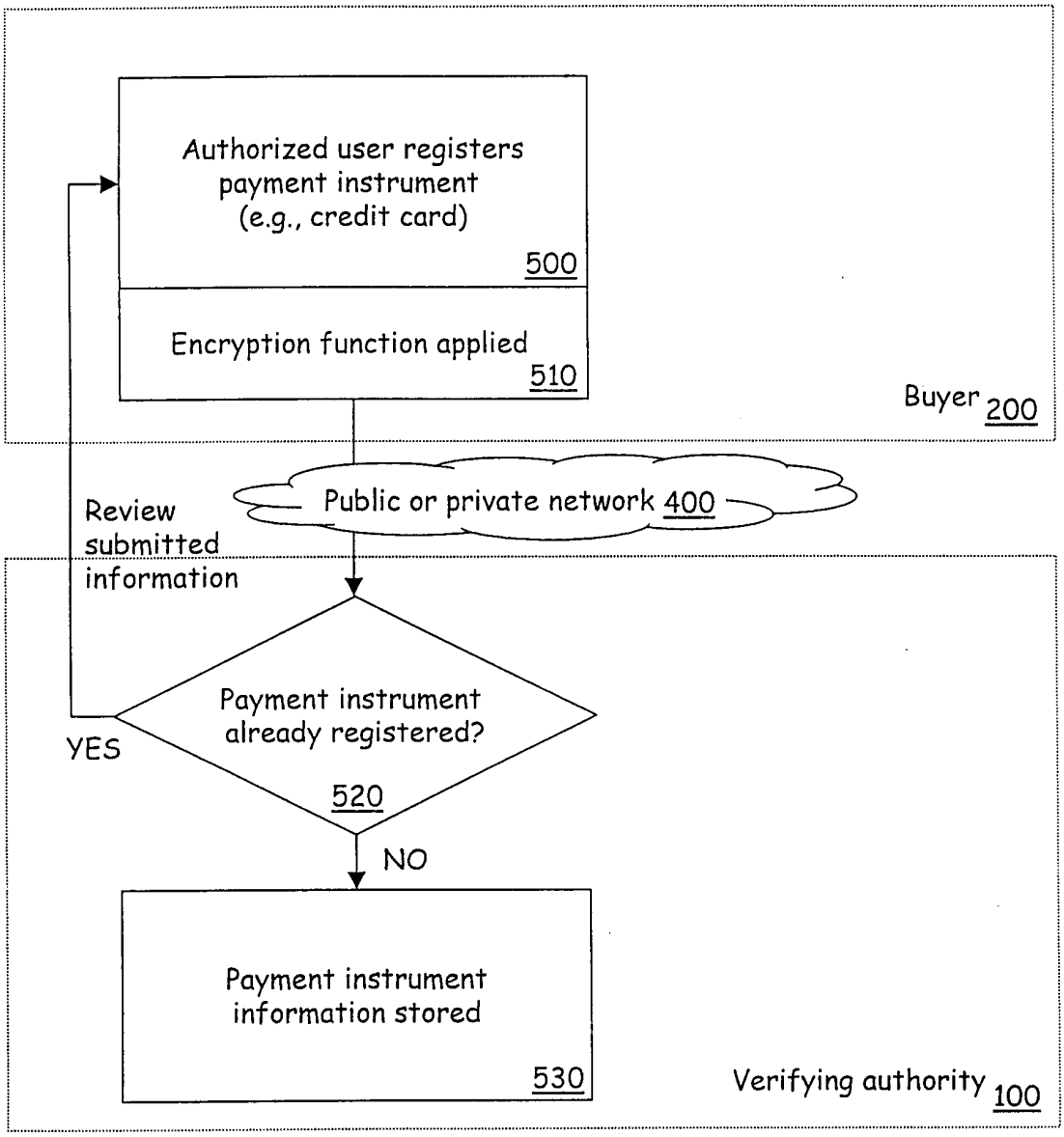

Authorized user registers payment instrument (e.g., credit card)
500
Encryption function applied
510
Buyer 200
Public or private network 400
Review submitted information
Payment instrument already registered?
520
YES
NO
Payment instrument information stored
530
Verifying authority 100

