PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07F 7/08

A2

(11) International Publication Number: WO 96/36025

(43) International Publication Date: 14 November 1996 (14.11.96)

(21) International Application Number: PCT/GB96/01104

(22) International Filing Date: 9 May 1996 (09.05.96)

(30) Priority Data:
9509582.4 11 May 1995 (11.05.95) GB

(71) Applicant *(for all designated States except US)*: NATIONAL WESTMINSTER BANK PLC [GB/GB]; 41 Lothbury, London EC2P 2BP (GB).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: EVERETT, David, Barrington [GB/GB]; 31 Ashdown Avenue, Brighton, East Sussex BN2 8AH (GB). VINER, John [GB/GB]; Hydes, Woodlands Lane, Wyndlesham, Surrey GU20 6AN (GB). BAILEY, Alan [GB/GB]; 24 Worcester Road, Sutton, Surrey SM2 6PG (GB).

(74) Agent: BOYDELL, John, Christopher; Stevens, Hewlett & Perkins, 1 Serjeants' Inn, Fleet Street, London EC4Y 1LL (GB).

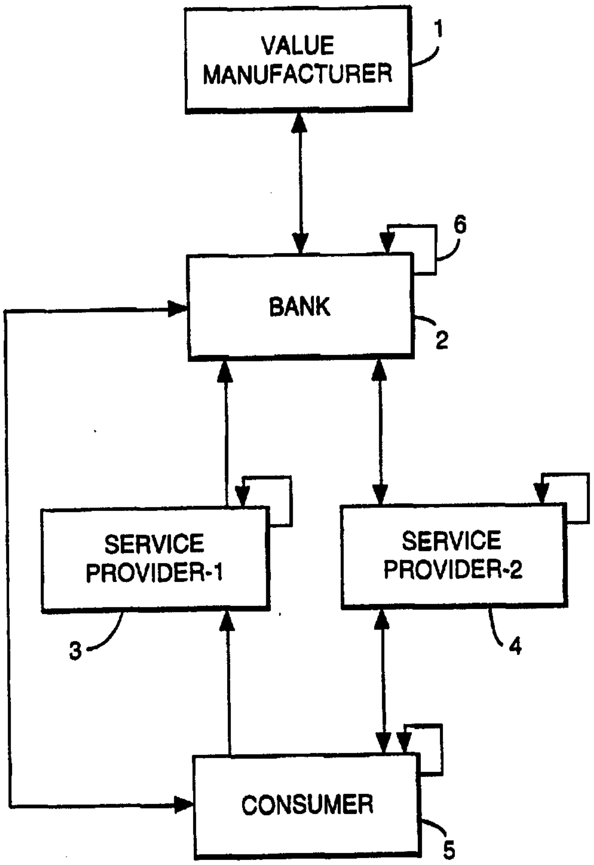
(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG),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

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: VALUE TRANSFER SYSTEM

(57) Abstract

The invention is concerned with systems for transferring value between electronic purses, usually in the form of IC or "Smart" cards, via the intermediary of an interface device. In order to control the flow of value between purses a hierarchical class structure is proposed. This is achieved by assigning to each purse a class which controls the conditions under which value may be transferred to an from (mainly from) a purse. Thus each purse stores in memory a representation of its own class, together with a list of those classes to which the purse can transfer value.



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.

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

"VALUE TRANSFER SYSTEM"

This invention relates to value transfer systems for transferring financial value between electronic purses which are carried by purse carrier devices.

A purse carrier device refers to any device which carries an electronic purse. In the short to medium term the purse carrier device will be a smart card, and this implementation will be assumed through- out the present specification for convenience. However, in the longer term other implementations are envisaged (the main requirement being tamper resistance) and the present invention is not limited to the smart card option.

Smart cards, also known as IC (integrated circuit) cards, are small plastics cards similar to the well known credit and debit cards but which contain some computing capacity in the form of an IC microprocessor. The smart card includes some form of memory, usually built in to the microprocessor itself. The memory may be of two types: volatile, and non-volatile. The typical smart card will possess both types of memory.

A value transfer system of the type with which the present invention is concerned is described for example in patent application WO 91/16691. This patent application describes a system which provides for the transfer of value equivalent to cash between two smart cards via an interface device, for example in the form of a point of sale device including at least card readers. In this way, goods and services can be paid for in an analogous manner to cash - i.e. without specific reconciliation between the payer and payee accounts.

In broad terms, the basic system with which the present invention is concerned comprises a plurality of electronic purses and interface devices by which purses may communicate with one another by means of transactions, each of which involves an exchange of electric signals between a pair of purses, one acting as a payer purse and one as a payee purse, said signals being operable to transfer financial value from the payer purse to the payee purse.

