



Delegatura de Propiedad Industrial
División de Nuevas Creaciones

SOLICITUD
PATENTE DE INVENCION

21. **EXPEDIENTE No.** _____

54. **TÍTULO** Method For remotely controlling and monitoring the
Data Produced on Desktop on desktop software

51. **CLASIFICACIÓN INTERNACIONAL** _____

71. **SOLICITANTE** Mandar Patil

DOMICILIO India

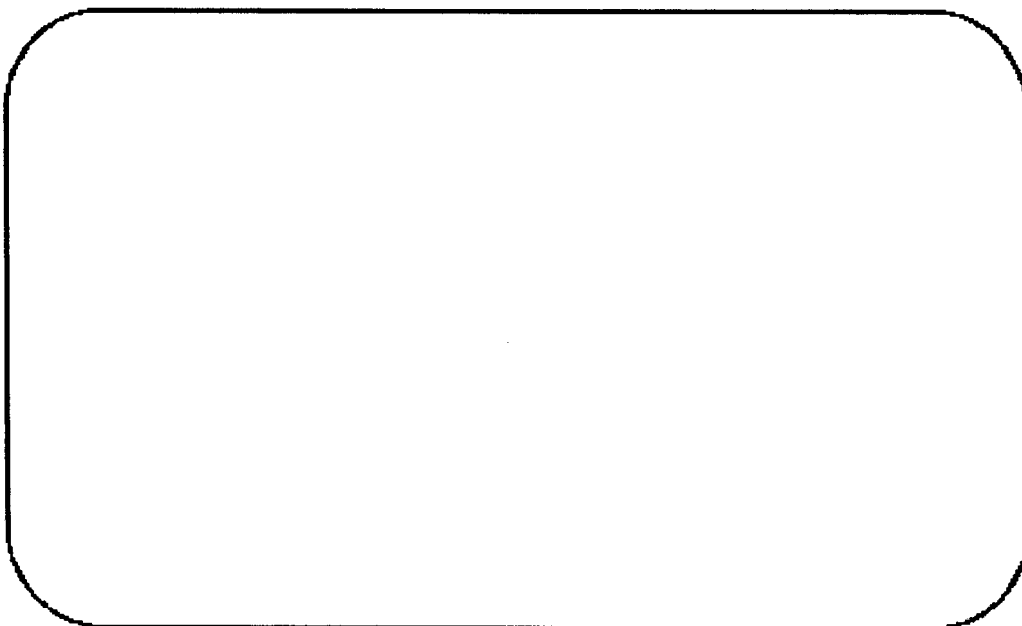
74. **APODERADO** Mauricio Pinzón Pinzón

22. **BOGOTÁ, D.C.,** 31 de enero de 2012

		PETITORIO	
INDUSTRIA Y COMERCIO SUPERINTENDENCIA		SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO No. 12-017138- -00000-0000 Fecha: 2012-02-01 15:28:33 Dep. 2020 DIR.NUEVASCR Tra. 11 PATENTEI/II Eve: 378 FASENACIONALI Act. 411 PRESENTACION Folios: 141	
FORMULARIO ÚNICO DE PCT ENTRADA EN FASE NACIONAL			
1 SOLICITUD DE: ☒ Patente de Invención ☐ Patente de Modelo de Utilidad			
☒ Capítulo I ☐ Capítulo II			
2 SOLICITANTE	Nombre: Mandar Patil Dirección: 85, NATIONAL SOCIETY, AUNDH, PUNE 411007 Nacionalidad o Domicilio: India Lugar de Constitución: India Teléfono: Fax: E-mail:	IDENTIFICACIÓN ☐ CC ☐ NT ☒ CE ☐ Otro Cúal Número	
3 REPRESENTANTE O APODERADO	Nombre: Mauricio Pinzón Pinzón Dirección: Calle 99 No. 12-39 p 4 Teléfono: 6219721 Fax: E-mail: Pinzonpinzon@pinzonpinzon.com	IDENTIFICACIÓN ☒ CC ☐ NT ☐ CE ☐ Otro Cúal Número 79.145.527 TP 37.242 En caso de haber presentado poder general para asuntos que se adelanten ante la Delegatura de Propiedad Industrial, sírvase indicar el número de radicación (del poder):	
4 INVENTOR (ES) (72)	Nombre: Mandar Patil Dirección: 85, NATIONAL SOCIETY, AUNDH, PUNE 411007 Nacionalidad o Domicilio: India		
5 PCT (86) Solicitud Internacional No. PCT/IB2010/052959 Fecha 29.06.2010 Publicación internacional No. WO/2011/001371 Fecha 06.01.2011			
6 Título (54) METHOD FOR REMOTELY CONTROLLING AND MONITORING THE DATA PRODUCED ON DESKTOP ON DESKTOP SOFTWARE			
7 Clasificación Internacional (51)			
8 Prioridad ☒ SI ☐ NO	(33) País de Origen India	(32) Fecha 01.07.2009	(31) Número de Solicitud 1543/MUM/2009
9 Comprobante de pago No. 12 00 10130 Fecha 12 00 10132			
Instrucciones para el diligenciamiento del presente formulario, ver reverso de esta página			

10 Anexos

- ☒ Comprobante de pago de la tasa de presentación de la solicitud.
- ☐ Documento que acredite la existencia y representación legal de la persona jurídica peticionaria, en cuanto no estén inscritas en alguna Cámara de Comercio Colombiana.
- ☒ Poderes, si fuere el caso.
- ☐ Documento de cesión del inventor al solicitante o a su causante.
- ☒ Traducción de la solicitud internacional al castellano (Resumen, descripción, reivindicaciones, dibujos)
- ☐ Copia del examen preliminar internacional efectuado por la Autoridad Internacional de Examen preliminar (IPEA)
- ☐ Traducción de examen preliminar internacional efectuado por la IPEA.
- ☐ De ser el caso, copia del contrato de acceso.
- ☐ De ser el caso, documento que acredite la licencia o autorización de uso de conocimientos tradicionales de las comunidades indígenas.
- ☐ De ser el caso, certificado de depósito del material biológico
- ☐ Arte final 12x12.
- ☐ De ser el caso, información sobre otras solicitudes de patente o títulos obtenidos en el extranjero por el mismo titular o su causante, relacionadas parcial o totalmente con la invención de esta solicitud.
- ☐ De ser el caso, modificaciones efectuadas a la solicitud internacional.
- ☒ Otros

11**FIGURA CARACTERÍSTICA:****12**

Solicito la concesión de la patente

NOMBRE Mauricio Pinzón Pinzón

FIRMA

C.C.

7914557

TP

39.230.

Instrucciones para el diligenciamiento del presente formulario, ver reverso de esta página

POWER OF ATTORNEY

Be it known that:

MANDAR PATIL, addressed at Survey Number 118 to 124 Plot Number 85, National society, Aundh, Pune, 411007, Maharashtra, India,

does hereby grant GENERAL POWER OF ATTORNEY

to:
MAURICIO PINZON PINZON
SILVIA GARCIA CHACON
JULIANA ORDUZ BELTRAN

lawyers in practice, of legal age, residing in Bogota D.C., Republic of Colombia, so that they may act in his own name and representation in order to carry out all the necessary steps and processes before the judicial, administrative or police authorities of the Republic of Colombia or any other countries if it could be necessary, as well as before third persons or parties in order to:

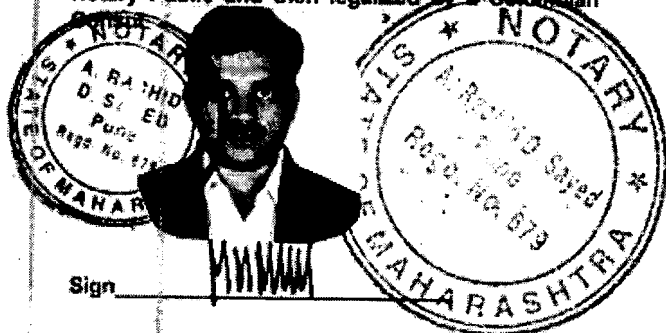
1) Obtain the registration and/or protection of the Intellectual Property Rights in general terms and in specific aspects such as Trademarks, industrial designs, utility models, patents, Plants Varieties, Denomination of Origin, Commercial Names and Ensigns, Copyrights, Domain Names, including all the steps, procedures and actions necessary for their defense, protection and conservancy, including the capability of granting licenses and to assign registrations.

2) Obtain the licenses or health registration or whatever necessary for the normal development of activities as well as the commercialization of its products or services.

3) Our proxies also are specifically authorized to carry out in our name, all the payments related with government expenses, rates, banking commissions, bearings, notarial expenses and in general all the other expenses that are required for the effects of the exact fulfillment of this mandate.

In carrying out the present mandate the proxy will be able to receive, withdraw, compromise, conciliate, substitute, resume, and in general, carry out all kinds of actions which would lead to the obtention of the pursued matter.

Note: This document must be signed before a Notary Public and then legalized by a Colombian



15 OCT 2011

PODER GENERAL

Compareció:

MANDAR PATIL, domiciliado en Survey Number 118 to 124 Plot Number 85, National society, Aundh, Pune, 411007, Maharashtra, India y,

otorgó PODER GENERAL a:

MAURICIO PINZON PINZON
SILVIA GARCIA CHACON
JULIANA ORDUZ BELTRAN

Abogados en ejercicio, mayores de edad, vecinos de Bogotá D.C., República de Colombia, para que en su nombre y representación adelanten ante las autoridades judiciales, administrativas o de policía de la República de Colombia y de los demás países que así le indique así como ante terceras personas, todos los trámites, acciones judiciales o extrajudiciales, o gestiones según sea el caso encaminadas a:

1) Obtener el registro y/o protección de los Derechos de Propiedad Intelectual en terminos generales y específicamente en materias tales como Marcas, Diseños Industriales, Modelos de Utilidad, Patentes, Variedades Vegetales, Denominaciones de Origen, Nombres y Enseñas Comerciales, Derechos de Autor, Nombres de Dominio, comprendiendo todos los trámites, gestiones y acciones que se hagan necesarios para su conservación y defensa, incluyendo la facultad de conceder licencias y efectuar cesiones.

