Milestones, 12 Esther Carling Lane, Rotherfield Peppard, Henley-On-Thames, Oxfordshire RG9 5 PW (GB).

VEKARIA, Rasik [GB/GB]; 35 Tythurst Gardens, Ilford, Essex IG1 2QL (GB).

Agents: FROST, Alex, John et al.; Boulton Wade Tennant, Verulam Gardens, 70 Gray’s Inn Road, London WC1X 8 BT (GB).


Title: SOFTWARE AUTHENTICATION DEVICE

Abstract: An authentication device (80) has electrical connections (100, 110) to a device indicator (120). The device indicator (120) is formed from an electrochromic material which is caused to change colour and/or to reveal an underlying image in dependence upon communication with software that the device (80) is to authenticate. In use, a device reader/writer (70) is connected to a computer (20) into the memory of which is loaded a video game or the like. Before the video game is startable, a user is required to authenticate that game by inserting a valid authentication device (80) into the device reader/writer. Once authenticated, the game may start. Completion of various levels of the video game may allow the device reader/writer to cause, in turn, signals to be sent to the electrochromic material so as to alter its state.
Published: without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.
SOFTWARE AUTHENTICATION DEVICE

FIELD OF THE INVENTION

This invention relates to a device for software authentication, and particularly, but not exclusively, to a device for authenticating video games.

BACK TO THE INVENTION

Software piracy has become a significant problem in recent years. It has been estimated that, in 2000 and in the United States alone, software piracy was responsible for lost revenue totalling more than $2.6 billion. Up to a quarter of all business software in the US is estimated to be unlicensed, and for domestic use the figure is likely to be higher still.

In order to address software theft, a number of solutions have been proposed. Perhaps the best known of these is the use of a so-called certificate of authenticity (CoA). Here, a computer program when installed onto a computer prompts a user to input a product identification code or key. Typically, this is listed as an alphanumerical code printed on the software packaging or on ancillary documentation such as a user manual.

Once the user enters this identification code, the program takes the entered data and passes it to an encryption algorithm. The encryption algorithm processes the entered product identification code and compares the output with a value already stored in the software. If the result is a match, then installation continues, otherwise it halts until a correct product identification code is employed. Once entered correctly, the product identification code is no longer needed (unless the software has to be reinstalled).

The product identification code (when entered) may instead be hard coded into the software. Either
way, the problem with this approach is that it is easy for the security measures to be circumvented. Typically, a particular program product has the same product identification code for all copies of that product. Security (that is, prevention of copyright infringement) then depends upon valid licensees (users) not copying the program and providing it to others along with the product identification code. With current CD writing technology and the provision of the product identification code printed on the packaging of most original copies of programs, the CoA does not provide a high level of security against copyright theft.

An alternative approach to securing the software code from piracy is to protect the software itself using proprietary cryptography. This approach is favoured for use with video games consoles. Here, the disc or other storage medium is inserted into the video games console which decodes the encrypted software.

A number of these proprietary cryptographic methods have now been cracked, allowing unauthorized copies of the programs to be made.

Yet another method for protecting the copying of software is a hardware key or 'dongle'. The hardware key is a copy protection device which typically plugs into one of the ports of a computer (e.g. a serial port) and is often supplied along with an item of software to be secured. During execution, the software sends out a unique bit pattern. The key looks for that pattern and responds by outputting its built-in serial number. The software locks if the serial number is not received. In other respects, the key acts as a passthrough for other data arriving at the serial port. Given the minimal profit margins on video games in particular, the provision of additional hardware in the form of a hardware key having
expensive components is currently not favoured.

EP-A-1,008,945 describes the use of a credit card which is read from and written to by an associated device that is configured to allow a game to be played electronically. The credit card acts both as a repository for funds necessary to allow playing of the game and also as an authentication device in that the device verifies the validity of the credit card and during game play. The credit card does not prevent copying of the game itself and in any event is unsuitable for use by the majority of game players who are children.

The present invention seeks to provide improved security against copying of software, and particularly video game software.

SUMMARY OF THE INVENTION

According to a first aspect of the present invention, there is provided a portable authentication device for authenticating software for a computer, the authentication device comprising an output for transmitting authentication information generated by the device to authenticate the software when executed by the computer, and indication means forming at least a part of the device, the indication means being visually changeable in response to the receipt of instructions to do so from the computer.

The present invention thus provides an improvement over the prior art, and hardware keys in particular. The device of the present invention combines hardware and software to provide a means for authenticating a program to be executed on a computer. Since the program to be executed on the computer is preferably prevented from running until authentication is achieved, even if the software is copied, it is of no use without the authentication device as well. Moreover, the authentication device of the present
invention changes visually as the program on the computer executes so that an indication of the progress of the program on the computer is shown on the authentication device as well.

