Title: SYSTEM AND METHOD FOR ELECTRONIC PURCHASE OF AUTHORIZATION PERMITTING USE OF A SERVICE

Abstract: Described herein is a method for purchasing, via telematics, an authorization to use a service, comprising the steps of: sending a request for purchase of a service, using a telecommunications network (6, 20), there being also provided, during the purchasing request, an identification code identifying a portable storage medium (8, 12, 14, 18); generating an authorization for use of an electronic device containing the identification code of the portable storage medium (8, 12, 14, 18); sending the authorization, using the aforesaid telecommunications network (6, 20); receiving the authorization sent; storing the authorization on the portable storage medium (8, 12, 14, 18); and exhibiting the authorization stored on the portable storage medium (8, 12, 14, 18). Exhibiting the authorization envisages: reading from the portable storage medium (8, 12, 14, 18) the authorization stored therein and the identification code of the storage medium itself; comparing the identification code contained in the stored authorization and the identification code read by the portable storage medium (8, 12, 14, 18); and authorizing use of the service in the event of said verification yielding a positive result.
"A SYSTEM AND METHOD FOR PURCHASING, VIA TELEMATICS, AN AUTHORIZATION TO USE A SERVICE"

TECHNICAL FIELD

The present invention relates to a system and method for purchasing, via telematics, an authorization to use a service, where by the term "service" is meant the contents of an obligation, i.e., that which the person obliged must provide or the behaviour that he must assume.

Comprised, therefore, in the above term are services, such as entrance to shows, exhibitions and events in general for which an admission fee must be paid (e.g., theatres, museums, sports grounds, concerts, etc.), or to structures of various types (e.g., car-parks, motorways, etc.), admission to places or to events where entrance is limited and where bookings or appointments are envisaged (e.g., medical examinations, visits to public offices, remote purchasing, for instance, of railway or aeroplane tickets), and, in general, to all those services, payment of which can be made by credit card (e.g., payment of taxes, bills, etc.). Furthermore, for reasons of simplicity of description, in the ensuing exposition explicit reference will be made to purchasing, via telematics, of a credit instrument, in particular, an entrance ticket to a show or event, without, of course, this implying any loss of generality.

BACKGROUND ART

As is known, the booking and payment, via telematics, of an entrance ticket to an event, made through the Internet, is rapidly spreading, above all as a result of the development of Web sites dedicated to electronic commerce, as well as to events specifically designed for attracting spectators and visitors to museums, theatres, concerts, etc.

Much of the effort so far made to make this type of
application possible has been concentrated on the part regarding secure payment of the entrance ticket. Nevertheless, up to the present day, purchasing of an entrance ticket to an event via telematics cannot disregard the aspect of withdrawal of the ticket itself, which must frequently be done in considerable advance with respect to the time of start of the event in question, in so far as the ticket is indispensable both to be able to prove that one has a right to admission to the event and for reasons of an administrative or tax nature (in the case of events for which there is an admission fee), for example, as regards the rights to be paid to an organization such as the Società Italiana Autori ed Editori (SIAE - the Italian Society of Authors and Editors), and this represents, without any doubt, a serious problem which is capable of limiting to a considerable extent the advantages afforded by new telematic technologies.

In order to overcome the above drawback, in the Italian patent application TO2000A000726, filed on July 21, 2000, in the name of the present applicant, there is proposed a system and method for purchasing via telematics, in which the need to withdraw the entrance ticket to the event or to receive it by post is eliminated by replacing the latter with an equivalent virtual or electronic ticket, which can be obtained via telematics in such a way that the entire operation of purchasing the entrance ticket can be made at a distance, at times and in places chosen by the user.

In particular, the virtual ticket is basically represented by an authorization for admission of a computer type or electronic type (duly encrypted for evident reasons of security), which can be received through the same means whereby the request for purchase of the entrance ticket was made, for instance, a personal computer, or else a portable terminal of the user, in particular a cellphone, or else some equivalent terminal, such as a palm-top computer, or else via
any one of the other means referred to above used for this purpose.