2) Obtener las Licencias o Registros Sanitarios o de cualquier otra índole, necesarios para el normal desarrollo de su actividad ordinaria, así como para la comercialización de sus productos o servicios.

3) Nuestros apoderados igualmente quedan expresamente facultados para efectuar por cuenta nuestra el pago a terceros de tasas, pagos de servicios prestados por terceros en Colombia como en el exterior, comisiones bancarias, portes, gastos notariales y en general todos los demás gastos que se requieran para los efectos del cabal cumplimiento de este mandato.

En desarrollo del presente mandato los apoderados podrán recibir, desistir, transigir, conciliar, sustituir, reasumir y en general realizar todo tipo de actos que contribuyan a la obtención del objeto perseguido.

Note: Este documento debe ser firmado ante Notario Publico y luego legalizado ante el consulado colombiano.

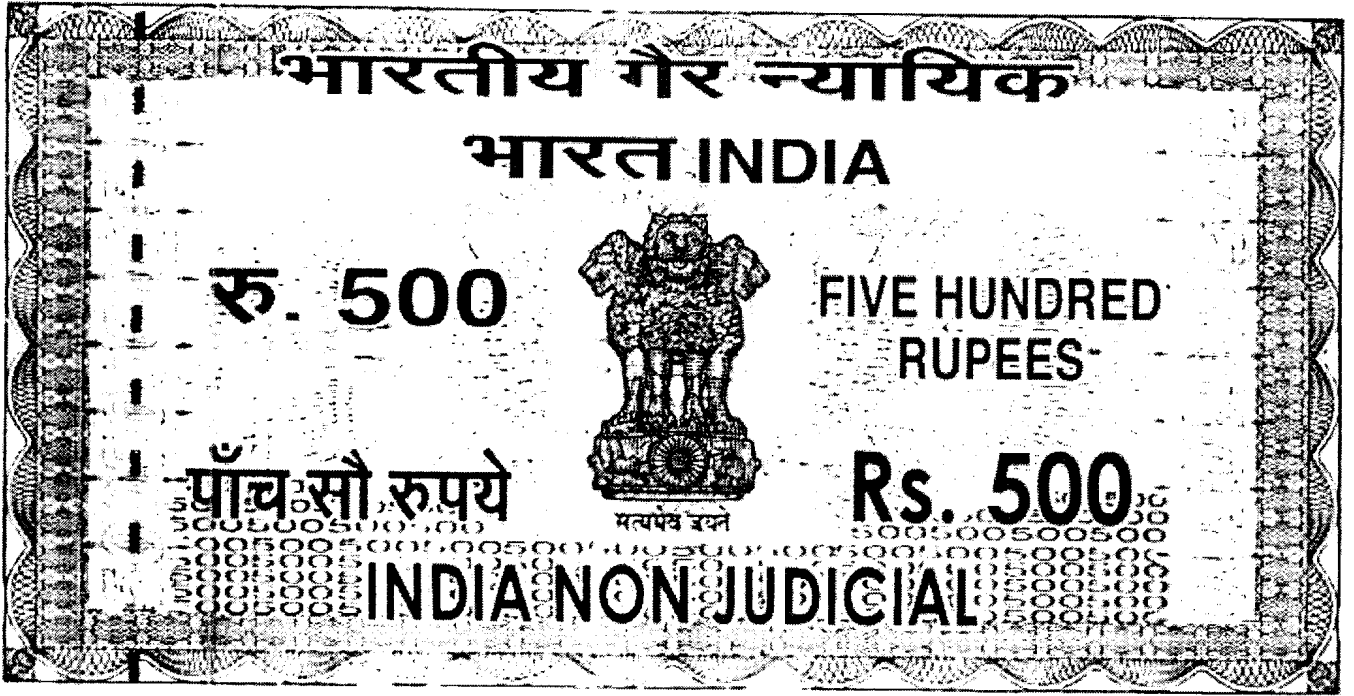
ATTESTED BY

A. Rashid D. S. Ed.
Notary State of Maharashtra
PUNE

Firma

Noted & Registered

At Sr. No. 9497



महाराष्ट्र MAHARASHTRA

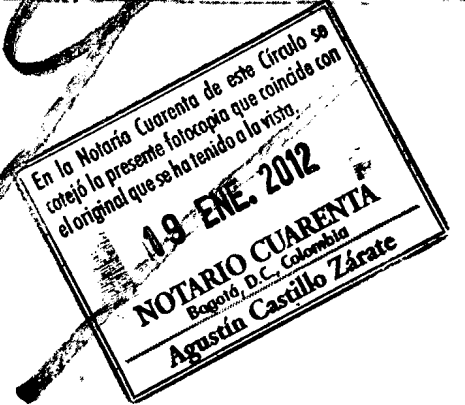
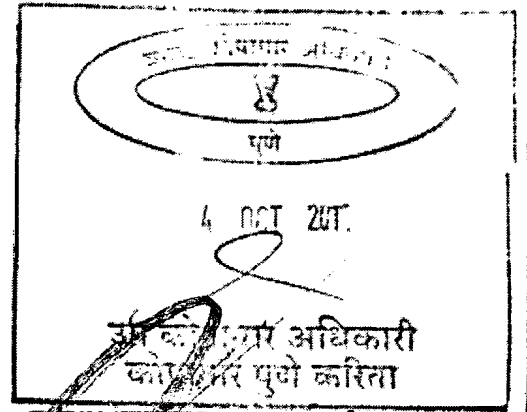
13 OCT 2011

L 606246

अनुक्रमांक १५८७० दिनांक रुपये ५००
मुद्रांक कोशस्थ कर्तव्यसाठी वापरावयाचा आहे P O A
मुंबई मुद्रांक अधिनियम १९५८ चे अनुच्छेद क
मुद्रांक वापरणारिया नाव मंदार पाटील
पूर्ण पत्ता नवीन कोठा पुणे ८
हस्ते व्यक्तीचे संपा का १५ जग
पत्ता पुणे
मुद्रांक धारकाची हस्ते व्यक्ती करी

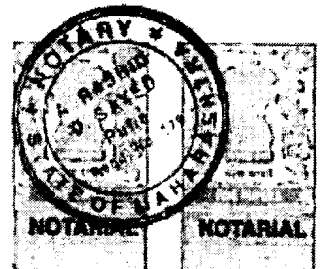
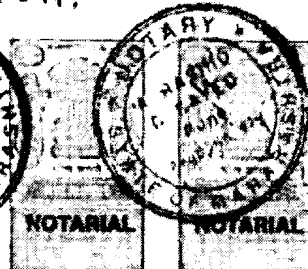


कोंडिराम पां. जगताप
मुद्रांक विक्रेता
परवाना क्र. ८८/१९९९, ए-१०
परवाना मुदत ३१ मार्च २०१२
स्मॉल कॉज कोर्ट बिल्डींग, पुणे.



Power of Attorney

This Power of Attorney is made & executed on
this 14th day of Oct 2011.

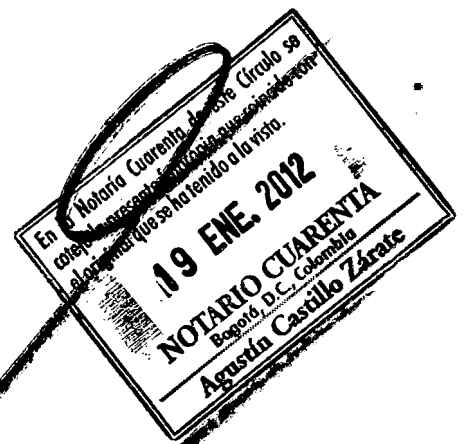


09 OCT 2011

SPE 1400A/1/50570L
Com

8299
T

27



भारत सरकार GOVERNMENT OF INDIA
अपोस्टिल / APOSTILLE
(Convention de La Haye du 5 octobre 1961)

Country **INDIA**

This public document of the type
POWER OF ATTORNEYS

is issued to **MANDAR PATIL**

has been signed by **SECTION OFFICER**

with the seal / stamp of **SECTION OFFICER, HOME DEPTT
GOVT. OF MH**

Certified by
Section Officer(OI) MINISTRY OF EXTERNAL AFFAIRS
on 15-Nov-2011 at NEW DELHI, INDIA
Reference no. MHMC0010104411



संसी लीचियस के.पि.
SASI LEACHIOUS K.P.
असिस्टेंट सेक्रेटरी (एओ.आई.)
Section Officer (O.I.)
वि. व. मंत्रालय, नई दिल्ली
Ministry of External Affairs
New Delhi



The Signature of Shri
..... is hereby Certified

[Signature]
Section Officer
Home Department
Government of Maharashtra
Mantralaya, Mumbai

20 OCT 2011

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
NIT : 800.176.089-2
- / -

 Industria y Comercio SUPERINTENDENCIA	RECIBO DE CAJA	No. 12 - 0010130
		Bogotá D.C., Febrero 01 de 2012 - 14:55:26

RECIBIDO DE : PINZON PINZON & ASOCIADOS ABOGADOS S.A.					NI 830.005.919
*** Soporte del Pago ***					
TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PAGO	VR. PAGO
CONSIGNACION	BANCO DE BOGOTA	062754387	445219504	01/02/2012	1.520.000.00

*** Conceptos Pagados ***				
CANT.	RENTISTICO	CONCEPTO	Vr.UNDITARIO	Vr.CONCEPTO
1	50005-01-01 SOLICITUDES	1 TRAMITES DE SOL. DE PATENTE DE INVENCIÓN	590.000.00	590.000.00
				\$590.000.00
=====				

