Data Storage Method and System

Field of the Present Invention

The present invention relates generally to a data storage method and system, of particular but by no means exclusive application in a transaction system for managing entitlements, such as reward entitlements in a loyalty or similar system.

Background of the Present Invention

The background art includes transaction systems that employ smart cards (i.e. cards with an IC chip) for storing data in a portable manner. Smart cards are advantageous in such transactions systems as they can store data in a secure manner; this makes them suitable for storing monetary value, such as in the form of “electronic coupons” (or “e-coupons”). A suitable electronic terminal is used to read, validate and mark (or “clip”) the e-coupons when they are redeemed for the benefits associated with them.

Such a system is typically made secure by employing cryptographic keys stored on the smart card and/or in the terminals. These keys are used by the smart cards and the smart card terminals to authenticate each other; the smart card gives the terminal access to the e-coupon(s) on the smart card only if this authentication is successfully performed.

However, it is cumbersome and costly to manage these cryptographic keys, as in the background art they are stored in each smart card and terminal. This is particularly so when smart cards are shared between organizations, such as where one organization wishes to allow another to access the first organization’s smart cards. Sharing of access to the smart cards require sharing of cryptographic secrets and such sharing reduces

accountability and increases the risk that the cryptographic secrets will be exposed or otherwise compromised.

Summary of the Invention

The present invention in a first aspect provides, therefore, a data storage system comprising:

a user token for storing said data; and

a data terminal for reading from and writing to said token;

wherein said data terminal includes a first module for generating a digital signature from at least some of said data and for writing said data and said signature to said token, and a second module for reading said data and said signature from said token, for regenerating said signature from at least some of said data in the same manner as said first module, and for comparing said signature read from said token with said regenerated signature to determine whether said signature is authentic.

Thus, the signature is generated from at least some of the data, so – in some of embodiments – it may be generated from all the data, in others from a subset of the data, and in still other embodiments from a combination of some or all of the data and other data.

In one embodiment, the data includes token identification data. In a particular embodiment, the data terminal is operable to read said token identification data from said token rather than from said data, and to perform said regenerating of said signature on the basis of said token identification data so read.

Thus, the system can detect whether the signature has been generated from the token on which the signature is stored, or – if not – has been generated on some other token and

copied to the immediate token.

It should be understood that the terminal may comprise a terminal housing with token reader, and a processor located remotely from the housing but in electronic communication therewith. In such embodiments, the first and second modules may be located with the processor.

The signature may be in the form of a message authentication code, and that code may be generated by means of a cryptographic key.

In one embodiment, the data terminal system is configured to write the data and the signature to the token as a record that can be read by one or more other data terminals without prior authorization of such other data terminals.

That is, the record can be read by anyone – the data's integrity is provided, rather, by the use of the digital signature.

The first and second modules may be provided as a single module (particularly since the signature generation and regeneration are performed in the same manner).

In a particular embodiment, the data storage system is an entitlement management system, wherein said token is one of a plurality of customer cards (such as smart cards), and said data terminal is one of a plurality of transaction terminals. A transaction terminal may be in the form of, for example, a credit card payment terminal, a personal computer, a personal digital assistant, a set-top box, or a mobile handset, where necessary provided with a suitable token reading peripheral device and software. Further, the data in such embodiments may be in the form of an electronic coupon.

The present invention in a second aspect provides a method of storing data comprising:

generating a digital signature from at least some of said data;

writing said data and said signature to a user token;

subsequently reading said data and said signature from said token;

regenerating said signature from at least some of said data in the same manner as said generating of said signature; and

comparing said signature read from said token with said regenerated signature to determine whether said signature is authentic.

In one embodiment, the data includes token identification data, and the method includes generating the signature from the data including at least the token identification data. In a particular embodiment, the method includes reading the token identification data from the token (rather than from said data), and performing said regenerating of the signature on the basis of the token identification data so read from the token. By this approach, it is possible to determine whether the data had been altered without a proper signature being generated for the altered data, thus rendering the data invalid.

Thus, the signature may be generated from any desired subset of the data but – in this embodiment – that subset includes the token identification data.

The method may include generating said signature in the form of a message authentication code, possibly by means of a cryptographic key.

The method in one embodiment includes writing the data and

the signature to the token as a record that can be read by other data terminals without authorization.