In addition to a change in the appearance of the indication means on the authentication device, it is also preferable that the program executed by the computer cause state data to be sent back to the authentication device for storage there. For example, where a video game is being executed by the computer, state data in the form of a script, for example, may be generated and sent to the authentication device at the completion of each stage of the game, the state data indicating that a level within that video game has been completed. Likewise, the change in the appearance of the indication means may be as a result of completion of different stages of that game. The state data and/or appearance of the device may be updated as further levels are completed.

It is particularly preferable that the indication means of the authentication device includes an electrochromic material, such as a polymer-based polyethylenedioxide phenol. Other electrochromic materials could also be used. One way is to incorporate the electrochromic material into an ink so that the authentication device can be manufactured using a printing process (and in particular a screen printing process). Alternatively, the electrochromic material may be sputter deposited or vacuum deposited. Other methods of laying down the electrochromic material will be apparent to the skilled reader.

Changes in the colour of the electrochromic material may be achieved through application of an electrical signal, such as a DC voltage, to an input of the authentication device.

In a preferred embodiment, the authentication device includes an integrated chip (IC) which is
arranged to store the authentication information and, when received, the state data.

The invention also extends to a read/write apparatus connectable to a computer and having an input/output port, the input/output port being adapted to receive the portable authentication device as described above, and to send signals to and receive signals from that device.

In yet another aspect, there is provided a computer system comprising a computer having a central processor and being arranged in use to execute a computer program, and a read/write apparatus in communication with the computer, the read/write apparatus being configured (a) to receive data from the computer in response to execution of the computer program, and to cause the said data to be forwarded to the portable authentication device described above, and (b) to receive information generated by the authentication device described above to permit authentication of the said computer program executed upon the computer.

According to a further aspect of the present invention, there is provided a portable authentication device for authenticating software for a computer, the authentication device comprising storage means for storing an authentication code thereon, an output for transmitting, to the computer, authentication information generated in dependence upon the authentication code so as to authenticate the software when executed by the computer, and an input for receiving software state data from the computer as a result of execution of the software, the storage means being arranged to store the said software state data when received.

It is desirable that authentication of a program to be executed upon a computer be carried out using a portable authentication device as this increases the
security of the program to copying. Moreover, by further providing storage means upon the authentication device, the state data can be stored there and can be updated as for example, different stages in the execution of the program are reached.

The invention also extends to a computer program executable by a computer, the program containing a first program module which, when executed, causing the computer to carry out the following steps: (a) to send a first signal requesting authentication to an authentication device which is separate from the computer; (b) to receive authentication information from the authentication device in response to the request therefor, the authentication information being generated from an authentication code stored upon the authentication device; (c) to process the received authentication information and to compare the processed information with preset authentication information; (d) to execute a second program module only if the first program module determines that there is a match between the received authentication information when processed and the preset authentication information; and (e) to send a second signal including state data following execution of the second program module, the state data being stored upon the authentication device.

In that case, the first program module may be arranged to cause the computer to send a third signal to the authentication device upon completion of the said second program module, which third signal causes the said authentication device to exhibit a visual change in an indication means thereupon.

In still a further aspect of the present invention, there is provided a method of authenticating software for a computer, comprising the steps of: (a) transmitting authentication information from an authentication device to the
computer to authenticate the software when executed thereupon; and (b) transmitting instructions from the computer to cause a visible change in at least a part of the said authentication device.

The invention also extends to a method of authenticating software for a computer comprising the steps of: (a) storing an authentication code upon an authentication device; (b) generating authentication information in dependence upon the authentication code and transmitting the authentication information to the computer so as to authenticate the software when executed by the computer; and (c) generating state data indicative of the attainment of a predetermined state of the software upon execution of that software.

In that case, the method may further comprise transmitting the state data to the authentication device, and storing the updated code information on the authentication device. Moreover, the state data may additionally or alternatively be transmitted to a remote site such as a central server computer; transmission may, for example, be by means of the Internet. In that case, when the state data is received by the remote site, it may trigger the generation of a prize such as a certificate or access to further software, for example.

In a particularly preferred embodiment, the method further comprises transmitting an alteration signal to a display device when the state data has been generated, the display device including a region which is adapted to change in visual appearance in response to receipt of the alteration signal.

The use of separate authentication and display devices is advantageous as it allows multiple players to play the same game on the same computer but to keep a record on their own display device of the progress through the game.

It will be appreciated that the cost of a video
game is largely a development cost. That is, the manufacturing cost of the optical disc and packaging is relatively minimal. This is of course why piracy is so common. The authentication device will, in preference, be difficult to reproduce. For example, the slot within the device reader/writer may be non-uniform in dimensions. In that case, the video games which are relatively easily copied may be sold at little more than unit cost. The authentication devices may be sold separately and at a much higher cost than their unit value.

