PCT/SG01/00237
Received 20 June 2003

19 MAY 2006



# A METHOD OF DISTRIBUTING AND REDEEMING TAMPER RESISTANT COUPONS USING AN ELECTRONIC MESSAGING SERVICE

## Field of the Invention

The present invention relates to a system and method for distributing and redeeming mobile electronic coupons using an electronic messaging service. The invention finds particular use in mobile commerce.

## Background of the Invention

Manufacturers, retailers and other organizations involved in sales or promotion of products or services often offer incentives in the form of discounts, special offers and promotional offers. One way in which an organization may offer a consumer such incentives is by issuing coupons in the form of vouchers, newspaper cuttings and the like. Such coupons may provide the consumer with an opportunity to purchase a product from organization (such as a retailer or a manufacturer) at a fixed discount (for example, "fifty cents off when you buy product X"), a percentage discount (for example, "25 percent off when you buy product Y") or a "buy one get one free" offer, inter alia.

Today, a large number of organizations issue printed coupons (that is, "paper coupons"). Printed coupons may be issued using a distribution means such as widely available print media (for example, magazines and newspapers). Alternatively, some organizations, such as credit card companies, offer printed coupons to specific market segments (for example, credit card holders having a particular type of credit card) by distributing coupons using targeted mail.

AMENDED SHEET
IPEA/AU

PCT/SG01/00237
Received 20 June 2003

19 MAY 2006



In addition to providing an incentive mechanism, coupons may also provide a valuable tool for obtaining marketing data. For example, by monitoring the proportion of coupons issued to those that are redeemed, an organization may obtain a measure for the success of a coupon issuance. In another example,

AMENDED SHEET
IPEA/AU

redeemed coupons may be used to collect demographic information. Such demographic information may include consumer details (for example, by the provision of an name and address fields which must be completed by a consumer to enable the coupon to be redeemed) or the source from which the coupon was retrieved (for example, magazine X, where the coupon was published in both magazines X and Y).

Marketing data such as the types described above may be beneficially used to assist an organization with decision making processes in relation to, for example, adjusting an existing, or formulating a new, marketing strategy.

Although offering some advantages, the costs associated with printing and distribution of printed coupons may be quite expensive. Furthermore, the gathering of marketing data in accordance with the methods described above is somewhat manually intensive and thus inefficient.

With the advent of computer networks, such as the Internet, methods have been realised for distributing of coupons electronically, thus providing a mechanism which overcomes some of the disadvantages associated with distributing printed coupons.

The use of the Internet to distribute electronic coupons is well established. For example, US patent 5,907,830 (the '830 patent) proposes an Internet based coupon distribution system whereby a consumer is able to use a computer connected to the Internet to download a coupon and prepare a paper copy of the coupon using a printer. A consumer can take the printed coupon to a retailer to redeem it, or return it to the source (for example, a manufacturer) along with a proof of purchase in order to receive a refund by mail. Accordingly, the consumer cannot redeem the coupon without having first printed it, thus requiring additional hardware in the form of a printer. Moreover, the process of redeeming the coupon and gathering marketing data from the coupon still requires processes which are manually intensive.

With the proliferation of an increasingly paperless lifestyle, paperless equivalents of coupons are finding increasing popularity. However, it appears that to date, existing paperless coupon systems either require the consumer to purchase customised software, hardware or smart cards, or are Internet based.

An Internet based system for generating and redeeming electronic coupons may be of the type described in US patent 5,855,007 (the '007 patent). The '007 patent describes an electronic coupon communication system for generating and redeeming unique product discount coupons over a public computer network such as the Internet.

The system described in the '007 patent comprises a first Internet node, an Internet coupon server and an Internet coupon notification centre. The Internet coupon server accepts an on-line selection of one of the available unique Internet coupons from a user of the Internet node and transmits the coupon back to the user's printing device or email storage. Thus, according to the '007 patent, to obtain an electronic coupon the user must use a computer (or other web enabled device) which is able to communicate with the coupon server over a public computer network such as the Internet. Ordinarily, such a computer will be equipped with specialised software (for example, a web browser) to enable it to interface to the public computer network.

In addition to the limitations described above, electronic coupons used in these systems may be subject to abuse in the form of tampering. Such tampering may performed by a hacker, and be directed towards manipulating the contents of the coupon to the benefit of the hacker. For example, a hacker may modify the contents of an electronic coupon so as to improve the value of the incentive.

In light of the preceding discussion it can therefore be appreciated that there appear to be numerous problems associated with existing coupon distribution and redemption schemes. It is thus an aim of the present invention to

ameliorate these deficiencies and provide a method for distributing and redeeming electronic coupons which exhibits improved security features.

Summary of the Invention

According to a first aspect of the present invention there is provided a method for distributing and redeeming tamper resistant electronic coupons using an electronic messaging service, the method including the steps of:

generating a tamper resistant electronic coupon using a coupon server, the electronic coupon containing coupon data items;

establishing a communications link between the coupon server and a mobile messaging device, the mobile messaging device being capable of sending and receiving tamper resistant electronic coupons using the electronic messaging service;

transmitting the tamper resistant electronic coupon to the mobile messaging device using the electronic messaging service;

the mobile messaging device receiving and storing the tamper resistant electronic coupon;

establishing a communications link between the mobile messaging device and a transaction server;

the mobile messaging device transmitting the tamper resistant electronic coupon to the transaction server using the electronic messaging service;

the transaction server receiving the tamper resistant electronic coupon; and

the transaction server redeeming the tamper resistant electronic coupon.

