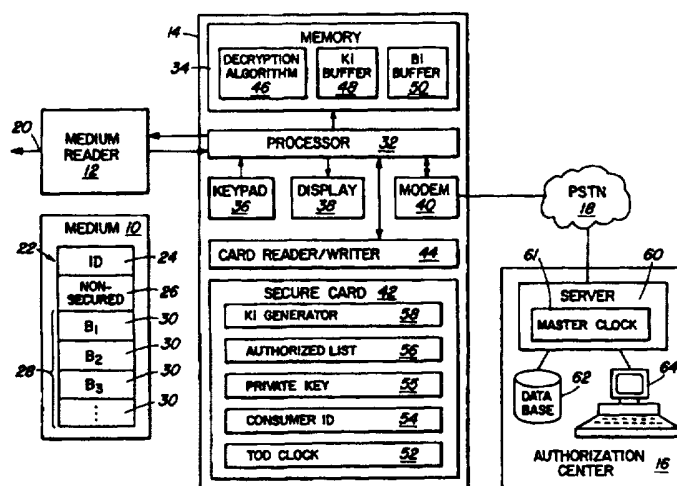




## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification <sup>6</sup> : <b>G06F 1/00</b>		<b>A1</b>	(11) International Publication Number: <b>WO 97/21162</b>
			(43) International Publication Date: 12 June 1997 (12.06.97)
(21) International Application Number: PCT/CA96/00790		(81) Designated States: AU, CA, CN, JP, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).	
(22) International Filing Date: 2 December 1996 (02.12.96)			
(30) Priority Data: 08/566,664 4 December 1995 (04.12.95) US 08/600,173 12 February 1996 (12.02.96) US		Published With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.	
(71) Applicant: NORTHERN TELECOM LIMITED [CA/CA]; World Trade Center of Montreal, 8th floor, 380 St. Antoine Street West, Montreal, Quebec H2Y 3Y4 (CA).			
(72) Inventor: PETERSON, Mendel, Lazear; Apartment #328, 1520 Richardson Drive, Richardson, TX 75080 (US).			
(74) Agent: GRANCHELLI, John, A.; Northern Telecom Limited, Patent Dept., P.O. Box 3511, Station "C", Ottawa, Ontario K1Y 4H7 (CA).			

(54) Title: TIME-BASED AVAILABILITY OF DATA ON A STORAGE MEDIUM



## (57) Abstract

A service methodology for time-based availability to content (28), such as, movies, music, games, information and the like, provisioned on a storage medium (10) whereby revenue may be generated for premier and pay-per-use access to the content. The service is manifested by the combination of a video disk reader (20), controller (14) and authorization center (16). A service provider, for instance, locks up a movie on a video disk for which a premier event viewing date and time may be defined and which the provider may then directly distribute, in advance of the premier event, to potential consumers. Each consumer may purchase the right to view the movie once for a certain fee, for example \$5.00, through online access from the controller (14) to the authorization center (16), but the single viewing will only be allowed by the controller on or after the premier event. Thereafter, the consumer pays for viewing of the movie on a pay-per-use basis or over a defined window of time, perhaps for reduced fee, such as \$1.00. Moreover, the online authorization process makes it possible to track consumer preferences at the authorization center, and as an alternative to the online payment processing, smart cards (88) may be utilized for such.

**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

<b>AM</b>	Armenia	<b>GB</b>	United Kingdom	<b>MW</b>	Malawi
<b>AT</b>	Austria	<b>GE</b>	Georgia	<b>MX</b>	Mexico
<b>AU</b>	Australia	<b>GN</b>	Guinea	<b>NE</b>	Niger
<b>BB</b>	Barbados	<b>GR</b>	Greece	<b>NL</b>	Netherlands
<b>BE</b>	Belgium	<b>HU</b>	Hungary	<b>NO</b>	Norway
<b>BF</b>	Burkina Faso	<b>IE</b>	Ireland	<b>NZ</b>	New Zealand
<b>BG</b>	Bulgaria	<b>IT</b>	Italy	<b>PL</b>	Poland
<b>BJ</b>	Benin	<b>JP</b>	Japan	<b>PT</b>	Portugal
<b>BR</b>	Brazil	<b>KE</b>	Kenya	<b>RO</b>	Romania
<b>BY</b>	Belarus	<b>KG</b>	Kyrgyzstan	<b>RU</b>	Russian Federation
<b>CA</b>	Canada	<b>KP</b>	Democratic People's Republic of Korea	<b>SD</b>	Sudan
<b>CF</b>	Central African Republic	<b>KR</b>	Republic of Korea	<b>SE</b>	Sweden
<b>CG</b>	Congo	<b>KZ</b>	Kazakhstan	<b>SG</b>	Singapore
<b>CH</b>	Switzerland	<b>LI</b>	Liechtenstein	<b>SI</b>	Slovenia
<b>CI</b>	Côte d'Ivoire	<b>LK</b>	Sri Lanka	<b>SK</b>	Slovakia
<b>CM</b>	Cameroon	<b>LR</b>	Liberia	<b>SN</b>	Senegal
<b>CN</b>	China	<b>LT</b>	Lithuania	<b>SZ</b>	Swaziland
<b>CS</b>	Czechoslovakia	<b>LU</b>	Luxembourg	<b>TD</b>	Chad
<b>CZ</b>	Czech Republic	<b>LV</b>	Latvia	<b>TG</b>	Togo
<b>DE</b>	Germany	<b>MC</b>	Monaco	<b>TJ</b>	Tajikistan
<b>DK</b>	Denmark	<b>MD</b>	Republic of Moldova	<b>TT</b>	Trinidad and Tobago
<b>EE</b>	Estonia	<b>MG</b>	Madagascar	<b>UA</b>	Ukraine
<b>ES</b>	Spain	<b>ML</b>	Mali	<b>UG</b>	Uganda
<b>FI</b>	Finland	<b>MN</b>	Mongolia	<b>US</b>	United States of America
<b>FR</b>	France	<b>MR</b>	Mauritania	<b>UZ</b>	Uzbekistan
<b>GA</b>	Gabon			<b>VN</b>	Viet Nam

- 1 -

## Time-Based availability of data on a storage medium

Background Of The Invention

The present invention relates, generally, to  
5 distribution of prerecorded content and, in particular, to  
a method and an apparatus for enabling access, dependent  
upon timed availability, to the secured content provisioned  
on a storage medium.

It is known to distribute in bulk (i.e., mass  
10 distribution) software packages. Such packages generally  
comprise a software application in encrypted format on a  
CD-ROM which is distributed in advance to potential  
consumers who would either have none or limited use of the  
software application. Each consumer desiring full use or  
15 access thereto typically is required to place a voice call  
to a 1-800 number and purchase, via credit card, from the  
distributor a password (decryption) key that is capable of  
unlocking the encrypted software. A decryption utility  
which is supplied with the package and executed by the  
20 consumer on a personal computer prompts for the key,  
responsive to which the consumer enters the key and  
subsequently is allowed to copy the software application  
onto a disk. Alternatively, the software package may  
execute functionality to invoke an online connection, when  
25 the computer includes a modem, with an automated  
authorization center from which the key may be downloaded  
to the computer.

The above distribution technique is limited in  
its ability to generate revenue from the software package,  
30 specifically, to receipt of a single payment for  
unrestricted use of the software application.

In United States patents Nos. 4,827,508 to Shear  
and 5,010,571 to Katznelson, systems for metering access to  
encrypted data in the form of a database provisioned on a  
35 CD-ROM are disclosed. Briefly, in Shear or Katznelson, a  
CD-ROM containing an encrypted database of interest to a  
user is distributed typically at nominal cost or at no

- 2 -

cost. The user terminal includes a CD-ROM reader, and a remote cryptographic control unit which is provided with stored cryptographic keys needed to access to the database. The amount of actual data use, i.e. the retrieval and decryption of data from the CD-ROM, is metered locally and recorded as a stored data usage record. The charge for data access may be either in accordance with the amount of data decrypted, or in accordance with price information recorded in the respective data headers of each individual data packet.

The local stored data usage record is reported by telephone modem from the remote user terminal to a cryptographic operations center. Each remote cryptographic control unit has a stored user secret key, unique to that user terminal. Communication between the user terminal and the cryptographic operations center is protected by encryption under the user secret key, which is stored in a secure memory in the cryptographic control unit. The user secret key for each user is also stored in the cryptographic operations center. When a remote user terminal calls in and identifies itself, the cryptographic operations center looks up the corresponding user secret cryptographic user key, which is then used to secure the subsequent communication data exchange between the remote user terminal and the cryptographic operations center. Also stored in the cryptographic operations center are the various cryptographic keys corresponding to the available CD-ROM database titles. The user secret key is also used to secure the delivery of secret database keys from the cryptographic operations center to the user terminal for a desired CD-ROM database. After the data usage report is successfully uploaded to the cryptographic operations center, the user is then billed for the actual database usage based on the content of the uploaded data usage report. Thus, rather than being required to purchase an entire CD-ROM database, the user pays only for the amount of data actually used or decrypted from the CD-ROM.

- 3 -

It is, therefore, apparent that more flexible and alternative capabilities to unlock secured prerecorded content whereby revenue generation from distribution thereof is expanded are desirable. Shear or Katznelson  
5 provide such capabilities on the basis of measuring actual use of the content. Capabilities based on timed availability to the secured content is a further alternative.