**BRIEF DESCRIPTION OF THE DRAWINGS**

The invention may be put into practice in a number of ways, and one preferred embodiment will now be described by way of example only and with reference to the accompanying drawings, in which:

Figure 1 shows a computer system including an authentication device embodying an aspect of the present invention;

Figure 2 shows, in more detail, a schematic diagram of the authentication device of Figure 1, in a first stage;

Figure 3 shows the first step in the manufacture of the authentication device of Figure 2;

Figure 4 shows the second step in the manufacture of an alternative authentication device;

Figure 5 shows a flow diagram illustrating the steps involved in the use of the authentication device of Figures 2, 3 and 4;

Figure 6 shows a flow diagram of the authentication process which constitutes a part of the use of the device as set out in Figure 5; and

Figure 7 shows a schematic diagram of the authentication device of Figure 2, in a second state.
DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Referring first to Figure 1, a computer system 10 is shown schematically. The computer system comprises a computer 20 having a screen 30, a processor/data storage 40 and a keyboard or joystick 50.

The computer 20 also has an output, such as a serial port (not shown). A device reader/writer 70 is in communication with the input/output port of the computer via a data transfer cable 60. The device reader/writer 70 has an aperture or slot therein which receives an authentication device 80. The authentication device will be described in more detail in connection with Figure 2 below.

The computer 20 also, in preference, has provision for connection to the Internet. This may be by means of a modem or the like.

Referring now to Figure 2, the authentication device 80 of Figure 1 is shown in more detail. The authentication device 80 may take many different forms. The device shown in Figure 2 is a thin rectangular cartridge or "smart card" of typical dimensions 85mm x 55mm and 1mm or greater in thickness.

The authentication device 80 has a body 150 formed of either glass or a plastics material such as PVC or PET, into which is embedded a silicon chip 90. A number of electrical connections to the chip are established, but these are not shown in Figure 2.

The authentication device 80 includes electrical connections 100, 110 which connect to a device indicator 120. The purpose and manner of manufacture of the authentication device 80 of Figure 2 will be described in further detail below.

The device indicator 120 is formed of an electrochromic material. As will be appreciated by those skilled in the art, an electrochromic material is a material which changes its colour during and/or
after application of an electrical potential across it. It is preferred, for reasons that will become apparent following explanation of the use of the device 80, that application of a potential to the electrochromic material causes a permanent change in its colour. Most preferably, the electrochromic material in the device indicator 120 changes from an opaque colour to become transparent.

Suitable materials are polymer-based polyethylenedioxylic phenols, viologen compounds, tungsten trioxide or Prussian blue. Viologen compounds and Prussian blue are not currently preferred because of health and safety issues with these materials.

Referring now to Figures 3 and 4, one preferred process for the manufacture of the authentication device of Figure 2 will now be described.

A PVC or PET-type plastic substrate or body 150 is used as a starting substrate and has a silicon chip 90 embedded therein. A first logo to be revealed 140 is printed directly onto the surface of the body 150. This first logo maybe a character from a video game to be authenticated, for example.

Next, and as shown in Figure 4, a device indicator 120 is laid down on top of the first logo 140. The device indicator is preferably a 'sandwich' construction including upper and lower electrodes between which is provided an electrochromic material, optionally with glass beads (not shown) to space the upper and lower electrodes and to increase reflectivity. Preferably, the upper and lower electrodes are formed from a transparent but conductive material such as InSnO, although other materials such as gold, tin or silver could be used. Electrical connections 100, 110 are formed during the process of applying the device indicator 120 to the substrate 150. These electrical connections extend from the device indicator to the edge of the body 150.
and allow electrical signals to be supplied to the
device indicator, as well as to and from the chip 90,
via the device reader/writer 70 (Figure 1). Any
suitable technique such as screen-printing, sputtering
or vacuum deposition may be employed to lay down the
device indicator 120 and/or electrodes. To complete
the authentication device 80, further logos 146 are
laid down on top of the device indicator 120, and the
completed device 80 is shown in Figure 2. Optionally,
a clear PET layer may be added to the device 80 to
encase the body 150 and the device indicator. This
layer may be added before or after the addition of the
further logos 146.

Having described a preferred method of
manufacture of an authentication device 80, its use in
the computer system of Figure 1 will now be described
with particular reference to Figures 5 and 6.

The computer 20 is started. Next, a video game to
be played is loaded into the memory of the computer 20
or, alternatively, software already resident there
(for example, on a hard disk or the like) is used
instead. The software, that is, the video game, is
started by pressing a button on the keyboard 50 or
selecting an appropriate dialogue box on the screen
30, for example, in known manner. Next, before the
game itself starts to run, a user is prompted, for
example by means of a message displayed upon the
screen 30, to insert an authentication device 80 into
the device reader/writer 70.