In one form of the invention, the electronic messaging service is a GSM (Global System for Mobile Communications) Short Message Service (SMS).

In this form of the invention the mobile messaging device may be a GSM SMS enabled mobile phone or a GSM SMS enabled Personal Digital Assistant (PDA).

In another form of the invention, the electronic messaging service is a Code Division Multiple Access (CDMA) messaging service. In this form of the invention, the mobile messaging device may be a CDMA messaging service enabled mobile phone or a CDMA messaging service enabled PDA.

In yet another form of the invention, the electronic messaging service is a Wireless Multimedia and Messaging Service (WIMS). In this form of the invention the mobile messaging device is a WIMS enabled device.

In a particular form of the invention the tamper resistant electronic coupon contains a cryptographic signature data item, and the coupon data items include:

identification data, which is representative of a unique identifier for identifying the coupon;

expiry date data, which is representative of a date up until which the coupon is able to be redeemed;

value data, which is representative of the value of the coupon; and

currency data, which is representative of a unit of measure associated with the value data.

In one form of the invention, the coupon data items are derived from a subset of data items contained in a pre-existing computer readable file stored on a database such that each coupon data item is related to a data item in the pre-existing file where a plurality of data fields are stored, each coupon data item being substantially identical to the related file data item

that they are derived from. In this form of the invention, the tamper resistant electronic coupon may, or may not, contain a signature data item.

The signature data item may be generated in any suitable process. In one suitable process, the following steps are performed:

encrypting the coupon data items using a symmetric encryption algorithm to provide a first ciphertext, wherein the symmetric encryption algorithm uses a symmetric key;

hashing the first ciphertext using a one way hashing function, the hashing providing a first unformatted signature data item;

formatting the first unformatted signature data item, to provide a first signature data item; and

appending the first signature data item to the tamper resistant electronic coupon.

In an alternative form of the invention, where the coupon data items have been derived from a pre-existing file, the signature data item may be created using a signature data creation process which includes the steps of:

encrypting the data items contained in the pre-existing file using a symmetric encryption algorithm to provide a first ciphertext, wherein the symmetric encryption algorithm uses a symmetric key;

hashing the first ciphertext using a one way hashing function, the hashing providing a first unformatted signature data item;

formatting the first unformatted signature data item, to provide a first signature data item; and

appending the first signature data item to the tamper resistant electronic coupon.

In this form of the invention, the first signature data item is able to be stored in the pre-existing file.

Preferably, the establishing of the communications link between the coupon server and the mobile messaging device is initiated by a user utilising the mobile messaging device to request the electronic coupon from the coupon server. Similarly, the establishing of the communications link between the mobile messaging device and the transaction server is performed by a user utilising the same mobile messaging device.

In a preferred form of the invention, the step of redeeming the tamper resistant electronic coupon includes authorising a transaction, wherein the authorisation of the transaction occurs subsequent to the tamper resistant electronic coupon being authenticated as being valid.

In one form of the invention, where the coupon data includes identification data, expiry date data, value data and currency data, authorisation of the transaction occurs subsequent to the tamper resistant electronic coupon being authenticated as valid. In this form of the invention the authentication of the tamper resistant electronic coupon includes the steps of:

obtaining the expiry date data from the tamper resistant electronic coupon;

comparing the expiry date data obtained from the tamper resistant electronic coupon with transaction date;

in response to determining that the coupon has not expired, obtaining the identification data from the tamper resistant electronic coupon;

retrieving a pre-existing file from the coupon server, the retrieved file having identification data which is the same as the coupon identification data; and

comparing each of the coupon value data item and coupon currency data item with the retrieved file data items related to the coupon value data

item and coupon currency data item, wherein the tamper resistant electronic coupon is valid if the data items being compared are the same.

In another form of the invention where the tamper resistant electronic coupon contains a signature data item which has been derived from the coupon data items as described previously, the authorisation of the transaction occurs subsequent to the tamper resistant electronic coupon being authenticated as valid, wherein the authentication of the tamper resistant electronic coupon includes the steps of:

obtaining the first signature data item from the tamper resistant electronic coupon;

encrypting the coupon data items using the symmetric encryption algorithm to provide a second ciphertext, wherein the symmetric encryption algorithm uses the symmetric key;

hashing the second ciphertext using the one way hashing function, the hashing providing a second unformatted signature data item;

formatting the second unformatted signature data item to provide a second signature data item; and

comparing the first signature data item to the second signature data item, wherein the tamper resistant electronic coupon is valid if the first signature data item is the same as the second signature data item.

In yet another form of the invention, where the signature data item has been derived from data items contained in the pre-existing file, the authorisation of the transaction occurs subsequent to the tamper resistant electronic coupon being authenticated as being valid, wherein the authentication of the tamper resistant electronic coupon includes the steps of:

obtaining the first signature data item from the tamper resistant electronic coupon;

obtaining the identification data from the tamper resistant electronic

coupon;

retrieving a pre-existing file from the coupon server, the retrieved file having identification data which is the same as the coupon identification data;

retrieving a pre-existing file from the coupon server, the retrieved file having identification data which is the same as the coupon identification data;

encrypting the retrieved file using the symmetric encryption algorithm, the symmetric encryption algorithm using the symmetric key, the encryption of the retrieved file providing a second ciphertext;

hashing the second ciphertext using the one way hashing function, the hashing providing a second unformatted signature data item;

formatting the unformatted second unformatted signature data item to provide a second signature data item; and

comparing the first signature data item to the second signature data item, wherein the tamper resistant electronic coupon is valid if the first signature data item is the same as the second signature data item.