Authorization for admission to the event is generated and sent, provided that payment is ensured, by the provider of the service of sale of entrance tickets to said event. This may be the body organizing the event or else a special agency capable of ensuring a generalized booking service. Such an organization handles the booking, the checking of the economic coverage, the payment of the ticket, the generation of the virtual ticket, and the sending thereof to the customer, using a special protocol.

The authorization for admission to the event is then stored on an appropriate portable storage medium so as to enable exhibition thereof or presentation thereof upon admission to the event itself in order to obtain authorization to enter the premises where the event is taking place.

In particular, the storage medium for authorizing admission may be represented either by a so-called “smart card” of the type with contacts or of the contactless type, or else by a portable terminal of the user, in particular a cellphone or some equivalent terminal, such as a palm-top computer.

Presentation of the authorization for admission to the event stored on the storage medium is made in the way commonly used for fast access to places that attract a big public, such as metropolitan undergrounds, ski-lifts, motorways (tele-passes), etc., i.e., getting the storage medium to interact with a reader or an electronic access gate envisaged for admission to the event, through which the entrance pass is checked and cancelled, and entrance to the event is allowed through an appropriate visual or acoustic communication.

In the case where the storage medium for authorizing admission
to the event is represented by a contactless smart card, this may be either of the so-called "stand-alone" type and hence, in effect, constitute a single multi-service document similar to an electronic credit card for controlled admission to places, events, or, more in general, to services of any nature for which payment is envisaged, or else be incorporated in the cellphone, which should therefore be modified to make possible activation of the smart card itself (such modifications may also require only interventions of a software type on the cellphone and/or on the Subscriber Identity Module (SIM) card).

In detail, in the case where the storage medium is represented by a smart card of the stand-alone type, the transfer of the authorization for entrance by the means with which it was received, whether this be a computer or a telephone, to the smart card itself, can be effected by means of an appropriate programming peripheral that can be connected to the computer or to the telephone itself.

In addition, in the case where the authorization for admission is received by means of a cellphone, programming of a smart card of the stand-alone type could then also be performed using the cellphone itself, setting the smart card at a very short distance from the circuit provided for the purpose (for example, by simply resting the smart card against the cellphone or else inserting it into a special opening present in the cellphone itself). Furthermore, exhibiting the entrance pass to the particular event stored on a smart card of the contactless type envisages that, when the owner of the smart card passes through the electronic access gate, the said smart card is brought up to the electronic access gate itself, which then emits a high-frequency activation signal to the smart card. Upon reception of the activation signal, the smart card is activated and establishes a communication with the electronic access gate, during which the electronic access
gate verifies and obliterates the entrance pass stored in the smart card and authorizes the owner of the smart card, by means of an appropriate acoustic or visual signal, to gain admission to the event.

Instead, incorporation of a smart card in a cellphone may be effected either by intervention on the SIM card of the cellphone or by intervention on the cellphone itself. In detail, in the first case, the SIM card currently used in cellphones is replaced by a card which incorporates the smart-card function of the contactless type, whereas, in the second case, in the cellphone, in addition to the SIM card, there is inserted a contactless smart card, with the corresponding activation antenna, and the cellphone is modified in such a way that the authorization received telephonically and possibly stored in the memory of the cellphone itself will be transferred into the contactless smart card.

Exhibiting the pass for admission to the event stored in a smart card incorporated in a cellphone may be done in a way similar to the one described previously for a contactless smart card, i.e., simply by bringing the cellphone, whether this be turned off, turned on, or receiving a call, up to the electronic access gate, which checks and cancels the entrance pass stored in the smart card of the cellphone in the way described previously.

Instead, in the case where the medium for storage of authorization for admission to the event is represented by a smart card with contacts, exhibiting the entrance pass may be performed by simply inserting the smart card into a special reader with which the electronic access gate is equipped. Finally, in the case where the medium for storage of authorization for admission to the event is represented by a portable terminal of the user, such as a cellphone or a palm-top computer, the entrance pass can be received directly by
the portable terminal itself or else be received by a computer and then, through an appropriate programming peripheral, be transferred onto the portable terminal itself.

Exhibiting the aforesaid entrance pass may therefore be performed by sending a communication (with appropriate protocol) between the portable terminal and the electronic access gate, which receives from the portable terminal authorization for admission and, once the authenticity thereof has been ascertained, authorizes admission to the event.