Next, and as indicated at step 200 in Figure 5,
code within the game itself is executed to determine
whether an authentication device 80 is present within
the device reader/writer 70 and, if so, whether the
authentication device is a valid device. The specifics
of this procedure will be described in further detail
below in respect of Figure 6. The software code
required to determine whether a device 80 is present
in the device reader/writer 70, and whether it is a valid authentication device, may either make the check a predetermined time after the message inviting the user to insert the device has been displayed upon the screen 30, or may carry out the authentication check when prompted to do so by, for example, pressing a button on the computer. Progress of the authentication check is shown on the screen 30, for example by displaying a message such as "authentication in progress".

If the software code determines that an authentication device 80 is not present on initial checking, then a message is displayed on the screen 30 informing the user of this. This is shown at step 210 in Figure 5. Next, after a short delay, the software checks again to see whether the device 80 has yet been introduced into the device reader/writer 70. This occurs at step 220 in Figure 5. If the device 80 has still not been introduced, then the routine may revert to step 210 and continue to display a message to the user indicating that an authentication device 80 is not present. After a predetermined time, or after a predetermined number of failed attempts to determine the presence of an authentication device within the device reader/writer 70, the code may revert to step 230 where an end message is displayed upon the computer screen informing the user that to activate the game requires a valid authentication device to be inserted into the reader and that the game cannot be played without it. The attempt to play the game will then terminate at step 240.

If, either in response to the initial check at step 200, or in response to an invitation to do so at step 210, a user inserts an authentication device 80 which is at least readable (indicated by a pass at step 220 in Figure 5), then the code moves on to the next stage in the authentication process. The code
sends an authentication request to the authentication device 80 within the device reader/writer 70 and awaits a response from the authentication device 80. At this stage, a further message is displayed upon the computer screen 30 indicating that verification is taking place. This is shown at step 250.

If, at step 260, the software code determines that the authentication device is present but is not valid for the particular game to be played, then a message is displayed at step 270 on the screen of the computer to indicate that the device has failed to authenticate the particular video game to be played. The message also invites the user to insert a new authentication device. At step 280, the software checks once more to see whether the device 80 can be authenticated by reverting to step 250. After a predetermined time, or predetermined number of failed attempts, the loop constituted by step 250, 260, 270 and 280 can terminate with the display of a message, at step 190, that the correct authentication device was not inserted. Again, the user may be advised to obtain such a device and, again, the game terminates before running.

If the authentication of the device 80 is achieved at step 260, then a digital certificate is displayed upon the screen 30, at step 310. The video game then commences as normal at step 320.

When the user wishes to stop playing the game, either because he has completed it or because he does not wish to continue at that time, a suitable instruction is sent to the computer. For example, the "power off" button may be depressed on the computer, or an "exit" dialogue box may be selected on the screen. In either case, the software code within the video game executing upon the computer ascertains the level within the game to which the user has progressed. In accordance with a preferred feature of
the invention, if the game has been completed, then a
Game Complete signal is sent from the computer to the
device reader/writer 70. In a simplest embodiment, the
receipt of the Game Complete signal at the
reader/writer 70 causes a voltage to be established at
terminals therein (not shown) which are in electrical
contact with the electrical connections 100, 110 on
the authentication device 80. Since the electrical
connections 100, 110 essentially form a part of the
device indicator 120, establishing such a voltage will
cause a voltage drop across the electrochromic
material. The application of a voltage to the
electrochromic material causes it to change colour. In
the device of Figures 2 and 7, the change is from an
opaque colour to become transparent. In that case, and
as shown in Figure 7, the first logo 140, previously
obscured by the opaque electrochromic material of the
device indicator 120, becomes visible. In this way, a
user can show to his or her peers that they have
completed the game. This is shown at step 330 in
Figure 5.

Once the electrochromic material has been
activated, the game can then terminate and/or the
computer may switch off. This is shown at step 340 in
Figure 5.

For added security, it is however preferable,
instead of applying the voltage directly to the device
indicator 120, to use the power supplied to the device
reader/writer 70 to power the chip 90. The chip 90 may
carry out further authentication checks before
completing the circuit between the two electrical
connections 100, 110 so that, until the Game Complete
signal has been verified, the voltage drop across the
electrochromic material of the device indicator 120 is
not established.

Such a technique is particularly useful in more
complex authentication devices where there are a
plurality of device indicators 120, or equally a single but rewritable device indicator. For example, separate device indicators (or, more specifically, separately addressable regions of the electrochromic material) may be formed on the body 150 of the authentication device 80. Then, different characters may be revealed as successive levels within the game are completed. A first character may be revealed after a first level has been completed, a second character may be revealed after the second level is complete, and so forth. This may be achieved by sending Level Complete signals, at the end of each level, to the authentication device to cause activation of the colour change in the electrochromic material. The Level Complete signal may be sent either upon completion of each level, or one or more difference Level Complete signals may be sent at the end of game play and/or on switch-off of the computer. Furthermore, the Level Complete signal may contain Level Complete data in the form of an executable script, for example, that is stored on the chip 90 to allow authentication of the game to the level previously attained, when that game is next played.