In yet another form of the invention, where the signature data item has been derived from data items contained in the pre-existing file and is stored in the pre-existing file, the authorisation of the transaction occurs subsequent to the tamper resistant electronic coupon being authenticated as being valid, wherein the authentication includes the steps of:

obtaining the first signature data item from the tamper resistant electronic coupon;

obtaining the identification data from the tamper resistant electronic coupon;

retrieving a pre-existing file from the coupon server, the retrieved file having identification data which is the same as the coupon identification data;

obtaining the first signature data item from the retrieved file; and

comparing the first signature data item obtained from the tamper resistant electronic coupon with the first signature data item obtained from the retrieved file, wherein the tamper resistant electronic coupon signature data items are the same.

Preferably, the step of authenticating the electronic coupon further includes communicating the results of the authentication to a display terminal.

It is also preferable that the step of authenticating the tamper resistant electronic coupon further includes communicating the results of the authentication to the mobile messaging device, wherein the communication of the results is performed using the electronic messaging service.

Ideally, the transaction server receives demographic information with an electronic coupon.

According to a second aspect of the present invention there is provided a system for distributing and redeeming tamper resistant electronic coupons using an electronic messaging service, the system including:

a plurality of mobile messaging devices which is able to transmit and receive more than one tamper resistant electronic coupons using an electronic messaging service;

a coupon server including a computer processor and associated memory, the coupon server being connected to a communications network, which network supports an electronic messaging service, the coupon server generating tamper resistant electronic coupons and transmitting electronic coupons to the mobile messaging devices using the electronic messaging service; and

a transaction server including a computer processor and associated

memory, the transaction server being connected to the communications network, and redeeming tamper resistant electronic coupons received from mobile messaging devices.

It will be recognised that the present invention includes a number of advantages in that the method is able to deployed using existing electronic messaging infrastructures, thus enabling the distribution and redemption of electronic messages using existing mobile phones and other similar messaging enabled devices.

In addition, the invention provides ~~an~~ a tamper resistant electronic coupon format having features which enable authentication and which use cryptographic signature verification to improve resistance to tampering. Furthermore, the invention enables each transaction to be acknowledged by means of a return receipt or confirmation message. It will also be recognised that the invention enables automated collection of marketing data, including demographic information.

Brief Description of the Drawings

The present invention will now be described in relation to various embodiments illustrated in the accompanying drawings. However, it must be appreciated that the following description is not to limit the generality of the above description.

In the drawings:

Figure 1 is a block diagram illustrating a system in accordance with a preferred embodiment of the invention;

Figure 2 is a flow diagram illustrating the process of generating an electronic coupon in accordance with a first preferred embodiment of the present invention;

Figure 3 is a flow diagram illustrating the process of generating an electronic coupon having a cryptographic signature in accordance with a second preferred embodiment of the present invention;

Figure 4 is a flow diagram illustrating the process of generating an electronic coupon having a cryptographic signature in accordance with a third preferred embodiment of the present invention;

Figure 5 is a flow diagram illustrating the process of generating an electronic coupon having a cryptographic signature in accordance with a fourth preferred embodiment of the present invention;

Figure 6 is a block diagram illustrating the operational sequence for requesting a mobile coupon in accordance with the preferred embodiments of the invention;

Figure 7 is a flow diagram illustrating the process of non cryptographic verification of an electronic coupon;

Figure 8 is a flow diagram illustrating the process of verifying an electronic coupon having a cryptographic signature, wherein the cryptographic signature was generated in accordance with the first preferred embodiment of the present invention;

Figure 9 is a flow diagram illustrating the process of verifying an electronic coupon having a cryptographic signature, wherein the cryptographic signature was generated in accordance with the second preferred embodiment of the present invention; and

Figure 10 is a flow diagram illustrating the process of verifying an electronic coupon having a cryptographic signature, wherein the cryptographic signature was generated in accordance with a third preferred embodiment of the present invention.

Detailed Description of the Invention

Throughout this description, reference will be made to "mobile coupons" and its derivatives "mCoupons" and "mobile electronic coupons". By the use of these terms, reference is made to a particular form of an electronic coupon which is able to be communicated to and from a mobile messaging device, such as a mobile phone, using an electronic messaging service.

A system for distributing and redeeming an mCoupon according to an embodiment of the present invention is shown in Figure 1. The system includes a mobile messaging device 10 which is operable to communicate with a coupon server 12 and a transaction server 16 over an communications network 14.

Specifically, the communications network 14 is a GSM SMS capable network, and accordingly, the mobile messaging device 10, is also able to communicate with the coupon server 12 and the transaction server 16 using the GSM SMS capable network. It is to be appreciated, however, that although reference will be made to the communications network 14 as being GSM SMS capable, the communications network 14 is to be understood not to be so limited. Indeed, the invention may be deployed using a communications network 14 which is capable of supporting an alternative electronic messaging scheme (such as, CDMA messaging or Wireless Multimedia Messaging) in which case the mobile messaging device 10 will also be so capable.

Also illustrated in Figure 1 is an intervening communications network 18. Such network 18 may be the Internet, a public switched telephone network (PSTN) an integrated services digital network (ISDN), a network capable of supporting an electronic messaging service different to that provided by the communications network 14, or a combination thereof. It is to be understood, however, that the provision of the intervening communications network 18 is optional. Indeed, the invention may be deployed without having the intervening communications network 18.

