Singapore Patent Application No. 200105667-0
SCM Microsystems GmbH

A Method of Securing Data in a Portable Mass Storage against Unauthorized Copying

The invention relates to a method of securing data in a portable mass storage against unauthorized copying and a replay system for performing the method.

Multimedia contents and software are quite predominantly disseminated commercially on data carriers which can be written to only once and constitute the trade product together with the contents stored thereon. A separate commercial dissemination of the contents independent of such data carriers would in principle be possible, for instance by remote access to networks including a payment function, but fails because of a lack of protection against unauthorized copying.

From Utility Model Document DE 298 02 270 U1 there is known a multimedia system comprising a base station, a portable operating device and a communication module for use in the multimedia system. In this reference, the communication between the aforesaid components and between the user and the multimedia system, respectively, is described; there are also quoted possibilities for the data security such as a supervision, implemented on a chip card, of an access to an order and payment function, without, however, explicitly disclosing a method of securing data.

The invention provides a method of securing data in a portable mass storage against unauthorized copying, which can be performed with little expenditure and using available technology. In accordance with the method of the invention the data is first stored in the mass storage in a scrambled form. In a replay system for the data at least one SAM module (Safe Access Module) is used which has stored

thereon a personal identity code of an authorized user. The descrambling keys required for descrambling the data are stored on the SAM module of the authorized user. Assigned to the data is an authorization code which is stored on the SAM module. Then an authorization code encoded by means of the personal identity code is formed on the SAM module. This encoded authorization code is stored on the mass storage with the scrambled data. Prior to a replay of the data, the encoded authorization code is decoded by the SAM module by means of the personal identity code. The decoded authorization code is then compared with the authorization code stored (non-encoded) on the SAM module. The descrambling by means of the descrambling keys of the data read out of the mass storage is then enabled only when the authorization codes are identical. Owing to this method, which can be performed using very simple hardware, a personalization of the data on the mass storage is effected. For the non-scrambled replay of the data an authorization code is required which may only be obtained via the SAM module of the authorized user because it is linked with the personal identity code of the authorized user.

In a further development of the method the descrambling keys required for descrambling the data are also encrypted with personal data of the authorized user stored on the SAM module, so that they can be decrypted only when using the appropriate SAM module.

In a further configuration of the method the data is output inseparably with a personal identification of the authorized user when the data is replayed via a suitable replay system. The personal identification may consist of a logo or the like, which in the case of image data is displayed in a corner of the picture field.

The replay system in accordance with the invention for performing the method essentially comprises: a read module for accommodating the mass storage, which is preferably a medium which is adapted to be written to by the user, such as, e.g., a miniaturized hard disk or an optical storage disk adapted to be written to by the user; a card reader for the SAM module; a data conditioning electronics for descrambling the data read out of the mass storage; and an output device for the

descrambled data. In order to be able to obtain data via a remote network, for instance from the Internet, preferably a payment system for the conditional access to a data provider via the remote network is additionally provided. The payment system is based on a chip card reader which in the preferred embodiment is designed as a plug-in type PC card in the PCMCIA format.

Further advantages and features of the present invention will be apparent from the following description and from the drawings to which reference is made and in which:

Fig. 1 is a block diagram of a replay system for carrying out the method according to the invention;

Fig. 2 shows an algorithm for the personalization of the data in the mass storage according to the method of the invention;

Fig. 3 shows an algorithm for checking the replay authorization according to the method of the invention;

Fig. 4 shows the replay process according to the method of the invention.

The block diagram as shown in Figure 1 of a replay system for performing the method in accordance with the invention diagrammatically shows the essential components of the system. An interface device accommodated in a compact housing is generally denoted by reference number 10 and comprises three interfaces 12, 14, 16 for plug-in type components as well as an output terminal 18 for a video output device 20. The interface 12 has a plug-in socket for a mass storage 22 which has a fingerprint sensor 24 on a surface accessible to the user. A first SAM module 26 is a part of the interface 12. A second SAM module is contained in the plug-in type mass storage 22, which may be a miniaturized hard disk or also a semiconductor storage, for instance in FLASH technology.

The interface 14 accommodates a chip card reader 28 in the format of a PC card (abbreviation for PCMCIA card). In conjunction with a chip card 30, also referred to as smart card, the chip card reader 28 constitutes a payment system for

the conditional access to a provider of multimedia contents and the like, in particular via the Internet.

Connected to the interface 16 is a modem 32 or a network adapter. Via the modem 32 or the network adapter a remote network may be accessed, more particularly the Internet.

A television set or a monitor is connected to the output terminal 18, which may be designed as a SCART interface.

The replay system may further be fitted with an infrared remote control 34.

An internal processor 36 includes the necessary functionality for descrambling and conditioning of the data read out of the mass storage 22 for the replay on the output device 20. The processor 36 is coupled with a synchronized clock 37, which is a part of a monitoring device by means of which the conditioning of the data for replay is made dependent on a certified time stamp which is recorded on the mass storage 22 with the data.

The method in accordance with the invention is illustrated in the charts of Figures 2, 3 and 4. It substantially consists of three stages. In the first stage of the method, illustrated in Figure 2, a personalization of the data in the mass storage takes place. The process is started by transmitting a system certificate to the provider of the data. The data involved is more particularly multimedia information, MMI in short. By the system certificate the replay system identifies itself before the MMI provider as a suitable system. A private key is then received on the part of the MMI provider from the SAM module of the replay system to generate a replay authorization code. The private key involved may be a personal identity code or also compressed data derived from the fingerprint sensor 24, or a combination thereof. The replay authorization code is then stored on the SAM module.