Fig. 4

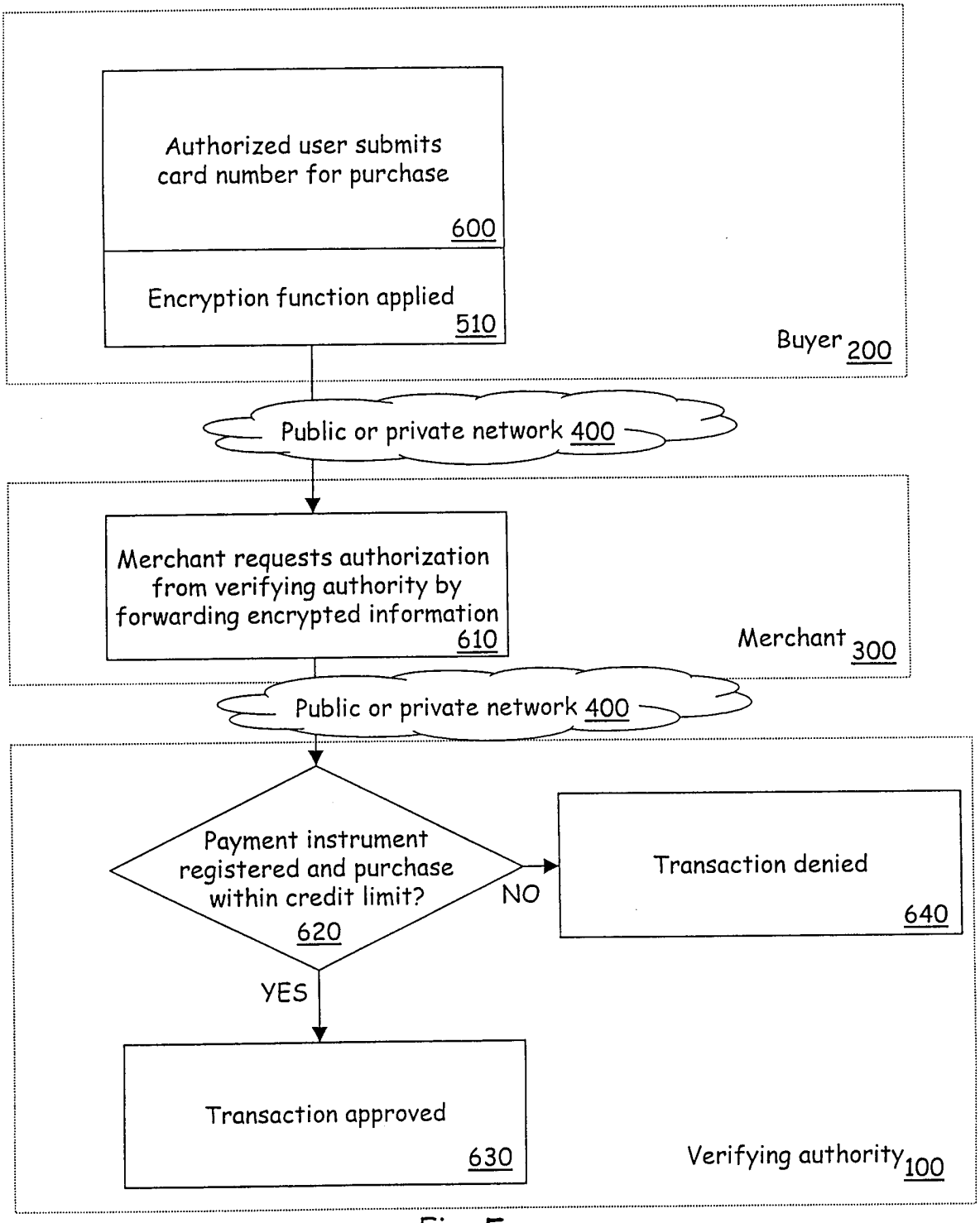

Authorized user submits card number for purchase
600
Encryption function applied
510
Buyer 200
Public or private network 400
Merchant requests authorization from verifying authority by forwarding encrypted information
610
Merchant 300
Public or private network 400
Payment instrument registered and purchase within credit limit?
620
NO
Transaction denied
640
YES
Transaction approved
630
Verifying authority 100

Fig. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/05248

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : G06F 17/00
US CL : 705/39
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)
U.S. : 705/39

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 practicable, search terms used)
EAST search of Derwent , Euro and Japio; DialogWeb dbs 9,15,16,148,625,810,813

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 5,883,810 A (FRANKLIN et al) 16 March 1999 (16.03.1999), Column 2, lines 5-55, Column 6, lines 28-58; Column 2, lines 5-55, Column 6, lines 28-58	13-19 --- 1-12
Y	US 5,870,723 A (PARE, Jr et al) 09 February 1999 (09.02.1999), see Fig 1, Column 9, line 11 - Column 36, line 39	1-12
A	HP 10171897 A (NITTSU SYSTEM KK) 26 June 1998 (26.06.1998) abstract	1-18
A	No author, Debit Issuers and Merchants Await An Internet Security Solution, Debit Card News, v2,n19,p7+, DialogWeb copy pages 1-4	1-18

☐ Further documents are listed in the continuation of Box C. ☐ See patent family 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 application or patent 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
	27 JUL 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Todd Voeltz James R. Matthews Telephone No. (703) 305-9714

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Ir ıational application No.
PCT/US00/05248

Box I Observations where certain claims were found unsearchable (Continuation of Item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claim Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claim Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☒ Claim Nos.: 4-7,10 and 12
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of Item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.
☐ No protest accompanied the payment of additional search fees.