PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :		(11) International Publication Number:
H04M 17/00, H04Q 7/32	**A1**	**WO 99/13636**
		(43) International Publication Date: 18 March 1999 (18.03.99)

(21) International Application Number: PCT/GB98/02729

(22) International Filing Date: 10 September 1998 (10.09.98)

(30) Priority Data:
9719100.1 10 September 1997 (10.09.97) GB

(71) Applicant *(for all designated States except US)*: TEKTON COMMUNICATIONS LIMITED [GB/GB]; Marsh House, 500 Montagu Road, London N9 0UR (GB).

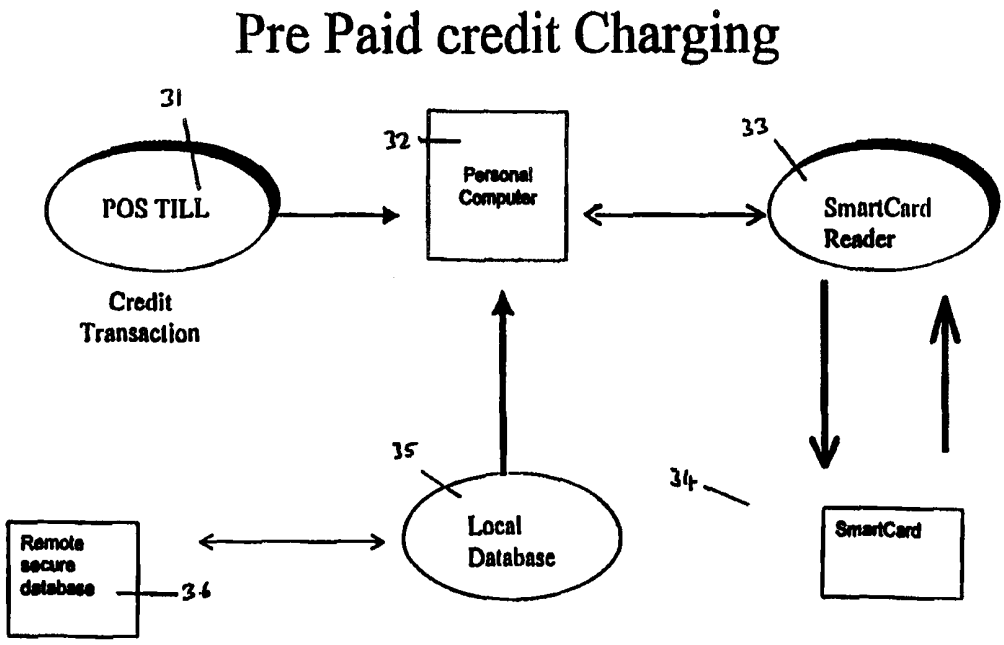
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: BISWELL, Anthony, James [GB/FR]; Villa Mas Souleou, Boulevard Plan des Abeilles, F–06230 Saint Jean Cap Ferrat (FR). CASTLE, Derek, Keith [GB/GB]; 4 Tavern Road, Wooley Bridge, Glossop, Derbyshire SK13 2RB (GB).

(74) Agent: COATES, Ian, Harold; Sommerville & Rushton, 45 Grosvenor Road, St. Albans, Herts AL1 3AW (GB).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: A PRE–PAYABLE COMMUNICATION DEVICE



(57) Abstract

A portable radio communications apparatus comprising: (i) a portable handset; (ii) a removable module comprising a rechargeable electronic purse and a subscriber identification unit; (iii) a recess in the handset adapted to accept the removable module; (iv) a reading device in the handset adapted to determine a content of the electronic purse; (v) an enabling means arranged to allow substantial operation of the communications apparatus on the basis of the content of the electronic purse; and wherein said module is adapted such that in use the communications apparatus is substantially inoperable when the module is removed.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

A Pre-payable Communication Device

Field of Invention

The present invention relates to pre-payable communication devices and more particularly to pre-payable communication devices which are suitable for use in radio communication networks.

Background to the invention

One problem with radio communication devices such as mobile telephones is that they are relatively expensive both to purchase and to run. This represents a problem both for the subscriber and for the service provider. For example, the service provider needs to rely on the creditworthiness of the mobile phone subscriber and both the service provider and the subscriber are at risk from fraudulent use of the subscriber's terminal. Many people who would otherwise benefit from the occasional use of a mobile phone are prevented from having this benefit because either the cost is too high and/or the service provider is unable to rely on their creditworthiness. For occasional users the monthly line rental charge is often prohibitively expensive.

There are many situations in which the use of conventional mobile telephones is problematic. For example, an employee may be given a mobile telephone by his employer to use only in essential circumstances. The employer would like to ensure that the employee does not run up additional costs by using the phone for personal use. However, this is difficult to do until after the event when the employer is able to check the telephone bill.

Another problem relates to the fact that in different geographic locations, different communication protocol systems are in operation. An example of a protocol system is Global system for Mobile Communications (GSM) which is a European protocol system. Typically, mobile telephone handsets are operable with only one, or perhaps two different communication protocol systems. This means that when the user

moves to a different geographical area, he may be unable to operate his mobile telephone, if the communication protocol system for that area is incompatible with his handset. This is often a problem for travellers and yet travellers often only have access to mobile communications devices and need them most when they are on the move.

Some attempts have been made to overcome these problems using SmartCard technology. A conventional SmartCard is typically a rectangular piece of plastics material, of a similar size and shape to a credit card, which contains integrated circuits, microprocessors and/or read write memory. The use of SmartCards in radio telephones is known, for example, as described in UK patent application number 2267794 in the name of Alan Kilpatrick Conroy. This application describes a pre-payable mobile cellular phone. However, the specification gives no details on how the pre-payment is achieved.

UK Patent 2266798 in the name of Motorola Inc. describes an apparatus for accepting, retaining and making electrical contact between a SmartCard and a radio telephone handset. The SmartCards used in radio telephones have been limited to subscriber identification module (SIM) cards for use in the European market. SIM cards are available in two sizes; a full size card and a chip card. SIM cards for GSM currently provide subscriber information (e.g. subscriber phone number, service provider) and plug into a GSM compatible mobile telephone handset to configure that handset for a particular subscriber. These cards only reference the subscriber data and do not include radio frequency circuitry or protocol information. If the SIM card is removed from the handset incoming calls cannot be received.

International patent application number WO/97/05729 in the name of Telecom Italia Mobile S. P. A. describes a radio mobile terminal that is provided with two SIM card readers. One of the SIM cards is described as a prepaid card and this can be loaded into the additional reader. This system is disadvantageous because the mobile

telephone handset needs to contain two SIM card readers which increases the cost and bulk of the terminal. Also the design of the handset is complex because two SIM card readers must be allowed for.

None of the above prior art provides either communications equipment or a method of operation which enables every would-be subscriber, regardless of creditworthiness to have access to a mobile phone on a pay-as-you-use basis.

It is accordingly an object of the present invention to provide a pre-payable communication device for use with radio communication networks and a method of using such equipment which overcomes or at least mitigates one or more of the problems noted above.

Summary of invention

According to the present invention, there is provided a portable radio communications apparatus comprising:

(i) a portable handset;

(ii) a removable module comprising a rechargeable electronic purse and a subscriber identification unit;

(iii) a recess in the handset adapted to accept the removable module;

(iv) a reading device in the handset adapted to determine a content of the electronic purse;

(v) an enabling means arranged to allow substantial operation of the communications apparatus on the basis of the content of the electronic purse;

and wherein said module is adapted such that in use the communications apparatus is substantially inoperable when the module is removed. This gives the advantage that every would-be subscriber, regardless of creditworthiness can have access to a mobile phone on a pay-as-you-use basis. When the module is removed from the device, the communications apparatus is inoperable which helps to prevent fraud. The subscriber

identification unit in the removable module provides "identification" for a particular subscriber, so that one subscriber can use several different handsets and configure these for his own use simply by adding the removable module. This helps subscribers when they travel between areas covered by different protocol systems. Such a traveller would be able to retain his or her removable module and simply insert this into a different handset that is operable with the new protocol system.

Preferably, the removable module comprises a SmartCard. This provides the advantage that the removable module is conveniently sized and shaped and can easily be stored and transported.

In one embodiment of the invention the subscriber identification unit comprises a conventional subscriber identification module. This provides the advantage that the subscriber identification unit can easily be obtained and is compatible with other known systems. Preferably the subscriber identification unit is adapted to be compatible with the Global System for Mobile Communications Protocol. This enables the communications apparatus to be used with a widely used European protocol system.

According to another aspect of the present invention there is provided a removable module suitable for use with a portable radio communications handset said module comprising an electronic purse and a subscriber identification unit, said module being adapted to be received in a recess in said handset, and wherein said module is adapted such that in use the handset is substantially inoperable when the module is removed from the communications apparatus. This provides the advantage that removable modules are provided which contain an electronic purse. Would-be subscribers can obtain a removable module, regardless of their creditworthiness, and use this to gain access to a mobile phone on a pay-as-you-use basis.

According to another aspect of the present invention there is provided a method of communicating using a portable radio communications apparatus said method comprising the steps of :

(i) purchasing air time from an air time provider or suitable intermediary;

(ii) charging said electronic purse with units equivalent to purchased air time;

(iii) inserting the removable module incorporating the electronic purse into the recess in the handset;

(iv) determining a content of the electronic purse;

(v) allowing substantial operation of the communications apparatus on the basis of the content of the electronic purse;

(vi) operating the communications apparatus and updating the content of the electronic purse on the basis of said operation. This provides the advantage that a service provider or air-time provider no longer needs to be responsible for the creditworthiness of all its subscribers. Individual subscribers may purchase air-time units using cash and "charge" a removable module in this way. The "charged" module can then be used to communicate using the mobile phone handset. The subscriber is then able to use the handset on a pay-as-you-use basis.

The present invention is intended to encompass both the removable module and the handset together and individually. The invention also encompasses a method for using the removable module and handset as well as a charging station for charging the removable module.