This is useful for the following reason. If the electrochromic material is activated by a user in an attempt to cheat (for example by placing a battery across the connections 100, 110 of the authentication device), the Level Complete data can be used to verify the state of the electrochromic material the next time the device 80 is inserted into the device reader/writer 70. Specifically, the software on the computer 20, in addition to containing device authentication routines as described in due course, may also contain a level validation routine. There, a level validation request is sent to the device 80 which returns the most recently stored Level Complete data (stored on the chip 90) to the computer 20. This
data can be used to refresh the device indicator(s) 120 so that, regardless of the apparent level obtained and shown before insertion and authentication of the device 80, the time level reached will be reset after insertion.

Other arrangements for the display of multiple characters will be apparent to the skilled person. For example, completion of a first level in the game may cause a first region of electrochromic material to become transparent, revealing a first character. When a second level of the game is completed, a second region of the electrochromic material may be caused to become transparent, revealing a second character, and, at the same time, the electrochromic material in the first region may be caused to become opaque. Likewise, instead of causing the electrochromic material to become transparent to reveal characters printed underneath it, the electrochromic material itself may form the character. Then, application of a voltage will cause the character to be revealed in the electrochromic material by changing a transparent layer of electrochromic material into a coloured layer of a defined shape.

The nature of electrochromic material means that the colour change caused either directly by the application of voltage to the electrical connections 100, 110 or via the chip 90 may not be permanent. Thus, it is particularly desirable that, each time an authentication device 80 is inserted into the device reader/writer 70, the authentication process to be described below causes refreshing of the colour of the electrochromic material, or the currently activated region of the electrochromic material where several different regions exist, on a regular basis. It is likewise to be understood that, where different regions exist, particularly with different electrochromic materials, a precise voltage may need
to be applied and this is achieved using a digital-to-analog converter formed as part of the chip 90 or otherwise formed within, or even external to, the device reader/writer 70. Then, receipt of a Game Complete signal, or a Level Complete signal where there are multiple regions of electrochromic material, can be converted directly from a digital value into an analogue voltage appropriate to cause the colour change in the electrochromic material.

Turning now to Figure 6, a more detailed flow chart showing the steps to be taken in the authentication in the authentication device is shown. The technique used employs a public key infrastructure (PKI) and relies upon asymmetric encryption.

As previously described in connection with Figure 5, the software module being executed on the computer 20 first checks to see whether an authentication device (referred to as 'A.D.' in Figure 6) is present within the device reader/writer 70, as shown at step 200 (Figures 5 and 6). Again as previously described, if the device is not detected to be present, then the user is informed by the display of a suitable message (step 210). The sequence is repeated by checking again to see if the authentication device 80 is present (step 200') until the presence of an authentication device is detected or the routine terminates (step 240).

When the device is detected to be present in the device reader/writer 70, the next stage of the authentication routine commences. The authentication routine executing upon the computer 20 generates a 20-byte (160-bit) pseudo random number which is used as a challenge to the authenticity of the authentication device 80 as set out below. Of course, the length of the pseudo random number can be longer or shorter if desired. This pseudo random number is processed to create a 160-bit hash value. Any suitable
hash function may be employed to allow appropriate processing of the pseudo random number; in the preferred embodiment, SHA-1 is used. Once the hash process is complete, the 160-bit hash value is sent to the device reader/writer 70 along with the request for the authentication device 80 to sign the hash value using a private key. This is all shown at step 350 in Figure 6. The specifics of the electronic signature of the 160-bit random number being sent by way of a challenge does not form a part of the present invention and will not be described in further detail.

Upon receipt of the challenge by the device reader/writer 70, it is forwarded via the electrical connections 100, 110 to the chip 90 thereon. A private key is stored upon the chip 90. The chip signs the received challenge with the private key. The signed challenge is then returned via the device reader/writer 70 to the computer 20. Further modules of software code access a digital certificate which is embedded within that software code for the game to be played. This digital certificate contains a public key, that is, a key which is common to all copies of a version of a particular game. The received, signed challenge is verified using the public key. If the received, signed challenge is authenticated, then the game commences following display of the digital certificate (step 310 onwards in Figure 5). If the authentication device 80 is not authenticated by the process described above, then the game ends following steps 270, 280 and 290 (Figure 5 again).

In preferred embodiments, the chip 90 stores additional information (such as the Level Complete data, which may be in the form of a script), which is dependent upon the level attained by the game player upon exiting the game and/or switching off the computer 20 as described previously. For example, upon completion of a first level, a unique script, for
example, may be generated by the software and sent for storage on the chip 90. The next time the game is run, the challenge may be returned, signed, along with the Level Complete data. If the software on the computer receives and verifies this Level Complete data, then the player may be provided with the option of playing the second level, whereas, absent this information, the player will not be provided with this option until they complete the first level once more.