In one embodiment, the method is used to store data in an entitlement management system, wherein said token is one of a plurality of customer cards. The data in such embodiments may be in the form of an electronic coupon.

In the various aspects of the present invention, the data may constitute a data record that is one of a plurality of such data records. The user token may then include software for automatically assigning a progressively incremented counter to each of these data records, so that each of the records is associated with a counter number that is assigned by this software. The terminal would preferably have no control over the counter value. In such embodiments, the signature for each data record is a function of the counter. It should be understood that, while the counter is described as “incremented”, this term is meant in the broadest sense and not merely to suggest that the counter’s value is increased by one each time. For example, the counter may be increased by some other value each time or, indeed, decreased or otherwise progressively altered each time, provided that a unique value is assigned to each data record so that such duplication can be detected.

Thus, if one copies a data record with a valid signature and adds it back onto the user token as another data record, the copy – although having a signature possibly calculated with the correct card number - would be assigned a new counter value (such as N+1). Hence, unless the signature is regenerated using the new counter value (e.g. N+1) before being written to the user token, the copy will be rendered invalid.

When the data storage system of the invention comprises an

entitlement management system, or the method of the invention is used to store data in an entitlement management system, and the data is in the form of an electronic coupon, a valid coupon may be redeemed and its value offset against the price of immediate purchase. Indeed, in some embodiments the redeemed electronic coupon may have been generated on the basis of that immediate purchase.

Brief Description of the Drawing

In order that the invention may be more clearly ascertained, an embodiment will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 is a schematic view of a transaction system according to an embodiment of the invention;

Figure 2 is a schematic view of a point-of-sale terminal and a customer card of the system of figure 1; and

Figure 3 is a schematic depiction of the Message Authentication Code generation procedure of the system of figure 1.

Detailed Description of Embodiments of the Invention

According to an embodiment of the present invention, there is provided a transaction system, shown schematically at 100 in figure 1. The system 100 includes a transaction server 102 and a plurality of point-of-sale ("POS") transaction terminals 104; the POS terminals communicate with the server by means of a public computer network, in the form of the internet 106.

The system 100 also includes user tokens in the form of customer smart cards (not shown in this view); these are issued to respective customers so that those customers can access and therefore use the system 100.

Figure 2 is a schematic view 200 of a representative POS terminal 104 and a customer card 202. The POS terminal 104 includes a digital processor 204 and, connected thereto, non-volatile memory 206 and random-access memory 208. The POS terminal 104 also includes a keypad 210, a receipt printer 212, a display unit in the form of a liquid crystal display 214, and a card acceptor 216. The card acceptor 216 is providing for reading from and writing to the customer cards 202, and conform to International Standards 7816 Parts 1 to 3 (such as those found on Electronic Draft Capture terminals used in credit card payment systems conforming to the Europay-Mastercard-Visa or EMV standard specifications).

Each customer card 202 includes an integrated circuit chip 218 comprising a digital processor 220 and, connected thereto, read-only memory 222 containing software (for performing a number of functions) in the chip 218, random-access memory 224, non-volatile memory 226 (which can be freely accessed) and an input/output interface 228. The input/output interface 228 is configured to communicate with the card acceptor 216 of the POS terminal 104.

Each customer card 202 includes a file stored in non-volatile memory 226 and referred to as the "coupon file", which can be accessed without initial mutual authentication; this allows any POS terminal 104 to read and modify data in the Coupon File without employing any cryptographic or other key. Each customer card 202 also contains a card identifier, being card identification information that – in this embodiment – comprises a card number. This card number is readable by the POS terminals. The POS terminals are provided in their non-volatile memory 206 with software (referred to as "issuing" and "redemption" modules) so that the terminals 104 can both write e-coupon records to the coupon files and allow the redemption of such e-coupons.

The e-coupon includes e-coupon data and a digital signature in the form of such a Message Authentication Code (MAC). The e-coupon data comprises a card identifier, a coupon identifier, validity dates (i.e. a date or dates defining the period during which the e-coupon is valid), the value of the e-coupon, the terminal identity number of the terminal that generated the coupon, and the date and time the e-coupon was issued or generated. The MAC is generated according to ANSI 9.9 standard specification, using cryptographic key known only to the issuer of the e-coupon. The card identifier is that of the card to which the e-coupon was originally issued and thus, in this embodiment, comprises a card number that is unique to that card. The coupon identifier comprises data indicative of or information about the marketing campaign under which the coupon was issued (e.g. a campaign identifier), the merchants or service providers to whom the coupon is applicable, a serial number, or any combination of these.