Description of the drawings

The invention will be further described, by way of example, with reference to the accompanying drawings in which:

Figure 1 is a flow diagram indicating a method of using the prepayable portable radio communications apparatus.

Figure 2 is a schematic diagram of a handset and removable module.

Figure 3 is a flow diagram showing a method of recharging a removable module.

Figure 4 is a flow diagram of actions and screen messages in a method of recharging a removable module.

Figure 5 is a flow diagram of actions and screen messages in a method of initialising a removable module.

Figure 6 is a schematic diagram of an external fraud detection system.

Figure 7 is a schematic diagram of an alternative external fraud detection system.

Description of preferred embodiments

Embodiments of the present invention are described below by way of example only. These examples represent the best ways of putting the invention into practice that are currently known to the Applicant although they are not the only ways in which this could be achieved.

Figure 2 is a schematic diagram of a portable radio communications apparatus 20 comprising a portable handset 21 and a removable module 22. The portable handset is shown as being similar to a conventional mobile telephone handset although any suitable type of handset may be used. In the example shown the handset comprises a display area 23, an aerial 24, a key pad 25 and a recess 26. The recess 26 is adapted to receive the removable module 22 as shown in figure 2. The handset may also comprise a microphone and a loudspeaker (not shown) as well as other elements typically contained in a conventional radio telephone handset. However, in one embodiment of the present invention, some components that would typically be contained in a conventional radio telephone handset are removed from the handset 21 and replaced by equivalent or alternative devices and circuitry in the removable module. This is explained further below.

The removable module 22 is shown as being generally rectangular in shape although any shape can be used. Preferably the removable module is a SmartCard and has a shape similar to that of a conventional credit card. The removable module comprises an electronic purse. The term "electronic purse" is used to refer to any form of memory that is capable of being read and updated, and which is capable of storing information about units of "air-time". Preferably, the electronic purse is rechargeable, that is once the units of "air time" that it contains have been used up, they can be replaced. However, this is not essential. The removable modules can be disposable, so that once the units are used up the module is simply replaced. Units of "air-time" are units of time for which a communications service is provided by a communications network service provider. The removable module 22 can be inserted into and removed from the recess 26 in the handset.

The removable module 22 also comprises a subscriber identification unit (not shown) which is preferably a conventional subscriber identification module (SIM). For example, the removable module 22 can be a SIM card which further comprises an electronic purse. When the removable module 22 is removed from the handset the SIM is also removed and this means that the communications apparatus 20 cannot be used to transmit or receive information. When the SIM is removed from the apparatus 20 there is no information in the handset about which subscriber is using the apparatus, for example, the user's telephone number. This means that the communications apparatus is substantially inoperable when the module is removed.

Figure 1 is a flow diagram indicating a method of using the prepayable portable radio communications apparatus. This represents one example of a method for using the prepayable portable radio communications apparatus; other methods may also be used. The user first obtains a removable module 22 and inserts this into the handset 22 and then a card validity check process 1 is carried out. The card validity check process

involves checking whether the removable module is in anyway "data corrupt" or is not in credit. The handset contains a reading device adapted to determine a content of the electronic purse and also an enabling means arranged to allow substantial operation of the communications apparatus on the basis of the content of the electronic purse. At this stage it is also possible for the subscriber to key in a personal identification number (PIN) to the key pad of the handset in order to allow use of the removable module. This provides extra security for the subscriber because it prevents unauthorised use of the removable module and/or the handset. However, use of a PIN number in this way is optional.

The next stage 2 involves a network authentication check by the airtime provider. This involves a check of the information provided in the subscriber identification unit or SIM (if a SIM is used). By making this check the service provider can help to prevent use of fraudulent removable modules. If the result of stage 2 is a "fail" i.e. the check is unsuccessful for any reason then the communications apparatus is not enabled as shown in box 3 in figure 1. That is, the enabling means prevents use of the communications apparatus. A warning message and instructions to the subscriber can be displayed on the display panel to indicate that access to the communications network by the service provider has not been granted.

If the result of stage 2 is successful then full functionality and dial facilities are granted by the service provider as indicated in box 4 of figure 1. The subscriber is then able to use the portable radio communications apparatus and as information is transmitted or received from the apparatus (indicated by box 7 in figure 1) the electronic purse is updated (as indicated by arrow 10 in figure 1). For example, as units of "air time" are used by the subscriber these are decremented from the electronic purse contents. Once the reading device determines that the electronic purse is empty the result of the airtime credit box 5 is a "fail" and the user is advised (box 6) and the

enabling device prevents use of the communications apparatus. At this point the user may remove the removable module from the handset and use a charging station to recharge the module. That is, the user may purchase more "air-time" units and store these in the electronic purse on the removable module.

This method provides the advantage that the service provider is not responsible for the creditworthiness of the subscriber. Also, the subscriber is able to use a mobile phone on a pay-as-you-use basis and is fully in control of his or her expenditure at any one time. It is not necessary for the whole mobile telephone to be configured for use specifically by one subscriber i.e. the telephone does not have to be configured for one telephone number. This is because the telephone number effectively "travels with" the subscriber within his removable module. When the subscriber moves between geographical regions over which different communications protocols are used the subscriber can simply obtain a new handset, that is preconfigured for the protocol of that area, and insert his removable module into the handset in order to configure that handset for his own personal use. For example, travellers could hire a telephone handset when they enter a new area.

The charging station comprises a recess which is able to accept a removable module and also means for entering "air-time" units onto the electronic purse on the module.

As described above, in one embodiment of the invention, some of the functionality from the handset is removed and placed onto the removable module. That is, the handset will typically contain electronic apparatus which will enable the handset to function as a radio communications apparatus when the electronic purse is "charged" and the subscriber identification unit is provided. This means that the handset is hugely more expensive relative to the removable module. However, in one embodiment of the invention, some of the functionality from the handset is removed and instead

incorporated into the removable module or SmartCard. This increases the value of the removable module relative to the handset and may also ensure that the handset will not function without the removable module. Examples of functions that could be removed from the handset include the enabling means, the reading device and other features such as circuitry for converting the speech signal from the user into digital form. These are only examples of functions that could be incorporated into the removable module. Other functions could also be incorporated by making use of conventional circuit design techniques such as would be know to the skilled person in the art.

By making the removable module more expensive with respect to the handset itself, the risk of theft of the handset is reduced and the consequences of theft of the handset are less severe.

In one example, the present invention is made available as an integral component of a customer loyalty programme. The pre-pay mobile telephone is made available to loyalty card holders as an extension of any existing loyalty scheme, on the basis of reward for tenure and spend within the loyalty scheme. Users are able to earn loyalty points on airtime and also to redeem loyalty points against purchase of airtime.

In this example of the invention, the SmartCard for use with the pre-pay mobile telephone handset is also functional as a customer loyalty card. The SmartCard contains an amount of airtime included at the time of purchase and subsequent recharging of the card is possible upon each visit to the loyalty scheme provider's premises.

A number of advantages are provided to the loyalty scheme provider including:

- provision of an "added value" service to existing customers
- ability to attract new customers
- broad customer availability - no credit rating checks
- rechargeable only at loyalty scheme provider's retail outlet

- minimal overheads and capital expenditure
- use of airtime derives gross revenues prior to month end settlement
- information about customers behaviour patterns is gained

Recharging the removable module

Figures 3 and 4 are flow diagrams which illustrate the process of recharging the removable module or SmartCard. When the user needs to recharge his or her SmartCard 34 he or she visits the loyalty provider's premises and at a point of sale till 31 carries out a credit transaction 41, 42 to pay for airtime units to be charged onto the SmartCard 34. After removal from the handset 43 the SmartCard 34 is then inserted 44, 45 into a SmartCard reader 33 that is connected to or integral with a secure personal computer 32. The personal computer 32 is connected to a local database 35 which contains information about the user's loyalty card and SmartCard 34. The local database 35 is in turn connected to a remote secure database 36.

A message 46 is displayed on the screen of the personal computer 32 which indicates the amount of pre-paid air time units that remain on the SmartCard 34. The amount of air time units that are to be credited to the card 34 is then entered onto the personal computer 46 and the personal computer updates the electronic purse in the SmartCard 34 accordingly using an encrypted transaction. The amount of units to be credited to the card can either be entered manually or can be transferred electronically from the till 31 to the computer. The updated amount of pre-paid air time units on the SmartCard 34 is displayed on the computer screen 47 and the SmartCard 34 is then returned to the user or customer 47. Finally the handset is returned to the customer 48.

The encrypted transaction involves the following steps:

1. The secure personal computer obtains secret data that is specific to the SmartCard from the SmartCard itself and/or the local and remote databases and builds an encrypted update command.

2. The software within the card deciphers the encrypted command and updates the airtime counter or electronic purse within the SmartCard.

Such an encrypted transaction is recorded by the personal computer and when a batch of such records are obtained this batch is sent to the remote secure database 36 for storage and to update that database.

Initialising the removable module

Each SmartCard contains secure key information which is stored on the card during the manufacturing process. Information about these secure keys is held on the main database 36 and is accessible by the local database 35.

When a user first obtains a removable module or SmartCard 34 this is initialised by placing the SmartCard 34 into the card reader 33. Information from the card 34 which identifies the card and provides security information (i.e. the secure key) is read by the card reader 33 and checked by the personal computer 32 using information from the local and/or remote databases 35, 36.

If this check is successful the card if authenticated 55 and a screen message asking for loyalty card details to be entered is displayed 55. The loyalty card details are entered 52 to the personal computer 32 and then the card is initialised by the personal computer 53. Details linking the loyalty card details and the secure key are stored on the local and/or remote database 35, 36 and an initial amount of airtime credit is charged to the card. The card is then removed from the reader and returned to the customer 57 in order to be inserted into the customer handset 54.