#### Summary Of The Invention

10 It is an object of the present invention to provide a new and improved method and apparatus for enabling access, dependent upon timed availability, to content provisioned on a storage medium.

The invention, therefore, according to a first  
15 broad aspect provides A method of controlling access to a data content of a storage medium, comprising the steps of: defining a start point in time prior to which access to the data content is to be inhibited; measuring time; enabling, responsive to the measured time effectively reaching the  
20 start point, access to the data content.

In accordance with a second broad aspect, the invention provides an apparatus for controlling access by a user to content of a storage medium, the medium being readable by a corresponding medium reader from which the  
25 apparatus is adapted to receive the content, comprising: means for defining a start point in time prior to which access to the data content is to be inhibited; means for measuring time; means for enabling, responsive to the measured time effectively reaching the start point, access  
30 to the data content.

A particular embodiment includes a local secure authorization clock which is set and controlled by an authorization center having a master clock. The local clock is secure in that its setting may not be altered by  
35 the consumer.

The invention manifests a novel service methodology based on distribution of prerecorded content,

- 4 -

such as, movies, music, games, information and the like, whereby revenue may be generated for premier and pay-per-use access to the content. A service provider, for instance, locks up a movie on a video disk for which a premier event viewing date and time may be defined and which the provider may then directly distribute, in advance of the premier event, to potential consumers. Each consumer may purchase the right to view the movie once for a certain fee, for example \$5.00, through online access to an authorization center, but the single viewing (i.e., unlocking) will only be allowed on or after the premier event time. Thereafter, the consumer pays for viewing of the movie either on a pay-per-use basis or over a defined window of time, and perhaps for reduced fee such as \$1.00. Moreover, the online authorization process makes it possible to track consumer preferences. As an alternative to the online payment processing, smart cards may be utilized for such.

This service creates premier events at a set date and time as well as for subsequent pay-per-view enjoyment of prerecorded movies, music, information, communications, and other electronic entertainment. The service may employ online capabilities to create new distribution options for digital video disk (DVD), CD-ROM, CD, multimedia games and other electronic media. Also, the service authorizes, controls, tracks and creates new billing options for premier events and pay-per view from the prerecorded content.

A particular system for carrying out the service may include a non-alterable, non-volatile read only control data recorded on the DVD, CD-ROM, CD, game cartridges and other electronic media. The control data may provide a content description, start, expiration and other option control marks. The control marks identify the contents and allow synchronization of event start and expiration times, and billing options. A master clock is controlled by an authorization center. A secure authorization clock, set

- 5 -

and controlled by the authorization center, is coupled to the consumer's DVD player, PC, CD player, game machine, external modem controller, smart card or PC card. The authorization clock is password protected and not alterable  
5 by the consumer. An online authorization process may be implemented which utilizes an authorization window, passwords, and the master and secure authorization clocks to set the start time for the premier event, and also set an expiration date/time if desired.

10           Locking and unlocking of content provisioned on a storage medium, in its simplest form, constitutes enabling and inhibiting access to the content in accordance with defined time based availability control conditions. Preferably, the content is locked through encryption for  
15 more security and unlocking requires decryption of the encrypted data content.

          Furthermore, the service creates many distribution and billing options. For example, in advance of viewing premier, a movie could be distributed on a DVD  
20 disk via courier, authorized at a convenient for the consumer during the authorization window in advance of the premier event but not viewed until the date and time of the regional, national or world premier event. Another example, a music video or multimedia game could be  
25 distributed on CD or CD-ROM in advance for a world premier on the event date with the option of live online interaction. Additional post premier event viewing could be authorized, tracked and billed via a number of commercial options.

30           Content of a storage medium may be partitioned into two classes of offering, namely basic content and premier content. The basic content is a global offering to which unlimited access may be allowed, for instance, on payment of a subscription fee. To maintain interest of  
35 users in the basic content, a technique is to unlock new content each day or on a surprise basis. New content, premier events, serials, cliffhangers, programs which

- 6 -

branch off of the prior days programs, celebrations, grand openings, prizes and birthdays, all may be controlled to unlock at a specific time announced or unannounced. This content may also be locked back up after it has been opened  
5 so if the user does not come back on time, the content is missed. The premier content is locked up and may only be accessed on a pay-per-use basis.

#### Brief Description Of The Drawings

The invention will be better understood from the  
10 following description in conjunction with reference to the accompanying drawings, in which:

Figure 1 is a block diagram representation of a first embodiment of an apparatus for unlocking, dependent upon timed availability, a secured content provisioned on a  
15 storage medium;

Figure 2 is a time line chart exemplifying the methodology, in accordance with the invention, for timed availability to content provisioned on the storage medium;

Figure 3 is a block diagram of another embodiment  
20 of the apparatus to unlock the secured content; and

Figure 4 illustrates yet another embodiment of apparatus that enables access to content in accordance with time based control conditions.

#### Detailed Description

Referring to Figure 1, depicted for illustration  
25 of one embodiment of the present invention is a storage medium 10 and corresponding medium reader 12 which is coupled to a controller 14. Located remotely from the controller 14 is an authorization center 16 to which the  
30 controller 14 may establish a communication connection, for example, via a public switched telephone network (PSTN) 18 or other communications link. The storage medium 10 may be provisioned with a data content which is secured in that  
the data may not be readily accessed or used. Access to  
35 the content is allowed according to defined time based availability conditions and, in this embodiment, prior authorization is required. The reader 12 is adapted to



- 7 -

receive the storage medium 10, the data content from which it retrieves and provides to the controller 14 which in turn functions to unlock the secured data. Unlocking is enabled when the controller 14 is authorized to do so by the authorization center 16 and associated with the authorization may be a time period only during which the unlocking is effected. The unlocked data from the controller 14 may be passed back to the medium reader 12 for further processing, if required, and then accessed at output 20 for utilization by a further device (not shown). As the storage medium 10 contains a secured data content, it may be first distributed in bulk to potential consumers each of whom must subsequently receive authorization in order to access the secured content.

Now having regard to Figures 1 and 2 together, illustrated in Figure 2 is a time line chart to exemplify various timed availability schemes, in accordance with the present invention, that may be implemented by the apparatus of Figure 1. One such scheme is to not allow access to the secured contents of the storage medium 10, having been distributed in advance, until a predetermined date and time. This scheme is otherwise referred to herein as a "premier event" type availability of the secured contents. For instance, a consumer may receive the storage medium 10 at time T0 after which there exists a time window W0 within which the consumer may, via the controller 14 and PSTN 18 in this particular embodiment, communicate with the authorization center 16 to request and subsequently receive authorization to access the contents of the storage medium 10. This process of requesting and receiving authorization is represented by the arrow at time T1. Authorization normally is granted on receiving payment from the consumer, in this case, for the requested premier event usage. The controller 14, however, will not enable access to the secured content until the date and time, represented by T2, which is associated with the premier event. Following time T2, a second timed availability scheme is exemplified

- 8 -

wherein the consumer requests authorization from the center 16 and receives same in return for payment at time T3, whereby another time window W1 is initiated. The payment for authorization at T3 may be less than that for the premier event made at T1. During window W1, the consumer may be allowed unlimited use of the content on the storage medium 10, as represented by times T4 and T5. This authorization is terminated following expiry of window W1 and thereafter is another window W2 which is initiated by the consumer requesting and receiving authorization at T6, in order to again access the secured content, at T7. A further scheme is to vary the lengths of successive windows, for instance, from one week, to one month and possibly indefinitely. Moreover, only a single use of the content may be allowed which use must occur within the authorized window. It is also possible to implement a combination of the above timed availability schemes, such as, defining a first window during which only single usage is authorized and thereafter defining a succession of windows which begin with a specified number of allowed uses and gradually increase the allowed number over consecutive windows to eventually allow unlimited access. A yet further variant is to provide an absolute expiration date, indicated at time T8, after which it will not be possible to access the secured content thereby effectively removing or withdrawing it from the commercial market. Although the consumer will still have possession of the actual storage medium, on and after time T8 unlocking of the secured content will not be authorized.

Turning back to Figure 1 only, the storage medium 10 and its data content are intended to be representative of conventional electronic media and content, for example, a compact disk (CD) encoded with a musical data content, a CD-ROM holding computer usable data, a cartridge having video game data, and the like. The preferred storage medium 10 is a digital video disk (DVD) which is capable of holding approximately two movie hours or five gigabytes of

- 9 -

data on each side thereof. Moreover, the DVD standard serves as video, CD-ROM, CD and data distribution and consequently a single DVD reader may be utilized in various applications.

5           The data content, visually represented by reference 22, of the storage medium 10 may include an identifier 24 and non-secured data 26 in addition to secured data 28. The identifier 24 is, for example, a serial number that may be utilized in the authorization  
10 process to identify the particular secured data 28 to which access is desired. The non-secured data 24 constitutes a "free" sampling of the secured data 28 as it may be readily accessed, without authorization, by a potential consumer and is provided as a means for enticing the consumer to pay  
15 for access to the secured data content.