SON: **QUINIENTOS NOVENTA MIL PESOS MONEDA CORRIENTE**

Responsable: _____
Recibo de Caja Aplicado al Expediente No. _____

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

No. 12-017138- -00000-0000
Fecha: 2012-02-01 15:28:33 Dep. 2020 DIR.NUEVASCR
Tra. 11 PATENTEIYII Eve: 378 FASENACIONALI
Act. 411 PRESENTACION Folios: 141

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO NIT : 800.176.089-2 - / -					
 Industria y Comercio SUPERINTENDENCIA	RECIBO DE CAJA			No. 12 - 0010132	
				Bogotá D.C., Febrero 01 de 2012 - 14:55:26	
RECIBIDO DE : PINZON PINZON & ASOCIADOS ABOGADOS S.A.				NI 830.005.919	
*** Soporte del Pago ***					
TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PAGO	VR. PAGO
CONSIGNACION	BANCO DE BOGOTA	062754387	445219504	01/02/2012	1.520.000.00
*** Conceptos Pagados ***					
CANT.	RENTISTICO	CONCEPTO	Vr. UNDITARIO	Vr. CONCEPTO	
1	50005-01-01 SOLICITUDES	82 INVOCACION DE UNA PRIORIDAD EN NUEVAS CREACIONES	170.000.00	170.000.00	
				\$170.000.00	
=====					
SON: **CIENTO SETENTA MIL PESOS MONEDA CORRIENTE***					
Responsable: _____ *****			SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO		
Recibo de Caja Aplicado al Expediente No. _____			 No. 12-017138- -00000-0000		
			Fecha: 2012-02-01 15:28:33 Dep. 2020 DIR.NUEVASCR Tra. 11 PATENTEIYII Eve: 378 FASENACIONALI Act. 411 PRESENTACION Folios: 141		
Sede Centro: Carrera 13 No. 27 - 00 Pisos 3,4,5 y 10 Bogotá, D.C.- Colombia					
Web: www.sic.gov.co e-mai: info@sic.gov.co Conmutador: (571) 5870000 Fax: (571) 5870284 Línea: 018000-910165 Call Center: (571) 6513240					
Febrero 1 de 2012 - 14:55:27					

7

Method and apparatus for remotely controlling and monitoring the data produced on
and by desktop software.

Mandar Madhukar Patil

An Indian National

Residing at Survey Number 118 to 124, Plot Number 85,
National Society, Aundh, Pune 411007, Maharashtra, India.

THE FOLLOWING SPECIFICATION PARTICULARLY DESCRIBES THE
INVENTION AND THE MANNER IN WHICH IT IS TO BE PERFORMED

FIELD OF INVENTION

This invention relates to a method namely ISO data system which provides a protection mechanism to safeguard the data generated by any software, using iso data system, from unauthorized usage.

In particular, iso data system is a method in which data created using the said system is unique and exclusive to the software installed on a particular computer. Data can be used only on the computer that has created it. To use this data on another computer, sufficient access permissions must be given to the data by the owner.

BACKGROUND OF THE INVENTION:

Many a times, data is confidential in nature. Data misuse can lead to serious losses due to which protecting it is very important. Data protection comprises of three main elements, Confidentiality, Integrity and Accessibility. Confidentiality means protecting the data from unauthorized access. Integrity means data can be modified only if appropriate permissions and authorization are given by the data owner. Availability simply means that the data must be available when it is required.

Current available solutions on data security are using passwords, hardware locks, encryptions and similar kind.

PRIOR ART:

US patent application number 20090259512 describes a method of controlling access to a media storage device for storing a plurality of media objects wherein the method includes receiving first data identifying the media storage device and second data identifying a list comprising at least one authorized recipient of the media storage device; storing first data in association with the second data; issuing the media storage device to at least one recipient on the list; using a delivery session identifier to establish a delivery session for the issued media storage device with a user identification system corresponding to recipients associated with the second data; and then updating the second data on the basis of data received from the user

identification system and the delivery session identifier, thereby to modify the list of authorised recipients of the issued media storage device.

Further there is also provided a distribution access control system which controls access to a media storage device, the media storage device storing a plurality of media objects, the distributed access control system wherein an interface arranged to receive first data identifying the media storage device and second data identifying a list comprising at least one authorised recipient of the media storage device; a storage system arranged to store the first data in association with the second data; and a device issuing system arranged to issue a media storage device to at least one recipient on the list is provided. Said device issuing system is arranged to create a delivery session identifier to establish a delivery session for the issued media storage device with a user identification system corresponding to at least one recipient associated with the second data, and a storage system is arranged to update the second data on the basis of the delivery session and data received from the user identification system, thereby to modify the list of authorised recipients of the issued media storage device.

OBJECTS OF THE INVENTION:

Data misuse means unauthorized access and usage of data. When data is made unusable for unauthorized recipients, its security no longer remains a problem. Current systems do not have comprehensive and foolproof methods to protect data.

It is an object of the present invention to provide a foolproof method to protect, access and usage of data by unauthorized recipients. Even if the data accidentally reaches

unauthorized access, it cannot be used and processed. The data created on a particular computer cannot be used on any other computer, unless the data owner has granted the required permissions to each computer on which he wants this data to be shared.

The present invention also provides an automated, easy and hassle free software reinstallation system for the user.

SUMMARY OF THE INVENTION:

Registration of the software in the vendor's online server is mandatory for usage of iso data system since this feature can be used only by registered users of the software. The registration system of the software and the iso-data system go hand in hand for data security. After successful registration of the software with the vendor's online server, a unique, permanent, customer id is issued to every registered software. This customer id is unique and important and is used to identify the user of particular software installed in a particular computer. During the software activation, a file is generated by the server. This file is sent to the software. This file is unknown to user and contains keys R1 and R2. The server generates these keys and permanently stores it. The function of these keys is to protect software data from unauthorized usage. These keys are used for encryption and decryption at required stages. Both R1 and R2 are permanent keys, unique to each registered software and are associated with a particular unique customer id with the vendor's online server and with the particular unique installed software. R1 key is used to protect data of the software installed in that particular computer that is owner's data. R1 key is not shared with any other user. By default, the data created by the particular software is always encrypted and stored with R1 key in the computer in which the software is installed. It is a private key. R2 is the key that can be registered with other users on other computers, if needed, with

the permission of the owner and is used to protect the data that is being shared. It is a public key of that particular unique software.

Ra and Rb are the private and public key of the recipient, respectively. The public keys and private keys are confidential and will not be used or shared without a purpose. Data owner can register his R2 key with as many recipients as he needs to. These may be recipients to whom owner may need to send data frequently. The data owner will send an instruction to the server to register his R2 key with the recipients, by entering the recipients' customer id's. This instruction will contain the data owner's customer id as well. When the recipient is connected to the online server, an alert will be displayed requesting the recipient to register the data owner's R2 key. It is up to the recipient to register the key or not. At any point of time the data owner can revoke the registration of his R2 key with the other recipients by instructing the server to do so. The server will not need the recipient's permission to revoke the data owner's R2 key registered with a particular recipient.

Data is information created while using the software. The software data can be shared by using any external storage device or by uploading data online to the vendor's server from where the recipient can download it. Owner can set full or partial access permissions for example view, read, print, save and amend. The control of data remains with the data-owner, even after sharing it with other users. Each time authorized recipient accesses shared data, the status of the access permissions will be checked with the online server, if needed. Only if the access permissions are still active, can the recipient access the data else the recipient will be alerted that the data access permissions are no longer valid. Data owner can also send an instruction to the online server to delete the data, he has shared, from the authorized recipient's computer, if needed. Process and storage of original data and data which is received

for sharing, are processed through two different and mutually exclusive sub systems which supports encryption system respectively and data is stored in two separate locations in the same computer/ system respectively. Data can be protected from unauthorized usage, using iso data system. The process to ensure authorized usage of data, using iso data system, is explained further. In the present embodiment, the environment contains a data owner, a recipient with whom the data owner needs to share the data and an online server. Owner can share data with other registered users. The recipient may or may not have the data owner's R2 key registered with him. In both cases, data sharing can be done by two methods, either by uploading the data set/packet to be shared to the online server or by copying the data to be shared on any external storage device and sharing this device with the intended recipient.

Consider the recipient does not have the data owner's R2 key and the data owner wants to share data by uploading it to the online server. Since the data to be shared is already in an encrypted form with the data owner's R1 key, it is decrypted by the same R1 key and then it is encrypted using the R2 key on the data owner's computer which is controlled by a standard password mechanism each time.

Also the customer id of the recipient as well as sender is entered in this data. Each data set/packet shared by the data owner will contain a particular data id generated by the data owner's system. The said data id will determine uniqueness of each set of data sent to be shared and also will help in the management of the said data. Access permissions and corresponding information of each set of data are associated with its data id. Server will keep a log of all data sets/packets, all attributes associated with their corresponding data ids. This data is then uploaded to the online server where it is again decrypted using the data owner's R2 key and converted into normal/original form. This data is then encrypted with the recipients Rb key. The online server sends

an alert to the recipient that certain data is waiting to be shared. The recipient then downloads this data and decrypts it using the data recipient's Rb key.

The same data can be given via an external storage device to the recipient. In this case the recipient will upload this data to the online server. The server will check if the data owner, has set the permission for the particular recipient, customer id which has uploaded the data and only if the permissions are set the data will be processed and sent back to recipient. If the permissions were not granted by the data owner, the online server will delete the data from the recipient's computer. When user uploads this data to the online server the decryption and encryption take place as explained above and when the recipient is connected to the online server he can download and use this data. Now consider the recipient has the data owner's R2 key registered with him. Again the data owner can share the data by uploading it to the online server or by storing the said data to an external storage device and sharing this device with the recipient. In this case the encrypted data is decrypted using the same R1 key and again encrypted using the data owner's r2 key. The recipient can either download this data from the server or from the external storage device; however the data owner has sent it. Since the recipient already has the data owner's r2 registered, the said data can be decrypted using the Owner's Rb key and use it.

Even if the data accidentally reaches unauthorized software which has the data owner's R2 key, the data will not be accessed as the customer id of the software in which the data is being opened will differ with the customer id instructed in the authorization.