External fraud detection system

A fraud detection system is provided that is external to the handset and removable module. This is provided in addition to any fraud detection system provided by the network operator. This system monitors traffic made on the pre-paid mobile telephone network and compares this traffic against information about recharging of

SmartCards on the system. For a particular SmartCard, if more traffic is being created than is justified by the amount of credit on that SmartCard then possible fraud is identified. After checks have been made, if it is found that fraud is occurring then the SmartCard is prevented from accessing the network.

Figures 6 and 7 show two examples of an external fraud detection system. Pre-paid mobile phone handsets 62 are used to communicate over an operator or service provider's communications network 61. Each time a call is made a call detail record (CDR) is created and stored by the operator 61, as is known in the art. A call detail record contains information about the calling party, the called party, the duration of the call, the time when the call was made and other information about the call. At the end of a certain period of time, for example 12 hours, the call detail records for that 12 hour period are downloaded to database 66,71 in the fraud management system.

A SmartCard reader 64 or other removable module reader is provided that is connected to a till 63 such that the card reader 64 and till 63 are uniquely matched for security reasons. When a SmartCard or removable module is recharged using the card reader 64 and till or PC 63 information about the recharge is downloaded to a database 65, 71 in the fraud management system. Information about new users from the card initialisation process can also be downloaded. The information can be stored within the local database 35 before being downloaded in batches.

In the example shown in figure 6 the fraud detection system comprises two separate databases 65 and 66. One database 66 stores the call detail records and the other 65 stores information about credit data and new users. The information from these two databases is accessed and compared by a processor 67 in order to identify potential fraud cases. The processor 67 generates action requests and reports of fraudulent activity. These outputs can be provided directly to a human operator 69 or

can be sent to the network operator 61. Information from the databases 65, 66 and processor 67 can also be provided to the clubcard database 68.

In the example shown in figure 7 a single database 71 is used which stores information about both call detail records and credit data. The network operator 61 has access to information from this database 71 as shown in figure 7. The database 71 also comprises a processor for analysing the data and producing management reports 73. Real time access 72 to the database 71 can also be provided.

Because there is a time delay whilst data enters the database(s) 71, 65, 66 then the database may state that no credit remains on a particular SmartCard, when in fact the user has recently recharged the SmartCard. Allowance is made for this in order to avoid detecting this situation as a case of fraud. This is described below.

The processor 71, 67 in the fraud management system is arranged to detect a potential case of fraud in situations such as:

- the total number of calls made for a particular SmartCard in a predetermined period exceed a threshold level;
- the total number of units used in a single call exceed a threshold level;
- the number of calls to a free helpline number exceed a threshold level;
- calls have been made by a user who has been barred or for whom a tamper alert has been generated by "in store" card reader systems;
- if a barred type of call set up is detected such as a call transfer;
- if the number of a certain type of outbound call events generated by a user or group of users exceeds a threshold;
- if the number of inbound verses outbound call events, in a given period, by a user or group of users falls within a certain range.
- if multiple use of a handset or SmartCard is detected from CDR data; and

- if geographically improbable use of a handset or SmartCard is detected from CDR data.

The interfaces to and from the fraud management system are now described.

Interfaces

- Imports of Call Detail Records (CDR) data from the network operator are performed on either a chronological push or pull basis at intervals that are viable by the system owner.
- Imports of "credit accumulated" data are performed on either a chronological push or pull basis at intervals that are variable by the system owner.
- Import of tamper alerts or "excess credit accumulated" general action requests for termination to the network operator.
- Export of management information reports and action requests to external systems located at the operator or at the system owners premises are performed on either a chronological push or pull basis at intervals that are variable by the system owner.

The fraud detection system itself is protected from unauthorised access by Firewall Security on call External Data Communications.

Security

- The fraud detection system is protected from unauthorised access by firewall security on all external data communications.
- Physical access to the system is only possible by authorised personnel who are required to pass security vetting procedures.
- Back up of the system data is performed at regular intervals and back up data is stored at a secure off site location.

Use of handset and removable module to monitor the duration of calls

Because the CDRs are downloaded to the fraud detection system at intervals, such as 12 hourly or 2 hourly intervals, then a time window is present during which fraudulent use of "unpaid for" airtime may occur. In order to reduce this problem the handset and removable module combination is able to monitor call durations during this time window. If more than a threshold level of total call duration is exceeded during this time window than a potential fraud is detected. In this event the communications apparatus is either shut down until the time window has passed or the network operator or security staff are alerted.

This is implemented by incorporating a timer mechanism into the removable module or SmartCard. At the start of a call a pulse signal is sent from the handset to the module and this activates the timer mechanism. At the end of a call another pulse signal is sent from the handset to the module to deactivate the timer. The timer thus monitors total call duration for all calls during a time window, after which it is reset to zero. A processor in the removable module or SmartCard compares the call duration value from the timer against a predetermined threshold and if the threshold is exceeded all outgoing calls are barred for the duration of the time window.

The time window, or exclusion time is set from within the handset/SmartCard combination. At the end of this time normal outgoing call usage is restored and the process counters are reset to zero time.

If the total call duration time as monitored by the handset and module is less than the prescribed threshold then no action is taken to terminate outgoing calls.

Emulation of advice of charging signals

In the situation that no pulses or signals are provided by the network operator which contain information about the current charging rates then the handset and

SmartCard combination is able to emulate these signals. For example, this is required when charging signals are blocked, disrupted or not provided.

A timer mechanism is provided in the handset or in the removable module in order to emulate the charging signals. This timer may be the same as the timer described in the section headed "use of handset and removable module to monitor duration of calls" above. This timer mechanism is activated by signals from the handset which are provided at the start and end of a call. Information about tariff rates is stored in the handset or removable module. For example, this information can be stored in the form of a look up table. Time information from the timer mechanism is then used in conjunction with the tariff information in order to determine the cost of the call. The electronic purse is then decremented accordingly.

Other security features

- The handset is provided with two personal identification number accesses. A first PIN access allows the handset to be activated and a second provides access to sub routings which can change values such as the value of charges or amount of charge time.
- Certain types of call, such as those to 0891 numbers may simply be barred to help prevent fraud.
- A particular handset and removable module or SmartCard are electronically "locked" together during the manufacturing process so that they may only be used in conjunction with each other. This is done by storing a secure key in either or both of the handset and the removable module or SmartCard. The secure key is a cryptogram or other encrypted code. Means for checking that this secure key is present and correct are provided in the handset or removable module. Each handset and module pair is given a unique key so that they will only function fully together. The term "key" is used to refer to stored cryptograms, encoded

information and other electronic keys as well as physical apparatus which ensures that a particular handset can only be used with a module which is able to operate the key.

SmartCard

Details about the SmartCard are described below:

Functionality

The SmartCard provides the means for storing an amount of credit in agreed currencies or units of time up to predetermined maximum values, which are variable by secure communication to a SmartCard reader. The credit is debited by the operation of a mobile telephone or by a card reader in a point of sale terminal.

The SmartCard provides control over the mobile Handset functions of:

- Network authentication per the GSM protocols.
- Phone book directory per Handset implementation.
- Short message service.
- Handset welcome and permanent message display
- Confirm that the credit remaining prior to call set up is above a pre-set threshold value held on the SmartCard, and prevent call set up if below this value.
- Monitor credit remaining for a call in progress, decrement the credit at specific usage rates derived from an advice of charge, (AOC) trigger signal on the signalling channel and interrogate the tariff information stored on the SmartCard. The network operator sends out signals which provide information about the charging rate. Examples of these signals are AOC or CAI (charging advice information). Any such type of signal can be used to enable the credit to be decremented correctly.
- Monitor total duration of calls made in a period and prevent additional calls until this period is expired, excluding all zero rated calls.

- Monitor call in progress duration, provide user warning and tear down when threshold reached.
- Holding pre-determined call limits and monitoring all calls made over a given period, and of a given duration, to allow for call barring should these pre-determined thresholds be exceeded. This is described in detail in the section headed "use of handset and module to monitor the duration of calls"
- The SmartCard is able to place restrictions that allow single language selection only.
- Provide advice of charge (AOC) charging information to the handset, when AOC emulation is used in the handset firmware for those instances where AOC is not presented or supported by the network.
- The SmartCard is able to hold a secure electronic purse function that is capable of managing and controlling units of currency that are stored within it.
- The SmartCard is capable of storing loyalty or other retailer defined units as "points" which may have no monetary value placed upon them. These "points" are redeemable via the SmartCard reader as units to be used in Prepay systems.

Interfaces

- A set of interface protocols are defined for secure transactions between the Handset and the SmartCard, to prevent fraud either through spoofing, or tamper of either the Handset or the SmartCard.
- A set of interface protocols are also defined for secure transactions between the card reader and the SmartCard, to prevent fraud either through spoofing, or tamper of either the card or the card reader.

Security

- No information generated by the SmartCard to the Handset relating to prepay usage is transmitted to the network by the radio interface or by any other means.

- The SmartCard is capable of detecting unauthorised tampering and ceases to function until returned to a card reader and reactivated. For example, if the wrong personal identification number is entered three times during the card validity check process.
- The SmartCard protocols prevent no more than 3 unauthorised actions to access any secure area before complete termination of the SmartCard functions.
- A limited number of master SmartCards may be provided for use by point of sale operators, issued under strict controls in store.
- A number of secure access modules (SAM's) for use in the card readers at point of sale can be provided. A SAM is a fixed SIM which contains cryptograms for accessing the identity or secure key information from the SmartCards.

The SmartCard:

- Allows remote disablement of the Handset and SmartCard upon authenticated request by the network or by the card reader.
- Allows remote enabling of the Handset and SmartCard upon authenticated request by the network or by the card reader in combination with user PIN entry.
- Does not allow re-enablement of the SmartCard once it has been disabled.
- Allows remote individual update of the threshold values held in the SmartCard, either by the card reader or over the network.
- Does not allow manual user reset of the Advice of charge indicators via the Handset, or access to PIN2 of the handset.
- Does not suffer any electrical or physical damage if withdrawn from the Handset or Card reader, while power is applied. The SmartCard retaining unit, in one embodiment, has retaining pins that are close together. The retaining unit is specially designed such that these pins do not flex and contact each other, so creating a short circuit.