          The secured data 28 may be encrypted as a measure for preventing unauthorized access thereto. Locking and unlocking of the secured data 28 may be effected through a combination of symmetric key cryptography and public key  
20 cryptography techniques which are compliant with the United States data encryption standard (DES). A characteristic of symmetric cryptography is that the same key, K, is utilized in both the encipherment and decipherment of data. The public key cryptography is applied to encrypt key K  
25 uniquely for a specific consumer under a public key associated with that consumer. A preferred embodiment of the secured data 28 consists of a plurality of contiguous blocks 30, labeled B<sub>1</sub>, B<sub>2</sub>, B<sub>3</sub>, etc., each containing data encrypted by respective keys K<sub>1</sub>, K<sub>2</sub>, K<sub>3</sub>, etc. The secured  
30 data 28 is arranged on the storage medium 10 and the reader 12 operated such that consecutive blocks 30 may be retrieved sequentially by the reader 12. The application of combined symmetric key and public key cryptography to the present invention is described in more detail below.

35           The controller 14 comprises a processor 32 operating in conjunction with a memory 34, keypad 36, display 38, modem 40 and a combination of a secure card 42

- 10 -

with a corresponding card reader/writer 44. The processor 32 functions, under the control of software stored in the memory 34, to receive data from the medium reader 12 and appropriately process the received data in order to unlock  
5 the secured (i.e., encrypted) data 28, subject to authorized and timed access, which data may then be provided via the reader 12 at output 20. The memory 34 includes a data block ( $B_i$ ) buffer 46, a block decryption key ( $K_i$ ) buffer 48 and a decryption algorithm 50. The  $B_i$   
10 buffer 46 stores individual encrypted data blocks 30 of the secured data 28 for the decryption process. The  $K_i$  buffer 48 stores a respective symmetric key which corresponds to a particular data block 30 in the  $B_i$  buffer 46 and is applied with algorithm 50 by processor 32 to decrypt (i.e., unlock)  
15 that encrypted data block. The keypad 36 and the display 38 constitute means by which a user may interact with the controller 14, and the modem 40 provides an interface to the PSTN 18 whereby the processor 32 may communicate with the authorization center 16.

20 The secure card 42 and reader/writer 44 are conventional devices. Smart cards and PCMCIA cards are examples of the secure card 42 which typically contain a processor, clock circuit and non-volatile memory. Furthermore, smart cards and PCMCIA cards are known to be  
25 equipped with security features to prevent access to and tampering with data in its memory. The card reader/writer 44 is adapted to removably receive the secure card 40 and enables the processor 32 to communicate therewith.

In this particular embodiment of the controller  
30 14, the secure card 42 is programmed to provide a time of day (TOD) clock 52, a consumer identifier 54, a private key 55, a list 56 of authorization records and a block decryption key ( $K_i$ ) generator 58. The TOD clock 52 represents means for measuring time and is a well known  
35 capability consisting of a time clock and a date calendar, the settings for which may be password protected and either set online by the authorization center 16 or preset prior

- 11 -

to issuance of the card 40 if it includes a battery cell whereby the clock circuit is constantly powered. Hence, the TOD clock 52 may not be altered by the consumer thereby ensuring compliance with the timed availability conditions  
5 for the secured content 28. The consumer identifier 54 is effectively an account number by which a particular consumer is known at the authorization center 16. The private key 54 may be a RSA (i.e., Rivest, Shamir and Adleman) key that is uniquely associated with the consumer  
10 and corresponds to a public key held at the authorization center 16, but the private key 54 is not known by the authorization center 16. The list of authorization records 56 contains a separate record for each secured content to which access has already been authorized by the  
15 authorization center 16. Each authorization record contains: the identifier 24 of the secured content 28 on storage medium 10; a start date and time at which access thereto may be enabled; an expiration date and time after which authorization lapses or is no longer in effect; a  
20 limit for usage; and a key K on which securing of the data content 28 was based. The start and expiration dates and times define the window or period of timed availability during which access to the secured content 28 may be enabled. The usage limit defines the number of accesses to  
25 the secured content that may be made during the window and typically is either one or unlimited.

The  $K_i$  generator 56 functions to generate a block decryption key  $K_i$  that is needed to decrypt the particular data block 30 stored in the  $B_i$  buffer 50. Generation of  
30 the block decryption key  $K_i$  is effected for each data block 30, represented by  $B_i$ , and is based on a proprietary algorithm which accepts as input the key K retrieved from the authorization record for that secured content 28 and another value uniquely associated with that data block 30,  
35 such as, an indication of its position in the sequence for the contiguous data blocks 30. For example,  $B_1$  denotes the initial or first block 30 of secured data 28 and its

- 12 -

corresponding decryption key  $K_1$  is derived by the  $K_i$  generator 56 based on key  $K$  and a sequence indicator value of 1. The sequence indicator may be encoded into each data block 30 or generated by the controller 14 which has an intimate knowledge of the physical arrangement of the storage medium 10 and the partitioning for its secured content 28. The use of a plurality of key  $K_i$ , derivable from a single key  $K$ , to encrypt and decrypt corresponding blocks  $B_i$  of secured content provides an extra layer of security from potential attackers. As the key  $K_i$  for decrypting the content changes frequently ( $K_1, K_2, K_3$ , etc.) during the decryption process, if the attackers are not able to compromise the security features of the secure card 42 to extract key  $K$  and the algorithm for  $K_i$  generator 58 therefrom then it would be necessary to convey the entire sequence of  $K_i$  keys to others in order to gain unauthorized access to the secured content 28. For example, if a new 8 byte key is supplied every millisecond over the course of a two hour movie, there is a total 55 Mbytes of keys that must be provided to the unauthorized others.

The authorization center 16 is embodied by an online computer server 60, a database 62 and a workstation 64. The server 60 functions to automatically accept incoming calls, process authorization requests and grant authorization where appropriate, and may provide a master clock 61 based on which the TOD clock 52 of the controller 14 may be set and controlled. It maintains in the database 62 a list of identifiers which correspond to the identifiers 24 of any secured content 28 that may have been distributed. Associated with each identifier is a control record defining availability conditions for the particular secured content 28. The control record may include the key  $K$  from which the sequence of decrypting keys  $K_i$  needed for decryption of the secured content 28 are derived, premier date and time values, and a window definition having

- 13 -

parameters for specifying: a time limit (i.e., number of days and/or hours) for which granted authorization is to be effective; a usage limit indicating whether a specific number, such as one, or unlimited use is authorized over  
5 the specified number of days; and a cost for the usage. Alternatively, a plurality of window definitions which are applicable over respective chronological time periods may be employed in order to alter the parameters, such as cost and usage limit, over time. Furthermore, the control  
10 record may include an absolute expiration date, after which authorized use of the secure content 28 will no longer be granted.

The server 60 also maintains in the database 62 a directory of identifiers for consumers and corresponding  
15 account records. Each consumer account record contains a public key associated with the consumer, and an amount of prepaid funds or credit limit available in the account. The workstation 64, operated by an attendant, interacts with the server 60 to provide manual assistance when needed  
20 for processing of an incoming call, to update certain records in the database 64, and it captures consumer identifiers together with secure content identifiers to generate statistical data whereby consumer usage and preferences may be tracked.

25 In operation, a consumer normally receives, in advance of a predetermined premier event date, a storage medium 10 having secured content 28, for instance, a DVD disk containing a movie production which is encrypted together with non-secured (non-encrypted) data 24 including  
30 a sample trailer and audio/visual instructions explaining particulars for access to the encrypted movie. The consumer would apply the medium 10 (DVD disk) to the medium reader 12 and the output 20 thereof would be connected, in this particular context, to a television set or monitor of  
35 a home theater system. The processor 32 of controller 14 forwards any non-encrypted video data received from the reader 12, without any processing of the that data, back to

- 14 -

the reader 12 which in turn processes the data stream to generate appropriate analog video signals at its output 20, thereby allowing the consumer to access and view the trailer and instructions but not the actual movie. If  
5 interested in viewing the movie production, the consumer indicates this desire to the controller 14 by depressing an appropriate key on the keypad 36 which generates a corresponding signal that is received by the processor 32. Responsive thereto, the processor 32 first determines  
10 whether an authorization record already exists in the list 56 for the identifier 24 provided on the medium 10 and received from the reader 12.

Assuming in this instance that authorized access to the secured content 28 had not been previously requested  
15 and granted, the processor 32 utilizes the modem 40 to establish a connection through the PSTN 18, by dialing a specific 1-800 number, with the authorization center 16 whereby online communication with the server 60 may be effected. The processor 32 transmits, via the modem 40, an  
20 authorization request message to the server 60. The authorization request message includes the identifier 24 of movie production and the identifier 54 of the consumer which it retrieves, via reader/writer 44, from the secure card 42. The server 60 at authorization center 16 utilizes  
25 the secured content identifier and the consumer identifier included in the authorization request message to retrieve, respectively, the corresponding control record and consumer account record which are stored in the database 62. The server 60 applies the amount specified for cost of usage in  
30 the control record against the consumer's account and where sufficient funds or credits are present, subsequently generates an authorization granted message which the server 60 transmits through the PSTN 18 to the controller 14. The authorization granted message indicates: the identifier 24  
35 of the secured content 28 to which access is now authorized; the start date and time at which access to the secured content (i.e., unlocking) may be enabled; the



- 15 -

expiration date and time after which authorization lapses; the usage limit; and the key K which is encrypted, for security, by the server 60 under the public key of the consumer. Alternatively, the entire content of the

5 authorization granted message may be encrypted under the consumer's public key. In connection with a premier event, the start date and time values are the premier date and time values taken from the control record, and the expiration date and time values may be calculated from the

10 start values plus a time limit offset which may be a predetermined default value, for example, twenty-four hours or the limit specified in the window definition. The usage limit may be any value but normally is one for a premier event. For authorizations following the premier event,

15 the start date and time values would be those current when the authorization request message is received in order to allow immediate access to the secured content 28, the expiration date and time being calculated therefrom using the time limit specified in the window definition of the

20 control record. The usage limit would be that specified in the control record. An alternative to specifying the exact date/time of expiration is to instead specify a window (i.e., period) of time, such as one day or one week, during which use is authorized and which window is

25 effective beginning on the specified start date. The TOD clock 52 may, in this context, be employed as a means to measure time by counting down the units of time in the window until it is no longer valid. The processor 32 of the controller 14 utilizes the secure card 42 to store the

30 contents of the received authorization granted message as an authorization record in the list 56.

