

AUTHENTICATION TECHNIQUE

This invention relates to a technique for authenticating products, cards, tokens and the like so as to combat illicit copying thereof.

5 Copying of products, cards, tokens and the like (hereinafter referred to generally as "valued articles" to avoid repetition) is a major problem and various techniques have been devised to combat such copying. In particular, techniques have been devised based upon the inclusion, on valued articles, of twin sets of data, one set being characteristic of the holder of the valued article or its producer or issuer (as the case may be) and the other set
10 being derived from the first set by some unique route that is difficult to replicate. When the valued article is to be authenticated, the two sets of data included thereon are read, the derivative set by way of a device which is conscious of the aforementioned unique route, and the two sets of data thus recovered are compared to authenticate the valued article, or at least to show that the person purporting to be the owner or holder of the valued article is
15 not an impostor.

Techniques of this general kind are described for example in United States Patents nos. 4,879,747 and 4,995,081 to Leighton and Micali.

This invention aims to further improve upon such techniques by (inter alia) taking advantage of certain special characteristics of recording media available for incorporation in
20 valued articles.

According to a first aspect of the invention, there is provided an authentication means for an article of value, comprising first and second data-storage means being carried by the article, each data-storage means storing data for authenticating or identifying the article and/or a transaction associated with the article, the first data-storage means storing
25 first data as a non-random permanently structured magnetic characteristic which varies from place to place on the first storage means, the second storage means storing data obtained by operation of the secret key of a secret key/public key cryptosystem pair upon data comprising the first data and additional data.

Such an authentication means can make copying and counterfeiting more difficult
30 than with a permanently structured magnetic characteristic alone whilst enabling conventional read heads to be employed to read the data in the first storage means.

According to a second aspect of the invention, there is provided a method of authenticating an article of value, comprising:

- a) storing authentication data in a first storage means carried by the article as a non-random permanently structured magnetic characteristic which varies from place to place on the storage means,
- 5 b) operating on said authentication data and additional data using the secret key of a secret key/public key cryptosystem pair hereby creating encrypted data,
- c) storing the encrypted data in a second storage means carried by the article,
- d) reading the encrypted data from the second storage means,
- 10 e) operating on the encrypted data with the public key of said cryptosystem pair to give decrypted authentication data and decrypted additional data, and
- f) comparing the decrypted authentication data with the authentication data stored in the first storage means thereby authenticating the article of value and/or the additional data..
- 15

In order that the invention may be clearly understood and readily carried into effect, some embodiments of the invention will now be described (by way of example only) with reference to the accompanying drawings, of which:

20 Figure 1 shows a credit card which can be authenticated by means of one example of the invention, and

Figure 2-4 illustrates schematically and by way of example the operation of various features of the invention in a typical transaction.

25 Figure 5 shows a block diagram of a method of authentication according to an aspect of the invention.

Referring now to Figure 1, there is shown in outline a technique in accordance with one example of this invention.

30 A valued article, in this case a credit card, is shown schematically at 1. The credit card 1 comprises conventional printed and/or embossed material 2 including holograms and trade marks or logos characteristic of the card issuing and/or handling company. There is also open information about the card holder and open account information and, on the reverse side, a signature strip 3 and a magnetic strip 4.

35 In accordance with this example of the invention, the magnetic strip 4 is formed with a magnetic watermark in the manner described, for example, in UK patent no. 1331604 whereby a structural variation of a magnetic characteristic from place to place

along the strip is indelibly formed into the strip. This information can be read quite readily but the structural variation is exceedingly difficult to replicate in any manner which is not immediately rejected by the technique used to read the relevant information. Thus the information stored on the card 1 in strip 4 although overt is secure. Tape containing the structural function described above is marketed by THORN Secure Science International Ltd under the trade mark Watermark Magnetism and thus the structural variation aforesaid will be referred to hereinafter as a magnetic watermark.