In particular, in order to render the communication between the portable terminal and the electronic access gate as fast as possible, in such a way that use of this system of presentation of entrance passes to events where there is a big public attendance may be enabled, it is convenient that such a communication should be of the short-distance type (from just a few metres to just a few centimetres) and should take place directly between the portable terminal and the electronic access gate itself, i.e., without involving the normal communication channels and the base stations of the cellphone system.

In detail, given that next-generation cellphones will be equipped with the so-called Blue Tooth, i.e., with a short-distance communication system, to make a short-distance communication between a cellphone and an electronic access gate, it is sufficient to equip also the latter with a short-distance communication system capable of communicating with that of the cellphone. According to this solution, in fact, the user, when he arrives in the vicinity of the electronic access gate, types the entrance request on the keypad of the cellphone, and then, by sending a simple OK signal, activates a local communication with the electronic access gate itself, which receives the entrance request from the cellphone, and, once authenticity thereof has been ascertained, authorizes
admission.

The short-distance communication system with which next-generation cellphones will be equipped may then also be used for transferring an entrance pass, received by means of a computer, into the cellphone, the said computer also being in future equipped with a short-distance communication system capable of communicating with that of the cellphone.

Exhibiting the entrance pass stored in a cellphone may then also be performed in the form of a normal telephone call, for example a telephone call that cancels credit that has previously been stored in the memory of the cellphone. However, this solution, by occupying the normal communication channels and the base stations of the cellphone system might not enable sufficiently fast admission and hence be undesirable in the case of events where there is a big attendance of public.

However, even with present-generation cellphones, i.e., ones not equipped with a communication system of a Blue-tooth type, it is possible to use admission entrances equipped with radio transceivers capable of taking the place of the base stations of the mobile telephone system of general use, in order to activate a short-distance (just a few metres) brief communication between the user’s cellphone and the entrance to authorize admission.

In order to make the short-distance communication between the portable terminal and the electronic entrance or electronic access gate, other short-distance communication systems can be used, in particular short-distance communication systems that do not use radio transmissions, such as infrared communication systems.

Purely by way of non-limiting example, Figure 1 illustrates
the working diagram of a system for purchasing an entrance ticket to an event described in the aforementioned Italian patent application.

In particular, in Figure 1, the reference number 1 designates the purchasing system as a whole; the reference number 2 designates the provider of the service for selling entrance tickets to the event in question; 4 designates the computer with which authorization for admission to the event can be requested and received; 6 designates, as a whole, the telecommunications network between the computer 4 and the provider 2, in the example illustrated constituted by the Internet and a traditional telephone network; 8 designates the cellphone that can be connected to the computer 4 for downloading the authorization for admission received; 10 designates the programming peripheral that can be connected to the computer 4 for programming the smart card with or without contacts, designated by 12; the reference number 14 designates the cellphone on which authorization for admission to the event can be directly received; 16 designates the programming peripheral that can be connected to the cellphone 14 for programming the smart card with or without contacts, designated by 18; and the reference number 20 designates the telecommunications network between the cellphone 14 and the provider 2, in the example illustrated a cellphone network operating according to GSM, or GPRS, or UMTS standards, or some other standard, through which the request for purchase of an entrance ticket to the event is sent from the cellphone 14 to the provider 2, and the authorization for admission to the event is sent from the provider 2 to the cellphone 14, which also uses in part the telecommunications network 6.

Figure 2, instead, illustrates a working diagram whereby an authorization is exhibited at entrance to an event, in the example shown an authorization stored in the cellphone, in which 22 designates the electronic access gate; 24 designates
the short-distance communication system of the cellphone; 26 designates the short-distance communication system with which the electronic access gate 22 must be provided to enable a short-distance communication with the short-distance communication system of the cellphone; 27 designates the activation and reading device of a contactless smart card; 28 designates the reading device of a smart card with contacts; and 29 designates the processing device, provided with an internal memory of its own, which checks authorization for admission, for example by connecting up to the provider of the authorization, and enables admission to the event.