In respect of secured content 28 for which an authorization record does exist in the authorization list 56, the processor 32 verifies when access thereto is

35 requested by the consumer that such access is to be enabled by comparing the current date and time, supplied by TOD clock 52, to the start and expiration dates and times

- 16 -

specified in the authorization record. When the start date and time are later than the present parameters, then the processor 32 will not attempt to decrypt the secured content 28. When the present date and time are later than  
5 the expiration parameters, again the processor 32 will not enable access to the secured content and also it will remove, via the reader/writer 44, that authorization record from the authorized list 56. Alternatively, the processor on board the secure card 46 may be programmed to govern  
10 issuance of the decrypting keys  $K_i$  only when warranted by verifying the requested access does comply with the conditions of the authorization record, and it may monitor for authorization records which lapse to automatically delete same.

15 When the current date and time are within the start and expiration dates and times of the authorization record, the processor 32 then proceeds with the decryption process whereby the secured content 28 is unlocked. Such involves the processor 32 providing a sequence indicator  
20 value of one to the  $K_i$  generator 58 which then initiates generation of decrypting keys  $K_i$  beginning with  $K_1$  that corresponds to the first block 30 ( $B_1$ ) of secured content 28 and continuous, unless interrupted by the processor 32, to automatically generate successive keys thereafter,  
25 namely  $K_2$ ,  $K_3$ , etc., knowing that the encrypted data blocks 30 are retrieved sequentially. The generation of decrypting keys  $K_i$  requires the secure card 42 first to decrypt encrypted key  $K$ , retrieved from the authorization record, using the private key 55. The  $K_i$  generator 58 then  
30 utilizes the decrypted key  $K$  and the sequence indicator value to generate the successive decrypting keys  $K_i$  each being provided sequentially to the processor 32 as needed.

The processor 32 continues with the decryption process by retrieving, via the medium reader 12, each  
35 encrypted data block 30 beginning with block  $B_1$  which is stored in  $B_i$  buffer 48 and, via card the reader/write 44, each decrypting key  $K_i$  beginning with key  $K_1$  which is

- 17 -

stored in B<sub>i</sub> buffer 48. Then the processor 32 applies the decryption algorithm 46 together with the key in K<sub>i</sub> buffer 48 to the encrypted data in B<sub>i</sub> buffer 50 thereby effecting decryption of that data block and the decrypted data is  
5 provided at output 20. The processor 32 repeats these steps for each block 30 of the secured content 28.

Another embodiment of the apparatus, in accordance with the invention, to unlock secured data of a storage medium dependent upon timed availability is  
10 illustrated in Figure 3. The content of the storage medium 70 includes, as visually represented by reference 72, control data 74 in addition to the content identifier 76, the non-secured data 78 and the secured data 79. The control data 74 may comprise premier date and time values  
15 80 with associated cost 81, window definition parameters specifying a time limit 82, usage limit 83 and cost 84 subsequent to premier event, and an absolute expiration date 85 after which access to the secured content will not be granted. Furthermore, in this embodiment of the  
20 controller 86 the secure card 88 is programmed to provide the TOD clock 90 and as well maintain an amount of funds 91 prepaid by the consumer, a list 92 of authorized access records and a decryption key 93. The amount of prepaid funds 91 may be adjusted in return for receiving monetary  
25 compensation and the particular decryption key 93 updated periodically, for instance, by an authorization center (not shown) which the consumer may visit for manual updating of these values or through an automatic online process.

To unlock the secured content 88, the processor  
30 94 provides the content identifier 76 and control data 74, via the reader/writer 89, to the secure card 88 which in turn performs authorization processing. The secure card 88 first determines whether an authorization record exists in the list 92 corresponding to the identifier 76. When an  
35 authorization record does not exist, the processor 94 then determines the start and expiration times/dates based on

- 18 -

the TOD clock 90 which together with the usage limit 83 defined a new authorization record that is added to the list 92. The prepaid funds 91 is decrement by the appropriate amount, either cost 75 or 78 as specified in the control data 74, which is applicable under the present access context. When the TOD clock 90 indicates the current date as being subsequent to the absolute expiration date 85 specified on the storage medium 70, the processor 94 will not authorize access to the secured content 79.

Following determination that an authorization record does exist or the addition of a new record if not, the secure card 88 next confirms that access to the particular secured content is valid in respect of the present date and time, responsive to which it either provides or refuses to provide the decryption key 93 to the processor 94. Upon receiving the decryption key 93 from the secure card 88, the processor 94 stores it in key buffer 95 of local memory 96 and applies it together with decryption algorithm 97 to the encrypted data received from the reader 98. The decrypted data is provided to the medium reader 98 for further processing, if appropriate, and then made accessible at output 99. The secure card 88 updates the authorization record upon the consumer accessing the secured data and when an authorization record is no longer valid, namely when the expiration date has passed or the usage limit has been reached, that record is deleted from the authorization list 92.

Turning now to Figure 4, illustrated is yet another embodiment for a system implementing the time based availability methodology, in accordance with the present invention, to content of a storage medium. The system constitutes a conventional multimedia workstation comprising a personal computer 100 which is equipped with a CD-ROM reader 102 and a modem 104. The computer 100 may be programmed with an appropriate content retrieval application, identified by reference 106, that is adapted to control access to the content of a CD-ROM 108 (or other

- 19 -

electronic media) according to time based control marks also stored on the CD-ROM 108 to provide the effect of locking and unlocking the content at specific times. The content of the CD-ROM 108 may be partitioned into two  
5 classes of offering, namely basic content and premier content, and time based delivery of the CD-ROM content can be implemented by utilizing the clock of the personal computer 100.

The basic content provided on the CD-ROM 108 may  
10 be considered a global offering to which a consumer may have unlimited access, for instance, simply for a subscription fee prior to receiving the CD-ROM 108. The basic content is not necessarily encrypted. As a technique to maintain interest of the consumer in the particular CD-  
15 ROM, the basic content may include multiple portions of data such as various segments, information or applications, which may each be associated with a start date/time and optionally an expiration date/time and to which the retrieval application 106 will enable access by the  
20 consumer at the start time and subsequently inhibit access following the termination time. This technique may be used to unlock new content on particular days or on a surprise basis thereby extending consumer interest in the CD-ROM 108. For example, new content, premier events, serials,  
25 cliffhangers, programs which branch off the prior days programs, celebrations, grand openings, prizes and birthdays may be programmed to open at specific times, announced or unannounced. Furthermore, content forming part of the basic offering may be also locked back up once  
30 it has been unlocked so that if the consumer does not make use of the CD-ROM 108 between the start and expiration times of the particular content then it is missed. An example is to unlock a clue or hint for assistance in solving a puzzle for an hour on a certain day. If the  
35 consumer is viewing the CD-ROM 108 during that hour, he/she will see the clue or otherwise it is lost.

- 20 -

While the basic offering is loaded with time based content as discussed above, the CD-ROM 108 may also offer a premium track. The premium content is locked up, access thereto being controlled by the retrieval application 106 and it may be accessed on a pay-per-use basis also with time based delivery. Authorization to access the premier content may be obtained via online, using modem 104, through a remote authorization center. Authorization records may be stored within the personal computer 100 and securely managed by the retrieval application 106 so that the consumer may not access these records, thereby effecting a virtual smart card. The virtual smart card may be characterized as a region of memory and software in the personal computer 100 which region is protected and accessed only remotely by the authorization center. Authorization is granted upon the consumer paying a fee for use of the premium content. The premier content is encrypted for extra security and granted authorization includes providing the user with a description key. Alternatively, the premier content may be accessed by retrieving keys embedded in the basic offering, for example, by finding or earning keys from playing a game or puzzle.

The retrieval application 106 executed by the computer 100 functions to control access to the data content of the storage medium, namely CD-ROM 108. For a data content having time control marks, the retrieval application 106 reads the indicated start time and compares it to the measured time provided by the computer's internal clock. If the measured time is earlier than the indicated start time then the retrieval application will not enable access to that data content in effect locking it from the user. When the measured time is subsequent to the start time, access to the data content is allowed by the retrieval application 106 whereby the data may be output to a further computer application for its use and hence the data is unlocked. Moreover, in instances where the data

- 21 -

content has an expiration time indicated the retrieval application 106 will inhibit access thereto when the measured time reaches the expiration time by not providing the data to the further computer application, thereby  
5 locking the content once again.