- Is delivered pre-registered with the network operator but not activated for use. Activation is only possible via the Card Reader.
- Permits Incoming calls when the credit has expired.

Standard Functions NOT required on the Card

Standard functions that are not required on the SmartCard, such as phone book options can be removed in order to make room for extra filters or algorithms for coding or decoding encrypted information.

- Phone Book Options

Form factor

- The SmartCard can be a full size SIM, mini SIM adapter based alternatives are also possible.
- The SmartCard can be delivered with a surface finish or other orientation mark to assist in identification of its correct insertion for visually impaired users.

Appearance

- The SmartCard can be capable of accepting various finishes e.g. silk screen printing for branding.
- In one embodiment each SmartCard is individually marked with a machine readable bar code and human readable serial number. Records of all SmartCard serial numbers and their distribution can then be kept.

SmartCard Reader

Functionality

The SmartCard reader:

- Allows SmartCards to be activated for first use and recharged with credit on a periodic basis. Allows SmartCards to be deactivated by the operator or automatically upon detection of tampering within the SmartCard by the SmartCard reader system.

- Allows the operator to read from a SmartCard remaining credit on a card inserted in the reader.
- Captures and temporarily stores the credit held on the card and the subscriber phone number to allow transfer to a replacement card.
- Allows transfer of credit remaining on the SmartCard to a new card or to a secure external system for point of sale transactions.
- Is intuitive to use by semiskilled checkout operators with a minimum of training, and employs the use of icons to indicate functions where possible.
- Is easily serviced by trained personnel, with a good supply of replacement parts and spares.
- The SmartCard reader allows a secure sign-on process at power on, user log on and log off. This process involves the use of master SmartCards coupled to PIN number entry.
- The SmartCard reader is capable of maintaining the system clock function to allow for daylight saving.
- The SmartCard reader is capable of recording the operator name and sign on/off date/times.
- The SmartCard reader has a supervisor login password for password administration.
- The SmartCard reader is able to hold a secure terminal key to identify each Card reader to the database to show where credit records have been generated.
- The SmartCard reader does not allow any new transactions to be made whilst, data is being transferred to the fraud detection system or remote database.
- The SmartCard reader is capable of creating batches of credit records with incrementing batch numbers.
- The SmartCard reader is capable of holding the previous 20 batches of credit records.

- Is capable of displaying simple text messages to prompt actions from operators to perform the following tasks:

    1. Authenticate new Card
    2. Apply credit to card
    3. Transfer credit between authenticated Cards
    4. Terminate Card after Credit transfer or discovery of fraudulent use.

Interfaces

- The card reader shall allow interaction to a PC or Point of Sale terminals via either a serial RS232 or other industry standard data transfer interface. The data transferred is encrypted according to a predetermined protocol.
- The card reader system allows remote polling of the system by an external data device, such as the fraud detection system, via modem dial up communications or network connection. This modem can be internal to the card reader system.
- The card reader system initiates communications with the external data device upon command by the program contained in the card reader system.
- The SmartCard reader is dismountable from a host PC if supplied as a separate unit, with minimal requirement for special tools or specialist knowledge by service personnel.
- The card reader is capable of arithmetically deriving SmartCard self identification or SRES based on algorithms held on a mini SmartCard held within the unit.
- The card reader unit is capable of supporting internal readers for plug-in SmartCards conforming to current industry standards.
- The card reader is capable of supporting a main card reader that takes full size cards. This reader has the following characteristics:
    - Push-pull reader with landing contacts;
    - MTBF of 250,000 insertion cycles (minimum);

- Interface deactivation according to ISO 7816/3;
- Active short circuit protection for the SmartCard;

- The unit is capable of supporting Industry standard protocols, for communication between the SmartCard and the reader, including Asynchronous protocols: T=0, T=1;
- The unit has sufficient memory capabilities to support the requirements of the data capture and transfer routines.
- The unit is capable of supporting Industry standard programming languages that are downloadable over an RS232 interface.
- The card reader system is capable of supporting common point of sale (POS) protocols to accept data transfer from POS systems to allow for updating of the values to the SmartCard.

Security

- The SmartCard reader communications with any external data device are encrypted.
- The SmartCard reader is capable of providing PIN controlled access to all of its functionality including initial access to the screen prompts prior to any form of authentication or credit related actions.
- The SmartCard reader protocols allow no more than 3 unauthorised actions to access any secure area before complete termination of the SmartCard functions.
- The SmartCard reader can detect unauthorised tampering of the SmartCard and causes the SmartCard to cease to function, in this situation.
- The SmartCard reader system software is protected from unauthorised access by either the use of PIN protection only or by the use of PIN protection and a system specific mini SmartCard being read before access to the program is granted.
- Data held on the card reader system is only transferable to other systems or devices upon the entry of security codes or devices as described previously.

Form factor

- The SmartCard reader is capable of accepting full size SmartCards and/or mini SIM's held within full size card adapters.
- Secondary card readers are provided to accept mini SIM
- The SmartCard reader has an integral display capable of displaying either text or Icons to prompt the operator.
- The SmartCard reader is of a compact size, suitable for co-location with a POS terminal or PC on a customer services desk within a retail store.
- If the SmartCard reader system consists of a PC and card reader, the overall footprint (or size of the system on the desk) does not exceed that of a standard desktop PC. Any screen used in this configuration is not larger than 12" and ideally forms a single unit with the card reader and processor.

Environmental

- The SmartCard reader system supports dual voltage input and is suitable for installation in a number of European countries, with conformance to all relevant environmental requirements e.g. EMC, Noise, Operator ergonomics etc.
- The unit is capable of being hard wired to power supply units (including UPS systems)
- All data, power, telephony communications, and internal SAM connections are capable of being secured in place to prevent unauthorised disconnection of any service.
- The unit can have battery back-up capabilities.

Handset

Functionality

The Handsets used in this project provide the following functionality:

- Be driven by a SmartCard developed for the Handset so as to provide feedback to a user of the service of the credit remaining on the SmartCard, via the Handset display.
- The Handset display shows the amount of credit available at the start of each call, the end of each call, and by quick access via a hot key sequence. This display is in minutes, viz "Time remaining =? Minutes".
- The Handset is capable of emulating AOC information when none is presented by the network for reference by the SmartCard for charging information purposes.
- Allow calls to predefined numbers held on the card, eg Emergency services and help line number(s) without debiting the credit on the card. The help line number(s) may be allowed a pre-set number of transactions per period at which point additional use is denied until the period is expired.
- The extended menu option which gives access to PIN2 is set to the "OFF" position.
- Allow remote enabling of the Handset and SmartCard upon authenticated request by the network, in combination with user PIN entry.
- Allow remote individual update to the threshold values held in the SmartCard over the network.
- Provide speed dial access to the network operator's voice mail system.
- Call waiting, call swap (in which a call is transferred to another number) and call hold are allowed as long as any outbound call in progress continues to decrement the credit on the SmartCard. The SmartCard allows the barring of calls by Calling Party Category (CPC).

- The Handset does not allow manual user reset of the Advice of charge indicators via the Handset, or access to PIN2.
- Roaming is not allowed by the Handset.
- The language default, ie the ability to access other network providers original is set to "English".
- The display is capable of displaying an alternating message in the style of "Emergency/Helpline Calls ONLY" and "Operator Name" when credit has expired.
- The display is capable of displaying the operator PLMN code rather than the operator name.
- Line 2 (ie a second line in a call swap) is not supported by the Handset.
- The Handset has the menu functions and associated GSM instruction sets removed or deleted, prior to despatch, for the following call types and menus:
    - Call Transfer;
    - Call forwarding (except Voice Mail);
    - Conference/Multiparty call set up;
    - Roaming facilities;
    - Restricted Dial lists;
    - Sub menu "Bar all incoming calls when roaming";
    - Call divert and sub menus;
    - Select phone line;
    - Call Charge settings;
- The purpose of this is to reduce fraud and costs. Also the space in the Handset that is otherwise used for these functions can be used for other things.
- In addition, the following call types and menus are removed because they cannot be provided by the pre-paid mobile phone system.
    - Change Greeting;

- All access to SIM memory for:
  - SMS;
  - Phonebook;
  - Capacity add or delete;
  - Copy functions;
  - One touch dialling;
  - Fixed Dialling;
  - Phone Status;
  - Network Selection;
  - Call Meters;

Also:

- The Master Reset or Clear functions are not able to reset or enable any features barred from use.
- Emergency 999/112 calls are allowed without a SmartCard being inserted into the Handset or when credit has expired.
- The Handset is capable of providing a user configurable decrement warning to indicate unit usage, in both visual and audible formats.
- The Handset is capable of providing a "Credit nearing expiry, please recharge" warning to the user in both visual and audible formats.
- The Handset is capable of providing a user warning and also of "tearing down the call" when credit is expired or when a threshold configurable via the card reader or over the radio interface is reached.
- The Handset is capable of providing a "Credit expired, please recharge", warning to the user in both visual and audible formats, and prevent call set up being activated except for emergency and helpline calls.

- The Handset supports voice calls and the Short Message Service. It supports restricted dialling, phone book, and diverts to voice mail.
- The default Caller line Identifier condition is set to "Present".
- The Handset is capable of being locked to a single network operator and to the SmartCard. These locks are not user addressable under any circumstances.
- The Handset has good standby battery life, in excess of 40 hours and talk time in excess of 90 minutes.
- The Handset supports one number dialling to the network voice mail service.
- The Handset display is easy to read and supports icons as well as text.
- The Handset is capable of supporting calls to pre-determined help line numbers on a toll free basis.
- The Handset manufacturer is able to unlock a SmartCard from its Handset in the repair centre. This is necessary if, for example, the Handset breaks when there is a large amount of credit on the SmartCard.
- The Handset permits Incoming calls when credit has expired.

