EXHIBIT C

A listing of all the claims confirmed as allowable by the United States Patent and Trademark Office.

Newly added limitations in Reexamination (control number: 90/008,772) are indicated by underline, whereas deleted parts are enclosed by square brackets.

Note that claims 11, 12 are cancelled, however, they are included herein. This is because their dependent claims 13, 17 are maintained as valid claims in the Reexamination and the scope of dependent claims 13, 17 should be considered in light of those claims that they are depending on, even though those claims are cancelled. See MPEP 2260.01.

1.(Amended): A method for protecting publicly distributed software, from unauthorised use, comprising the steps of:

determining if identity information, is existing in a processing apparatus;

using a positive result of said determination as a pre-condition for causing said processing apparatus to provide user access to said software desired to be protected;

wherein:

said identity information [,if so existing,] being capable of being used in enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible;

said access to said software desired to be protected is being provided without causing a said operation being performed and said identity information being specific to said rightful user(s) ;

and said software desired to be protected is being made available to said rightful user(s) in the form of protected file(s), through a communication network.

2.(Original) A method for protecting software from unauthorised use, as claimed in claim 1, wherein further comprising the steps of:

authenticating said identity information;

determining said identity information as existing, if said identity information being authentic and as not existing if otherwise.

3.(Amended): A method for protecting software from unauthorised use, as claimed in claim 1,wherein said operation being [operation related to] for making payment from an account of said rightful user(s),for obtaining a service/product ;

and said responsibility of said rightful user(s) as recited in claim 1 is referring to said payment said rightful user(s) has to be responsible for ;

and said access being an access to the use of said software desired to be protected ;

and said software desired to be protected being supplied to said rightful user(s), before said determining step ;

and said access being provided independently of, at a site said access being obtained by human user(s),any hardware specific for protecting said software desired to be protected from unauthorized use；

and in additional to said processing apparatus, said method also being capable of being used on at least one more processing apparatus.

4.(Original) A method for protecting software from unauthorised use, as claimed in claim 1, wherein said software desired to be protected comprises a plurality of protected programs; each of said protected programs having validity information in a first predetermined location therein for indicating a valid identity of its rightful user exists in a second predetermined location therein, and an encrypted identity of its rightful user therein; and each of said protected programs, when being executed, will fail to operate if said validity information therein being altered, or said identity therein and the decryption result of said encrypted identity therein being inconsistent.

5.(Original) A method for protecting software from unauthorised use, as claimed in claim 4, wherein further comprising the steps of:

storing an encrypted identity of a user in said processing apparatus; and if all of said protected programs stored in said processing apparatus has a valid user identity which being consistent with the decryption result of said stored encrypted identity, permitting use of said protected programs and not

permitting if otherwise.

6.(Original) A computer software product for protecting software publicly and individually distributed against unauthorised use;

said software product comprising:

identity program code for enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible;

authorising software effectively under the control of said rightful user(s) for, when executed, providing user access to said software desired to be protected, without causing a said operation being performed;

a computer readable medium having said identity program code and said authorising software;

wherein:

said identity program code and said authorising software are stored in said medium in such a manner that said authorising software is prevented from being copied therefrom individually; and

the improvement resides in said protection basing on no hardware and/or software specific to said rightful user(s) other than said identity program code and said identity program code being specific to said rightful user(s).

7.(Original) A computer software product as claimed in claim 6, wherein said operation being operation related to making payment from an account of said rightful user(s).

8.(Original) A computer software product as claimed in claim 6, wherein said authorising software contains said identity program code therein.

9.(Original) A computer software product for protecting other software against unauthorised use, comprising:

authorising program for, when being executed on a processing apparatus, providing user access to said software desired to be protected;

a computer readable medium having said authorising program

wherein:

information specific to rightful users) of said software desired to be protected, exists in said authorising program as a part thereof;

said existing information being capable of being used in enabling electronic commerce operation(s) for which said rightful user(s) has to be responsible, but not being usable by said processing apparatus for said electronic commerce purpose, when said authorising program being loaded on said

processing apparatus as a part thereof, and access to said software desired to be protected is being provided without causing a said operation being performed.

10.(Original) A computer software product as claimed in claim 9,wherein said operation being operation related to making payment from an account of said rightful user(s).

11. (Cancelled) A method for protecting publicly distributed software from unauthorised use, comprising the steps of:

obtaining first information from a user of a processing apparatus having an identity software;

using said first information received being correct as a pre-condition for causing said processing apparatus to provide user access to said software desired to be protected;

wherein:

said identity software being for providing a second information specific to rightful user(s) of said software desired to be protected, if said correct first information is being obtained from a user thereof; and said second information

being capable of being used in enabling electronic commerce operation(s) for which said rightful user(s) has to be responsible;

access to said software desired to be protected is being provided without causing a said operation being performed.

12. (Cancelled) A method for protecting software from unauthorised use, as claimed in claim 11, wherein said operation being operation related to making payment from an account of said rightful user(s) and said first information being a password.

13.(Original) A method for protecting software from unauthorised use, as claimed in claim 11, wherein said software desired to be protected being first software used on said processing apparatus for determining third information related to hardware and/or software of said processing apparatus;

wherein further comprising second software for, when being executed, authenticating the identity of the computer on which said second software runs as being said processing apparatus, basing on at least a part of said third information;

and for providing user access to third software if said computer has an

authentic identity.