Of course, such information need not be sent for storage on the chip of the authentication device 80 and can instead be stored locally within the software code. However, the main advantage of storing the level authentication information on the chip 90 is that it allows players to use their authentication device on any copy of a particular version of a specific game, for example on someone else's computer running an entirely different copy of the same game. Then, the authentication device 80 allows that game to be started at an appropriate level even if the person who owns the game to be played has not reached that level himself. It is likewise to be understood that the device 80 authentication process is not necessarily linked directly to the level validation process. In other words, although the signed hash used to validate the device 80 may be sent to the device 80 simultaneously with the previously stored Level Complete data, in preference the two are requested by separate software routines on the computer 20.

Whilst some form of authentication is desirable to reduce copyright piracy, and whilst Level Complete data relating to the completion of a level of the game may also be sent for storage on the authentication device for example, to change the colour of the device indicator or indicators, other information can be provided for storage as well. For example, upon first authenticating the video game with the authentication
device 80, the computer may additionally invite the user to personalise the authentication device 80 by inserting his or her name, for example using the keyboard or joystick 50. Once the name has been entered into the computer, it may be passed to the authentication device 80 for permanent storage upon the chip 90. Thus, even if the authentication device is lost or stolen with one or more levels completed, the name of the owner of the authentication device is still recorded upon it. Information such as high scores and previous levels completed may be included as information stored upon the chip 90 as well. Each can be called separately by routines on the computer.

The foregoing description of a preferred embodiment has referred to an authentication device which both authenticates the game to be played and also stores updated information as levels are completed, along with other profile information such as the owner’s name. The authentication device described above also includes a region of electrochromic material which is arranged to change colour when instructed to do so, for example by completion of a level within the game. Nevertheless, it is to be understood that the various functions above do not all need to be included on the same physical apparatus. In an alternative embodiment, the authentication device is instead constituted by a master device which contains just the information necessary to authenticate the game to be played, with a physically separate profile device that does not contain authentication information but does include the user profile information, such as the player’s name, as well as the information on levels completed within the game and also the electrochromic material which changes colour as various stages in the game are completed.

The use of a separate master device and profile
device or profile devices is particularly advantageous when it is desired to have multiple players of a particular game. A single master authentication device, which may, for example, be supplied with the (single) copy of the game to be played, is first used to authenticate the game and allow it to start in accordance with steps 200 to 320 of Figure 5. Once the game has started, the master authentication device is removed and each player, in turn, inserts his or her own profile device, including profile information on that user. Each profile device can be updated, along with changes in colour to the electrochromic material where appropriate, as the game progresses. Multiple device readers/writers can be employed, or profile devices can be removed and inserted by each player if they play sequentially.

Whilst the foregoing has described a single game played on a single computer, it is to be understood that the invention is not so limited. Multiple computers may be linked to one another via central server. One version of the game may be executed on the server. Authentication requests may, in that case, be sent from the server, via each client computer, to a corresponding authentication device on a device reader/writer connected to that client computer. The response to the challenge is then sent via the computer and back to the server to validate the game and allow it to be played on that particular client. The process for that client is, then, independent of an identical process for different client computers connected to that server. The server maintains a public key for any valid authentication device for the game executing upon the server.

Still a further option presents itself when the computer 20 is provided with access to the Internet. Then, upon completion of levels within the video game, the video game or a separate software engine may
automatically or on request cause the computer to access a remote server. Upon connecting with the remote server, the various keys and information on completed levels of the game can be transferred between the video game or, more preferably, the authentication device and the server to which the computer is connected. Standard cryptographic techniques would then be used to transfer such data. Upon receipt by the server, along with personal details, prizes may be provided. These may take the form of a framed certificate, pre-releases of the next version of that video game, and so forth.

Alternatively, the server could write an active server page or Java applet, for example, to send a token back to the computer. This in turn may cause the authentication device to be updated, for example, may cause the electrochromic material to change colour. This authentication device could then be taken to a shop and a prize could be claimed, with the colour change in the electrochromic material verifying that such a prize may be awarded. In still a further modification, the server could send back Level Complete data for storage by the chip 90. The next time the game is played, the validation of this newly-received Level Complete data may provide access to hidden or bonus levels.

Whilst electrochromic materials are preferred, it is of course to be understood that thermochromic materials could be used instead with a heater employed within the device reader/writer 70 to change the colour of the material. Both thermochromic and electrochromic materials could be used if appropriate. The changes in the colour of the device indicator may be temporary; for example, application of a varying voltage to certain materials may cause the colour change to be temporary so that the device indicator appears to flash or pulse whilst the authentication
device 80 is inserted into the device reader/writer 70. Instead of applying a voltage, the device reader/writer may instead employ laser ablation to a region of the authentication device 80 so as permanently to remove a part of the surface thereof, which results in removal of a masking layer from the surface of the authentication device. The appearance of the device indicator following such ablation may thus be of a different shape or different colour.