Interfaces

- The Handset user interface is intuitive to the novice user and presents information in a logical and clear fashion. The use of multiple level menu access for the most common activities is avoided. Integral context sensitive user help is desirable.
- The Handset can support interfaces to data cards for connection from modem or laptop for example, and may have a connection for external power supplies.
- The Handset supports full size SIM cards and ideally contains a SIM release mechanism such that the user does not need to disassemble the Handset or battery to remove the SIM for recharging.
- The SIM does not suffer any harm due to withdrawal of the SIM while the Handset is switched on.

- The SIM to Handset interface supports insertion of the card with a duty cycle in excess of 5000 insertions before any degradation of the interface to the SIM is observed.

Security

- The Handset allows the suppression of access to PIN2 and other Handset menu functions by means of instruction from the SmartCard.
- The access control features are not addressable by the user from the Handset user interface, except for PIN1.
- The Handset has intrinsically good security to prevent unauthorised access to the data transfer between the SmartCard and the Handset.
- The physical design of the Handset is arranged to deter tamper or access to the contacts of the SIM. Ideally any attempt at access to the interior of the Handset leads to the destruction of the Handset.
- Preferably SIM card extenders which enable manipulation of a SIM card by keeping it outside the Handset cannot be with the Handset, when in operation.

Form factor

- The Handset supports full size SIM cards.
- The Handset is of a compact design and subject to evaluation on the basis of appearance, layout, clarity of markings, innovative features, user friendliness, audio quality etc.
- The Handset is of robust construction and provides good ergonomic operation to the user both in call set up and during a call.

Environmental

The Handset is capable of being marked with branding marks, on the front or on the keypad cover as appropriate.

Accessories

- A full range of accessories including car kits, desk top chargers, desktop hands free kits, data cards (if appropriate) and a range of battery options, can be used with the Handset.
- The Handset is supported by a manufacturer's User Guide, Frequently asked Question and Answer sheets.

Operational requirements

- The network supports advice of charge (AOC) or other suitable systems which can be used to decrement credit held on the prepay SmartCards.
- The network is capable of setting the AOC decrement interval to 10 seconds at delivery and can allow this interval to be configurable over the radio interface to the Handset.
- The network supports remote enabling and disabling of the Handset and SmartCard via authenticated request by the network to the Handset in combination with user PIN entry.
- The network is capable of monitoring the destinations of calls initiated and restrict calls to predefined destinations by National Number Group.
- The network is capable of barring all calls to premium or international destinations.
- The network is capable of preventing call transfer, call forwarding (except to voice mail), conference calls or any non standard or basic call types from being initiated.

The network is capable of allowing Data calls and Short Message Service (SMS) calls on the basis that these are charged at the same rate as voice calls. If this is not possible inbound data and SMS calls only are allowed. The network should be capable of barring these outbound calls if charging on the above basis is not possible.

Rating and tariff requirements

- A tariff or look up table to be stored in the SmartCard to generate AOC information to the Handset on the basis of flat rate charging is required from the operator.
- The network operator provides the facility to zero rate calls to specified numbers such as helpdesk numbers and emergency calls.
- Over time other tariffs may be introduced, and the network operator is able to support the introduction of new tariff plans via AOC in reasonable time scales.
- Call Detail Records (CDR) produced within the network by use of the present invention are segregated from the operator's other traffic and moved to a secure area for export to the fraud detection system. The frequency of the collation and export of the CDR data shall not exceed 12 hours and may be as frequent as hourly.

Claims

1. A portable radio communications apparatus comprising:

(i) a portable handset;

(ii) a removable module comprising a rechargeable electronic purse and a subscriber identification unit;

(iii) a recess in the handset adapted to accept the removable module;

(iv) a reading device in the handset adapted to determine a content of the electronic purse;

(v) an enabling means arranged to allow substantial operation of the communications apparatus on the basis of the content of the electronic purse;

and wherein said module is adapted such that in use the communications apparatus is substantially inoperable when the module is removed.

2. A portable radio communications apparatus as claimed in claim 1 wherein the removable module comprises a SmartCard.

3. A portable radio communications apparatus as claimed in claim 1 or claim 2 wherein the subscriber identification unit comprises a conventional subscriber identification module.

4. A portable radio communications apparatus as claimed in any preceding claim wherein said handset and said removable module are electronically locked such that a particular handset and module pair only function fully together.

5. A portable radio communications apparatus as claimed in claim 4 wherein said handset and said removable module contain information about a secure key that is unique to a particular handset and removable module pair.

6. A portable radio communications apparatus as claimed in any preceding claim which further comprises a timer mechanism adapted to monitor call duration, said timer

mechanism being adapted to be activated by signals from the handset at the start of a call.

7. A portable radio communications apparatus as claimed in claim 6 which further comprises a store of information about costs and a processor adapted to decrement the electronic purse on the basis of the cost information and the monitored call duration.

8. A portable radio communications apparatus as claimed in claim 6 which further comprises a processor adapted to compare the monitored call duration with a prespecified threshold value and to bar outgoing calls in the event that the threshold value is exceeded.

9. A communications network comprising at least one portable radio communications apparatus as claimed in any preceding claim.

10. A communications network as claimed in claim 9 comprising a fraud detection system, said fraud detection system comprising database means for storing information about calls made from the handset over the communications network, and information concerning the number of airtime units credited to the electronic purse associated with said portable radio communications apparatus.

11. A communications network as claimed in claim 10 wherein said fraud detection system further comprises a processor adapted to compare the information about calls and the information about electronic purse contents.

12. A removable module suitable for use with a portable radio communications handset said module comprising a rechargeable electronic purse and a subscriber identification unit, said module being adapted to be received in a recess in said handset, and wherein said module is adapted such that in use the handset is substantially inoperable when the module is removed from the communications apparatus.

13. A removable module as claimed in claim 12 which contains information about a secure key that is unique to the particular removable module and its handset pair.

14. A removable module as claimed in claim 12 or claim 13 which comprises a timer mechanism adapted to monitor call duration said timer mechanism being adapted to be activated by signals from the handset at the start of a call.

15. A removable module as claimed in any of claims 12 to claim 14 which further comprises a store of information about costs and a processor adapted to decrement the electronic purse on the basis of the cost information and the monitored call duration.

16. A removable module as claimed in any of claims 12 to claim 15 which further comprises a processor adapted to compare the monitored call duration with a prespecified threshold value and to bar outgoing calls in the event that the threshold value is exceeded.

17. A recharging system adapted to recharge an electronic purse of a removable module as claimed in any of claims 12 to 16.

18. A recharging system as claimed in claim 17 comprising a reader adapted to read the contents of the electronic purse and means for sending an encrypted update message to the removable module in order to update the electronic purse.

19. A recharging system as claimed in claim 17 or claim 18 comprising at least one database of stored subscriber information and means for comparing the subscriber identification unit with said stored information.

20. A recharging system as claimed in claim 19 comprising at least one local database and at least one remote database.

21. A recharging system as claimed in any of claims 17 to 20 wherein said reader and means for sending an encrypted update message to the removable module are connected to a point of sale apparatus.

22. A recharging system as claimed in claim 21 wherein said reader and said means for sending an encrypted update message to the removable module are electronically locked to the point of sale apparatus.

23. A portable radio communications handset adapted for use with a removable module as claimed in any of claims 12 to 16, said handset comprising a recess adapted to accept the removable module; and a reading device adapted to determine a content of an electronic purse in the removable module.

24. A portable radio communications handset as claimed in claim 23 wherein said handset is adapted to send a signal to the removable module at the start and end of a call.

25. A portable radio communications handset as claimed in claim 23 or claim 24 wherein said handset contains information about a secure key that is unique to the particular handset and its removable module pair.

26. A method of communicating using a portable radio communications apparatus as claimed in any of claims 1 to 8 said method comprising the steps of :

(i) purchasing air time from an air time provider or suitable intermediary;

(ii) charging said electronic purse with units equivalent to purchased air time;

(iii) inserting the removable module incorporating the electronic purse into the recess in the handset;

(iv) determining a content of the electronic purse;

(v) allowing substantial operation of the communications apparatus on the basis of the content of the electronic purse;

(vi) operating the communications apparatus and updating the content of the electronic purse on the basis of said operation.

27. A method as claimed in claim 26 wherein said step of updating the content of the electronic purse involves transmission of encrypted messages between the handset and removable module.