To add further security, however, this example of the invention provides that the information recorded indelibly in strip 4, together with further information, is operated on, as described hereinafter, to generate a second piece of information which (hereinafter called a "certificate") is also recorded on the card 1, but in a conventional "soft magnetic" form; either on the strip 4 itself or on a further strip (not shown). It will be appreciated that information can be recorded conventionally on strip 4, superimposed upon the structural variations which have been referred to hereinbefore. Usually, there are two or more tracks of the strip 4 which are assigned to conventionally recorded data, and the strip is read by a composite head which contains normal magnetic heads for the conventionally recorded information and one or more special heads for the information recorded by structural variation.

The operation upon the information recorded indelibly in strip 4 referred to above comprises, in its most basic form, signature by the secret key of a cryptosystem pair. The signed information is recorded on the card 1, in this example on one of the tracks of strip 4 read by a conventional head. It can thus be reproduced and, after being operated on by the public key of the cryptosystem pair to "de-sign" it, compared with the information indelibly recorded as described earlier, to confirm that the "de-signed" information contains information which matches that recorded indelibly as the magnetic watermark.

Thus not only is the card authenticated as genuine because it contains the magnetic watermark but also the transaction information recorded less securely on the card is authenticated because it contains the signed version of the watermark.

This prevents watermarked cards being acquired illegally and false information entered in the accessible, conventional recording tracks. It also enables the logistics of card manufacture and distribution to be made more secure, because card stock is useless without the watermarked magnetic stripe and vice versa, and even if the two are acquired together, they cannot be used without knowledge of the secret code used to sign the watermarked information for incorporation in the certificate to be recorded conventionally on the card.

Thus, in principle, the watermarked information is easy to read but difficult to replicate in a manner that will not be rejected on reading, and the conventionally recorded information, whilst easily read and replicated, does not reveal its connection through the secret key to the watermarked information.

5 The conventionally recorded information need not be recorded on the strip 4. It could, for example, be recorded on a separate magnetic strip on the card, or in a different medium altogether, such as an integrated circuit chip. In this latter event, the chip can be relatively cheap since it is not required to contain high levels of security or complex anti-copying procedures. In essence it operates as a low-level storage medium only.

10 The certificate information which is conventionally recorded, eg., on strip 4 or on a separate strip or in a chip, can usefully comprise a commencement date for the card's utility and also other information, such as the expiry date, credit limit, transaction availability and one or more pieces of information about the card-holder and/or biometric information derived from and characteristic to the holder.

15 In particular, the maiden name of the holder's mother might be included, as may basic physiological information such as height, hair colour, eye colour, etc., or a scan of a fingerprint or some other data peculiar to the card holder. In this latter respect, a particularly beneficial technique for deriving fingerprint data in a form that readily lends itself to recordal as described above is described in European Patent Application
20 No.91302280.2 (Publication No. 450786), the contents of which are incorporated herein by reference.

 The invention may, as mentioned previously, be used on a wide variety of value articles, such as (without limitation) sound recordings, spirits, vehicle components, and a wide range of secure documents, such as passports, identity cards, driving licences and the
25 like.

 It will be appreciated that, since the information recorded together with the signed version of the magnetic watermark, in the certificate contains a number of conformatory and/or instructional pieces of information, all of that information can be trusted as being genuine, since it was signed together with the watermark information, using the secret key.
30 Thus nothing that is outside the control of the card issuer/manufacture needs to be treated secretly or kept in confidence.

 The strength of the magnetic watermark and the use of the secret key is all that is required to obtain the significantly improved level of security provided by this invention.

Thus, the technique ensures that valued articles cannot be used before they have officially been issued, or after they have expired. For off-line transactions, the reader can be sure that card expiry data and credit limits, for example are genuine. If the off-line reader includes biometric sensing, the reader can also be sure that the registered card holder is present. During on-line operations, the credit limit, expiry date and PIN (if present) can be up-dated if required since the central computer can generate a new signed certificate to be written on the card.