Each purse comprises a data area and a computer program for carrying out the purse functions, both being stored in memory within the smart card. The data area contains, amongst other things, a record of the accumulated value currently contained within the purse. That part of the data area of the purse which holds the accumulated value is known as a pocket. A purse may have several pockets, each storing value in a different currency. Unused pockets can contain zero value, or be unassigned within the program. For the purpose of the present specification, it is assumed that the smart card and the purse are effectively the same entity; however, it is possible for a single smart card to carry multiple purses and/or to additionally carry programs for performing other functions not connected with the transfer of electronic cash.

In the present invention, means are provided for more closely controlling the transfer of financial value from one purse to another. It is not at present envisaged that any control needs to be placed on the receipt of value by a purse (although this could change), but there is a need to control the issuance of value by a purse.

To effect this, in accordance with the present invention, each purse is assigned a class in a hierarchical structure, and a record of the class - for example in the form of a number - is stored in the data area of the purse. Also stored in the data area of the purse is a class list, which is a list of those classes to which the purse can transfer value. In a purse which supports more than one currency, there is a class list for each currency. Thus, each purse is assigned a single purse class and includes within its memory one or more purse class lists depending upon the number of currencies supported.

It has already been mentioned that the transfer of value between purses proceeds by exchange of electric signals between the two, via the intermediary of an interface device. As explained in some detail in the aforementioned WO 91/16691, the actual transfer is preceded by exchange of various check signals in the form of commands and responses issued by the two purses and by the interface device.

In the present invention these checks additionally include a check on whether the purse class of the payee purse appears in the class list of the payer purse before allowing the transfer to proceed. This can be achieved by passing the purse class of the payee purse via the interface device to the payer purse which latter uses its computing capacity to carry out the necessary check. Integrity is maintained by protecting the purse class cryptographically before it is passed out of the purse to which it belongs. Detail of typical cryptographic methods are described in WO 91/16691; for example, the record of the purse class may be stored in that part of the purse which is signed by the global secret key. However, the mechanism does not depend on any particular cryptographic implementation. It requires only that the payer purse can verify the integrity and authenticity of the purse class it has been sent. In practice, purse class is only one of a number of data items which are protected in this way during a value transfer.

The mechanism has the following benefits:

a. Purse class provides a security and control mechanism, which enables exposure to be limited in a flexible manner, by control of the types of purse to which a given purse can transfer value. For example, this enables purse issuers to limit the opportunities for realising value in a stolen purse by constraining the types of purses it can pay.

b. Purse classes should be considered as forming a hierarchy composed of at least the following major groupings: consumer, service provider, bank, value manufacturer. The ascending hierarchy would typically be associated with an ascending set of value limits. The position in the hierarchy reflects the likely importance of the purse in value terms, and relates to the care which should be exercised in its control.

c. The variability of purse class list by currency enhances the flexibility to control value transfer. Different rules can be supported for different currencies if this is appropriate from a business point of view.

d. The use of purse class category (for example, consumer, service provider, bank) is useful in conjunction with other control measures. For example, in some remote payment scenarios it is vital to know that payment is being made to a bank purse, and not to any other. This can be achieved by verifying the cryptographically protected payee purse class sent from the remote purse.

In this example, four major purse groupings are identified and can be placed in hierarchy order as follows:

Value manufacturer
Bank
Service Provider
Consumer

The Value manufacturer, sometimes known as the originator, is the central bank or equivalent in the country concerned which is responsible for minting and issuing cash. The value manufacturer is at the top of the hierarchy. A service provider is an entity that provides goods or services or equivalent - for example a point of sale device in a shop or garage. The bank and consumer groupings are self-explanatory. Each grouping is given an identifying code, for example a number, which is stored in the purse memory as will be described in more detail below. For example, the following purse class category values will be used herein:

1. Value manufacturer
2. Bank
3. Service Provider
4. Consumer

In an embodiment of the invention, a subset of purse classes, at least one from each of the above groupings, is globally defined to support interworking between groupings (for example, a purse provider must know what minimum set of classes he should allocate in the purse class list for consumer cards, so that they are certain to be able to interwork with service provider and bank purses). Consideration of practical operational scenarios suggests that at least four service provider, three bank, and two consumer purse classes and a single value manufacturer purse class are required. These "global purse classes" may for example be represented symbolically as:

Value manufacturer-1
Bank-1, Bank-2, Bank-3
Service-Provider-1, Service-Provider-2,
Service-Provider-3, Service-Provider-4
Consumer-1, Consumer-2

The following table thus summarises the global purse classes:

Name	Purse class category	Purse class number
Value manufacturer-1	1	1
Bank-1,2,3	2	1,2,3
Service-Provider-1,2,3,4	3	1,2,3,4
Consumer-1,2	4	1,2

It will be seen from the above that the purse class is composed of two separate items of information, details of which may be stored in memory as two separate numbers, purse class category and purse class number, in the following format:

Purse class = Purse class category +
Purse class number

where the purse class category is defined above and the purse class number is the subset number as represented symbolically in the above example.