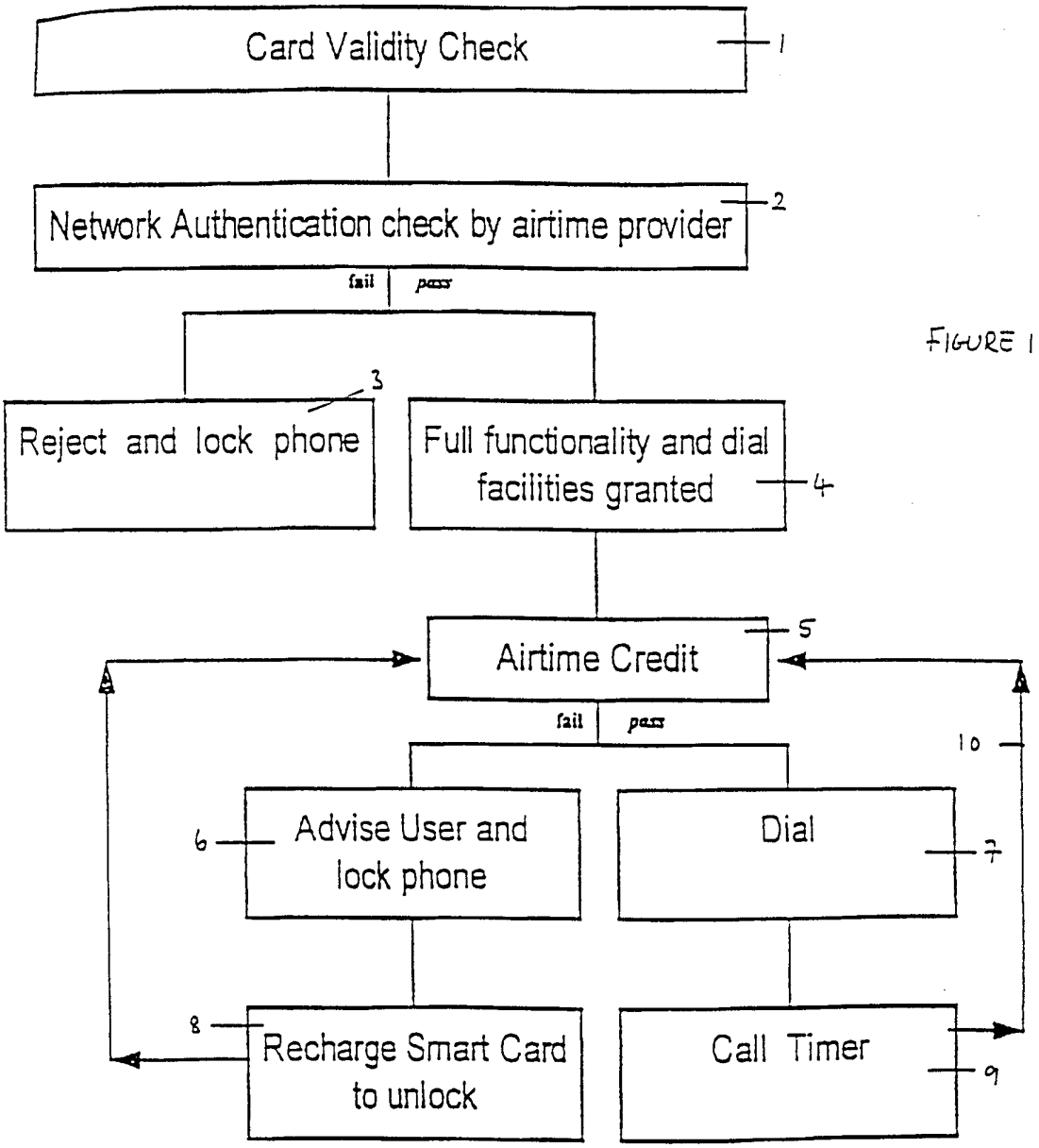

Card Validity Check
1
Network Authentication check by airtime provider
2
fail
pass
3
Reject and lock phone
Full functionality and dial facilities granted
4
Airtime Credit
5
fail
pass
10
6
Advise User and lock phone
Dial
7
8
Recharge Smart Card to unlock
Call Timer
9

FIGURE 1

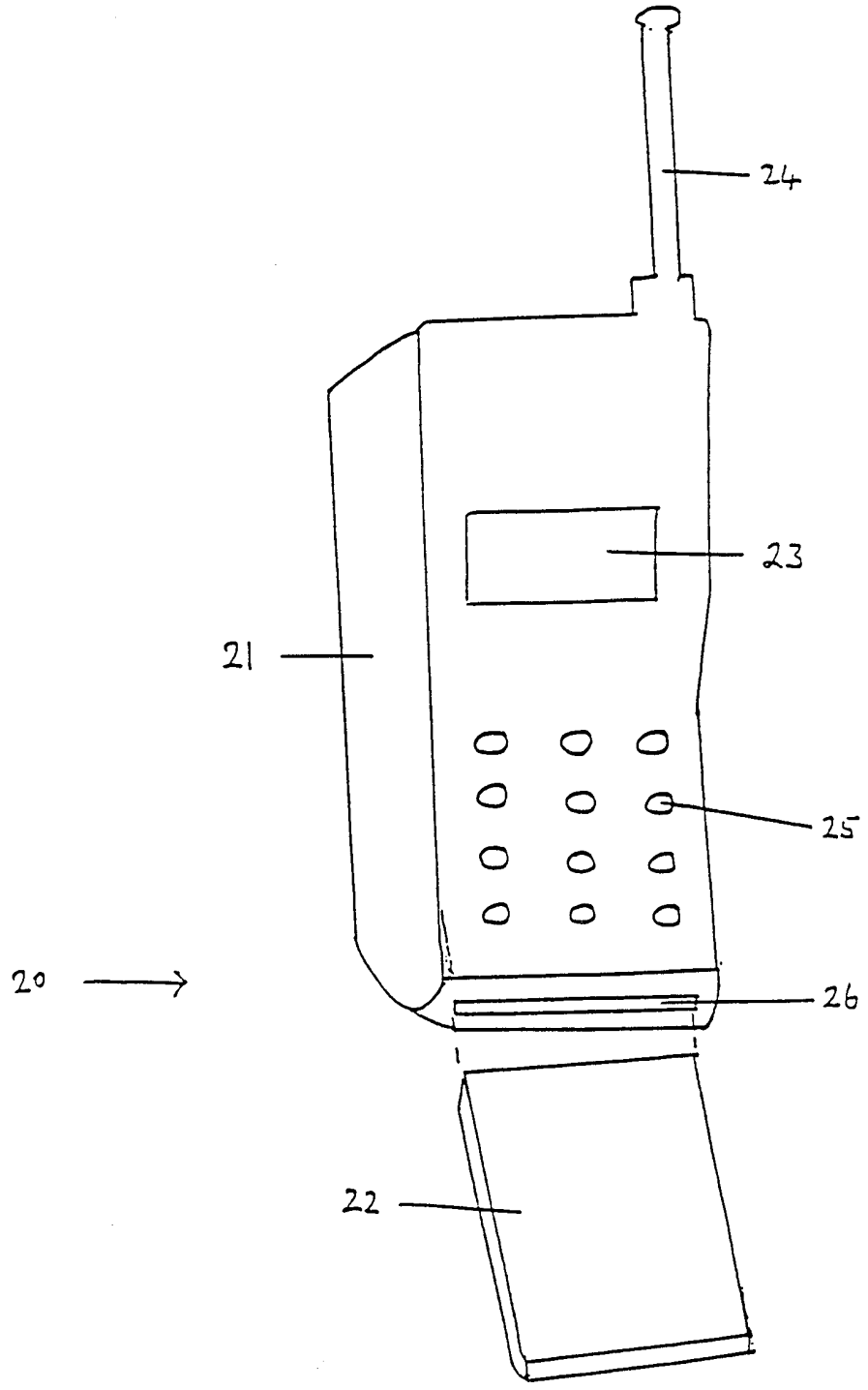


FIGURE 2

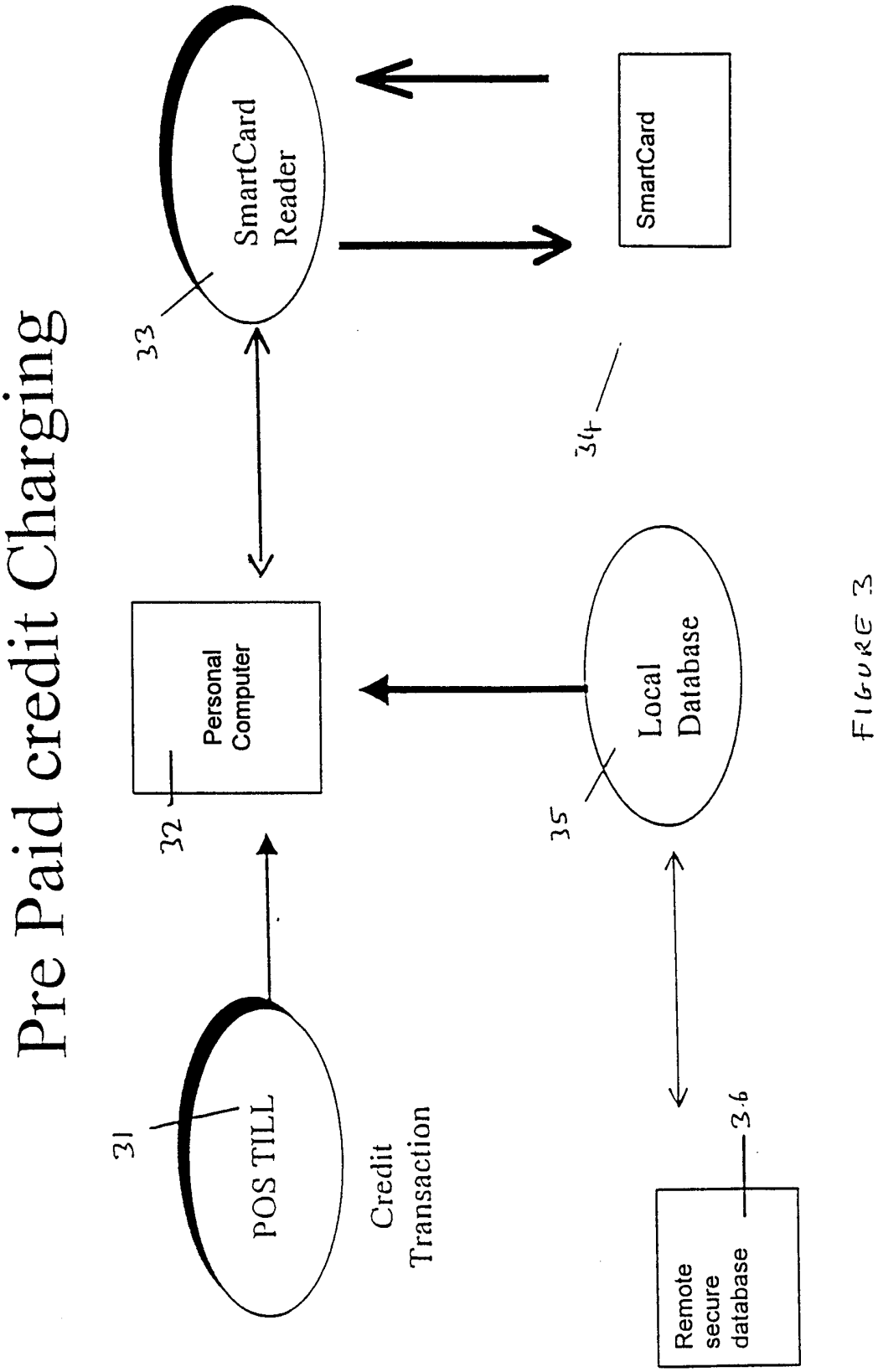

Pre Paid credit Charging
SmartCard Reader
33
SmartCard
34
Personal Computer
32
Local Database
35
POS TILL
31
Credit Transaction
Remote secure database
36