In a system of the present invention which includes an intervening network 18, the intervening network 18 is able to facilitate protocol conversion (for example TCP/IP to SMS). It is envisaged that the intervening network 18 will enable devices coupled to the intervening network 18 to interoperate where those devices would otherwise not have been to communicate (for example, where the coupon server uses TCP/IP and the mobile messaging device 10 uses a CDMA messaging protocol)

The coupon server 12 may be a programmed computer which is capable of generating mCoupons by translating pre-existing data files containing coupon data. The pre-existing files are preferably stored on a database 13 (herein referred to as the "vVoucher database") which preferably resides on the coupon server 12. The coupon server 12 is also capable of sending and receiving mobile coupons using a protocol which is compatible with the communications network 14 or the intervening communications network 18 if provided.

Figure 1 also includes a transaction server 16 which is preferably a programmed computer, which computer includes sufficient hardware and software to enable the transaction server 16 to redeem mCoupons received from a mobile messaging device 10 and, if required, access pre-existing files from the coupon server 12.

Throughout this specification reference will be made to the coupon server 12 and the transaction server 16 as being separate entities. However, It is to be understood that the coupon server 12 and the transaction server 16 need not be separate. Indeed, in a preferred form of the invention, the coupon server 12 and the transaction server 16 will be a single entity, capable of providing the required dual functionality.

As is illustrated in Figure 2, in one form of the invention, the coupon server 12 (refer to Fig 1) is able to generate a particular type of mCoupon 19 using data

derived from data stored in a pre-existing data file, which data file, for the purposes of this description, will herein be referred to as a "vVoucher". A vVoucher 20 may include a plurality of data fields 22, each field having a respective data item 24.

In operation, the coupon server 12 extracts particular data items 26, 28, 30 and 32 from the vVoucher 20 and arranges the particular data items in the form of an mCoupon 19. For the purposes of this discussion, the particular data items will herein be referred to as "coupon data items".

In an exemplary form of the mCoupon 19, the coupon data items include a coupon identifier (the "COUPONID") 26, an expiry date (the "EXPIRYDATE") 28, a coupon value (the "VALUE") 30 and a currency (the "CURRENCY") 32. For the purposes of this description, this exemplary form of the mCoupon 19 will herein be referred to as an "unsigned mCoupon" 19.

Turning now to Figure 3, a cryptographic signature 34 may be appended to the unsigned mCoupon 19. Such cryptographic signature 34 (the "MCSIGNATURE") is preferably generated by the coupon server 12 (refer to Fig 1). For the purposes of this description, an mCoupon 19 having a respective MCSIGNATURE 34 will be refered to as a "signed mCoupon" 36.

In Figure 3 there is illustrated a first preferred method for generating a signed mCoupon 36. In accordance with the first preferred method, an MCSIGNATURE 34 is able to be generated using the coupon data items 26, 28, 30 and 32.

In the first preferred method of generating a signed mCoupon 36 the coupon data items 26, 28, 30 and 32 are encrypted 37 using a symmetric encryption key algorithm (such as DES, IDEA or Blowfish) and a symmetric encryption key ('the symmetric key'), the symmetric key being known only to the issuer of the mCoupon 19 and the transaction server 16 where the coupon is able to be

redeemed. Advantageously, the symmetric key may be changed on a daily basis, or on a per-coupon basis, or based on some other policy in accordance with the requirements of the coupon issuer. In this respect, reference to the term "issuer" throughout this specification is to be understood to be reference to the organization (for example, a retailer or manufacturer) on whose behalf the mCoupon 19 or 36 has been issued.

The encryption of the coupon data items may be represented as:

$$C_e = E_k (C_p)$$

where

$C_p$ is the coupon data items before encryption;
$E_k$ is the process of encrypting $C_p$ with a symmetric key k; and
$C_e$ is ciphertext which results from the encryption process (herein refered to as the encrypted mCoupon 38).

The encrypted mCoupon 38, in the form of ciphertext, is then hashed using a one way hash function 39 (such as MD5, SHA-1, RIPEMD-160). In this respect, references to the term "hash" and its derivatives "hashing" and "hashed" are to be understood to be references to a process which takes a variable length input message (for example, the coupon data items) and translates it to a fixed length output. Furthermore, reference to the term "hashing function" throughout this specification is to be understood to be reference to a function which performs hashing (for example, MD5, SHA-1, RIPEMD-160).

This process may be represented as:

$$S = H (C_e)$$

where

H is the one way hash function; and

S is the result of the one way hashing.

The result of the hashing S is then converted 41 into its hexadecimal ASCII text representation, which representation is able to be used as the MCSIGNATURE 34 for use with the signed mCoupon 36. In this form of the invention it will thus be recognised that the signed mCoupon 36 is provided with improved protection against deliberate or accidental tampering.

The following example (Example 1) is provided to assist the reader with the understanding of first preferred method of generating a signed mCoupon 36.