Conveniently RSA public key cryptography is used, but alternative procedures can be used if desired. In any event, a particular "certificate" (ie., signed information including the watermark data) is relevant only to one specific card and could only have been generated by one specific issuer - the one with access to the secret key of the RSA (or other) cryptosystem pair. As a result, the certificate can be stored on a soft magnetic track with no loss of security.

Some refinements of and enhancements to the invention will now be described in order to explain more fully the operation of a typical system.

Secure operation of an extended system is largely concerned with communication among system components, some of which are more trusted than others. The functionality of several of those data links which are particularly relevant to valued articles, protected as described hereinbefore, will now be described.

A simplified diagram of key usage is shown in Fig. 2. As it is based on RSA public key cryptography, only the public keys are communicated. Each secret key remains in a highly secure location, within the organisation that generated it.

The system provider's public key (PPK) is stored within each card reader (CAD), in a memory location which cannot be overwritten. It is used by the CAD to check other data that has been signed by the provider, and is therefore trustworthy.

An example of this is each issuer's public key (IPK), which is signed by the system provider's secret key (PSK), as shown above.

In practice, there will be large numbers of CADs, each holding the same data. In addition, each CAD holds its own unique key (not shown), which distinguishes it from all other CADs, and enables it to communicate unambiguously with the issuer.

To initialise a card, the issuer first collects all the data that the CAD might need to know about the card holder and the card, as shown in Fig. 3 in a block marked DATA. This includes the number recorded as the magnetic watermark, the PAN, expiry date, PIN

policy, and so on, and is sufficient for the CAD to decide when an off-line transaction is appropriate.

The DATA block, when signed by the issuer's secret key (ISK), becomes the secure certificate, which is then copied onto a soft data area on the card.

5 In normal use, the CAD reads the certificate from the card, and decrypts the original data.

The production of updated certificates on-line also follows the above procedure, the CAD acting as intermediary between the issuer and the card.

10 The card is preferably provided with a transaction counter, which resides on the card, and the main purpose of which is to restrict the number of off-line transactions allowed before a new certificate is required. In addition, the availability of a transaction count allows the issuer to carry out further checks against attempted fraud. Printing the transaction number on each receipt gives the card holder a convenient indication of card usage.

15 In Fig. 4 the CAD has read the DATA block from the certificate, as described above. Held within the data block is the issuer's off-line policy, and the maximum off-line transaction count. The CAD also reads the card transaction count (CTC) from the card. It then has enough information to decide whether the transaction can continue off-line or not.

20 In either case, provided that the transaction is approved, the CAD increments the CTC on the card, and prints the CTC as part of the card holder's receipt.

The increment line to the card has been shown in Fig. 4 as a separate connection, for clarity. In practice, it would be part of a digital interface, whose operation could not readily be blocked. To check that the transaction count has indeed incremented, the CAD re-reads the new transaction count from the card.

25 It is highly unusual for systems to be provably secure. Even when a system is believed to be secure, it is wise to plan for the contingency that supposedly secret information might become public knowledge. In the system described, the secret key of the system provider, and the secret keys of the issuers, should be kept securely. However, even if these keys become known, the system provided by this invention can be re-
30 configured, quickly and economically to use new key sets.

For instance, suppose that an issuer's secret key becomes known. The consequent threat is that a fraudster might produce certificates purporting to come from the issuer, and thereby use out-of-date cards for off-line transactions.

To recover from this situation, the issuer generates a new key set, and gets the public key signed by the system provider. As each CAD comes on-line, the suspect public key is replaced by the new one. To allow this, the CAD must have a protocol which allows issuer keys to be updated. As the new key is signed by the system provider, it can be
5 accepted by the CAD as genuine.

Then, as each card is presented to the updated CAD, any card using the old public key is given an on-line transaction, which results in its next certificate being signed with the new public key. Furthermore, an updated card, when presented to a CAD which was still using the old public key, would result in an on-line transaction during which the CAD
10 would be updated.