Although the above embodiments describe attaching control conditions to a particular content, it should be apparent to a skilled artisan that a possible variant is to incorporate a single set of control data into the memory of  
10 the controller whereby the control data may be applied as the default timed availability conditions to unlocking of all secured content. Another variant is to build a secure memory and secure TOD clock directly into the controller as a substitute to utilizing the combination of a secure card  
15 and card reader/writer. A yet further variant is to have the consumer manually carry out the authorization request and grant process by placing a voice call to the authorization center and interact either with an automated or human attendant to obtain an authorization code, encoded  
20 into which would be the decryption key and which may then be entered manually at the controller though the keypad.

Those skilled in the art will recognize that these and other modifications and changes could be made to the invention without departing from the spirit and scope  
25 thereof. It should therefore be understood that the claims are not to be considered as being limited to the precise embodiments set forth above, in the absence of specific limitations directed to each embodiment.

- 22 -

## I CLAIM:

1. A method of controlling access to a data content of a storage medium, comprising the steps of:  
5 defining a start point in time prior to which access to the data content (28) is to be inhibited;  
measuring time (52);  
enabling, responsive to the measured time effectively reaching the start point, access (99) to the  
10 data content.
2. A method as claimed in claim 1, wherein the data content (28) is encrypted and enabling access to the data content includes enabling decryption (46) of the encrypted  
15 data.
3. A method as claimed in claim 2, comprising:  
requesting access to the encrypted data from an authorization center (16); and  
20 receiving authorization (56) which includes a key for the decryption of the encrypted data.
4. A method as claimed in claim 3, wherein the step of defining the start point includes providing an  
25 indication of the start point with the authorization (56).
5. A method as claimed in claim 1 or 3, wherein the step of defining the start point includes providing an indication of the start point (80) on the storage medium  
30 (70).
6. A method as claimed in claim 1, comprising the steps of:  
35 defining an expiration point in time (82, 85);  
and



- 23 -

inhibiting, responsive to the measured time effectively reaching the expiration point, access to the data content (79).

5 7. A method as claimed in claim 6, wherein the data content (28) is encrypted, enabling access to the data content includes enabling decryption (46) of the encrypted data, and inhibiting access to the data content includes inhibiting the decryption of the encrypted data.

10

8. A method as claimed in claim 7, comprising the steps of:

requesting access to the encrypted data from an authorization center (16); and

15

receiving authorization (56) which includes a key for the decryption of the encrypted data.

9. A method as claimed in claim 8, wherein the steps of defining the start point and defining the expiration point includes providing an indication of the start point and an indication of the expiration point with the authorization (56).

20

10. A method as claimed in claim 6 or 8, wherein the steps of defining the start point and defining the expiration point includes providing an indication of the start point (80) and an indication of the expiration point (82, 85) on the storage medium (72).

25

30

11. A method as claimed in claim 6, comprising the steps of:

defining a usage limit (83);

metering usage of the data content (79); and

35

inhibiting, responsive to the metered usage reaching the usage limit, access to the data content.

- 24 -

12. A method as claimed in claim 11, wherein the data content (79) is encrypted, enabling access to the data content includes enabling decryption (97) of the encrypted data, and inhibiting access to the data content includes  
5 inhibiting the decryption of the encrypted data.

13. A method as claimed in claim 12, comprising the steps of:  
requesting access to the encrypted data from an  
10 authorization center (16); and  
receiving authorization (56) which includes a key for the decryption of the encrypted data.

14. A method as claimed in claim 13, wherein the  
15 steps of defining the start point, defining the expiration point and defining the usage limit include providing an indication of the start point, an indication of the expiration point and an indication of the usage limit with the authorization (56).

20 15. A method as claimed in claim 11 or 13, wherein the steps of defining the start point, defining the expiration point and defining the usage limit include providing an indication of the start point (80), an  
25 indication of the expiration point (82, 85) and an indication of the usage limit (83) on the storage medium (72).

30 16. A method as claimed in claim 1, wherein the step of measuring time includes providing secure time clock means (52) for measuring the time.

17. A method as claimed in claim 16, wherein the  
35 secure time clock (52) means is password protected.

- 25 -

18. A method as claimed in claim 3, wherein the step of measuring time includes providing secure time clock means (52) for measuring the time.

5 19. A method as claimed in claim 18, comprising setting the secure time clock means (52) by the authorization center (16).

20. A method as claimed in claim 18, wherein the  
10 secure time clock means (52) is password protected.

21. A method as claimed in claim 3, comprising providing a secure device (42) having a time clock for measuring the time and a memory in which a key for  
15 decryption of the encrypted data is stored.

22. A method as claimed in claim 21, wherein the secure device (42) is any of a smart card or a PCMCIA card.

20 23. A method as claimed in claim 1, wherein the data content (79) comprises multiple portions of data which are associated with respective start points in time, and enabling access to a particular portion of the data content is in response to the measured time effectively reaching  
25 the respective start point for that portion.

24. A method as claimed in claim 6, wherein the data content (79) comprises multiple portions of data which are associated with respective start points and expiration  
30 points in time, enabling access to a particular portion of the data content is in response to the measured time effectively reaching the respective start point for that portion and inhibiting access to the particular portion of the data content is in response to the measured time  
35 effectively reaching the respective expiration point for that portion.

- 26 -

25. A method as claimed in claim 1, wherein the storage medium (70) is any of a compact disk, CD-ROM, cartridge and digital video disk.

5 26. An apparatus for controlling access by a user to content of a storage medium, the medium being readable by a corresponding medium reader from which the apparatus is adapted to receive the content, comprising:

means for defining a start point in time prior to  
10 which access to the data content (28) is to be inhibited;

means for measuring time (52);

means for enabling, responsive to the measured time effectively reaching the start point, access (99) to the data content.

15

27. An apparatus as claimed in claim 26, wherein the data content (28) is encrypted and the means for enabling access includes means for enabling decryption (46) of the encrypted data.

20

28. An apparatus as claimed in claim 27, comprising:

means for requesting access to the encrypted data from an authorization center (16); and

means for receiving authorization (56) which  
25 includes a key for the decryption of the encrypted data.

29. An apparatus as claimed in claim 28, wherein an indication of the start point is provided with the authorization and the means for defining the start point  
30 includes means for retrieving the start point indication from the authorization (56).

30. An apparatus as claimed in claim 26 or 28, wherein an indication of the start point (80) is provided  
35 on the storage medium and the means for defining the start point includes means for retrieving the start point indication from the storage medium (70).

- 27 -

31. An apparatus as claimed in claim 26, comprising:  
means for defining an expiration point in time  
(82, 85); and

5 means for inhibiting, responsive to the measured  
time effectively reaching the expiration point, access to  
the data content (79).

32. An apparatus as claimed in claim 31, wherein the  
10 data content (79) is encrypted, the means for enabling  
access to the data content includes means for enabling  
decryption (97) of the encrypted data, and the means for  
inhibiting access to the data content includes means for  
inhibiting the decryption of the encrypted data.

15

33. An apparatus as claimed in claim 32, comprising:  
means for requesting access to the encrypted data  
from an authorization center (16); and

means for receiving authorization (56) which  
20 includes a key for the decryption of the encrypted data.

34. An apparatus as claimed in claim 33, wherein an  
indication of the start point and an indication of the  
expiration point are provided with the authorization, the  
25 means for defining the start point includes means for  
retrieving the start point indication from the  
authorization, and the means for defining the expiration  
point includes means for retrieving the expiration point  
indication from the authorization.

30

35. An apparatus as claimed in claim 31 or 33,  
wherein an indication of the start point and an indication  
of the expiration point are provided on the storage medium,  
the means for defining the start point includes means for  
35 retrieving the start point indication from the storage  
medium, and the means for defining the expiration point

- 28 -

includes means for retrieving the expiration point indication from the storage medium.

36.           An apparatus as claimed in claim 31, comprising:  
5               means for defining a usage limit (83);  
              means for metering usage of the data content; and  
              means for inhibiting, responsive to the metered  
usage reaching the usage limit, access to the data content  
(79).

10

37.           An apparatus as claimed in claim 36, wherein the  
data content (79) is encrypted, the means for enabling  
access includes means for enabling decryption (97) of the  
encrypted data, and the means for inhibiting access  
15 includes means for inhibiting the decryption of the  
encrypted data.

38.           An apparatus as claimed in claim 37, comprising:  
              means for requesting access to the encrypted data  
20 from an authorization center (16); and  
              means for receiving authorization (56) which  
includes a key for the decryption of the encrypted data.

39.           An apparatus as claimed in claim 38, wherein an  
25 indication of the start point, an indication of the  
expiration point and an indication of the usage limit are  
provided with the authorization (56); the means for  
defining the start point includes means for retrieving the  
start point indication from the authorization; the means  
30 for defining the expiration point includes means for  
retrieving the expiration point indication from the  
authorization; and the means for defining the usage limit  
includes means for retrieving the expiration point  
indication from the authorization.