FIGURE 3

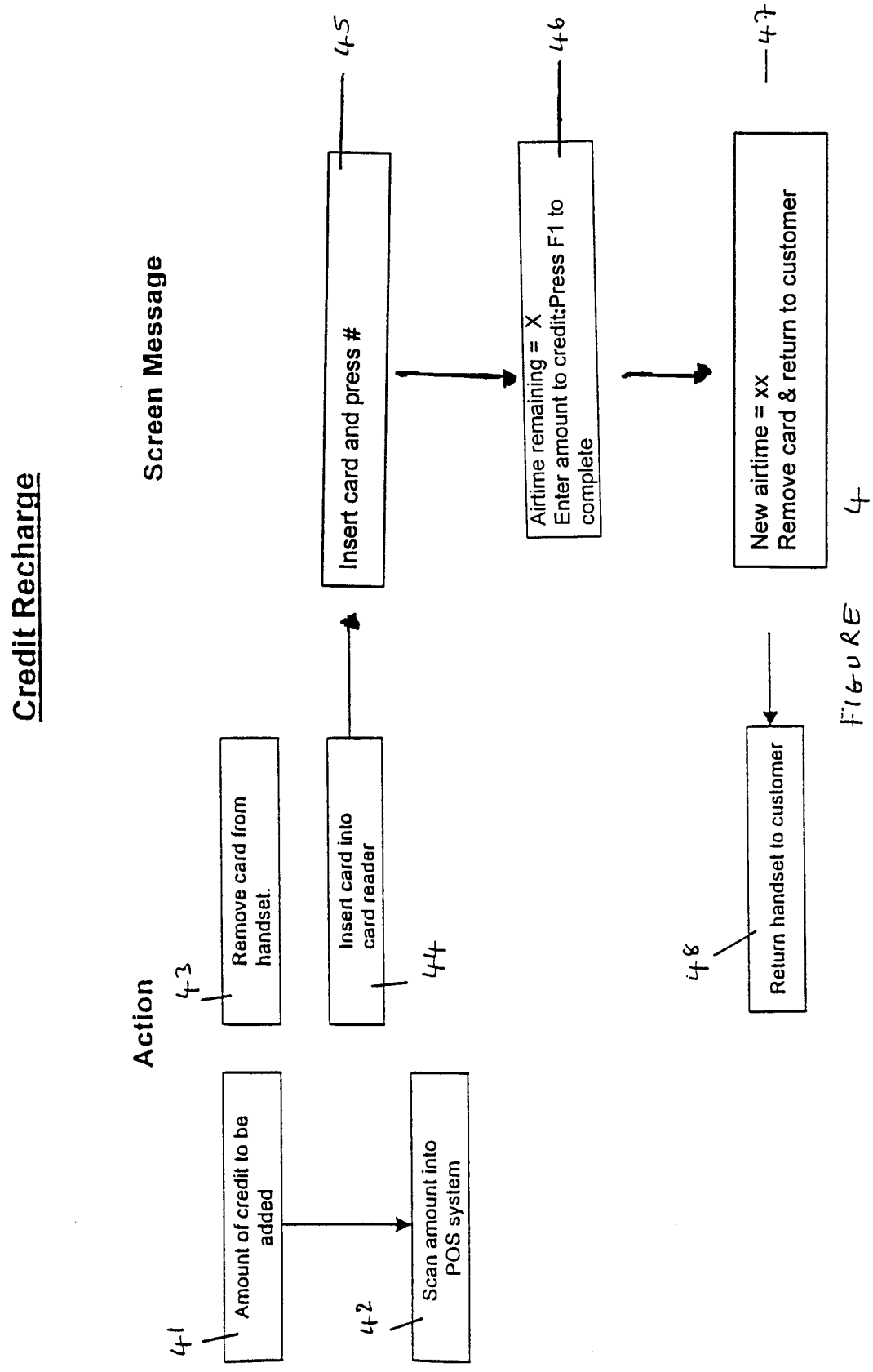

Credit Recharge
Action
Screen Message
Amount of credit to be added
41
Scan amount into POS system
42
Remove card from handset.
43
Insert card into card reader
44
Insert card and press #
45
Airtime remaining = X
Enter amount to credit:Press F1 to complete
46
New airtime = xx
Remove card & return to customer
47
Return handset to customer
48

FIGURE 4

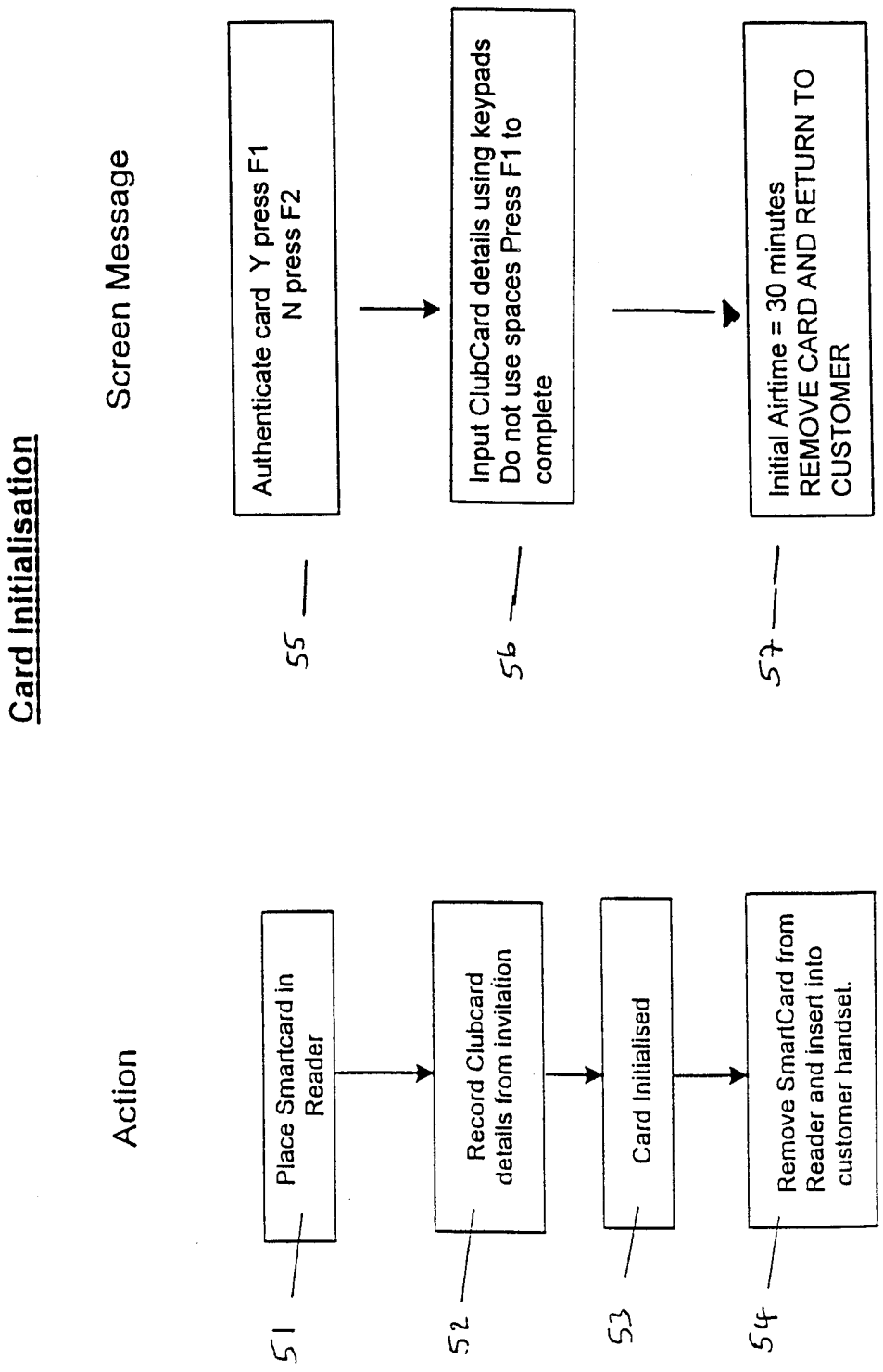

Card Initialisation
Action
Screen Message
Place Smartcard in Reader
Record Clubcard details from invitation
Card Initialised
Remove SmartCard from Reader and insert into customer handset.
Authenticate card Y press F1
N press F2
Input ClubCard details using keypads
Do not use spaces Press F1 to complete
Initial Airtime = 30 minutes
REMOVE CARD AND RETURN TO CUSTOMER
51
52
53
54
55
56
57