The e-coupon data is used, together with a cryptographic key, to generate the MAC for the e-coupon. Hence, the MAC is a signature that is derived from the e-coupon data itself and, because that data includes the original card number, is tied to the particular customer card to which it was originally issued.

Figure 3 is a schematic depiction of the MAC generation procedure 300. Referring to figure 3, this procedure employs an initial vector IV that is kept as a secret so that the resulting data block to be encrypted in the derivation of the MAC is unknown; this is essential to the security of the algorithm. The procedure also uses a cryptographic key (the MAC key). According to this procedure, the e-coupon data – including the card number - is divided into 8-byte blocks, $Data_{1\text{-}8}$ being the first 8-

byte block, $Data_{9-16}$ the second 8-byte block, and so on. Thus, an Exclusive OR operation is performed on the initial vector "IV" and $Data_{1-8}$. The triple DES (Data Encryption Standard) operation is performed on the result using the MAC Key. The resulting output vector is the input for a repeat of the Exclusive OR operation and triple DES steps, but this time the next portion of the e-coupon data ($Data_{9-16}$) is used, as shown in figure 3.

This process is repeated until all of the 8-byte blocks of e-coupon data have been used. The last output is the MAC.

Alternatively, in this embodiment the IV may be created by generating a "message digest" of the e-coupon data using commonly used hashing algorithms such as SHA or MD5, and then generating the MAC using the resulting hash as input to the MAC generation procedure described above.

In use, system 100 is employed by customers either to store e-coupons issued by retailers or other service providers, or to redeem such e-coupons. When an e-coupon is issued, the POS terminal 104 – by means of its issuing software module – generates the e-coupon (including coupon data and MAC), and writes the e-coupon to the coupon file on the customer card 202. The MAC is generated as described above and illustrated in figure 3.

Depending on the coupon issuing authority and as programmed in the issuing module, the "value" of the e-coupon may be expressed as, for example, discount entitlement information (e.g. percentage of discount), an absolute monetary value (e.g. $10), or an "electronic ticket" comprising entry permission (such as to a cinema to watch a movie, take a ride on a train or bus, etc.).

When a customer wishes to redeem an e-coupon (or in some

cases a part thereof), the redemption module of the POS terminal 104 to which the card 202 is presented reads the coupon file, locates an e-coupon valid for the date, place, Coupon Id, etc. of the transaction, and verifies the MAC for the e-coupon by recomputing the MAC using the e-coupon data and the procedure described above. If the redemption module finds that the regenerated MAC is the same as the MAC stored in the coupon file on the customer card 202, the e-coupon is deemed valid and the POS terminal 104 allows the customer to redeem the e-coupon for the benefits encoded in the "value" field of the e-coupon. If the customer does so, the POS terminal 104 removes the redeemed e-coupon from the coupon file.

The software of the issuing and redemption modules uses the card number of the customer card 202 as recorded in the e-coupon in the derivation of the MAC; this associates the e-coupon with the particular card. Since the card number of each customer card 202 is separately readable from the card by the POS terminal 104, the redemption module can detect when the e-coupon is inconsistent with the card in which it is recorded, that is, has been copied from another card. If this is detected, the redemption module rejects such a copied e-coupon and deletes it from the customer card 202.

The MAC also allows the receiving POS terminal to check – by determining any such inconsistencies between MAC and regenerated MAC - whether the e-coupons' coupon data has been altered without the proper MAC key; if the MAC is invalid, the POS terminal rejects the e-coupon or e-coupons.

Thus, the issuer of e-coupons need only have a cryptographic key (the MAC key) and the IV –in order to generate MACs, and to provide the MAC key and the IV to merchants and service providers who will ultimately accept

the e-coupons for redemption. Authentication keys are not required when accessing the coupon files on the customer cards 202, which simplifies the sharing of the customer cards between multiple parties. One example of the sharing of cards might be where a large retailer collaborates with a number of banks to issue coupons to holders of the banks' cards; the retailer would subsequently accept the coupons for redemption, either at the same retailer or at other partner retailers. This embodiment would allow the various participants to use customer cards from all the participating banks without first exchanging cryptographic keys for card authentication and access.