For example the purse class could be stored in purse memory as a 1 byte number whose first 4 bits represent the purse class category and whose second 4 bits represent the purse class number. This gives the possibility of 16 purse classes which is currently considered adequate, bearing in mind commercial requirements.

The purse class list may be stored, likewise in the memory, as a bit map of 16 bits (2 bytes). For example, assuming the 16 bits are numbered 0 to 15, a four element table offset may be defined such that entries 1, 2, 3 and 4 are bits 0, 2, 6 and 12 respectively. Then a purse class belongs to the class list if and only if bit position:

offset (category) + class number - 1 is set.

For example service provider-1 corresponds to bit position 6:

$6 + 1 - 1 = 6$

Likewise consumer-2 corresponds to bit position 13:

$12 + 2 - 1 = 13$

Thus a purse in which just bits 6 and 13 of the class list bit map are set will be able to transfer value only to purses having service provider-1 class or consumer-2 class (this example is for the purpose of illustration only - such a purse would not be practicable).

This implementation allows for one spare value manufacturer and Bank purse class and two spare Service Provider and Consumer purse classes.

An example of a simple global purse class scheme will now be described by way of example only and with reference to the accompanying drawing which is a chart summarising the interworking rules between the purse classes of the exemplary scheme.

In the exemplary scheme a limited number of purse classes are defined as follows:

Value manufacturer
The most sensitive, highest value purse class. Note that it can only interface with bank purses, and not with service provider or consumer purses.

Bank
Used generally for distribution of value to, and receipt of value from consumers, service providers, and banks.

Service-Provider-1
"Standard". This would be configured not to give refunds to consumers, but could pay upwards to bank purses. It can pay its own class, and thus offers options for value movement within purses of the class.

Service-Provider-2
"Refund". This is more capable than the Service Provider-1 purse class, and hence the one with potentially the most exposure. It can pay a consumer for refund purposes, and would be the purse class used for receipt of value from a bank, should this be required. Note, this is the only route for a Service Provider to receive funds from a bank purse.

Consumer	The standard consumer purse class, capable of interfacing to the bank purse.

The choice of purse class list is a commercial decision which would normally be made by the purse provider, subject to predetermined rules. Most of the decisions would be made on an understanding of how the service providers or banks to whom they are issuing purses require to operate.

The purse class "rules" - the sets of purse class lists associated with each purse class - are defined for each individual payment scheme. Each purse is "personalised" with the purse class lists applicable to its allocated purse class.

Thus there is a clear separation between the purse class mechanism and the set of rules defined for a payment scheme. Different schemes, with quite different rules, could use exactly the same purse class mechanism.

A summary of the interworking rules between purse classes according to the above rules is given for the exemplary scheme in the chart shown in the accompanying drawing. In the drawing, the global purse classes are indicated by the following reference numerals:

Ref 1: Value manufacturer
Ref 2: Bank
Ref 3: Service provider-1 (standard)
Ref 4: Service provider-2 (refund)
Ref 5: Consumer

The arrows indicate the direction in which value can be transferred: thus a double ended arrow, as between the value manufacturer and bank means that value can be transferred both ways between the respective purses. A single ended arrow means that value can be transferred only in one direction, such as between service provider-1 and the bank. An arrow which returns to the same block, such as the arrow 6associated with block 2 (the bank) means that the respective purse can transfer value to other purses of the same class.

It must be emphasised that the above is a hypothetical set of purse classes and rules, and deliberately does not correspond to any known scheme. In fact, a practical scheme would use many more classes, particularly at the bank and service provider levels.

CLAIMS

1. A value transfer system comprising a plurality of electronic purses, and interface devices whereby purses may communicate with each other to transfer value by means of transactions, each of which involves an exchange of electric signals between a pair of purses, each purse including memory means storing a record of the accumulated value currently contained within the purse, the system being characterised in that each purse is assigned a class in a hierarchical structure and in that said memory means further stores a record of the class of that purse, together with a list of those classes to which that purse can transfer value.

2. A value transfer system as claimed in claim 1 wherein, in each purse or associated transfer device, is a microprocessor which is programmed so that each value transfer transaction from a payer purse to a payee purse includes at least the step of checking whether the purse class of the payee purse appears on the class list of the payer purse before allowing the transfer of value to take place.