Subsequently, payment is effected by means of the payment system 28, 30, whereupon the MMI data is downloaded in a scrambled form and stored on the

MMI mass storage 22. The MMI keys necessary for descrambling the MMI data are thereafter transferred to the SAM module in an encrypted form and stored there. The MMI provider further sends an encrypted watermark which may be stored in the SAM module if the volume of the corresponding data is comparatively small; otherwise, storage is effected in the mass storage. Optionally, a certified time stamp is sent with the MMI data and is recorded on the mass storage 22.

As the last step of the first process stage, an encrypted authorization code is sent by the MMI provider and is stored in the MMI mass storage together with the MMI data.

If the data supplied by the fingerprint sensor is incorporated into the private key, such data may be processed or operated on by the SAM module integrated in the mass storage 22.

The method step as shown in Figure 3 relates to the verification of the replay authorization. To this end, the encrypted authorization code read out of the mass storage is decrypted in the SAM module by means of the private key; the authorization code retrieved in this manner is then compared with the authorization code stored on the SAM module. In case the authorization codes are identical, the replay process will be enabled.

In the replay process as illustrated in Figure 4, first the MMI key is decrypted in the SAM module by means of the private key. Then the MMI data is read out of the mass storage and is descrambled by means of the decrypted MMI key. The descrambled MMI data is then overlaid with the personal logo or the watermark and supplied to the output device.

Due to the certified time stamp optionally recorded with the MMI data the permitted replay of the data can be limited in time.

16 SEP 2003

Claims

1. A method of securing data in a portable mass storage (22) against unauthorized copying, in particular for the protection of multimedia information and software, characterized in that:

a) the data is stored in the mass storage (22) in a scrambled form;

b) in a replay system for the data at least one personal SAM module for secured access (27), in the following referred to as SAM module, is used which has stored thereon a personal identity code of the authorized user;

c) at least one descrambling key required for descrambling the data is stored on the SAM module (27) of the authorized user;

d) an authorization code is assigned to the data and is stored on the SAM module (27);

e) an authorization code encoded by means of the personal identity code is formed on the SAM module (27);

f) the encoded authorization code is stored on the mass storage (22);

g) prior to a replay of the data, the encoded authorization code is decoded by the SAM module (27) by means of the personal identity code;

h) the decoded authorization code is compared with the authorization code stored on the SAM module (27), and descrambling by means of the descrambling key of the data read out of the mass storage (22) is enabled only when the authorization codes are identical.

16 SEP 2003

2. The method according to claim 1, characterized in that prior to the purchase of the data from a provider, a system certificate is transmitted from the SAM module to the provider and verified by the latter.

3. The method according to claim 1 or 2, characterized in that a session key is used for the secured transfer of the authorization code to the SAM module of the authorized user.

4. The method according to any of the preceding claims, characterized in that for personalizing the data on the mass storage (22) an identification consisting of personal features of the authorized user is formed and linked with the data in such a manner that the data can be output only with the identification.

5. The method according to any of the preceding claims, characterized in that the personal identity code of the authorized user is formed at least in part from data supplied by a fingerprint sensor (24).

6. The method according to any of the preceding claims, characterized in that the mass storage (22) is arranged in a module adapted to be plugged into a replay system.

7. The method according to claims 5 and 6, characterized in that the fingerprint sensor (24) is arranged on a surface of the plug-in type module.

8. The method according to any of the preceding claims, characterized in that the communication and transaction with the provider of the data is conducted by means of a first SAM module (26) arranged in the replay system, and the personalization of the data is carried out by means of a second SAM module (27) assigned to the mass storage (22).

9. The method according to claims 6 and 8, characterized in that the SAM module (27) assigned to the mass storage (22) is integrated in the plug-in type module.

10. The method according to any of the preceding claims, characterized in that the mass storage (22) is configured as a miniaturized hard disk.

16 SEP 2003

11. The method according to any of claims 1 to 9, characterized in that the mass storage (22) is configured as flash semiconductor storage.

12. The method according to claim 11, characterized in that the flash semiconductor storage is removably arranged in an interface module adapted to be plugged into the replay system.

13. The method according to claim 12, characterized in that the interface module comprises a SAM card reader.

14. The method according to any of the preceding claims, characterized in that for purchasing the data a communication and transaction with a provider is effected by means of a remote access to a network.

15. The method according to claim 14, characterized in that the transaction with the provider is effected using a card reader module which is adapted to be plugged into the replay system and which includes a chip card reader (28) and a SAM card reader accommodating the at least one SAM module (26).

16. The method according to any of the preceding claims, characterized in that the descrambling key is for its part encrypted with personal data stored on the SAM module and is decrypted with such data during replay.

17. The method according to any of the preceding claims, characterized in that a certified time stamp is generated and stored with the data on the mass storage (22).

18. A replay system for performing the method according to any of the preceding claims, characterized by:

- a read module for accommodating the mass storage (22);
- a card reader (28) for the SAM module;
- a data conditioning electronics for descrambling the data read out of the mass storage (22); and
- an output device (20) for the descrambled data.

19. The replay system according to claim 16, further characterized by a payment system based on a chip card reader (28), for conditional access to a data provider via a remote network.

20. The replay system according to claim 17, characterized in that the chip card reader (28) is configured as a plug-in type PC card in the PCMCIA format.

21. The replay system according to any of claims 18 to 20, characterized in that a monitoring device is provided which evaluates a certified time stamp read out of the mass storage (22) with the data.