The system 100 can be further enhanced so that coupon records redeemed at the terminal are checked against a list of previously redeemed coupons to prevent cardholders from making copies of the e-coupons and redeeming the coupons multiple times (if the business rules for coupon redemption so prohibit).

The customer card 202 may also contain further applications, such as a credit card payment application and a loyalty application. Further, the POS terminal 104 is configured to inform the customer or other cardholder of any coupon award being issued in association with a transaction by displaying and/or printing on the receipt printer 212 the relevant messages pertaining to the e-coupon award.

In addition, records of redeemed e-coupons are either deleted from the customer card 202 if they are not required for further analysis or processing, or captured by the POS terminal 104 and transmitted to the server 102 for further analyses and management decision support.

A customer card 202 is presented at a POS terminal 104 for

redemption of an e-coupon typically in connection with the payment for purchase of an item. The customer card 202 may, in such circumstances, be a payment card such as a credit card complying with the EMV standard. In such cases, the POS terminal may be programmed to locate, as part of the payment process, an applicable coupon in the non-volatile memory 226, mark the coupon as 'redeemed', and then proceed with the payment authorization process based on a nett payment amount that is equal to the sales amount less the value of the redeemed e-coupon. By thus linking the redemption of an e-coupon with the payment process, it is possible to minimize the risk that the retailer will fail to process the e-coupon electronically at the POS terminal 104. Such an arrangement is useful to prevent the retailer from under-reporting the number of e-coupons presented for redemption, as retailers may be tempted to under-report when they have to pay a fee to a service provider for each e-coupon presented for redemption.

In another embodiment, the customer card 202 includes software in non-volatile memory 226 for automatically assigning a progressively incremented counter to each of the e-coupons written to the free accessible non-volatile memory 226, so that each of the records is associated with a counter number that is assigned by this software. The transaction terminals 104 have no control over the counter value. In this embodiment, the signature for each e-coupon is a function of the counter. To generate the signature, a transaction terminal 104 first interrogates the non-volatile memory 226 of a customer card 202 to determine the counter number (N) to be associated with the next e-coupon to be written to the non-volatile memory 226, and includes that counter value N in the data used in the derivation of the signature. When the e-coupon is written to the non-volatile memory 226, the customer card 202 automatically assigns N to that record. Thus, if one

were to duplicate that e-coupon (having a valid signature) by reading it from and immediately writing it back to the non-volatile memory 226 of a particular customer card 202, the second copy would – when written - be assigned a new counter value N+1. Both would have the same signature, so both would have a signature generated on the basis of the correct card number. However, only the original would have a signature consistent with its counter value. Hence, unless the signature is regenerated using the new counter value N+1 before the copy of the e-coupon is written to the non-volatile memory 226, that copy will be rendered invalid.

In yet another embodiment, each of the terminals 104 may be in the form of a “set-top box”, of the type used to access cable and satellite television networks; in this embodiment, the network 106 is in the form of the television network and thus comprises a fibre optic cable network or a satellite network. Each of the set-top boxes is equipped with a smart card reader and an issuing module. The issuing module can be installed at the manufacture or sale of the set-top box, or programmed subsequently via the network 106. The set-top box can then be controlled remotely to write e-coupon data and signatures into smart cards. This occurs when a customer, possibly prompted by messages broadcast on the television, inserts his or her smart card into such a set-top box. The smart card loaded with e-coupons and can then be used at merchant outlets equipped with conventional POS terminals that have been loaded with the redemption module for the purpose of redeeming the e-coupons loaded by a set-top box.

Modifications within the scope of the invention may be readily effected by those skilled in the art. It is to be understood, therefore, that this invention is not limited to the particular embodiments described by way of example hereinabove.

Claims:

1. A data storage system comprising:

a user token for transporting said data; and

data terminal for reading from and writing to said token;

wherein said data terminal includes a first module for generating a digital signature from at least some of said data and for writing said data and said signature to said token, and a second module for reading said data and said signature from said token, for regenerating said signature from at least some of said data in the same manner as said first module, and for comparing said signature read from said token with said regenerated signature to determine whether said signature is authentic.

2. A system as claimed in claim 1, wherein said data includes token identification data.

3. A system as claimed in claim 2, wherein said data terminal is operable to read said token identification data from said token rather than from said data, and to perform said regenerating of said signature on the basis of said token identification data so read.