Example 1:

Consider an organization O issuing vVouchers and mCoupons which are able to be redeemed at a shop S1 having a transaction server. Consider the case of one user and one coupon. Organization O generates a vVoucher vC which is as follows:

BEGIN VVOUCHER
COUPONID: 102030405060708090A0
ISSUER: Muncho Noodles Inc
ISSUEDATE: 10102001101010
EXPIRY DATE: 10112001101010
USE: SINGLE
VALUE: 5
CURRENCY: USD
MERCHANTS: XYZ Eating House
BEAMED: 0
SIGNATURE:
END VVOUCHER

The vVoucher will be converted to an mCoupon C having the following format:

10203040506070809OAO 1011200110101010 5 USD

The issuer O generates a symmetric key k which he uses to sign the mCoupon C. For the purposes of this example, say the issuer O also agrees to use Triple-DES (DES3) as the symmetric encryption algorithm, and MD5 as the hash algorithm. The issuer O generates the MCSIGNATURE 34 for mCoupon C as follows:

$C_e$ = DES3 ( C, K ) where K is the symmetric key chosen by issuer O, and $C_e$ is the ciphertext;

H = MD5 ( $C_e$ );

MCSIGNATURE = BinToHex (H) where BinToHex represents the conversion of the hash value H from binary to hexadecimal form.

Let {MCSIGNATURE} represent the actual hexadecimal signature obtained from the above sequence of operations. Thus, the final signed mCoupon $C_s$ will have the following format:

10203040506070809A0 100112001101010 5 USD {MCSIGNATURE}

When a customer desires a coupon, he is able to send a request message to a pre-arranged phone number, which in turn responds by sending $C_s$ as a message back to the user.

In Figure 4 there is illustrated a second preferred method for generating a signed mCoupon 36. In accordance with the second preferred method, an MCSIGNATURE 34 is generated using a vVoucher 20. Here, the data items 22, 24 contained in vVoucher 20 are encrypted 37 using a symmetric encryption

key algorithm (such as DES, IDEA or Blowfish) to provide an encrypted vVoucher 40. The symmetric key is known only to the issuer of the mCoupon 19 and the transaction server 16 where the coupon is able to be redeemed. Advantageously, the symmetric key may be changed on a daily basis, or on a per-coupon basis, or based on some other policy in accordance with the requirements of the issuer.

The encryption of the coupon data may be represented as:

$$C_e = E_k (C_p)$$

where

$C_p$ is the vVoucher data items before encryption;
$E_k$ is the process of encrypting $C_p$ with a symmetric key k; and
$C_e$ is ciphertext which results from the encryption process (herein refered to as the encrypted vVoucher 40).

The encrypted vVoucher 40 is then able to be hashed using a one way hash function such as MD5.

The hashing process may be represented as:

$$S = H (C_e)$$

where

H is the one way hash function; and
S is the result of the one way hashing.

The result of the hashing S is then converted 41 into its hexadecimal ASCII text representation, which representation is able to be used as the MCSIGNATURE 34 for use with the signed mCoupon 36.

In Figure 5 there is illustrated a third preferred method for generating a signed mCoupon 36 which is substantially similar to the second preferred method as described above, with the exception that the MCSIGNATURE 34 is preferably stored in the vVoucher database 13 residing on the coupon server 12.

Having described the processes for generating an unsigned mCoupon 19, or a signed mCoupon 36, the following section will now describe the mechanisms for facilitating distribution and redemption of an mCoupon 19, 36. In this respect, turning to Figure 6 there is illustrated a representation of the operational sequence for requesting an mCoupon 19, 36.

It is envisaged that a user having a mobile messaging device 10 will be able to request an mCoupon 19, 36 from a coupon server 12 (refer to Fig 1), by sending a request, in the form of an GSM SMS message, to a pre-arranged phone number. Preferably, the pre-arranged number will be associated with a service 42 (such as a billboard service) which is preferably able to be accessed via the communications network 14 (refer to Fig 1) or intervening communications network 18 and able to communicate the request to the coupon server 12. In response to receiving the request, the coupon server 12 transmits a GSM SMS message containing the mCoupon 19 or 36 back to the user's mobile messaging device 10.

Following the receipt of the mCoupon by the mobile messaging device 10 the mCoupon 19 or 36 may be stored on the mobile messaging device 10 until such time as a user wishes to redeem it, or transfer it to another mobile messaging device. In this respect, it is to be understood that although reference has been made to storing a single mCoupon 19 or 36, the mobile messaging device 10 may be able to store more than one. In such a case, a user may be able to select a particular mCoupon 19 or 36 for redemption from a plurality of mCoupons 19 or 36 stored on the mobile messaging device 10.

In order to redeem a mCoupon 19 or 36 , a user utilises the mobile messaging device 10 to forward a selected mCoupon 19 or 36 to a pre-arranged phone using the GSM SMS. Preferably, the pre-arranged number is associated with a communications service which is able to communicate the selected mCoupon 19 or 36 to a transaction server 16. According to the present invention, in response to receiving the mCoupon 19 or 36 the transaction server 16 may or may not verify the authenticity of the mCoupon 19 or 36. Furthermore, the transaction server 16 may extract information, such as demographic information, from the message containing the mCoupon 19 or 36. Such demographic information may include, the source from where the mCoupon 19 or 36 was received, an identification tag for the user's mobile messaging device (for example, a user's mobile phone number) and the time at which the mCoupon 19 or 36 was received. Ideally, the demographic information extracted from the message containing the mCoupon 19 or 36 is able to be used for marketing purposes.

The user may also utilise the mobile messaging device 10 to transfer the mCoupon to another mobile messaging device by forwarding the message containing the mCoupon to another mobile messaging device.

A first preferred method for verifying the authenticity of an mCoupon 19 or 36 is illustrated in Figure 7. It is envisaged that in the first preferred method for verifying the authenticity of an mCoupon 19 or 36, particular data items from the mCoupon 19 or 36 will be tested to enable an assessment of the validity of the mCoupon 19 or 36.