16.(Amended): A method for protecting software from unauthorised use, comprising the steps of:

(a) obtaining by protection software running on a processing apparatus, say, first processing apparatus, first information from the user thereof;

(b) determining by said protection software, from said processing apparatus second information related to the hardware or/and software thereof for future reference in step (c) below, in response to said first information obtained being consistent with third information contained in said protection software, thereafter

(c) authenticating a processing apparatus, say, second processing apparatus, as being said first processing apparatus, basing on at least a part of said second information;

(d) using a positive result of said authentication as a pre-condition for permitting use of said software desired to be protected on said second processing apparatus;

wherein said third information being confidential information of a rightful user of said software [desire] desired to be protected and being necessary for

enabling electronic commerce transaction(s) for which said rightful user has to be responsible; and said method is being performed without causing a said transaction take place.

17.(Original) A method for protecting software from unauthorised use, as claimed by claim 12, wherein said software desired to be protected being purchased commercial software.

20.(Original) A method for protecting software, for use by a user, from unauthorised use; comprising a sub-method;

wherein said sub-method a protection software being used and "the presence of identity information in a processing apparatus" is being used in the creation of said protection software as an "installation" pre-condition for said protection software to perform in said processing apparatus step (a) below; and said identity information being specific to said user and capable of being used in enabling electronic commerce operation(s) for which said user has to be responsible;

said sub-method comprising the steps of:

(a) determining by said protection software running on a processing apparatus,

say, first processing apparatus with said "installation" precondition being met, first information related to the hardware or/and software of said first processing apparatus, for future reference in step (c) below; thereafter

(b) determining from a processing apparatus, say, second processing apparatus, second information related to the hardware or/and software thereof;

(c) determining if said second information is consistent with said first information;

(d) using a positive result of said determination of consistence as a pre-condition for permitting use of said software desired to be protected on said second processing apparatus, with said "installation" pre-condition not being met;

thereafter, said sub-method being capable of being used on a processing apparatus, say, third processing apparatus, without causing any user responsible operation(s) being performed therefor and with no step relating to a new user payment therefor.

21. (Amended): A method for verifying identity of a user of a data processing apparatus, comprising the steps of:

receiving, by said data processing apparatus, information specific to [a] said user and necessary for accessing an account of said user;

verifying said account being valid, by an electronic transaction system by use of said information received by said data processing apparatus;

using by said data processing apparatus, a positive result of said verification as a precondition for providing user access to at least a part of the functionality of said data processing apparatus;

wherein said method is being performed without charging said account and said at least a part of functionality being not related to said validity status of said account ;

and functionality identical as said at least a part of functionality being made available to at least one more user other than said user ;

and said access being provided independently of , at a site said access being obtained by user(s), any hardware specific for protecting said at least a part of functionality from unauthorized use.

23.(new): A method for protecting publicly distributed software, from unauthorised use, comprising the steps of:

authenticating identity information associated with a processing apparatus;

using a positive result of said authentication as a pre-condition for causing said processing apparatus to provide user access to said software desired to be protected;

wherein:

said identity information being capable of being used in enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible;

said access to said software desired to be protected is being provided without causing a said operation being performed；

and said software desired to be protected is being made available to said rightful user(s) in the form of protected file(s)；

and in additional to said processing apparatus, said method also being capable of being used on at least one more processing apparatus and said identity information being specific to said rightful user(s).

27. (New) A method for protecting software which being made available to a person in the form of protected file(s),from unauthorised use, by restricting the use thereof to be under control of said person, comprising a sub-method; said sub-method comprising the steps of:

(a) establishing a communication between a processing apparatus, say, first processing apparatus and a remote electronic transaction system;

(b) verifying said person having a valid account, by said remote electronic transaction system, basing on authenticated information related to said person, said authenticated information being information [being] communicated to said remote electronic transaction system from said processing apparatus and then authenticated by said remote electronic transaction system;

(c) using a positive result of said verification as a pre-condition for permitting use of said software on said first processing apparatus;

wherein said sub-method a cost is being charged from said account; and thereafter, said sub-method being capable of being used on a processing apparatus, say, second processing apparatus, without said cost;

wherein said use of said software being permitted independently of, at a site said person using said software, any hardware specific for protecting said software from unauthorized use.

28.(New): A method for protecting publicly distributed software, from unauthorised use, comprising the steps of:

obtaining first information from a user of a processing apparatus having an identity software;

using said first information received being correct as a pre-condition for causing said processing apparatus to provide user access to said software desired to be protected;

wherein:

said identity software being for providing a second information specific to rightful user(s) of said software desired to be protected, if said correct first information is being obtained from a user thereof; and said second information being capable of being used in enabling electronic commerce operation(s) for which said rightful user(s) has to be responsible;

said access to said software desired to be protected is being provided without causing a said operation being performed ;

and said software desired to be protected is being made available to said rightful user(s) in the form of protected file(s) and is being received by said rightful user(s), through a communication network.

29. (New): A method for protecting software from unauthorised use, as claimed in claim 11,wherein said operation being [operation related to] for making payment from an account of said rightful user(s) ;

and said responsibility of said rightful user(s) as recited in claim 11 is referring to said payment said rightful user(s) has to be responsible for ;

and said first information being a password ;

and said access being an access to the use of said software desired to be protected ;

and said software desired to be protected being supplied to said rightful user(s), before said receiving step ;

and said access being provided independently of , at a site said access being obtained by human user(s), any hardware specific for protecting said software desired to be protected from unauthorized use ;

and in additional to said processing apparatus, said method also being capable of being used on at least one more processing apparatus.