As yet another alternative, the device reader/writer 70 may include a printer to print images or the like onto the authentication device at the completion of a level of a game, for example. Most suitably, then, the image is temporary and/or may be overwritten. A thermo-rewritable foil and thermal printer, such as is supplied by Clearjet GmbH of Germany, is particularly suitable for this.

The software module which carries out the authentication checks and allows the video game to start is preferably supplied as a module to programmers writing video games. However, it is of course to be understood that the authentication process may be a dedicated part of the operating system of the computer, particularly when that computer is a dedicated video game computer such as the Microsoft® Xbox™ or the Sony® Playstation®.

Different authentication devices may be used to authenticate different levels of a game being played on the computer. There is, of course, a limit to the number of different regions of electrochromic material that can be applied to an authentication device, although it is to be understood that the device may have such material on just one or both of its faces. Thus, different authentication devices, authenticating successively higher levels of the game, may have different characters printed on them.

Finally, whilst the specific description has
referred to software for computers, and video games in particular, the combined symmetric/asymmetric authentication techniques can be equally applied to other products such as DVDs or audio compact disks. DVDs currently use symmetric-based encryption which means that, once the encryption for one DVD has been cracked, it is possible to copy all such DVDs.
WHAT IS CLAIMED IS:

1. A portable authentication device for authenticating software for a computer, the authentication device comprising an output for transmitting authentication information generated by the device to authenticate the software when executed by the computer, and indication means forming at least a part of the device, the indication means being visually changeable in response to the receipt of instructions to do so from the computer.

2. The device of claim 1, further comprising a storage means arranged to store an authentication code upon the device to allow generation of the said authentication information.

3. The device of claim 1 or claim 2, in which the indication means includes a region which, when activated, is caused to change colour or shape.

4. The device of claim 3, in which the said region contains an electrochromic material which, when activated, is caused to change colour.

5. The device of claim 4, in which the electrochromic material is selected from the list comprising a viologen compound, a polymer-based polyethylenedioxide phenol, tungsten trioxide and Prussian blue.

6. The device of claim 4 or claim 5, in which the electrochromic material is incorporated into a printable ink carrier.

7. The device of claim 4 or claim 5, in which the electrochromic material is laid down upon the
authentication device by sputtering or vapour deposition.

8. The device of any one of the preceding claims, further comprising at least one input electrode arranged to receive an electrical input, the input electrode being in communication with the indication means such that an electrical signal applied to the electrical input causes a change in the visual appearance of the indication means.

9. The device of claim 2, the device being arranged to receive a digital challenge issued by the computer, to sign it using the authentication code stored upon the authentication device and to transmit the signed digital challenge back to the computer as the said authentication information.

10. The device of claim 2 or claim 9, in which the storage means is further arranged to store state data which is related to at least one state of the software to be executed by the said computer.

11. The device of claim 10, in which the storage means is arranged to store updated state data received from the computer upon completion of successive modules of the software.

12. A read/write apparatus connectable to a computer and having an input/output port, the input/output port being adapted to receive the portable authentication device of any of the preceding claims and to send signals to and receive signals from the said device.

13. A computer system comprising a computer having a central processor and being arranged in use
to execute a computer program, and a read/write apparatus in communication with the computer, the read/write apparatus being configured

(a) to receive data from the computer in response to execution of the computer program, and to cause the said data to be forwarded to the portable authentication device of any of claims 1 to 13, and

(b) to receive information generated by the authentication device of any of claims 1 to 12 to permit authentication of the said computer program executed upon the computer.

14. The computer system of claim 13, in which, following execution of the said computer program, the computer is arranged to send an alteration signal to the authentication device via the read/write apparatus, the said signal causing a change in the visual appearance of the indication means of the authentication device.

15. The computer system of claim 13 or claim 14, in which, upon instructing the computer to execute the said program, the computer is arranged to send a digital challenge via the read/write apparatus to the authentication device, the authentication device, in response to the received digital challenge, sending back the said authentication information via the read/write apparatus to the computer, the computer being further configured to process the authentication information and to compare the processed authentication information with corresponding preset authentication information and to cause the program to continue execution only in the event that the received authentication information matches the corresponding preset authentication information.

16. The computer system of any one of claims 13
to 15, in which the computer is a server, the server being connected in use to at least one client to which the read/write apparatus is in turn connected.

17. A portable authentication device for authenticating software for a computer, the authentication device comprising storage means for storing an authentication code thereon, an output for transmitting, to the computer, authentication information generated in dependence upon the authentication code so as to authenticate the software when executed by the computer, and an input for receiving software state data from the computer as a result of execution of the software, the storage means being arranged to store the said software state data when received.