The shared data can be used with only the authentication of the server and stored in a location separate from original location. The recipient will download the data and import it into the software. Data can be used as per the access rights given with the

data. Access rights could be of two types, one is view only where the data can be only viewed not saved and second is full or partial access to use or change the data. The data will behave only in the way the data access and usage permissions have been set by the data owner. For example, the data can be used for x number of days, x number of hours, x number of times, data can or cannot be amended, data can or cannot be saved, data can or cannot be printed.

In case the recipient amends the data and wants to share it back with the data owner, the same can be done by four methods. In method 1, consider, the recipient did not have the R2 key of the data owner. The recipient will encrypt the data to be sent back to the owner with his Rb key. This data which can be sent to the data owner via two methods; one by which the recipient uploads the data to the online server wherein the server converts the data encrypted with Rb key to data owner's R2 key and sends this data to the data owner upon his connection to the online server. The data owner downloads this data and converts it from R2 key to R1 key in order to use it. The recipient can adopt a second method of giving the data encrypted with Rb key to be shared on an external storage device. In this case, the data owner will receive the external storage device and upload this received data to online server where the server will convert the data from Rb key to R2 key and the data owner can download this data and convert the data from R2 key to R1 key and use the data.

In method 2, consider the recipient has the R2 key of the data owner; in this case again the recipient can send the amended data back to the data owner via an external storage device or via uploading the data to be shared to the online server. In both cases the data is encrypted using the data owner's R2 key and sent. Data owner can download this data via the online server or from the external storage device however the recipient has sent it and convert the data from R2 to R1 and use the it.

c5

Amendment of data will be shown to data owner, only if he accepts the amendment, the data will be imported and merged. A facility will be given to the data owner to merge the data that has been amended by the recipient. The data that is to be shared, amended is kept in a separate location from the original location of the software and does not interfere in any way with the original data/records of both users' softwares until an instruction is given to do so. Data owner can keep the original copy if required before amalgamating/integration of the recipient's changes. Same procedure will be applied if data owner wants to share data with more than one recipient.

In case a need arises for the user to reinstall the software, a reinstallation wizard will open. This wizard will take the input of user's email id.. After verification, the account details will be fetched from the server and the software will be reinstalled. The server will send a confirmation key to the user's registered email id. The confirmation key is valid only for one particular transaction and is associated to the activation file of that software. The user has to enter the confirmation key sent to the registered email id, into this activation wizard after which an activation file is sent to the software from the server. Incase the motherboard id's of the computer matches with the mother board id registered with the online server when the software was registered, the keys R1, R2 will be restored by the server into the software, The user will have to send a request back to the other users to re register their R2 keys with his software. Incase the motherboard id of the computer differs during the time of reinstallation, the software will be installed but the R2 keys previously registered with the server will not be registered again due to the discrepancy found in the

motherboard id and the software will also alert the user to send request again to the various data owners for re registration of their R2 key with the said software.

Each time the software opens, an authorization component matches the motherboard id embedded in the software with the motherboard id of the computer. Incase a discrepancy in the motherboard id is found; the software will get blocked and alert the user to validate with the online server. Once the user validates with the online server, a confirmation key will be sent to the user's registered email id after which the R1 and R2 keys will be sent and restored to the software. The software will also alert the user to send request again to the various data owners for re registration of their R2 key with the said software. Only after data owner's confirmation, their R2 key will be registered with the recipient again. Each time the computer is connected to internet, the server will check the status of the R2 key which is registered with the software. If the server notes that the R2 key of a particular data owner, has been revoked, it will revoke the registration of this R2 key with the recipient. Similarly the recipient can also remove the registration of a particular R2 key by informing the server. In this case the data owner will be alerted about his R2 key being unregistered by a particular recipient.

ADVANTAGES AND APPLICATIONS

Present invention method Iso data system helps the software owner to protect his software data from unauthorized access. The software owner can set restrictions on data usage by the recipient. Data can be shared by any external drive or by uploading it to the online server.

In view of the wide variety of embodiments to which the principles of the present invention can be applied, it should be understood that the illustrated embodiments are

exemplary only. The illustrated embodiments should not be taken as limiting the scope of the present invention. While various elements of the preferred embodiments have been described as being implemented, other embodiments implications may alternatively be used, and vice-versa.

BRIEF DESCRIPTION OF THE DRAWINGS:

Figure 1a and 1b illustrates the process of Software registration and use of data by owner.

Figure 2a and 2b illustrates the procedure for sharing of data online.

Figure 3a and 3b illustrates the process of sharing of data using an external drive like a Compact Disk.

Figure 4a and 4b illustrates the process of software reinstallation and reassigning of keys.

Figure 5 illustrate the process of sharing of R2 key with various potential recipients.

Figure 6 illustrate the process of revoking R2 key from potential recipients.

Figure 7 illustrate the process of authorization.

DETAILED DESCRIPTION OF THE INVENTION:

The ISO data system program is a byte code program written in Microsoft .NET programming language.

The description generally provides method of protecting the user's data from unauthorized access. A method for registering a user to the online server includes receiving an initial access to desktop software by a prospective user and determining

whether the user has provided valid user identification information. Referring to Figure 1a, User installs the software on his computer by executing function 101, upon successful installation user is ready to use the software. User clicks on the software executable for first time to run the software, method 102 is invoked. When owner uses the software for first time, software registration window 103 will appear to register user to vendor's online server from desktop software. Owner enters registration information via 104 into registration wizard 103. If internet connection is available 105 verifies the integrity of the 105 method associated with each loaded object, if the method 106 is successfully executed the method 107 validates user information upon successful invocation of 108, user is registered to the vendor's online server by invoking method 109 and the server issues unique customer id to the user and embeds customer id in the software by executing method 110. Method 111 (as referred in Figure 1b) is invoked to display activation wizard, user chooses subscription option i.e. trial or subscription method 112 is invoked to send confirmation key to user's registered email id. Owner enters confirmation key into activation wizard by executing function 113, software executes internet connection availability class 114 to check the internet connection if internet is available, then function 116 execute to validate the confirmation key with the online database by executing internet availability class 117. Upon successful validation server sends activation file with encrypted customer id 118, this activation file also contains two unique keys R1 and R2 for encryption and decryption of software data, installation id, period of authorized usage transferred from online server to user's machine and store users motherboard id to online database. Software creates database encrypted with R1 key of owner.

Referring to Figure 2a, if the data owner wishes to share his data with another registered recipient by executing method 201, Since the data is originally encrypted

with the data owner's R1 key at time of data creation, software data is decrypted with data owner's R1 key and then encrypted using data owner's R2 key after the data owner enters a password and customer id is entered by performing method 202; owner sets the data access permissions, system assigns a unique data id to this set of data by executing function 203. User needs to choose the method of sharing of the data, 204. If user chooses the online data sharing method by performing method 205, and If internet connection is available, the software verifies the integrity of the 206 method associated with each loaded object, If the method 206 is successfully executed, 207 is invoked to check whether owner have recipients Rb key If owner have recipients Rb key then function 208 is executed to encrypt the data with Rb key and stores it on online server else method 209 is executed to store the data on the online server with the R2 key, online server decrypts the data with data owner's R2 key and encrypts the data again with Rb key of recipient. If internet connection is available software verifier 210 verifies the integrity of the 210 method associated with each loaded object, If the method 210 is successfully verified 211 is invoked to alert recipient about the data. Recipient downloads the data of owner through server by performing method 212. If the method 214 is successfully verified 215 (as referred in Figure 2b) is invoked to decrypt the data with receivers Rb key and import it into receiver's software in a separate location. Software verifier 216 checks the data sharing permission, software checks if recipient is having permission to amend the data by performing 217; if method 217 is successfully executed then method 219 is invoked to amend the data according to permission set. If permission is denied to amend the data, recipient can only view the data 218.

After completion of the amendment of the data; Function 220 verifies to check whether recipient have owners R2 key if 220 is successfully executed method 221 is

invoked to encrypt the data with owners R2 key and upload it to the online server, else amended data is encrypted with recipient's Rb key and upload the data back to the server by performing method 222. At server, data is decrypted with recipient's Rb key and again encrypted with data owner's key R2 by performing method 223. After this the owner will get the alert of amended data by method 225, If internet connection is available software verifier 224 verifies the integrity of the 224 method associated with each loaded object, If the method 225 succeed to alert the owner, method 226 is invoked to download the data. Software checks if user is intended recipient by performing method 227 and If user verification is correct then verifier 228 verifies the integrity of the 228 method associated with each loaded object, If the method 228 is successfully verified 230 is invoked by owner to import the data into the software at a separate location and if verification failed then data is discarded by performing the method 229. If owner accepts the data by performing method 231, method 232 invoked to merge the data into the original data.

Referring to Figure 3a, if data owner wishes to share his data with other registered recipients by executing method 301, Since the data is originally encrypted with the data owner's R1 key at time of data creation, software decrypts the data using the R1 key and then encrypts the data using key R2 by performing method 302; this occurs only after the data owner enters a password to execute this transaction. Owner sets the permissions to amend the data and a unique data id is assigned to this set of data by executing function 303. Owner chooses the method of sharing of the data 304 i.e. through online method or through an external drive. If data owner chooses the data sharing method through external drive by performing method 305, Function 306 is invoked to check whether owner have recipients Rb key If owner have recipients Rb key then function 307 is executed to encrypt the data with Rb key and stores it on

online server else method 308 is executed to encrypt the data with R2 key and receivers details. Owner sends encrypted data to recipient through external drive by performing method 309. Receiver accepts the data by performing method 310. Software checks the validity of the user by cross checking with customer id by performing method 311 software verifier 312 verifies the integrity of the 312 method associated with each loaded object, If the method 312 is successfully verified 313 (as referred in Figure 3b) is invoked to decrypt the data and import it into receiver's software. Verifier 314 checks the permission set for the amendment of the data, if receiver is having permission to amend the data by performing 315, if method 315 is successfully executed then method 316 is invoked to decrypt the data with key Ra associated with receiver else receiver can only view the data by performing method 317. With this recipient updates the data of owner according to permission set by performing method 316, After completion of the amendment of the data; Function 318 verifies to check whether recipient have owners R2 key if 318 is successfully executed updated data is encrypted with owner's R2 key by performing methods 322. Recipient uploads the data back to the external drive by performing the function 323, the owner will get the external drive of the updated data by method 324. Else software encrypts the data with recipients Rb key and upload back to external drive by performing method 319, owner receive the data and upload it to the server by performing method 320, at the end of server online server decrypt the data with Rb key and encrypt it again with R2 key and send it to the owner by performing method 321. Software checks if user is intended recipient by performing method 325 and If recipient verification is correct then verifier 326 verifies the integrity of the 326 method associated with each loaded object, If the method 326 is successfully verified 328 is invoked by owner to import the data into the software and if verification fails,

the data is discarded by performing the method 327. If owner accepts the data by performing method 329, method 330 is invoked to merge the received data into owner's original data. According to this scenario the given data is protected from unauthorized access.