Specifically, the EXPIRYDATE 28 will initially be compared with the current date and time (that is, the date and time at which the mCoupon 19 or 36 was received by the transaction server 16) to determine whether the mCoupon 19 or 36 has expired. If the mCoupon has not expired then the COUPONID 24 is extracted from the mCoupon 19 or 36. The transaction server 16 then retrieves the vVoucher 20 having the same COUPONID 24.

Once the vVoucher 20 has been retrieved, the transaction server 16 is able to extract the VALUE 30 and CURRENCY 32 from the mCoupon 19 or 36 and compare these data items with the respective data items in the vVoucher 20. In the event that the respective data items have a different value to those obtained from the mCoupon 19 or 36, the mCoupon 19 or 36 is invalid, and thus unable to be redeemed. Alternatively, if the data items have the same value then the mCoupon 19 or 36 is considered to be valid and thus redeemable.

Figure 8 illustrates a preferred method for verifying the authenticity of a signed mCoupon 36 having an MCSIGNATURE 34 which has been generated in accordance with the first preferred method of generating an MCSIGNATURE 34 as described earlier.

Pursuant to this method the MCSIGNATURE 34 is extracted from the signed mCoupon 36. The signed mCoupon 36 is then stripped of the MCSIGNATURE 34 to provide an unsigned mCoupon 19. The unsigned mCoupon 19 is encrypted with the issuer's symmetric key using the symmetric encryption algorithm specified by the issuer. The hash value for this encrypted coupon is then able to be calculated using the hashing function specified by the issuer. The hash value may then be converted into an equivalent hexadecimal representation for comparison with the MCSIGNATURE 34 extracted from the mCoupon 19. If, on the basis of the comparison, the extracted MCSIGNATURE 34 is the same as the hexadecimal representation then the mCoupon is valid and thus may be able to be redeemed.

The following example (Example 2) is provided to assist the reader with the understanding of the preferred method for verifying the authenticity of an mCoupon having an MCSIGNATURE 34 which has been generated in accordance with the first preferred method of generating an MCSIGNATURE 34.

Example 2:

Assume that the user is honest, and doesn't tamper with or replicate $C_s$ as, he goes to shop S1 to redeem his coupon. The redemption process according to the preferred method for verifying the authenticity of an mCoupon having an MCSIGNATURE 34 might be as follows:

1. The user U forwards his mCoupon $C_s$ to the server at shop S1 through his messaging network;

2. The shop S1 extracts MCSIGNATURE 34 from mCoupon $C_s$;

3. The coupon $C_s$ is stripped of its MCSIGNATURE 34 field, resulting in an unsigned mCoupon C';

4. Coupon C' is encrypted with K using Triple-DES to give $C_e$'. This operation is indicated as follows:

$$C_e' = DES\ 3\ (C', K)$$

5. $C_e$' is hashed using MD 5 to generate H', that is:

$$H' = MD5\ (Ce')$$

6. H' is converted to its hexadecimal representation, that is:

$$SIG = BinToHex\ (H')$$

7. SIG is compared with MCSIGNATURE 34. In this case, they are identical, and the user's coupon is valid.

Assuming now that the user tampers with the coupon. Instead of a currency value of 5 USD, the user changes his coupon to 20 USD. In this case, step (7) of the above procedure will fail and the coupon will be rejected. The same is true if the user tampers with any field in the mCoupon.

Figure 9 illustrates a preferred method for verifying the authenticity of a signed mCoupon 36 having an MCSIGNATURE 34 which has been generated in accordance with the second preferred method of generating an MCSIGNATURE 34 as described earlier. In this preferred method, the COUPONID 24 is extracted from the signed mCoupon 36. The vVoucher 20 corresponding to the COUPONID 24 is then able to be retrieved from the vVoucher database 13. Following the retrieval of the vVoucher 20, the vVoucher 20 is encrypted with the issuer's symmetric key using the symmetric encryption algorithm specified by the issuer. The hash value for the encrypted vVoucher 20 is then calculated using the hashing function specified by the issuer. If, on the basis of the comparison, the extracted MCSIGNATURE 34 is the same as the hexadecimal representation then the signed mCoupon 36 is valid and thus may be able to be redeemed.

The following example (Example 3) is provided to assist the reader with the understanding of the preferred method for verifying the authenticity of an signed mCoupon 36 having an MCSIGNATURE 34 which has been generated in accordance with the second preferred method of generating an MCSIGNATURE 34.

Example 3:

Assume the user might have cracked the issuer's symmetric key. If this is done, then the user can generate any number of "valid" mCoupons which will appear to be valid if not cross checked against the contents of the original vVoucher obtained from the vVoucher database 13 (which is typically read-only

to the world). We also assume that the issuer does not want to distribute his symmetric key to the coupon redemption outlets.

An example scenario is detailed below.

Consider organization O issuing a vVoucher vC which can be redeemed at shops S1 and S2. The vVoucher vC is as follows:-

BEGIN VOUCHER
COUPONID: 30405060701020304050
ISSUER: WhizBang Computers Ltd
ISSUEDATE: 10102001101010
EXPIRY DATE: 10112001101010
USE: SINGLE
VALUE: 100
CURRENCY: SGD
MERCHANTS: RipMeOff Sales and Marketing outlets
BEAMED: 0
SIGNATURE:
END VVOUCHER

The issuer agrees to use Blowfish as his symmetric encryption algorithm with symmetric key K, and RIPEMD160 as his hash function. The issuer proceeds as follows