35

40.           An apparatus as claimed in claim 36 or 38,  
wherein an indication of the start point (80), an

- 29 -

indication of the expiration point (82, 85) and an indication of the usage limit (83) are provided on the storage medium (70); the means for defining the start point includes means for retrieving the start point indication  
5 from the storage medium; the means for defining the expiration point includes means for retrieving the expiration point indication from the storage medium; and the means for defining the usage limit includes means for retrieving the expiration point indication from the storage  
10 medium.

41. An apparatus as claimed in claim 26, wherein the means for measuring time includes a secure time clock (52).

15 42. An apparatus as claimed in claim 41, wherein the secure time clock (52) is password protected.

43. An apparatus as claimed in claim 28, wherein the means for measuring time includes a secure time clock (52).  
20

44. An apparatus as claimed in claim 43, comprising means for setting the secure time clock (52) by the authorization center (16).

25 45. An apparatus as claimed in claim 43, wherein the secure time clock (52) is password protected.

46. An apparatus as claimed in claim 28, comprising a secure device (42) having a time clock for measuring the  
30 time and a memory in which a key for decryption of the encrypted data is stored.

47. An apparatus as claimed in claim 46, wherein the secure device (42) is any of a smart card or a PCMCIA card.  
35

48. An apparatus as claimed in claim 26, wherein the data content (28) of the storage medium comprises multiple

- 30 -

portions of data which are associated with respective start points in time, and the means for enabling access operates on a particular portion of the data content in response to the measured time effectively reaching the respective start point for that portion.

49. An apparatus as claimed in claim 31, wherein the data content (79) of the storage medium comprises multiple portions of data which are associated with respective start points and expiration points in time, the means for enabling access operates on a particular portion of the data content in response to the measured time effectively reaching the respective start point for that portion, and the means for inhibiting access operates on the particular portion of the data content in response to the measured time effectively reaching the respective expiration point for that portion.

50. An apparatus as claimed in claim 26, wherein the storage medium (70) is any of a compact disk, CD-ROM, cartridge and digital video disk.

51. A method of controlling access by a user to a data content of a storage medium, the data being encrypted, comprising the steps of:

defining a start point in time prior to which decryption of the encrypted data (28) is inhibited; measuring time (52); and enabling, responsive to the measured time effectively reaching the start point, the decryption of the encrypted data whereby the user has access (99) to the data.

52. A method as claimed in claim 51, comprising the steps of:

requesting access to the encrypted data from an authorization center (16); and



- 31 -

receiving authorization (56) which includes a key for the decryption of the encrypted data.

53. A method as claimed in claim 52, wherein the step  
5 of defining the start point in time comprises providing an indication of the start point with the authorization (56).

54. A method as claimed in claim 52, wherein the step  
of defining the start point in time comprises providing an  
10 indication of the start point (80) on the storage medium (70).

55. A method as claimed in claim 52, wherein the  
access request includes an identifier of the user and an  
15 identifier of the encrypted data, and further comprising tracking by the authorization center (16) usage of the user.

56. A method as claimed in claim 51, wherein the step  
20 of defining the start point in time comprises providing an indication of the start point (80) on the storage medium (70).

57. A method as claimed in claim 51, comprising the  
25 steps of:

defining an expiration point in time; and  
inhibiting, responsive to the measured time  
effectively reaching the expiration point, the decryption  
(46) of the encrypted data (28) whereby the user is  
30 prevented access to the data.

58. A method as claimed in claim 57, comprising the  
steps of:

requesting access to the encrypted data from an  
35 authorization center (16); and  
receiving authorization (56) which includes a key  
for the decryption of the encrypted data.

- 32 -

59. A method as claimed in claim 58, wherein the steps of defining the start point in time and defining the expiration point in time comprise providing an indication  
5 of the start point and an indication of the expiration point with the authorization (56).

60. A method as claimed in claim 58, wherein the steps of defining the start point in time and defining the  
10 expiration point in time comprise providing an indication of the start point (80) and an indication of the expiration point (82, 85) on the storage medium (70).

61. A method as claimed in claim 58, wherein the  
15 access request includes an identifier of the user and an identifier (24) of the encrypted data (28), and further comprising tracking by the authorization center (16) usage of the user.

20 62. A method as claimed in claim 57, wherein the steps of defining the start point in time and the expiration point in time comprise providing an indication of the start (80) point and an indication of the expiration point (82, 85) on the storage medium (70).

25 63. A method as claimed in claim 57, comprising the steps of:  
defining a usage limit (83);  
metering usage of the data content; and  
30 inhibiting, responsive to the metered usage reaching the usage limit, the decryption (97) of the encrypted data.

64. A method as claimed in claim 63, comprising the  
35 steps of:  
requesting access to the encrypted data from an authorization center (16); and

- 33 -

receiving authorization (56) which includes a key for the decryption of the encrypted data.

65. A method as claimed in claim 64, wherein the  
5 steps of defining the start point in time, defining the expiration point in time and defining the usage limit comprise providing an indication of the start point (80), an indication of the expiration point and an indication of the usage limit with the authorization (56).

10

66. A method as claimed in claim 64, wherein the  
steps of defining the start point in time, defining the expiration point in time and defining the usage limit  
comprise providing an indication of the start point (80),  
15 an indication of the expiration point (82, 85) and an indication of the usage limit (83) on the storage medium (70).

67. A method as claimed in claim 64, wherein the  
20 access request includes an identifier of the user (54) and an identifier of the encrypted data, and further comprising tracking by the authorization center usage of the user.

68. A method as claimed in claim 63, wherein the  
25 steps of defining the start point in time, defining the expiration point in time and defining the usage limit comprise providing an indication of the start point (80), an indication of the expiration point (82, 85) and an indication of the usage limit (83) on the storage medium  
30 (70).

69. A method as claimed in claim 52, wherein the step  
of measuring time includes providing secure time clock  
means (52) for measuring time, the time clock means being  
35 secure such that it can not be altered by the user.

- 34 -

70. A method as claimed in claim 69, comprising setting the secure time clock means (52) by the authorization center (16).

5 71. A method as claimed in claim 70, wherein the secure time clock means is password protected.

72. A method as claimed in claim 52, comprising providing a secure device (42) having a time clock means  
10 (52) for measuring time and a memory in which a key for decryption of the encrypted data is stored.

73. A method as claimed in claim 52, comprising providing non-encrypted data (26) on the storage medium,  
15 and enabling access thereto without authorization.

74. A method for controlling decryption of encrypted data, comprising the steps of:  
defining a start point (80) in time prior to  
20 which decryption of the encrypted data (28) is inhibited;  
measuring time (52); and  
enabling the decryption (46) of the encrypted data on and after the measured time effectively reaches the start point.

25 75. A method as claimed in claim 74, comprising the steps of:  
defining an expiration point in time (82, 85);  
and  
30 inhibiting the decryption of the encrypted data after the measured time effectively reaches the expiration point.

76. A method as claimed in claim 74, comprising the  
35 steps of:  
defining a usage limit (83);  
metering usage of the data content; and

- 35 -

inhibiting the decryption of the encrypted data once the metered usage reaches the usage limit.

77. An apparatus for controlling access by a user to  
5 content of a storage medium (10), the content including encrypted data (28) and the medium being readable by a corresponding medium reader (12) from which the apparatus is adapted to receive the content, comprising:

means for defining a start point in time prior to  
10 which decryption (46) of the encrypted data (28) is inhibited;

means for measuring time (52); and

means for enabling, responsive to the time clock effectively reaching the start point, the decryption of the  
15 encrypted data whereby the user has access (20) to the data.

78. An apparatus as claimed in claim 77, comprising:

means for requesting access to the encrypted data  
20 from an authorization center (16); and

means for receiving authorization (56) which includes a key for the decryption of the encrypted data.

79. An apparatus as claimed in claim 78, wherein the  
25 means for defining the start point in time comprises providing an indication of the start point with the authorization (56).

80. An apparatus as claimed in claim 78, wherein the  
30 means for defining the start point in time comprises providing an indication of the start point (80) on the storage medium (70).