Referring to Figure 4a, If user needs to reinstall the software due to any reason method 401 is invoked. User reinstalls the software by executing function 402. Method 403 is executed while user clicks to start the software, software registration window 404 will appear, user enters registered email id and password and clicks next, to proceed by executing function 405. If internet connection is available 406 verifies the integrity of the 406 method associated with each loaded object, if the method 407 is successfully verified, 408 is invoked to check entered registration information with vendors online server database. If registration information is validated successfully, 409 verifies its integrity associated with each loaded object, if the method 409 is successfully verified 410 is invoked to fetch all information of customer who has already registered to online server. Method 411 reinstalls the software and invokes method 412 (as referred in Figure 4b) to send confirmation key to user's registered email id, method enters confirmation key and click next by performing method 413. Software validates confirmation key 415 with online database if key is validated by 416 then disables all previous installation ids for particular user and generates new unique installation id, store machine code to online database by executing function 417. Software checks motherboard id embedded in software with machine motherboard id by executing method 418. Verifier 419 successfully verifies the motherboard id function 420 executes to assign new keys R1 and R2 to user and alert user to send request again to the various data owners for re registration of their R2 key

with the software. Only after data owner's confirmation, their R2 key will be registered with the recipient again.

Referring to Figure 5, if owner wants to share R2 key with other registered users 501 method is invoked. Wizard 502 appears to enter customer id of recipients. Owner enters the customer id of recipients with whom he want to share his data by performing function 503, If internet connection is available connection verifier 504 verifies the integrity of the 505 method associated with each loaded object, If the method 505 is successfully verified 506 is invoked to store R2 key with receivers customer id to the online server. If internet connection is available connection verifier 507 verifies its integrity associated with each loaded object, If the method 507 is successfully verified 508 is invoked to alert the recipient to register the key. Now if user accepts to register the key by executing function 509 then If internet connection is available connection verifier 511 verifies the integrity of the 511 method associated with each loaded object, If the method 511 is successfully verified 512 is invoked to alert owner about registration of R2 key with recipient. If user does not accept 510, the key is not registered.

Referring to Figure 6, if data owner wants to revoke, R2 key shared with other users 601 method is invoked. Interface 602 appears with list of customer id's with whom the data owners R2 key is registered. Owner selects the customer id of recipients from whom he wants to revoke his R2 key and sends this request to online server by performing function 603, If internet connection is available on the recipients computer connection verifier 604 verifies the integrity of the 605 method associated with each loaded object, If the method 605 is successfully verified 606 is invoked to revoke registered R2 key from intended recipient from online server. If internet connection is available on the data owners computer connection verifier 607 verifies its integrity

associated with each loaded object, If the method 607 is successfully verified 608 is executed to alert owner about successful revoking of R2 key from intended recipient.

Referring to figure 7, Whenever the software is opened, authorization component 701 checks for motherboard id embedded in software with machine's motherboard id. Function 702 checks whether the motherboard ids' have changed, then function 703 will execute to block the software and alert user to validate with online server. If internet connection is available connection verifier 704 verifies the integrity of the 705 method associated with each loaded object, If the method 705 is successfully verified 706 is invoked to validate the software with online server and send confirmation key to user's registered email id. User enters confirmation key into the activation wizard by executing function 707. If verifier 708 validates confirmation key with online server, then function 709 is executed to register new motherboard id with server and identify the software with this motherboard id. Function 710 executes to send and restore R1 R2 keys to user's software. Function 711 will execute to alert owner to request other data owners to register their R2 key with the said software. Only after data owner's confirmation, their R2 key will be registered with the recipient again.

I claim;

1. A method of controlling usage of data and prevent unauthorized usage of data which is generated by software, using iso data system.
2. A method of claim 1 wherein data can be used only on the computer which has created it using iso data system; to use said data on another computer, data

owner must authorize a recipient, using the same iso data system on another computer.

3. A method of claim 1, comprising:
 - selecting the data to be shared and embedding data owner's customer id;
 - identifying and authorizing at least one recipient with whom the data is to be shared by entering the recipient's customer id;
 - identifying each set of data being shared by a unique data id generated by the data owner's system where in the access permissions to each set of data are associated with each particular data id ;
 - issuing required access permissions to authorized recipient to use the data;
 - using appropriate data sharing methods i.e. sharing via uploading the data to the online server or by copying the data to any external storage device.
4. A method of claim 1 wherein, during software activation, the vendors' online server sends two keys namely R1 and R2 to the software. Key R1 is used to encrypt owner's data to protect it from unauthorized usage of this data on any other computer. When data is created in the software it is automatically encrypted with the R1 key and stored in this encrypted form. Key R2 is used to protect the data that is to be shared with one or more intended recipients on their computer system. Ra and Rb are the private and public keys of the recipient.
5. A method of claim 3, wherein data owner can share the data with the recipient via uploading the data to the online server or by transferring data to an external storage device and sharing this device with the recipient.

6. A method of claim 3 where incase the recipient has not yet registered the data owner's R2 key and data to be shared is uploaded to the online server, data is first decrypted using the data owner's R1 key and then encrypted with the data owner's R2 key. This data is uploaded to the server where it is decrypted with data owner's R2 key and again encrypted with the recipient's Rb key. Recipient downloads this data and uses it with his Rb key.
7. A method of claim 3 where incase the recipient has not yet registered the data owner's R2 key and data to be shared is sent to the recipient via an external storage device, data is first decrypted using the data owner's R1 key and then encrypted with the data owner's R2 key. This data transferred to the external storage device and shared with the recipient. The recipient uploads this data to the online server and incase the data owner has given sufficient permissions, the server decrypts this data with the data owner's R2 key and encrypts this data with the recipients Rb key after which recipient can download and use this data with his Rb key.
8. A method of claim 3 where incase the recipient has previously registered the data owner's R2 key and data to be shared is uploaded to the online server, data is first decrypted using the data owner's R1 key and then encrypted with the data owner's R2 key. This data is uploaded to the server, the recipient downloads this data from the server and decrypts and uses the data with the data owner's R2 key.

9. A method of claim 3 where incase the recipient has registered the data owner's R2 key and data is shared via an external storage device, data is first decrypted using the data owner's R1 key and then encrypted with the data owner's R2 key. This data is transferred to the external storage device and shared with the recipient. Recipient downloads this data from the storage device and decrypts and uses the data with the data owner's R2 key.
10. A method of claim 1 wherein, the data system can be used to protect any data on the data owner's computer/system.
11. A method of claim 3 wherein, the data downloaded by the authorized and designated recipient is bound by certain access rights issued by the data owner; said data can be used by the recipient only as per the access rights set, where said set access rights are viewing, amending, printing and saving.
12. Method of claim 3 wherein, the authorized recipient can amend the data and send it back to the data owner if needed. This amended data will be recognized using a new data id. The data is encrypted with Rb key and uploaded to the server where it is decrypted with the Rb key and again encrypted with the data owner's R2 key. Owner can download this data and convert it back to the R1 key and use it.
13. A method of claim 12, wherein recipient can amend the data shared by the data owner, if needed, and send amended data back to the data owner either

via uploading the data to the online server or by transferring data to an external storage device and sharing this device with the data owner.

14. A method of claim 12 where incase the recipient has not yet registered the data owner's R2 key. Amended data to be shared is encrypted with recipient's Rb key and uploaded to the online server, where it is decrypted with the recipient's Rb key and later encrypted with the data owner's R2 key. Data owner downloads this data and converts it from R2 to his R1 key and then uses it.
15. A method of claim 12 where incase the recipient has not yet registered the data owner's R2 key and amended data to be shared is sent to the data owner via an external storage device, data is encrypted using the recipient's Rb key transferred to the external storage device and shared with the data owner. The data owner uploads this data to the online server and incase the recipient has given sufficient permissions, the server decrypts this data with the recipient's Rb key and encrypts this data with the data owner's R2 key after which data owner can download this data, convert it from the R2 key to R1 key and use it.
16. A method of claim 12 where incase the recipient has previously registered the data owner's R2 key and amended data to be shared is uploaded to the online server, data owner downloads this data and decrypts it using his R2 key. Said data can be converted from the R2 key to R1 key and then used.

17. A method of claim 12 where incase the recipient has previously registered the data owner's R2 key and shares the amended data via an external storage device, data owner downloads this data from the storage device and decrypts it using his R2 key. Said data can be converted from the R2 key to R1 key and then used.
18. Method of claim 3 where process and storage of original data and data which is received for sharing, are processed through two different and mutually exclusive sub systems and are at two separate locations in the same computer/system.
19. A method of claim 12 wherein, the data owner is alerted about the amendment done by the authorized recipient in the shared data and can merge it into the original data if required.
20. A method of claim 1 wherein, the data owner can register his R2 key with other recipients for secured data sharing purpose by sending the server an instruction to do so and entering both customer's as well as data owner's customer id. The registration of this key can be revoked at any time by either parties, by sending an instruction to the vendor's online server about the same.
21. A method of claim 3 wherein, the data owner can block the access rights to the data shared with a recipient, by instructing the server to block or delete the data sent to the recipient.