4. A system as claimed in claim 1, wherein said signature is in the form of a message authentication code.

5. A system as claimed in claim 1, wherein said terminal is operable to generate said signature by means of a cryptographic key.

6. A system as claimed in claim 1, wherein said data terminal system is configured to write said data and said signature to said token as a record that can be read by one or more other data terminals without prior authorization

of such other data terminals.

7. A system as claimed in claim 1, wherein said first and said second modules are provided as a single module.

8. A system as claimed in claim 1, wherein said data storage system is an entitlement management system, wherein said token is one of a plurality of customer cards, and said data terminal is one of a plurality of transaction terminals.

9. A system as claimed in claim 8, wherein said data is in the form of an electronic coupon.

10. A system as claimed in claim 9, wherein said data terminal is operable to locate any valid electronic coupons stored on any of said customer cards presented for reading to said data terminal.

11. A system as claimed in claim 10, wherein said data terminal is operable to redeem the value of a valid electronic coupon so located against the price of an immediate purchase.

12. A system as claimed in claim 1, wherein said data constitutes a data record that is one of a plurality of such data records, and said user token includes software for automatically assigning a progressively incremented counter to each of these data records.

13. A system as claimed in claim 12, wherein said signature for each data record is a function of said counter.

14. A method of storing data comprising:

generating a digital signature from at least some of said data;

writing said data and said signature to a user token;

subsequently reading said data and said signature from said token;

regenerating said signature from at least some of said data in the same manner as said generating of said signature; and

comparing said signature read from said token with said regenerated signature to determine whether said signature is authentic.

15. A method as claimed in claim 14, wherein said data includes token identification data, and the method includes generating the signature from the data including at least the token identification data.

16. A method as claimed in claim 15, wherein said method includes reading said token identification data from said token, and performing said regenerating of said signature on the basis of said token identification data so read from the token.

17. A method as claimed in claim 14, including generating said signature in the form of a message authentication code.

18. A method as claimed in claim 14, including generating said signature by means of a cryptographic key.

19. A method as claimed in claim 14, including writing said data and said signature to said token as a record that can be read by other data terminals without authorization.

20. A method as claimed in claim 14, wherein said method is used to store data in an entitlement management system, and said token is one of a plurality of customer cards.

21. A method as claimed in claim 20, wherein said data is in the form of an electronic coupon.

22. A method as claimed in claim 21, including locating any valid electronic coupons stored on any of said customer cards presented for reading to a data terminal.

23. A method as claimed in claim 22, including redeeming the value of a valid electronic coupon so located against the price of an immediate purchase.

24. A method as claimed in claim 14, wherein said data constitutes a data record that is one of a plurality of such data records, and said method includes automatically assigning a progressively incremented counter to each of these data records.

25. A method as claimed in claim 24, wherein said signature for each data record is a function of said counter.

26. A system as claimed in claim 1, wherein:

said user token has unique token identification data and a data storage divided into a plurality of records, each of said records being associated with a unique number stored on said user token and having a value that is incremented by said user token each time data is written into said respective record, and said value of said unique number cannot be set by said data terminal;

wherein said data includes said respective unique number and said token identification data.

27. A system as claimed in claim 26, wherein said data terminal is operable to read said token identification data and said respective unique number from said user token rather than from said data, and to perform said

regenerating of said signature on the basis of said token identification data so read.

28. A system as claimed in claim 1, wherein said user token includes a free access data storage, whereby said data storage can be accessed without providing cryptographic data, a key, secret data or unique token identification data.

29. A method as claimed in claim 14, wherein:

said user token has unique token identification data and a data storage divided into a plurality of records, each of said records being associated with a unique number stored on said user token and having a value that cannot be set by a data terminal employed to write said data to said user token;

said data includes said unique token identification data and said respective unique number; and

said method comprises said user token incrementing said respective unique number each time data is written into said respective record.

30. A system as claimed in claim 29, wherein said user token includes a free access data storage, whereby said data storage can be accessed without providing cryptographic data, a key, secret data or said token identification data, and said method includes generating said signature from at least said token identification data and said respective unique number.

31. A method as claimed in claim 30, wherein said method includes reading said token identification data and said respective unique number from said user token, and verifying said signature on the basis of said data so read from said user token.