From what has been described and from the illustrations of Figures 1 and 2, it is immediately evident how, in a purchasing system via telematics of the type proposed in the above-mentioned Italian patent application in the name of the present applicant, the authenticity of the credit instrument purchased represents an essential characteristic of the system, in so far as it must not be possible for said credit instrument to be manipulated in any way (i.e., for forging it, extending it, post-dating it, or pre-dating it), duplicated or transferred to others in such a way that the said credit instrument might be used a number of times.

DISCLOSURE OF THE INVENTION
The purpose of the present invention is to provide a method and a system for purchasing via telematics, in which the authenticity of the credit instruments purchased will be guaranteed against any type of manipulation.

According to the present invention, a purchasing system via telematics for acquiring authorization to use a service is provided, as defined in Claim 1.

Also provided according to the present invention is a method for purchasing, via telematics, an authorization to use a
service, as defined in Claim 7.

BRIEF DESCRIPTION OF THE DRAWINGS
In order to provide a more detailed understanding, a number of preferred embodiments of the present invention will now be described, purely by way of non-limiting example, with reference to the attached drawings, in which:
- Figure 1 illustrates a working diagram of a first part of a system for purchasing authorization to use a service, devised according to the invention;
- Figure 2 illustrates a working diagram of a second part of a system for purchasing authorization to use a service, devised according to the invention; and
- Figures 3, 4 and 5 illustrate flowcharts of operations implemented in respective embodiments of the present invention.

BEST MODE FOR CARRYING OUT THE INVENTION
In particular, for reasons of simplicity of description, the inventive principle underlying the present invention will now be described with reference to the case where the credit instrument is purchased, stored and spent by means of a portable terminal consisting of a cellphone, obviously without this implying any loss of generality.

In detail, in order to guarantee the authenticity of the credit instruments purchased via telematics, the present invention is based upon the principle of using an identification code for identifying the user’s terminal that will be unique and will be automatically transferred at the moment of transmission between the user’s terminal and the reader on which the credit instrument is used, without there being any possibility of intervention on the part of the user himself.

There are numerous possible embodiments of the inventive
principle underlying the present invention.

A preferred embodiment consists in the use of the International Mobile Equipment Identity (IMEI) code for cellphones, in so far as the said code meets the requirements referred to previously, in particular as regards transmissions via infrared port.

As is known in fact the IMEI code for identifying a cellphone is a 15-figure code which enables the cellphone network to identify the cellphone in a unique way, in that the said code is automatically transmitted by the cellphone at each phone call, without there being any possibility of intervention on the part of the user, and is traceable in the network, this constituting an element of convenience and advantage, even though not altogether indispensable.

The IMEI code for cellphones can then be advantageously used in combination with an infrared transmission and/or a Blue-tooth transmission, in so far as these types of transmission meet the requisites previously referred to, in terms of speed of communication between the portable terminal and the electronic access gate in such a way as to enable use of this system of presentation of the authorization for admission to events where there is a high public attendance.

By the use of the above code, the authenticity and uniqueness of purchase via telematics is guaranteed in the way described in what follows with reference to the flowchart of Figure 3.

At the moment of purchase, via telematics, of the credit instrument, the Service Centre which carries out the ticket-office and telematic-register function receives from the purchaser the IMEI code identifying the cellphone on which it must send the credit instrument (block 100).

In particular the IMEI code of the cellphone can be “captured”
automatically by the Service Centre in the case where, in order to purchase and receive the credit instrument, the cellphone is used, or else if not, the customer will have to communicate explicitly to the Service Centre the IMEI code identifying the cellphone on which the credit instrument is to be sent.

However the IMEI code may have come into the possession of the Service Centre, the Service Centre enters the IMEI code of the cellphone on which it is to send the credit instrument inside the text of the credit instrument purchased, together with the other information necessary, such as the date of the event in question, the number of seats or places booked, the type of payment, etc. (block 110).

The Service Centre then transmits the credit instrument purchased, typically in encrypted form, to the cellphone that is the destinee, for instance in the form of an SMS message (block 120), and the credit instrument received is then stored in the memory of the cellphone (block 130).

At the moment of use of the credit instrument stored in the cellphone, i.e. during communication between the cellphone and the reader or the electronic access gate, the reader receives not only the credit instrument stored in the cellphone, which is possibly to be decrypted, but also the IMEI code identifying the cellphone on which the credit instrument was sent (block 140).