3. A value transfer system as claimed in claim 2 wherein said step of checking comprises passing an electric signal representative of the purse class of the payee purse from the payee purse to the payer purse via said interface device, and carrying out the check in said payer purse.

4. A value transfer system as claimed in claim 3 wherein the information relating to the purse class of the payee purse is cryptographically protected before being passed to the payer purse.

5. A value transfer system as claimed in any one of the preceding claims wherein the purse class is representative of a category of purse user, in a hierarchical tree.

6. A value transfer system as claimed in claim 6 wherein said class categories include or comprise any one or more of the following categories:

Value manufacturer

Bank

Service Provider

Consumer

or their equivalent.

7. A value transfer system as claimed in claim 6 wherein the class lists of the respective purses in said categories are such that the value manufacturer purse can only transfer value to and from the bank purse and cannot transfer value directly to or from the service provider purses and/or the consumer purses.

8. A value transfer system as claimed in either one of claims 5, 6 or 7 wherein one or more of said purse categories each includes a subset of purse classes representative of a hierarchy within the category.

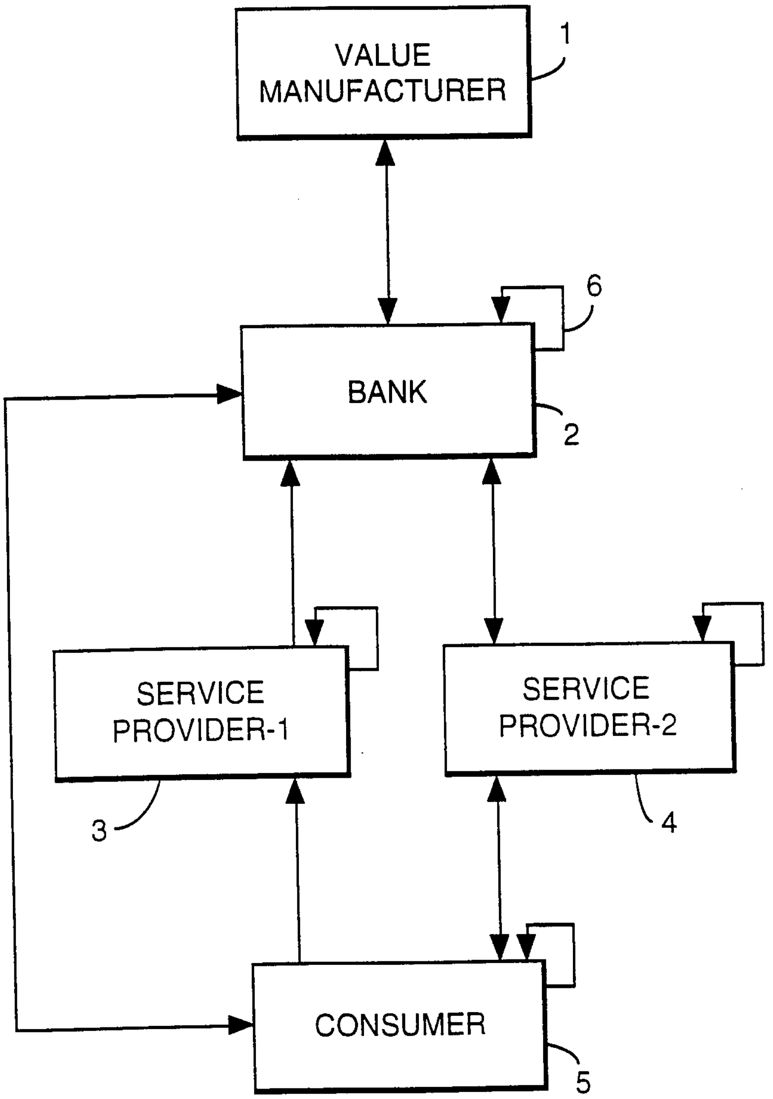
9. A value transfer system as claimed in claim 8 wherein the purse class is stored in said memory means as a 1 byte number whose first 4 bits represent the purse class category and whose second 4 bits is a number which represents the subject within the purse class category.

10. A value transfer system as claimed in either one of claims 8 or 9 wherein the class list is stored in said memory means as a bit map comprising a pattern of bits, and wherein each category and/or subject within each category is represented by one bit within the pattern of bits.

11. A value transfer system as claimed in claim 10 wherein each class category is given a unique offset within said bit map such that a purse class belongs to the class list only if bit position n within the bit map has a particular value, where:

n = offset + subset class number - 1.

12. A value transfer system according to any one of the preceding claims wherein at least some of said purses store in their memory means a plurality of class lists, each class being assigned to a particular currency.


VALUE MANUFACTURER
1
6
BANK
2
SERVICE PROVIDER-1
3
SERVICE PROVIDER-2
4
CONSUMER
5