Thus the procedure required to change the issuer's public key is secure, fast, economical, and transparent to the user.

The procedure for updating the system provider's key is similar, but somewhat more complex, since the system provider is the centre of trust. One option is to store a choice of
15 system provider public keys in each CAD, when the system is initialised. If one key becomes compromised, the system can move over to the next key. This involves re-signing all the issuer's keys, and updating the CADs as and when they come on line. The cards need not be updated. As before, the change is transparent to the user.

In the event that the article contains a PIN, that information may be secured within
20 a relatively inaccessible region of an integrated circuit chip. In this case, the card itself can check the PIN when keyed in. Alternatively, an encrypted PIN may be stored within the "certificate" on the article and the CAD can then check the PIN, as is presently done at off-line ATMs.

In another embodiment, the integrated circuit chip is replaced by a two dimensional
25 bar code which can be read optically.

Figure 5 shows a flow diagram of a method according to the second aspect of the invention. The blocks have the following significances. Block 50 denotes storing authentication data in a first storage means carried by the article as a non-random permanently structured magnetic characteristic which varies from place to place on the
30 storage means.

Block 51 denotes operating on said authentication data and additional data using the secret key of a secret key/public key cryptosystem pair hereby creating encrypted data. This will normally be performed by, for example, the card issuing authority in the case of credit or other cards.

Block 52 denotes storing the encrypted data in a second storage means carried by the article.

Block 53 denotes reading the encrypted data from the second storage means.

5 Block 54 denotes operating on the encrypted data with the public key of said cryptosystem pair to give decrypted authentication data and decrypted additional data. This will normally be performed by, for example, the card reading machine in the field in the case of credit or other cards.

10 Block 55 denotes comparing the decrypted authentication data with the authentication data stored in the first storage means thereby authenticating the article of value and/or the additional data. This will normally also be performed by the card reading system.

In general, the data stored in the second storage means may be read magnetically, optically or electronically depending upon the nature of the storage means employed.

CLAIMS

This Sheet Has Been Replaced



1. Authentication means for an article of value, comprising first and second data-storage means being carried by the article, each data-storage means storing data for authenticating or identifying the article and/or a transaction associated with the article, the first data-storage means storing first data as a non-random permanently structured magnetic characteristic which varies from place to place on the first storage means, the second storage means storing data obtained by operation of the secret key of a secret key/public key cryptosystem pair upon data comprising the first data and additional data.
2. Authentication means according to claim 1 in which the first and second storage means comprise respective tracks on a common magnetic strip.
3. Authentication means according to claim 1 in which the second storage means comprises a magnetic strip separate from said first storage means.
4. Authentication means according to claim 1 in which the second storage means is carried by the first storage means.
5. Authentication means according to claim 1 in which the second storage means comprises a two dimensional bar code.
6. Authentication means according to claim 1 in which the second storage means comprises an integrated circuit.
7. Authentication means according to claim 6 in which the integrated circuit includes relatively open and relatively secure data storage areas, the relatively secure data storage area storing a personal identification number (PIN) associated with an authorized user or possessor of the article of value.
8. An article of value having authentication means according to any preceding claim carried thereby
9. A method of authenticating an article of value, comprising:
 - a) storing authentication data in a first storage means carried by the article as a non-random permanently structured magnetic characteristic which varies from place to place on the storage means,



THIS SHEET HAS BEEN
REPLACED

10

This Sheet Has Been Replaced



- b) operating on said authentication data and additional data using the secret key of a secret key/public key cryptosystem pair hereby creating encrypted data,
- c) storing the encrypted data in a second storage means carried by the article,
- d) reading the encrypted data from the second storage means,
- e) operating on the encrypted data with the public key of said cryptosystem pair to give decrypted authentication data and decrypted additional data, and
- f) comparing the decrypted authentication data with the authentication data stored in the first storage means thereby authenticating the article of value and/or the additional data..



* C L M S *