1. The entire vVoucher vC is encrypted with K using Blowfish;

$$vC_e = \text{Blowfish}\ (\ vC, K\ )$$

2. $vC_e$ is hashed using RIPEMD 160

$$H =\text{- ripemd160}\quad (\ v\,C_e\ )$$

3. H is converted to hexadecimal. This becomes the MCSIGNATURE 34 which will later be appended to the mCoupon

MSIGNATURE = BinToHex ( H )

MCSIGNATURE 34 and Vc are entered into the vVoucher database 13 maintained by the issuer, along with a USED field indicating whether the vVoucher has been used. Initially, the USED field is set to FALSE;

4. vVoucher vC is converted the usual way into mCoupon C, which will appear as follows after MCSIGNATURE 34 is appended:

30405060701020304050 1011200110101010 100 USD {MCSIGNATURE}

5. C is sent to the user on demand.

Figure 10 illustrates a preferred method for verifying the authenticity of an signed mCoupon 36 having an MCSIGNATURE 34 which has been generated in accordance with the third preferred method of generating an MCSIGNATURE 34 as described earlier. In this preferred method, the COUPONID 24 is extracted from the signed mCoupon 36. The vVoucher 20 corresponding to the COUPONID 24 is then able to be retrieved from the vVoucher database 13. Following the retrieval of the vVoucher 20, the MCSIGNATURE 34 of the vVoucher 20 is obtained from the vVoucher 20. The MCSIGNATURE 34 obtained from the vVoucher 20 is then compared to the MCSIGNATURE 34 obtained from the signed mCoupon 36. If, on the basis of the comparison, the MCSIGNATURE 34 obtained from the vVoucher is the same as the MCSIGNATURE 34 obtained from the signed mCoupon 36 then the coupon is valid and thus may be able to be redeemed.

The following example (Example 4) is provided to assist the reader with the understanding of the preferred method for verifying the authenticity of a signed mCoupon 36 having an MCSIGNATURE 34 which has been generated in accordance with the third preferred method of generating an MCSIGNATURE 34.

Example 4:

Assume a user is a determined hacker who has cracked the issuer's symmetric key. As a result of cracking the key, he is able to generate a "bogus" coupon whose value is 500 USD instead of 100 USD. Using his cracked key, he encrypts and signs his coupon $C_b$, which is presented to the store for redemption. Also assume that the store does not have access to the issuer's symmetric key.

The store validates the coupon as follows:

1. The COUPONID filed is extracted from the mCoupon $C_b$ and is used to identify the original vVoucher vC from which the $C_b$ was supposed to have been generated;

2. The store fetches the signature MCSIGNATURE 34 corresponding to vC from the issuer's vVoucher database 13; and

3. The signature retrieved from the issuer is compared with the signature presented by the user. Since the user has forged the coupon, the signatures will not match and the coupon is rejected.

A second user who gets a legitimate coupon (C, derived from vC) who does not have enough resources to crack the issuer's symmetric key may try the following with a single use coupon:

1. Redeems the valid mCoupon C at store S1; and

2. Try to redeem the same mCoupon C at store S2.

To protect against such attacks, each store needs to perform the following actions:

1. For each mCoupon C received by the store, the COUPONID field is used to identify the corresponding vVoucher vC;

2. The USED field for vC is checked on the issuer's vVoucher database 13 server;

3. If the USED field is FALSE, then the coupon has not yet been redeemed. The store informs the issuer's database 13 system to update the USED field for vC to TRUE and accepts the coupon as valid; and

4. If the USED field is TRUE, then the coupon has already been used, and is rejected as invalid.

It will thus be recognised that the present invention provides a system and method for distributing and redeeming electronic coupons which is able to utilise existing electronic messaging frameworks, thus rendering the present invention usable on most existing mobile and other similar messaging enabled devices and therefore requiring no additional hardware or software investment by the user. Furthermore the present invention also beneficially provides an automated method for collecting demographic information.

Finally, it will be understood that there may be other variations and modifications to the configurations described herein that are also within the scope of the present invention.

Claims

1. A method for distributing and redeeming tamper resistant electronic coupons using an electronic messaging service, the method including the steps of:

generating a tamper resistant electronic coupon using a coupon server, the electronic coupon containing coupon data items;

establishing a communications link between the coupon server and a mobile messaging device, the mobile messaging device being capable of sending and receiving tamper resistant electronic coupons using the electronic messaging service;

transmitting the tamper resistant electronic coupon to the mobile messaging device using the electronic messaging service;

the mobile messaging device receiving and storing the tamper resistant electronic coupon;

establishing a communications link between the mobile messaging device and a transaction server;

the mobile messaging device transmitting the tamper resistant electronic coupon to the transaction server using the electronic messaging service;

the transaction server receiving the tamper resistant electronic coupon; and

the transaction server redeeming the tamper resistant electronic coupon.

2. A method according to claim 1 wherein the tamper resistant electronic coupon contains a cryptographic signature data item, wherein the coupon data items include:

identification data, which is representative of a unique identifier for identifying the coupon;

expiry date data, which is representative of the date up until which the coupon is able to be redeemed;

value data, which is representative of the value of the coupon; and

currency data, which is representative of a unit of measure associated with the value data.

3. A method according to claim 2 comprising the steps of:

deriving the coupon data items from a subset of data items contained in a preexisting computer readable file stored on a database;

each coupon data item having a respective data item in the pre-existing file where a plurality of data fields are stored,

each coupon data item being substantially identical to the respective data item that they are derived from.