22. A method of claim 3 wherein, even if the data from the recipients computer, is used on any other computer, it cannot be accessed, used or processed, due to lack of permissions from the data owner.
23. A method of claim 1 wherein, in case the software is required to be reinstalled, an easy method of reinstallation is provided to the software user and the server sends the encryption and decryption keys again to the software after activation. It also sends the previously registered R2 keys of other user's into the software.
24. A method of claim 16, wherein incase during reinstallation or each time the software is opened, it is detected that there is the motherboard id of the computer has changed, then the software will have to be revalidated with the server and also the R2 keys will have to be revalidated again by the data owners only then the data sharing from these owners can occur.
25. A method of claim 1 wherein, the iso data system can also be used as an independent encryption module to secure data storage.

I claim;

1. A method of controlling usage of data and prevent unauthorized usage of data which is generated by software, using iso data system.
2. A method of claim 1 wherein data can be used only on the computer which has created it using iso data system; to use said data on another computer, data owner must authorize a recipient, using the same iso data system on another computer.
3. A method of claim 1, comprising:
 - selecting the data to be shared and embedding data owner's customer id;
 - identifying and authorizing at least one recipient with whom the data is to be shared by entering the recipient's customer id;
 - identifying each set of data being shared by a unique data id generated by the data owner's system where in the access permissions to each set of data are associated with each particular data id ;
 - issuing required access permissions to authorized recipient to use the data;
 - using appropriate data sharing methods i.e. sharing via uploading the data to the online server or by copying the data to any external storage device.
4. A method of claim 1 wherein, during software activation, the vendors' online server sends two keys namely R1 and R2 to the software. Key R1 is used to encrypt owner's data to protect it from unauthorized usage of this data on any other computer. When data is created in the software it is automatically encrypted with the R1 key and stored in this encrypted form. Key R2 is used

to protect the data that is to be shared with one or more intended recipients on their computer system. R_a and R_b are the private and public keys of the recipient.

5. A method of claim 3, wherein data owner can share the data with the recipient via uploading the data to the online server or by transferring data to an external storage device and sharing this device with the recipient.
6. A method of claim 3 where incase the recipient has not yet registered the data owner's R_2 key and data to be shared is uploaded to the online server, data is first decrypted using the data owner's R_1 key and then encrypted with the data owner's R_2 key. This data is uploaded to the server where it is decrypted with data owner's R_2 key and again encrypted with the recipient's R_b key. Recipient downloads this data and uses it with his R_b key.
7. A method of claim 3 where incase the recipient has not yet registered the data owner's R_2 key and data to be shared is sent to the recipient via an external storage device, data is first decrypted using the data owner's R_1 key and then encrypted with the data owner's R_2 key. This data transferred to the external storage device and shared with the recipient. The recipient uploads this data to the online server and incase the data owner has given sufficient permissions, the server decrypts this data with the data owner's R_2 key and encrypts this data with the recipients R_b key after which recipient can download and use this data with his R_b key.

8. A method of claim 3 where incase the recipient has previously registered the data owner's R2 key and data to be shared is uploaded to the online server, data is first decrypted using the data owner's R1 key and then encrypted with the data owner's R2 key. This data is uploaded to the server, the recipient downloads this data from the server and decrypts and uses the data with the data owner's R2 key.
9. A method of claim 3 where incase the recipient has registered the data owner's R2 key and data is shared via an external storage device, data is first decrypted using the data owner's R1 key and then encrypted with the data owner's R2 key. This data is transferred to the external storage device and shared with the recipient. Recipient downloads this data from the storage device and decrypts and uses the data with the data owner's R2 key.
10. A method of claim 1 wherein, the data system can be used to protect any data on the data owner's computer/system.
11. A method of claim 3 wherein, the data downloaded by the authorized and designated recipient is bound by certain access rights issued by the data owner; said data can be used by the recipient only as per the access rights set, where said set access rights are viewing, amending, printing and saving.
12. Method of claim 3 wherein, the authorized recipient can amend the data and send it back to the data owner if needed. This amended data will be recognized using a new data id. The data is encrypted with Rb key and uploaded to the

server where it is decrypted with the Rb key and again encrypted with the data owner's R2 key. Owner can download this data and convert it back to the R1 key and use it.

13. A method of claim 12, wherein recipient can amend the data shared by the data owner, if needed, and send amended data back to the data owner either via uploading the data to the online server or by transferring data to an external storage device and sharing this device with the data owner.

14. A method of claim 12 where incase the recipient has not yet registered the data owner's R2 key. Amended data to be shared is encrypted with recipient's Rb key and uploaded to the online server, where it is decrypted with the recipient's Rb key and later encrypted with the data owner's R2 key. Data owner downloads this data and converts it from R2 to his R1 key and then uses it.

15. A method of claim 12 where incase the recipient has not yet registered the data owner's R2 key and amended data to be shared is sent to the data owner via an external storage device, data is encrypted using the recipient's Rb key transferred to the external storage device and shared with the data owner. The data owner uploads this data to the online server and incase the recipient has given sufficient permissions, the server decrypts this data with the recipient's Rb key and encrypts this data with the data owner's R2 key after which data owner can download this data, convert it from the R2 key to R1 key and use it.

16. A method of claim 12 where incase the recipient has previously registered the data owner's R2 key and amended data to be shared is uploaded to the online server, data owner downloads this data and decrypts it using his R2 key. Said data can be converted from the R2 key to R1 key and then used.
17. A method of claim 12 where incase the recipient has previously registered the data owner's R2 key and shares the amended data via an external storage device, data owner downloads this data from the storage device and decrypts it using his R2 key. Said data can be converted from the R2 key to R1 key and then used.
18. Method of claim 3 where process and storage of original data and data which is received for sharing, are processed through two different and mutually exclusive sub systems and are at two separate locations in the same computer/system.
19. A method of claim 12 wherein, the data owner is alerted about the amendment done by the authorized recipient in the shared data and can merge it into the original data if required.
20. A method of claim 1 wherein, the data owner can register his R2 key with other recipients for secured data sharing purpose by sending the server an instruction to do so and entering both customer's as well as data owner's

customer id. The registration of this key can be revoked at any time by either parties, by sending an instruction to the vendor's online server about the same.

21. A method of claim 3 wherein, the data owner can block the access rights to the data shared with a recipient, by instructing the server to block or delete the data sent to the recipient.
22. A method of claim 3 wherein, even if the data from the recipients computer, is used on any other computer, it cannot be accessed, used or processed, due to lack of permissions from the data owner.
23. A method of claim 1 wherein, in case the software is required to be reinstalled, an easy method of reinstallation is provided to the software user and the server sends the encryption and decryption keys again to the software after activation. It also sends the previously registered R2 keys of other user's into the software.
24. A method of claim 16, wherein incase during reinstallation or each time the software is opened, it is detected that there is the motherboard id of the computer has changed, then the software will have to be revalidated with the server and also the R2 keys will have to be revalidated again by the data owners only then the data sharing from these owners can occur.
25. A method of claim 1 wherein, the iso data system can also be used as an independent encryption module to secure data storage.

ABSTRACT

According to this invention there is provided a method of controlling usage of data and prevent unauthorized usage of data that is generated by software using iso data system where data can be used only on the computer which has created the data or use and/or access the data on other computers only if the owner of such data has given access/permission to such data.