In particular the IMEI code identifying the cellphone on which the credit instrument was sent is transmitted from the cellphone to the reader in an altogether automatic way and without there being any possibility of intervention on the part of the user.

The reader then compares the two IMEI codes, the one transmitted independently and the one contained in the credit
instrument (block 150), and only in the case of perfect correspondence of the two codes does the reader authenticate the credit instrument, in so far as it is arriving from the only terminal to which it had been destined (this terminal being moreover known to the Service Centre and easily identifiable in the event of complaints or disputes), and hence authorizes admission to the event (block 150). In this way, whatever attempt may be made to reproduce, re-send, duplicate, etc., the credit instrument purchased has no possibility of success.

It may be readily understood how the principle of the invention described above regarding the purchase and use of the entrance ticket to shows, museums, concerts, sports grounds, etc. can be used for an extremely wide range of applications and payments, such as the purchasing of train tickets (which the ticket inspector can read on a special reader in the railway carriage, without any need for queues at the ticket office), air tickets, payments with receipt (consisting of the SMS received on the cellphone), etc.

Another possible application is then represented by automatic vending machines (for drinks, food, etc.) or tickets (for parking, etc.) in this case the user purchases the goods or the ticket with a transaction by telephone or computer and receives the corresponding credit instrument (with the indication of the vending machine) on the cellphone. At the moment of use the vending machine, which is equipped with a special reader (for example an infra-red or Blue-tooth reader) verifies the authenticity of the credit instrument, in the sense described previously, and dispenses the goods (or the parking ticket together with the time corresponding to the amount paid). In particular, the latter type of application is not specifically reserved to the solution with infrared or Blue-tooth reader, but regards all the technological solutions referred to in the present invention.
Amongst the numerous embodiments of the inventive principle underlying the present invention, yet another of these consists in using, instead of the IMEI code identifying the cellphone, the cellphone number itself, in the way described previously for the IMEI code, and with different types of organization at a system level.

In particular, a first type of organization at a system level consists in using the mobile-telephone network in the way described hereinafter with reference to the flowchart illustrated in Figure 4.

In detail, in this case the reader present at the entrance to the event is provided with a cellphone and when the entrance doors are opened already possesses all the electronic entrance tickets booked for the event, each containing the telephone number of the corresponding user and generated in the way previously described with reference to blocks 100 and 110 of the flowchart of Figure 3.

At the moment of admission to the event, the user simply telephones the reader (the number of which has been communicated to him at the moment of booking), which "captures" the telephone number of the caller (block 200) and compares it with the numbers of the electronic entrance tickets booked (block 210). Only in the event of the numbers coinciding will the reader grant admission to the user to the extent and for the number of seats or places booked (block 220).

The above system could be integrated with some element designed to check the "locality" of the call in order to prevent (if this were necessary) authorization for admission or purchase from being made at a long distance, without any real check on the use (even though the credit instrument
purchased would in any case be unique and could be spent only once). In this connection, it would be possible to use the indication of the microcell of the mobile-telephone system to be entered into the ticket to check correspondence with the user call. Other solutions in this regard are likewise possible.

A second type of organization at a system level consists in using optical readers for reading the credit instrument purchased directly by the display of the cellphones in a way described hereinafter with reference to the flowchart of Figure 5.

In particular, in this case the electronic ticket purchased via telematics and stored in the cellphone of the purchaser in the way described previously with reference to blocks 100 to 120 of the flowchart of Figure 3 is represented by a bar code or by a two-dimensional code which is practically impossible to forge and which contains the telephone number of the user. Once again, taking as our example the admission to a show, at the moment of entrance the customer telephones to the reader, which captures the caller’s telephone number as a signal indicating that the customer is present and is asking to enter (block 300), and keeps it for a limited period of time, for example a few minutes (block 310). When the customer appears at the entrance to the event, the optical reader reads the encoded ticket from the display of the cellphone (block 320), compares the telephone number contained therein with any of the ones that it is temporarily withholding (block 330), and in the event of the numbers coinciding, enables admission (block 340).