18. A computer program executable by a computer, the program containing a first program module which, when executed, causing the computer to carry out the following steps:
   (a) to send a first signal requesting authentication to an authentication device which is separate from the computer;
   (b) to receive authentication information from the authentication device in response to the request therefor, the authentication information being generated from an authentication code stored upon the authentication device;
   (c) to process the received authentication information and to compare the processed information with preset authentication information;
   (d) to execute a second program module only if the first program module determines that there is a match between the received authentication information when processed and the preset authentication information; and
(e) to send a second signal including state data following execution of the second program module, the state data being stored upon the authentication device.

19. The program of claim 18, in which the first program module is arranged to cause the computer to send a third signal to the authentication device upon completion of the said second program module, which third signal causes the said authentication device to exhibit a visual change in an indication means thereupon.

20. A computer storage medium upon which is stored at least the first program module of claim 18 or claim 19.

21. An electromagnetic signal when carrying the computer program of claim 17 or claim 18 or claim 19.

22. A method of authenticating software for a computer, comprising the steps of:
   (a) transmitting authentication information from an authentication device to the computer to authenticate the software when executed thereupon; and
   (b) transmitting instructions from the computer to cause a visible change in at least a part of the said authentication device.

23. The method of claim 22, in which the authentication information is generated by the authentication device in dependence upon an authentication code stored thereon, the method further comprising transmitting state data from the computer following execution of the software, and storing the said state data on the authentication device.
24. The method of claim 22 or claim 23, in which the step of causing a visible change in the authentication device comprises supplying a signal to the authentication device to cause a change in one of colour or shape of an indication means upon the authentication device.

25. The method of claim 24, further comprising providing an electrochromic material within the indication means of the authentication device, application of the signal causing a change in the colour of the electrochromic material.

26. The method of claim 25, in which the step of providing an electrochromic material comprises incorporating the electrochromic material into an ink, and printing the said ink onto the authentication device.

27. The method of claim 25, in which the step of providing an electrochromic material comprises sputtering or vapour depositing the material onto the said authentication device.

28. The method of any of claims 22 to 27, in which the step of transmitting authentication information comprises transmitting cryptographic messages using a hybrid symmetric/asymmetric cryptographic technique.

29. A method of authenticating software for a computer comprising the steps of:
   (a) storing an authentication code upon an authentication device;
   (b) generating authentication information in dependence upon the authentication code and transmitting the authentication information to the
computer so as to authenticate the software when executed by the computer; and

(c) generating state data indicative of the attainment of a predetermined state of the software upon execution of that software.

30. The method of claim 29, further comprising:
(d) transmitting the state data to the authentication device; and
(e) storing the state data on the authentication device.

31. The method of claim 29 or claim 30, further comprising generating a digital challenge for receipt by the authentication device, and signing the said challenge with the stored authentication code so as to generate the said authentication information.

32. The method of claim 31, further comprising verifying the authentication information at the computer and comparing the verified information with the original challenge.

33. The method of claim 29, claim 30, claim 31 or claim 32, further comprising transmitting the state data or a signal related thereto, to a remote site.

34. The method of claim 33, further comprising sending a prize to an owner of the authentication device upon receipt of the state data or related signal.

35. The method of claim 34, in which the nature of the prize is dependent upon the state data.

36. The method of claim 29, further comprising transmitting an alteration signal to a display device
when the state data has been generated, the display device including a region which is adapted to change in visual appearance in response to receipt of the alteration signal.

37. The method of claim 36, further comprising storing user input information upon a memory of the display device.

38. The method of claim 36 or claim 37, further comprising transmitting the state data for storage upon the display device.
FIG. 5.

START

200

AUTHENTICATION DEVICE PRESENT?

210

"AUTHENTICATION DEVICE NOT PRESENT"

220

PASS/FAIL

230

END MESSAGE

240

END GAME

250

"PLEASE WAIT WHILST VERIFICATION TAKES PLACE"

260

PASS/FAIL

270

FAILED MESSAGE

280

NEW AUTHENTICATION DEVICE

290

"SORRY, THE CORRECT AUTHENTICATION DEVICE WAS NOT INSERTED"

300

END GAME

310

DISPLAY CERTIFICATE ON SCREEN

320

GAME PLAY

330

UPDATE COLOUR OF AUTHENTICATION DEVICE

340

END GAME
**FIG. 6.**

START

CHECK TO SEE IF A.D. IS IN THE DEVICE READER/WRITER

200

NO

YES/NO

"AUTHENTICATION DEVICE NOT PRESENT"

200

YES

CHECK TO SEE IF A.D. IS IN THE DEVICE READER/WRITER

210

NO

GAME GENERATES RANDOM NUMBER, HASHES IT THEN SEND TO A.D.

360

YES

A.D. SIGNS THE HASH AND SENDS IT TO THE GAME FOR VERIFICATION

350

YES/NO

NO

END

240, 300

START GAME