COMPLETE SPECIFICATION

Figure 1 - Registration and transfer of keys

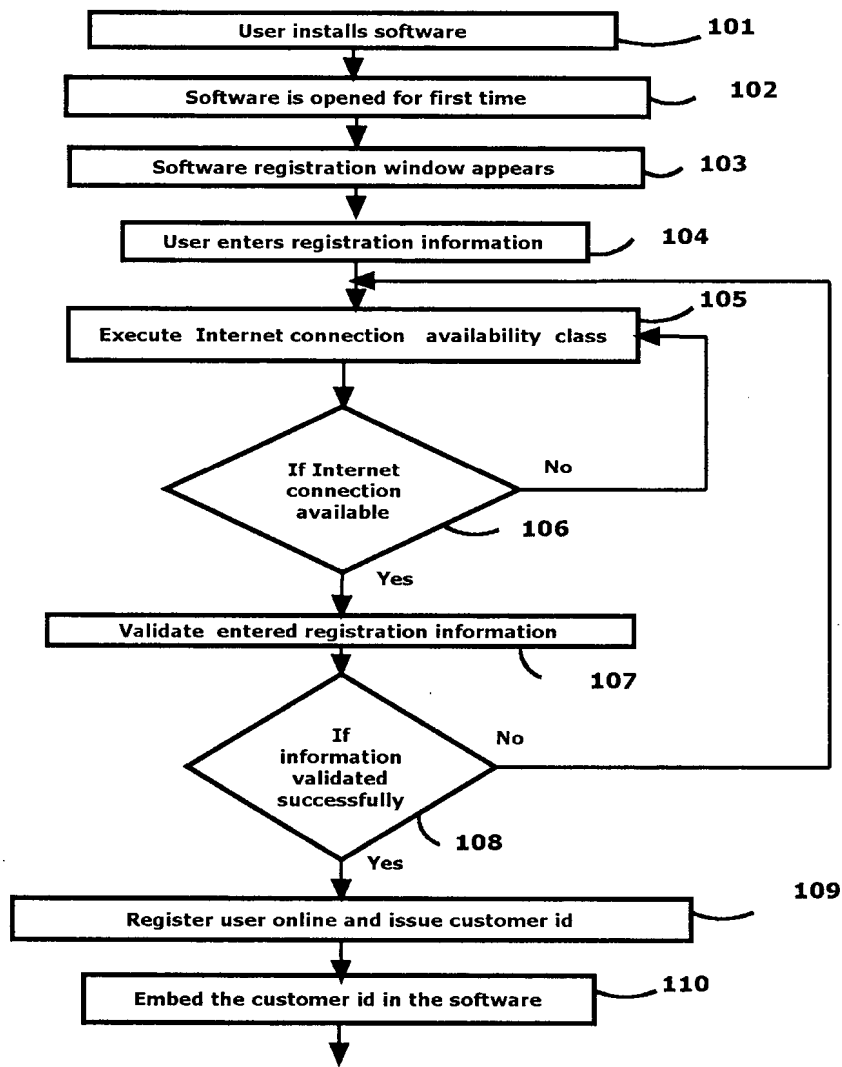


FIGURE 1a

Mandar Madhukar Patil

COMPLETE SPECIFICATION

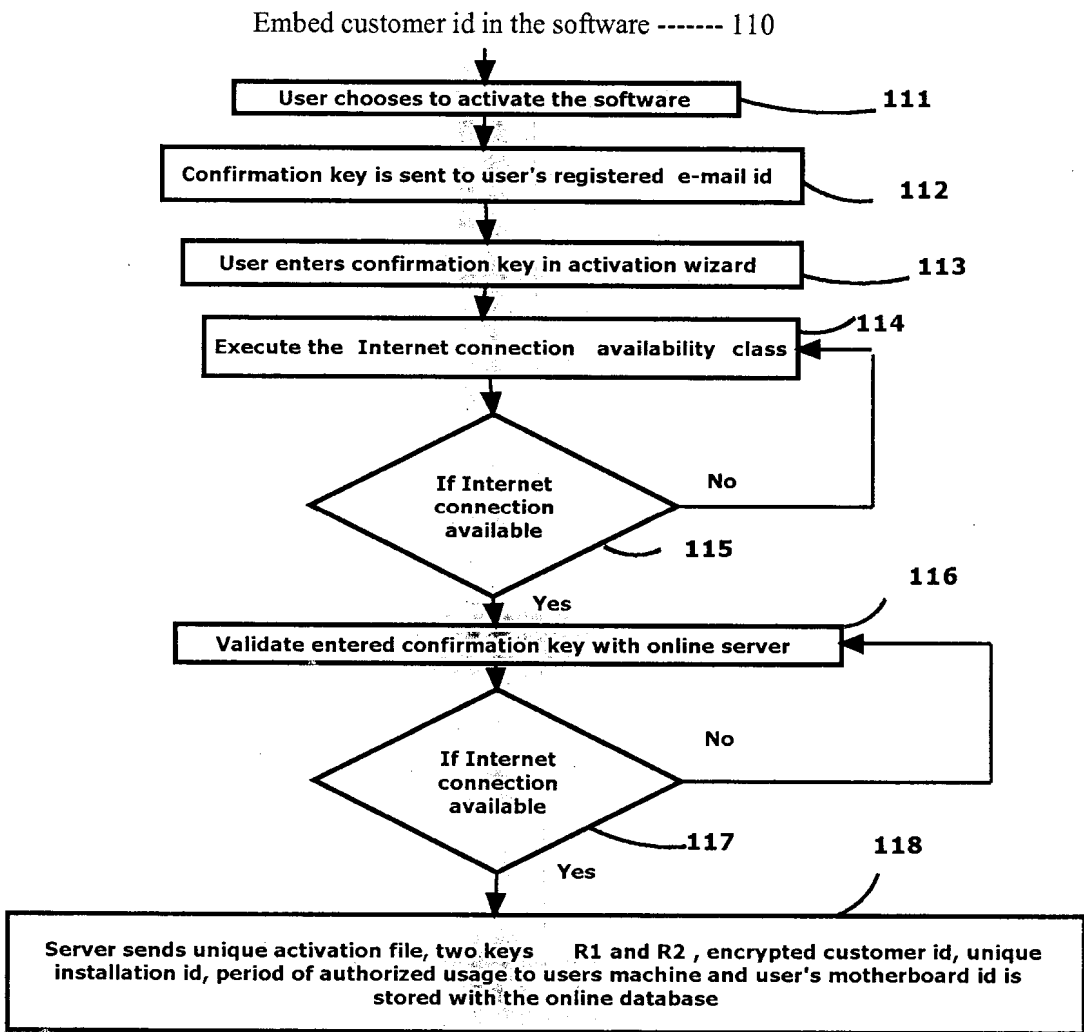


FIGURE 1b

Mandar Madhukar Patil

COMPLETE SPECIFICATION

Figure :2 Sharing of data via online method

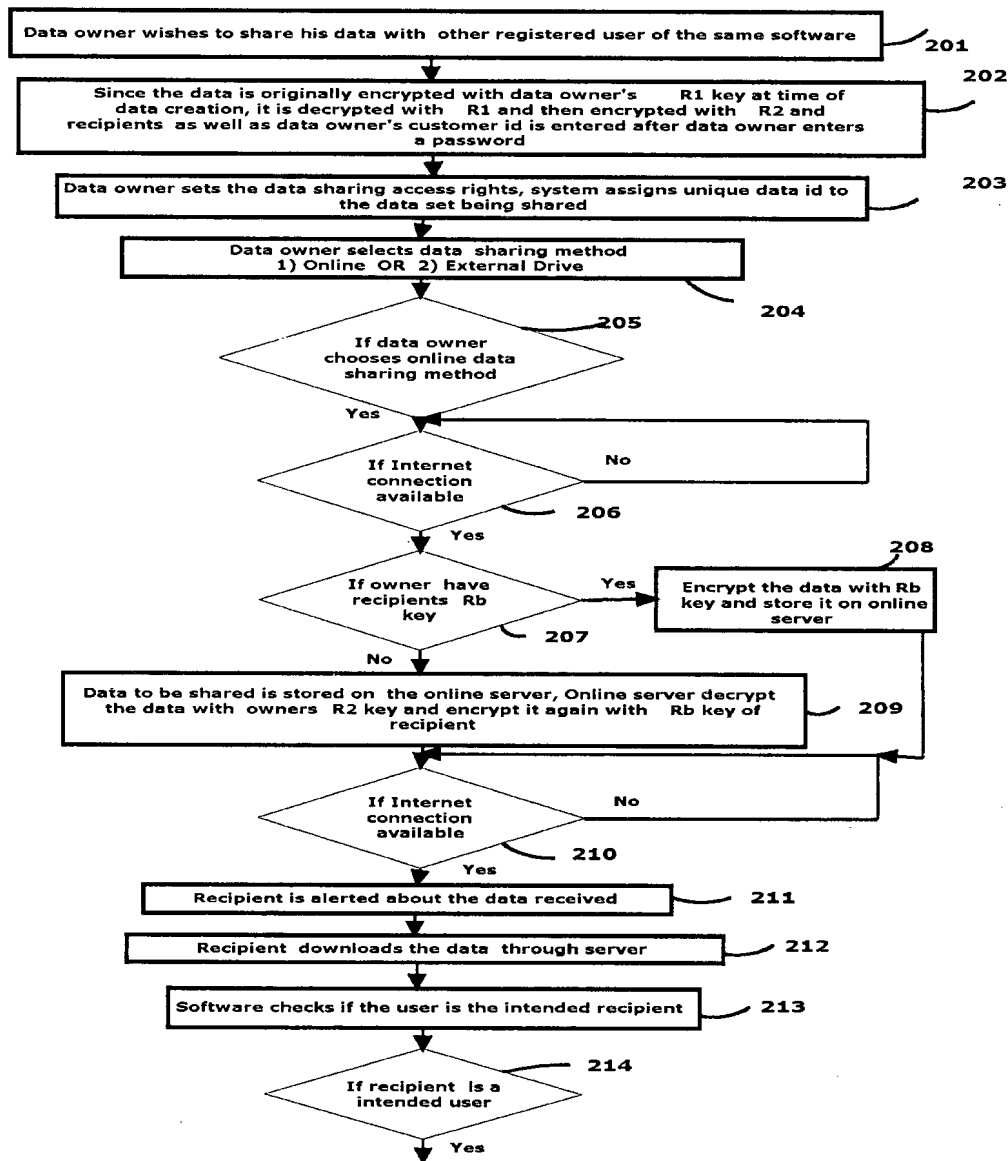


FIGURE 2a

Mandar Madhukar Patil

COMPLETE SPECIFICATION

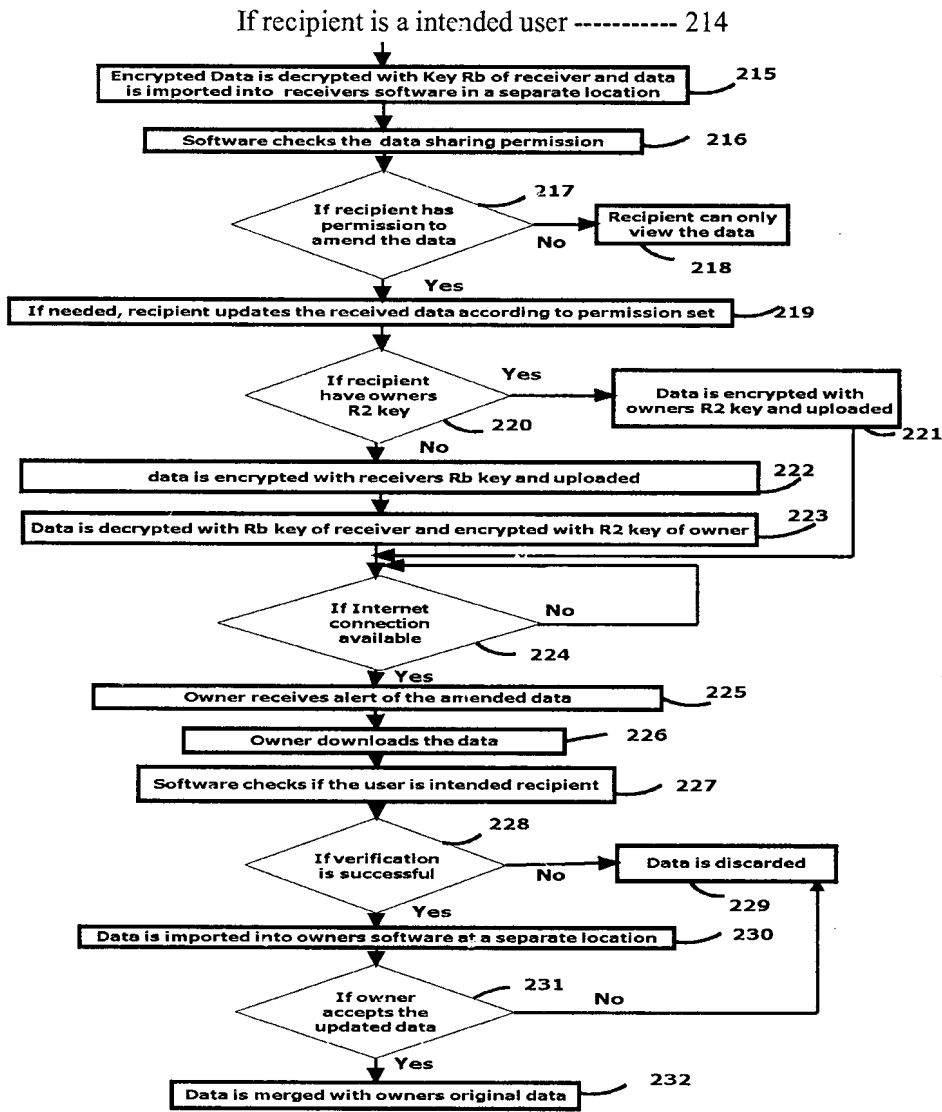