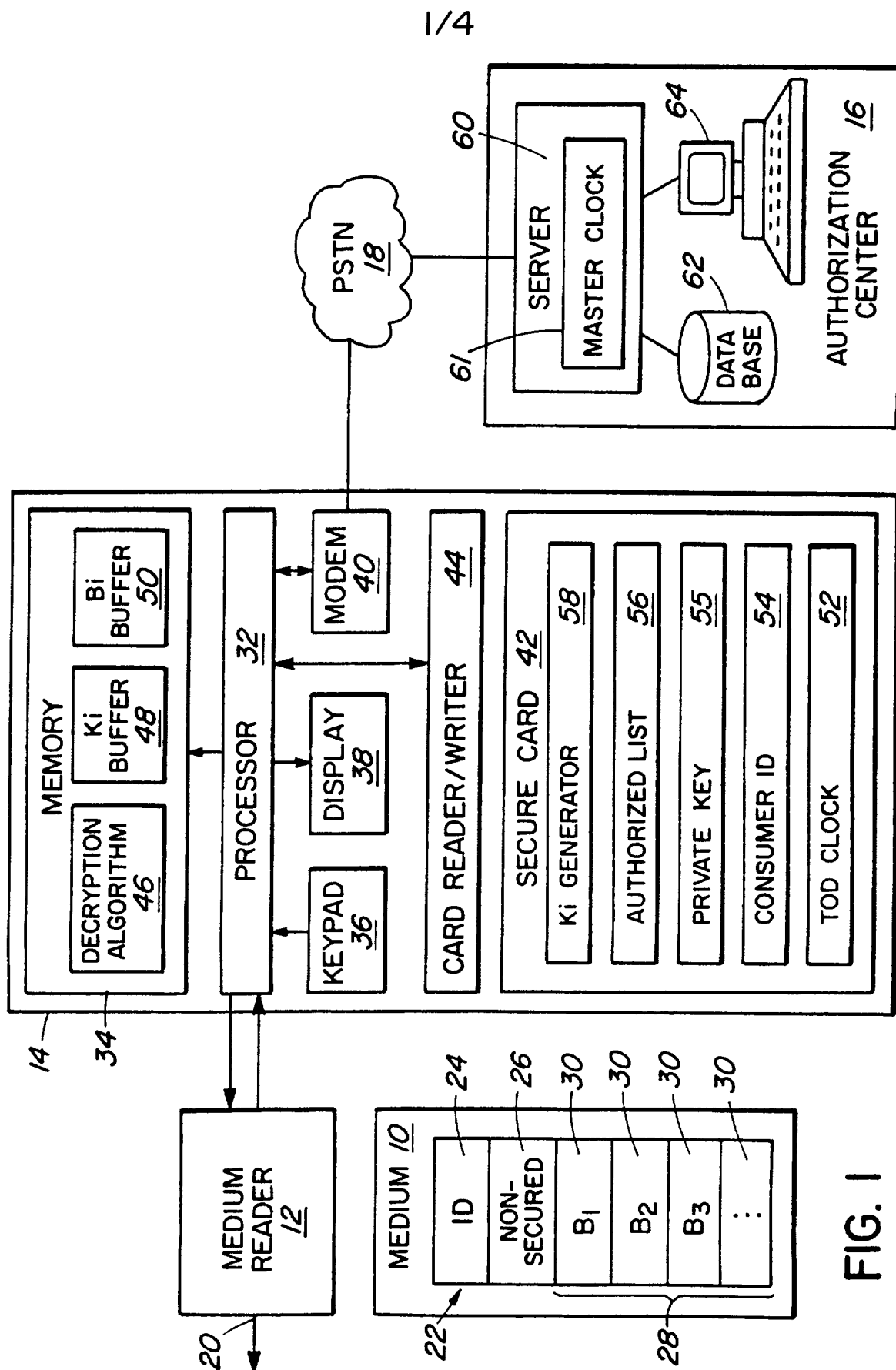
81. An apparatus as claimed in claim 77, wherein the  
35 means for defining the start point in time comprises providing an indication of the start point (80) on the storage medium (70).

- 36 -

82. An apparatus as claimed in claim 77, comprising:  
means for defining an expiration point in time  
(82, 85); and  
5 means for inhibiting, responsive to the measured  
time effectively reaching the expiration point, the  
decryption of the encrypted data (79) whereby the user is  
prevented access to the data.
- 10 83. An apparatus as claimed in claim 82, comprising:  
means for requesting access to the encrypted data  
from an authorization center (16); and  
means for receiving authorization (52) which  
includes a key for the decryption of the encrypted data.
- 15 84. An apparatus as claimed in claim 83, wherein the  
means for defining the start point in time and means for  
defining the expiration point in time comprise providing an  
indication of the start point and an indication of the  
20 expiration point with the authorization (56).
85. An apparatus as claimed in claim 83, wherein the  
means for defining the start point in time and means for  
defining the expiration point in time comprise providing an  
25 indication of the start point (80) and an indication of the  
expiration point (82, 85) on the storage medium (70).
86. An apparatus as claimed in claim 82, wherein the  
means for defining the start point in time and means for  
30 defining the expiration point in time comprise providing an  
indication of the start point (80) and an indication of the  
expiration point (82, 85) on the storage medium (70).
87. An apparatus as claimed in claim 82, comprising:  
35 means for defining a usage limit (83);  
means for metering usage of the data content; and

- 37 -

means for inhibiting, responsive to the metered usage reaching the usage limit, the decryption of the encrypted data.