As mentioned previously, the inventive principle underlying the present invention described above with reference to a portable terminal consisting of a cellphone can be applied, just as it is, to any storage medium provided with an
identification code of its own.
In fact, at the moment of purchase of the credit instrument, whether this purchase be made via a portable terminal or via a computer, it is sufficient to communicate to the Service Centre the code identifying the storage medium and an address, either a telephone number or an e-mail address, to which the credit instrument can be transmitted. Upon receipt of the credit instrument, it is sufficient to transfer it onto the storage medium indicated at the moment of purchase and then use it in the way described above.

In the case, for example, where the storage medium is represented by a smart card provided with an identification code of its own at the moment of purchase of the credit instrument, it is sufficient to communicate the identification code of the smart card to the Service Centre and, once the credit instrument has been received, it will suffice to transfer it onto the smart card by means of a programming peripheral and then use it in the way mentioned above.

From an examination of the characteristics of the purchasing system provided according to the present invention, the advantages that this makes possible are evident.

In particular, it is pointed out that the purchasing system according to the present invention enables elimination of the need to withdraw the entrance ticket to the event by replacing it with an equivalent virtual ticket that can be obtained via telematics, thus enabling the entire operation for purchasing the ticket to be performed at a distance, at times and in places chosen by the user.

In addition, the purchasing system provided according to the present invention does not require particular technological effort in that it uses technologies already available on the market.
Finally, the purchasing system according to the present invention fully guarantees the authenticity of the credit instrument purchased via telematics.

Finally, it is clear that modifications and variations may be made to the purchasing system described and illustrated herein, without thereby departing from the sphere of protection of the present invention, as defined in the attached claims.

In particular, it is emphasized that what has been described above with reference to the purchase of an entrance ticket to an event also applies to the purchase of any service of the type referred to initially, and that the reading and verification of the authorization to use the service purchased, as well as the granting of the authorization, may be performed using means that are congruous with the service itself.

Furthermore, for sending the request for purchase of authorization to enter the event and for sending the authorization for admission, it is possible to use any type of telecommunications network that is currently available or will be available in the future, just as the data transmission protocols and the communication standards used in cellphone communications may be of any type available either at present or in the future.

In addition, the receiving means and the portable storage medium for storing the credit instrument may be of any type currently available or available in the future. In the abovementioned Italian application in the name of the present applicant, to which the reader is referred for further details, there is proposed a storage medium different from the ones described previously, in particular a storage medium
having the shape and the dimensions of an ordinary credit card, but capable of operating as a cellphone for making brief communications, in which transfer of small amounts of data over a short distance is made (for example from a cellphone or from a peripheral connected to a computer during storage of the authorization for admission, and from the storage medium to the electronic access gate when the entrance pass is being exhibited), with obvious advantages from the point of view of convenience of use (it could, for instance, be put in a wallet, be easily lent to another person, or transferred, etc.).
CLAIMS

1. A system for purchasing (1), via telematics, an authorization to use a service, comprising:
   - purchase-request means (4, 14) for making a request to purchase said service;
   - authorization-generation means (2) for generating an authorization to use said service of an electronic type;
   - authorization-sending means for sending said authorization, using a telecommunications network (6, 20)
   - authorization-receiving means (4, 14) for receiving said authorization through said telecommunications network (6, 20)
   - authorization-storage means (4, 8, 10, 12, 14, 16, 18) for storing said received authorization;
   - request-for-use means (8, 12, 14, 16) for making a request to use said service; and
   - authorization-for-use means (29) for authorizing use of said service;
characterized in that said purchase-request means comprise:
   - first identification-code-supplying means (4, 14) for supplying to said authorization-generating means (2) a first identification code;
in that said authorization-generating means (2) comprise:
   - first acquisition means (100) for acquiring said first identification code supplied by said first identification-code-supplying means (4, 14) at the moment of the request for purchase of the service; and
   - entry means (110) for entering said identification code in said authorization;
in that said request-for-use means comprise:
   - second identification-code-supplying means (4, 14) for supplying to said authorization-for-use means (29) a second identification code;
and in that said authorization-for-use means (29) comprise:
   - second acquisition means (140; 200; 300) for acquiring said second identification code supplied by said second identification-code-supplying means (4, 14) at the moment of
request for use of said service;
- comparing means (150; 210; 330) for comparing the first identification code contained in said stored authorization and the second identification code supplied at the moment of the request for use of said service; and
- enabling means (160; 220; 340) for enabling use of said service, should said verification yield a positive result.