4. A method according to claim 3 wherein the tamper resistant electronic coupon contains a signature data item.

5. A method according to claim 4 wherein the signature data item is created using a signature data item creation process, the process including the steps of:

encrypting the coupon data items using a symmetric encryption algorithm to provide a first ciphertext, wherein the symmetric encryption algorithm uses a symmetric key;

hashing the first ciphertext using a one way hashing function, the hashing providing a first unformatted signature data item;

formatting the first unformatted signature data item, to provide a first signature data item; and

appending the first signature data item to the tamper resistant electronic coupon.

6. A method according to claim 4 wherein the signature data item is created using a signature data creation process, the process including the steps of:

encrypting the data items contained in the pre-existing file using a symmetric encryption algorithm to provide a first ciphertext, wherein the symmetric encryption algorithm uses a symmetric key;

hashing the first ciphertext using a one way hashing function, the hashing providing a first unformatted signature data item;

formatting the first unformatted signature data item, to provide a first signature data item; and

appending the first signature data item to the tamper resistant electronic coupon.

7. A method according to claim 6 wherein the first signature data item is stored in the preexisting file.

8. A method according to claim 1 wherein the step of redeeming the tamper resistant electronic coupon further includes authorising a transaction, wherein the authorisation of the transaction occurs subsequent to the tamper resistant electronic coupon being authenticated as valid.

9. A method according to claim 3 wherein the step of redeeming the tamper resistant electronic coupon further includes authorising a transaction, wherein the authorisation of the transaction occurs subsequent to the tamper resistant electronic coupon being authenticated as valid, the authentication of the tamper resistant electronic coupon including the steps of:

obtaining the expiry date data from the tamper resistant electronic coupon;

comparing the expiry date data obtained from the tamper resistant electronic coupon with a transaction date, in response to determining that

the coupon has not expired, obtaining the identification data from the tamper resistant electronic coupon;

retrieving a pre-existing file from the coupon server, the retrieved file having identification data which is the same as the coupon identification data; and

comparing each of the coupon value data item and coupon currency data item with the retrieved file data items related to the coupon value data item and coupon currency data item, wherein the tamper resistant electronic coupon is valid if the data items being compared are the same.

10. A method according to claim 5 wherein the step of redeeming the tamper resistant electronic coupon further includes authorising a transaction, wherein the authorisation of the transaction occurs subsequent to the tamper resistant electronic coupon being authenticated as valid, the authentication of the tamper resistant electronic coupon including the steps of:

obtaining the first signature data item from the tamper resistant electronic coupon;

encrypting the coupon data items using the symmetric encryption algorithm to provide a second ciphertext, wherein the symmetric encryption algorithm uses the symmetric key;

hashing the second ciphertext using the one way hashing function, the hashing providing a second signature data item;

formatting the unformatted signature data item;

comparing the first signature data item to the second signature data item, wherein the tamper resistant electronic coupon is valid if the first signature data item is the same as the second signature data item.

11. A method according to claim 6 wherein the step of redeeming the tamper resistant electronic coupon further includes authorising a transaction, wherein the authorisation of the transaction occurs subsequent to the tamper

resistant electronic coupon being authenticated as valid, the authentication of the tamper resistant electronic coupon including the steps of:

obtaining the first signature data item from the tamper resistant electronic coupon;

obtaining the identification data from the tamper resistant electronic coupon;

retrieving a preexisting file from the coupon server, the retrieved file having identification data which is the same as the coupon identification data;

encrypting the retrieved file using the symmetric encryption algorithm, the symmetric encryption algorithm using the symmetric key, the encryption of the retrieved file providing a second ciphertext;

hashing the second ciphertext using the one way hashing function, the hashing providing a second signature data item;

formatting the unformatted second signature data item; and

comparing the first signature data item to the second signature data item, wherein the tamper resistant electronic coupon is valid if the first signature data item is the same as the second signature data item.

12. A method according to claim 7 wherein the step of redeeming the tamper resistant electronic coupon further includes authorising a transaction, wherein the authorisation of the transaction occurs subsequent to the tamper resistant electronic coupon being authenticated as valid, the authentication of the tamper resistant electronic coupon including the steps of:

obtaining the first signature data item from the tamper resistant electronic coupon;

obtaining the identification data from the tamper resistant electronic coupon;

retrieving a pre-existing file from the coupon server, the retrieved file

having identification data which is the same as the coupon identification data;

obtaining the second signature from the retrieved file; and

comparing the first signature data item obtained from the tamper resistant electronic coupon with the first signature data item obtained from the retrieved file, wherein the tamper resistant electronic coupon signature data items are the same.

13. A system for distributing and redeeming tamper resistant electronic coupons using an electronic messaging service, the system including:

a plurality of mobile messaging devices which is able to transmit and receive more than one tamper resistant electronic coupons at a time using an electronic messaging service;

a coupon server including a computer processor and associated memory, the coupon server being connected to a communications network, which network supports an electronic messaging service, the coupon server generating tamper resistant electronic coupons and transmitting tamper resistant electronic coupons to the mobile messaging devices using the electronic messaging service; and

a transaction server including a computer processor and associated memory, the transaction server being connected to the communication network, and redeeming tamper resistant electronic coupons received from mobile messaging devices.

14. A system according to claim 13 wherein a tamper resistant electronic coupon includes data items representative of one or more of

identification data, which is representative of a unique identifier for identifying the coupon;

expiry date data, which is representative of a date up until which the coupon is able to be redeemed;

value data, which is representative of the value of the coupon;

currency data, which is representative of a unit of measure associated with the value data; and

a signature data item.

15. A system according to claim 14 wherein the coupon server and the transaction server are the same server.