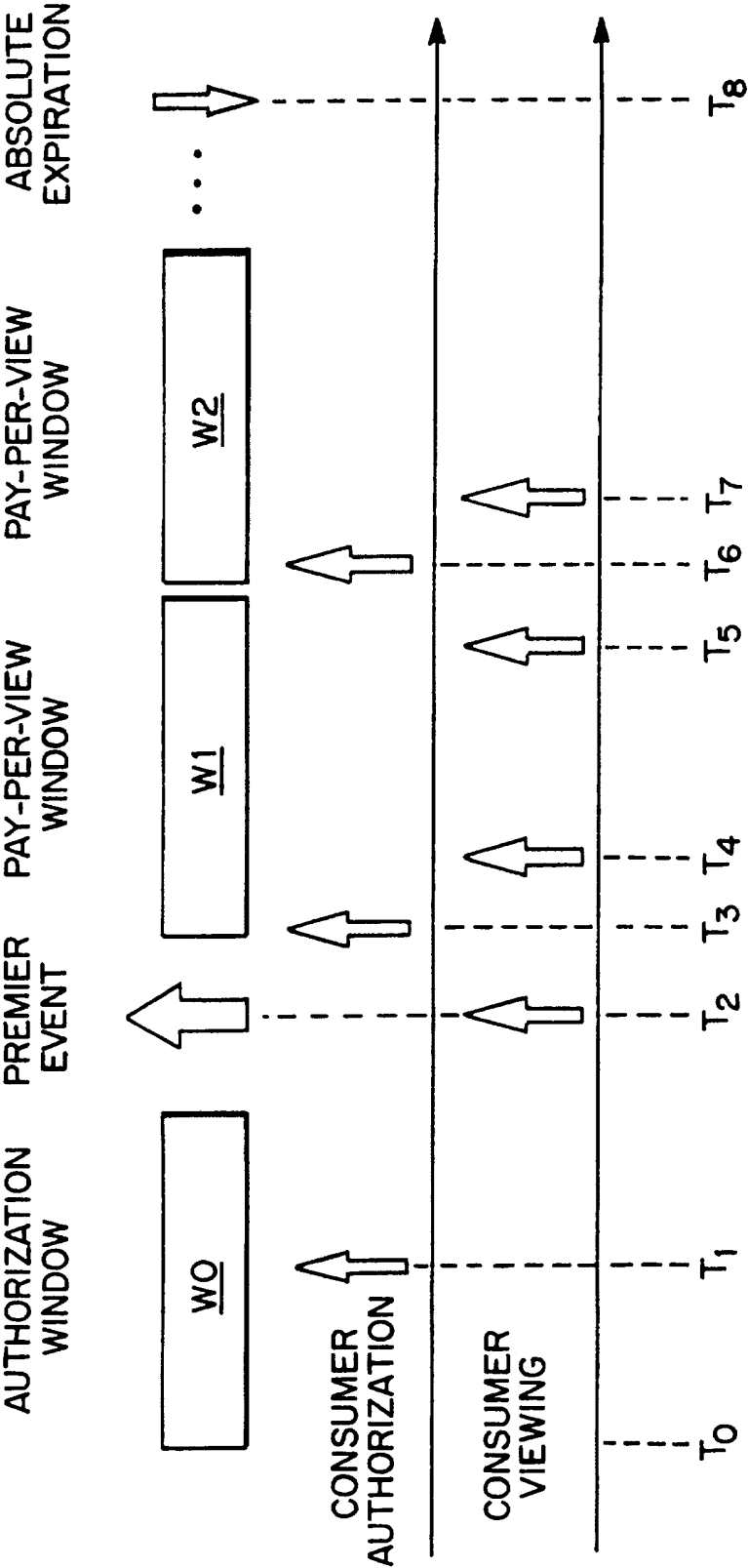


FIG. 2

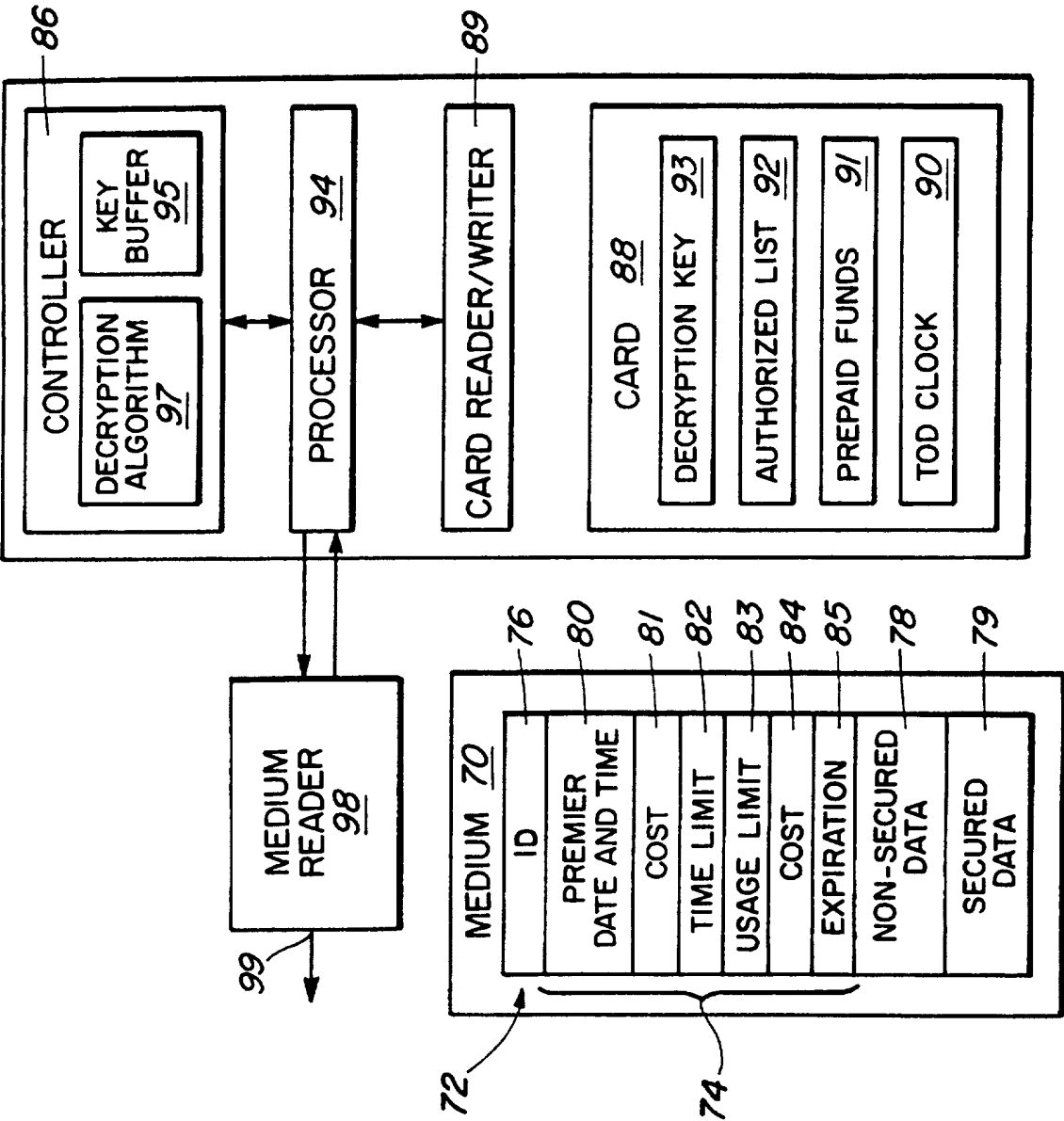


FIG. 3

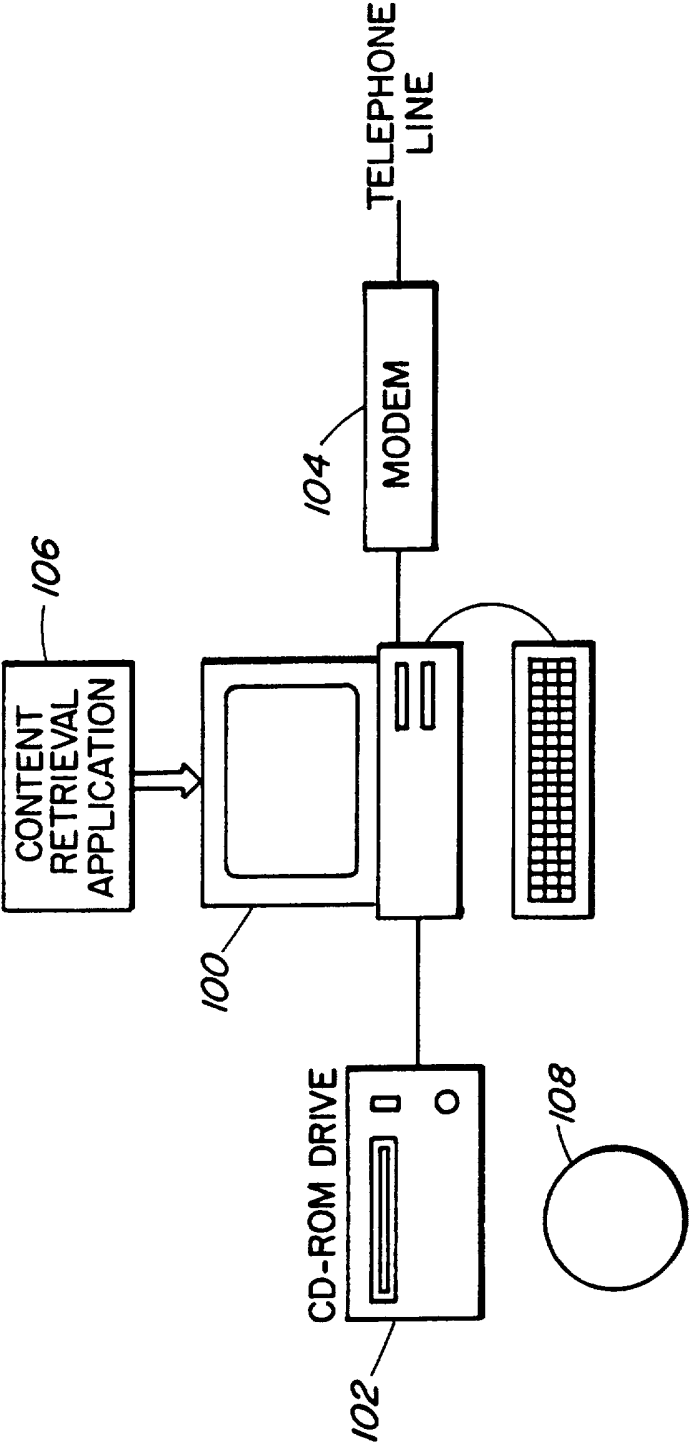


FIG. 4

# INTERNATIONAL SEARCH REPORT

International Application No.  
PCT/CA 96/00790

<b>A. CLASSIFICATION OF SUBJECT MATTER</b> IPC 6 G06F1/00		
According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b> Minimum documentation searched (classification system followed by classification symbols) IPC 6 G06F		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used)		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 92 20022 A (DIGITAL EQUIPMENT CORP) 12 November 1992  see abstract; figure 1 see page 1, line 1 - page 2, line 7 see page 4, line 3 - page 6, line 2 see page 16, line 19 - page 17, line 15	1,6,11, 16,25, 26,31, 36,41,50
Y	--- -/--	2,3,7,8, 12,13, 18,27, 28,32, 33,43, 51,52, 57,63, 64, 74-77, 82,87
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C. <span style="margin-left: 100px;"><input checked="" type="checkbox"/> Patent family members are listed in annex.</span>		
* Special categories of cited documents :  <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p> </div> <div style="width: 45%;"> <p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&amp;" document member of the same patent family</p> </div> </div>		
1	Date of the actual completion of the international search  <div style="text-align: center; font-weight: bold;">12 March 1997</div>	Date of mailing of the international search report  <div style="text-align: center; font-weight: bold;">11. 04. 97</div>
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+ 31-70) 340-3016		Authorized officer  <div style="text-align: center; font-weight: bold;">Powell, D</div>

# INTERNATIONAL SEARCH REPORT

International Application No.  
PCT/CA 96/00790

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 010 571 A (KATZNELSON RON D) 23 April 1991 cited in the application	2,3,7,8, 12,13, 18,27, 28,32, 33,43, 51,52, 57,63, 64, 74-77, 82,87
	see the whole document ---	
A	EP 0 635 790 A (IBM) 25 January 1995	16-21, 41-46, 69-71
	see abstract; figure 1 see column 8, line 21 - line 38 ---	
A	US 4 827 508 A (SHEAR VICTOR H) 2 May 1989 cited in the application -----	

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/CA 96/00790

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9220022 A	12-11-92	AU 659652 B	25-05-95
		AU 2015892 A	21-12-92
		AU 2247092 A	21-12-92
		EP 0538453 A	28-04-93
		EP 0538464 A	28-04-93
		JP 6500878 T	27-01-94
		NZ 242627 A	26-07-95
		WO 9220021 A	12-11-92
		IL 102114 A	14-05-96
		NZ 243277 A	26-10-95
		US 5204897 A	20-04-93
		US 5438508 A	01-08-95
		US 5260999 A	09-11-93
		-----	
US 5010571 A	23-04-91	AT 107818 T	15-07-94
		AU 614693 B	05-09-91
		AU 5680290 A	27-09-90
		AU 600763 B	23-08-90
		AU 8024787 A	07-04-88
		CA 1296104 A	18-02-92
		DE 3750131 D	28-07-94
		DE 3750131 T	24-11-94
		EP 0282570 A	21-09-88
		JP 1501274 T	27-04-89
		WO 8802202 A	24-03-88
		-----	
EP 0635790 A	25-01-95	US 5444780 A	22-08-95
		JP 7036559 A	07-02-95
		US 5500897 A	19-03-96
		-----	
US 4827508 A	02-05-89	AT 133305 T	15-02-96
		DE 3751678 D	29-02-96
		DE 3751678 T	14-11-96
		EP 0329681 A	30-08-89
		WO 8802960 A	21-04-88
		US 4977594 A	11-12-90
		US 5410598 A	25-04-95
		US 5050213 A	17-09-91
		US 5272750 A	21-12-93
		-----	