2. The system for purchasing according to Claim 1, characterized in that said authorization-storage means comprise:
- a portable storage medium (8, 12, 14, 18) having an identification code of its own;
in that said first identification-code-supplying means (4, 14) supply to said authorization-generating means (2) the identification code of the storage medium (8, 12, 14, 18);
and in that said authorization-for-use means (29) comprise:
- reading means (140) for reading from said storage medium (8, 12, 14, 18) said authorization and the identification code of the storage medium (8, 12, 14, 18) itself.

3. The system for purchasing according to Claim 2, characterized in that said storage medium comprises a portable terminal (8, 14).

4. The system for purchasing according to Claim 3, characterized in that said portable terminal comprises a cellphone (8, 14).

5. The system for purchasing according to Claim 3 or Claim 4, characterized in that said identification code comprises the IMEI code of said portable terminal (8, 14).

6. The system for purchasing according to Claim 3 or Claim 4, characterized in that said identification code comprises the telephone number associated to said portable terminal (8, 14).
7. A method for purchasing, via telematics, an authorization to use a service, comprising the steps of:
   - making a request to purchase said service;
   - generating an authorization to use said service of an electronic type;
   - sending said authorization using a telecommunications network (6, 20);
   - receiving said authorization sent through said telecommunications network (6, 20);
   - storing said received authorization;
   - making a request to use said service; and
   - authorizing use of said service; characterized in that said step of making a request to purchase said service comprises the step of:
     - supplying a first identification code;
   in that said step of generating an authorization to use said service comprises the steps of:
     - acquiring said first identification code supplied at the moment of request to purchase said service; and
     - entering said first identification code in said authorization;
   in that said step of making a request to use said service comprises the step of:
     - supplying a second identification code;
   and in that said step of authorizing use of said service comprises the steps of:
     - acquiring said second identification code supplied at the moment of request to use said service;
     - comparing the first identification code contained in said stored authorization and the second identification code supplied at the moment of request to use said service; and
     - authorizing use of said service should said verification yield a positive result.

8. The method for purchasing according to Claim 7,
characterized in that said step of storing said received authorization comprises the step of:
- using a portable storage medium (8, 12, 14, 18) having a first identification code;

5 in that said step of making a request to purchase said service comprises the step of:
- supplying the identification code of said storage medium (8, 12, 14, 18);
and in that said step of authorizing use of said service comprises the step of:
- reading from said storage medium (8, 12, 14, 18) said authorization and the identification code of the storage medium (8, 12, 14, 18) itself.

9. The method for purchasing according to Claim 8, characterized in that said storage medium comprises a portable terminal (8, 14).

10. The method for purchasing according to Claim 9, characterized in that said portable terminal comprises a cellphone (8, 14).

11. The method for purchasing according to Claim 9 or Claim 10, characterized in that said identification code comprises the IMEI code of said portable terminal (8, 14).

12. The method for purchasing according to Claim 9 or Claim 10, characterized in that said identification code comprises the telephone number associated to said portable terminal (8, 14).
START

100
ACQUIRE IDENTIFICATION CODE

110
ENTER IDENTIFICATION CODE IN CREDIT INSTRUMENT

120
SEND CREDIT INSTRUMENT

130
STORE CREDIT INSTRUMENT

140
READ CREDIT INSTRUMENT AND IDENTIFICATION CODE

150
COMPARE IDENTIFICATION CODES

160
AUTHORIZE ADMISSION TO EVENT

END

Fig. 3
Fig. 4

START

1. ACQUIRE TELEPHONE NUMBER

2. ACQUIRE TELEPHONE NUMBER WITH NUMBERS STORED

3. AUTHORIZE ADMISSION TO EVENT

END

Fig. 5

START

1. ACQUIRE TELEPHONE NUMBER

2. STORE NUMBER TEMPORARILY

3. READ CREDIT INSTRUMENT

4. COMPARE TELEPHONE NUMBERS

5. AUTHORIZE ADMISSION TO EVENT