Figure 5

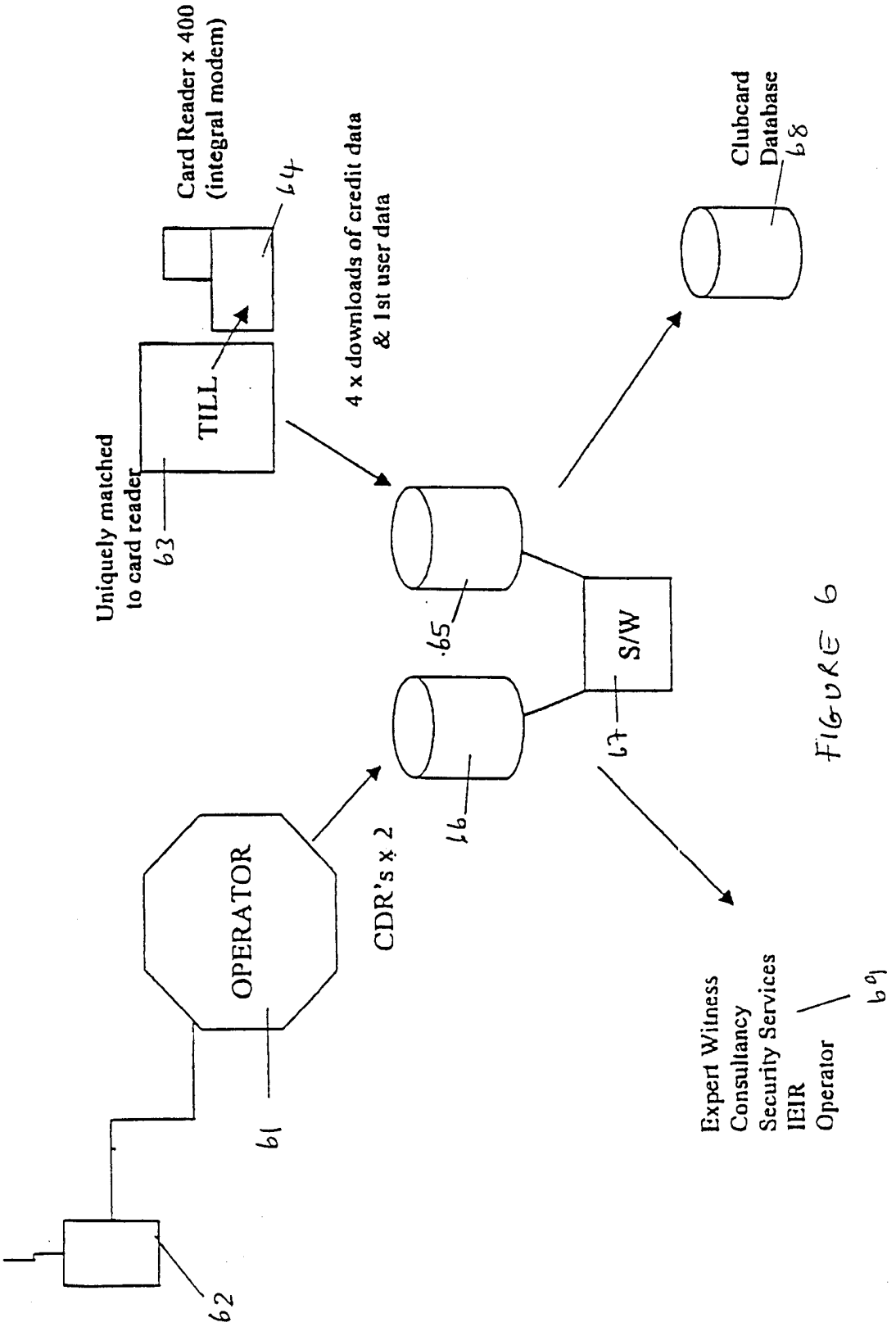

Card Reader x 400
(integral modem)
64
Clubcard
Database
68
4 x downloads of credit data
& 1st user data
TILL
Uniquely matched
to card reader
63
65
S/W
67
OPERATOR
CDR's x 2
66
Expert Witness
Consultancy
Security Services
IEIR
Operator
69
61
62

FIGURE 6

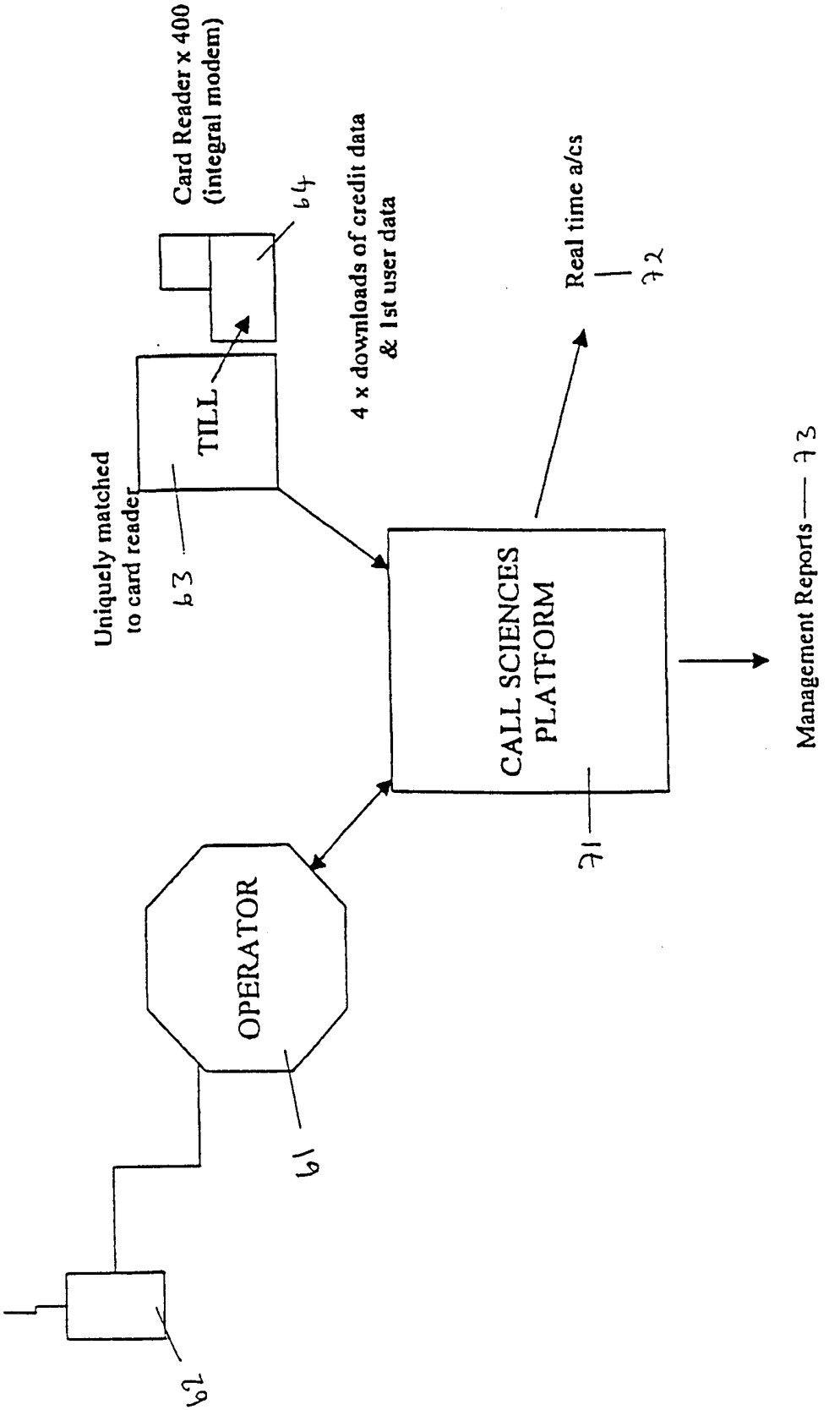

Card Reader x 400
(integral modem)
64
4 x downloads of credit data
& 1st user data
Real time a/cs
72
TILL
Uniquely matched
to card reader
63
CALL SCIENCES
PLATFORM
Management Reports
73
OPERATOR
61
71
62

FIGURE 7

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/GB 98/02729

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04M17/00 H04Q7/32

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 H04M H04Q

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.
X	EP 0 790 587 A (PHILIPS ELECTRONICS NV) 20 August 1997	1-3,6-9, 12, 14-17, 23,24, 26,27
A	see column 3, line 26 - column 4, line 21	10
X	WO 95 28062 A (NOKIA TELECOMMUNICATIONS OY) 19 October 1995	1-3,6-9, 12, 14-17, 23,24,26
	see page 3, line 1 - page 4, line 5 see page 8, line 24 - page 10, line 3 see page 11, line 35 - page 13, line 16	
	-/--	

[X] 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
16 December 1998	29/12/1998

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	Neves Appelt, D

1

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

INTERNATIONAL SEARCH REPORT

Inter onal Application No
PCT/GB 98/02729

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	GB 2 308 528 A (KARAGOEZLUE IBRAHIM MURAT ;RAMIS HARRY (GB)) 25 June 1997 see abstract see page 4, line 1 - page 6, line 27 see page 11, line 26 - page 12, line 22 see page 14	1-9, 12-17, 23-27
A	US 5 577 109 A (STIMSON CHARLES J ET AL) 19 November 1996 see column 1, line 59 - column 3, line 6	17-22
A	GB 2 267 794 A (CONROY ALAN KILPATRICK) 15 December 1993 cited in the application see page 3	1,2,5,9, 12,13, 17,23, 25,26
A	WO 97 05729 A (TELECOM ITALIA MOBILE S P A ;SENTINELLI MAURO (IT)) 13 February 1997 cited in the application see page 6 - page 7	1-3,6,7, 9,12,14, 15,23,26

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte[illegible]onal Application No
PCT/GB 98/02729

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0790587 A	20-08-1997	FR 2744822 A	14-08-1997
		CN 1168609 A	24-12-1997
		JP 9233541 A	05-09-1997
WO 9528062 A	19-10-1995	AU 691604 B	21-05-1998
		AU 2216795 A	30-10-1995
		CN 1151240 A	04-06-1997
		EP 0754394 A	22-01-1997
		FI 963996 A	05-12-1996
		JP 10501931 T	17-02-1998
		US 5748720 A	05-05-1998
GB 2308528 A	25-06-1997	NONE	
US 5577109 A	19-11-1996	US 5511114 A	23-04-1996
		AU 2770795 A	04-01-1996
		CA 2192310 A	14-12-1995
		WO 9534161 A	14-12-1995
		US 5721768 A	24-02-1998
GB 2267794 A	15-12-1993	NONE	
WO 9705729 A	13-02-1997	IT RM950521 A	27-01-1997
		AU 6667896 A	26-02-1997
		CA 2227340 A	13-02-1997
		CN 1192308 A	02-09-1998
		CZ 9800233 A	15-07-1998
		EP 0840973 A	13-05-1998
		NO 980341 A	26-03-1998
		PL 324646 A	08-06-1998