FIGURE 2b

Mandar Madhukar Patil

COMPLETE SPECIFICATION

Figure :3 Sharing of data via external drive

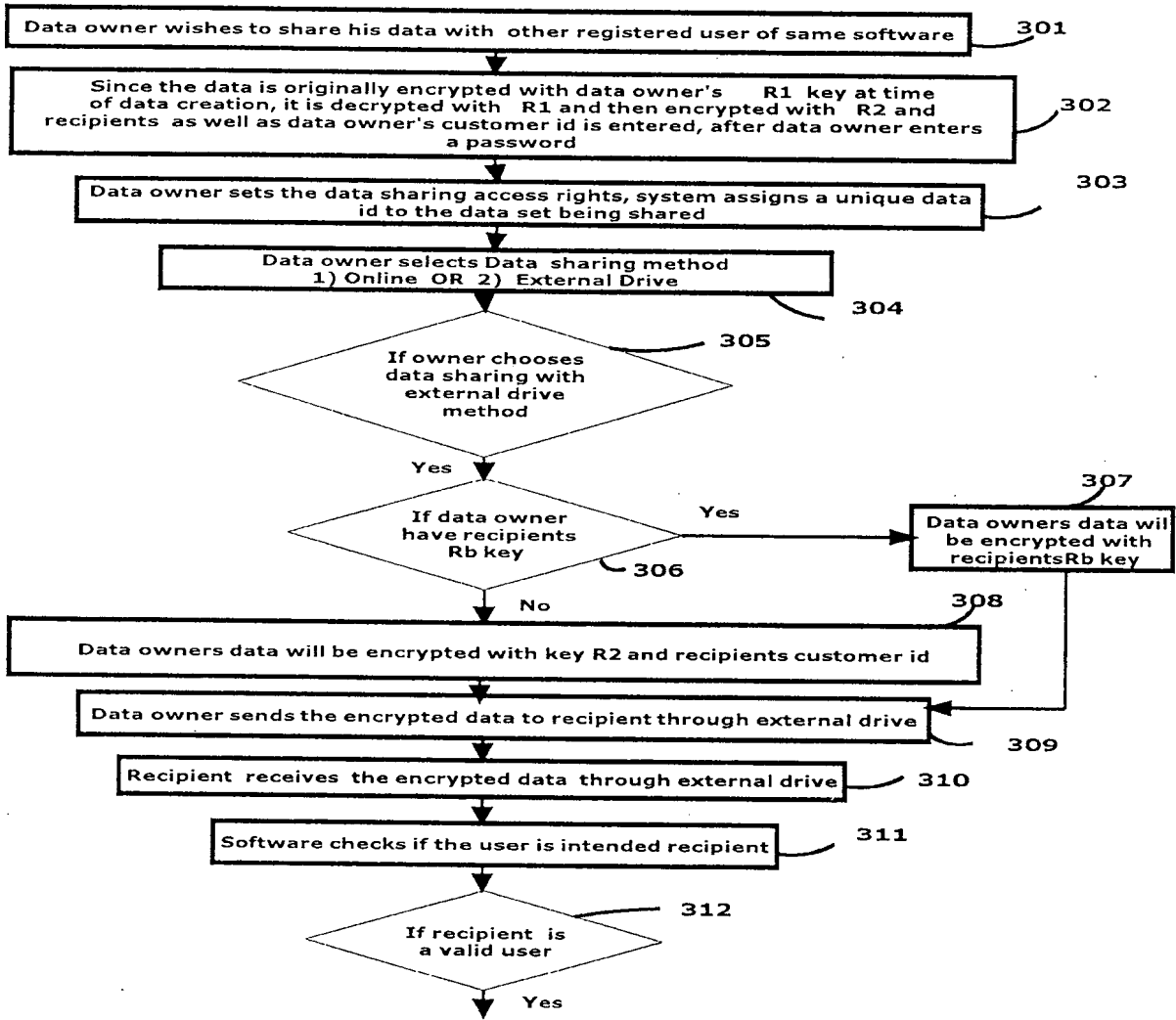


FIGURE 3a

Mandar Madhukar Patil

Name :Mandar Madhukar Patil
No. :1543/MUM/2010

No. of Sheets :11
Sheet No. :06

COMPLETE SPECIFICATION

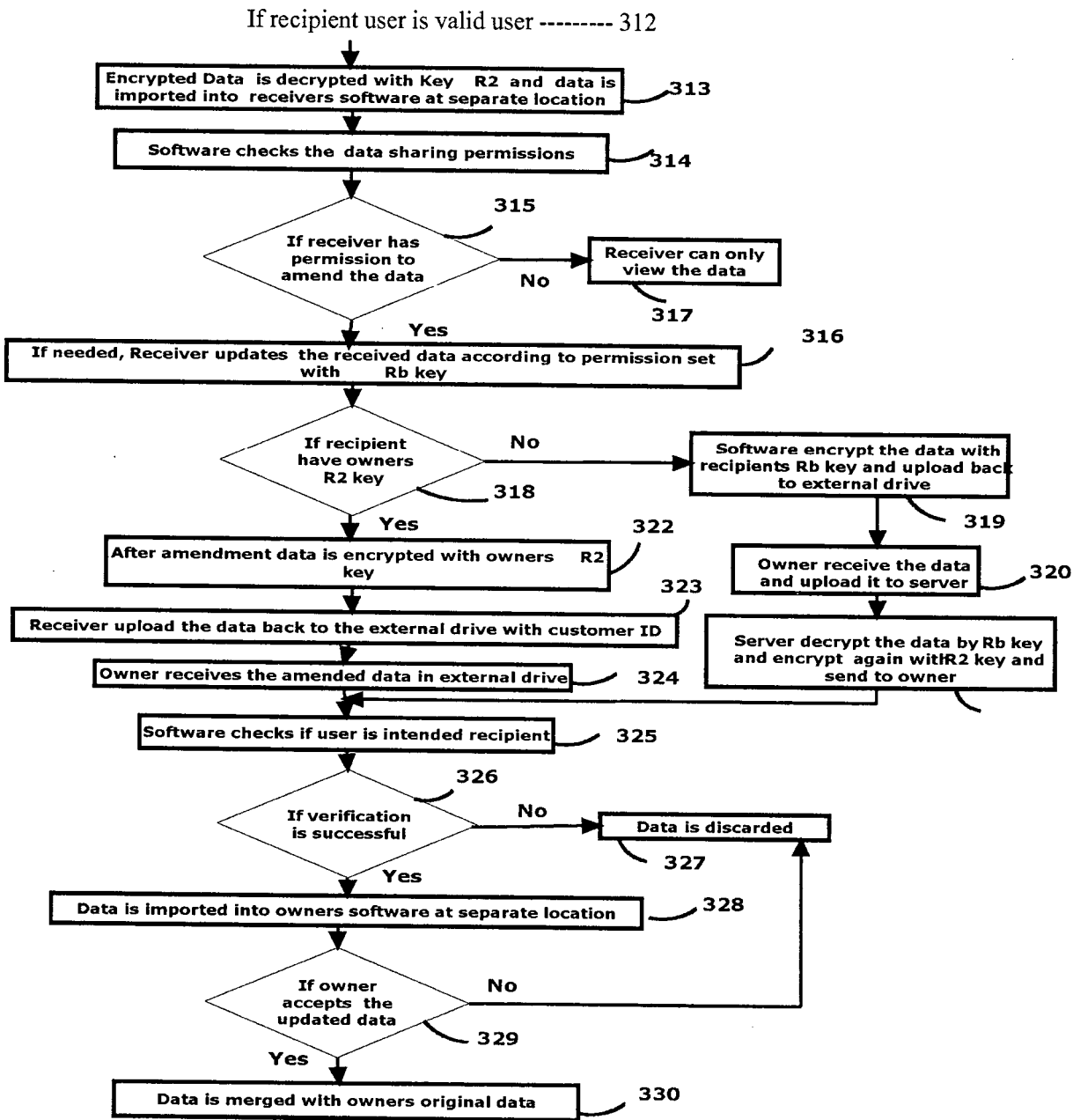


FIGURE 3b

Mandar Madhukar Patil

COMPLETE SPECIFICATION

Figure 4 - Software Reinstallation and Re-Assigning keys

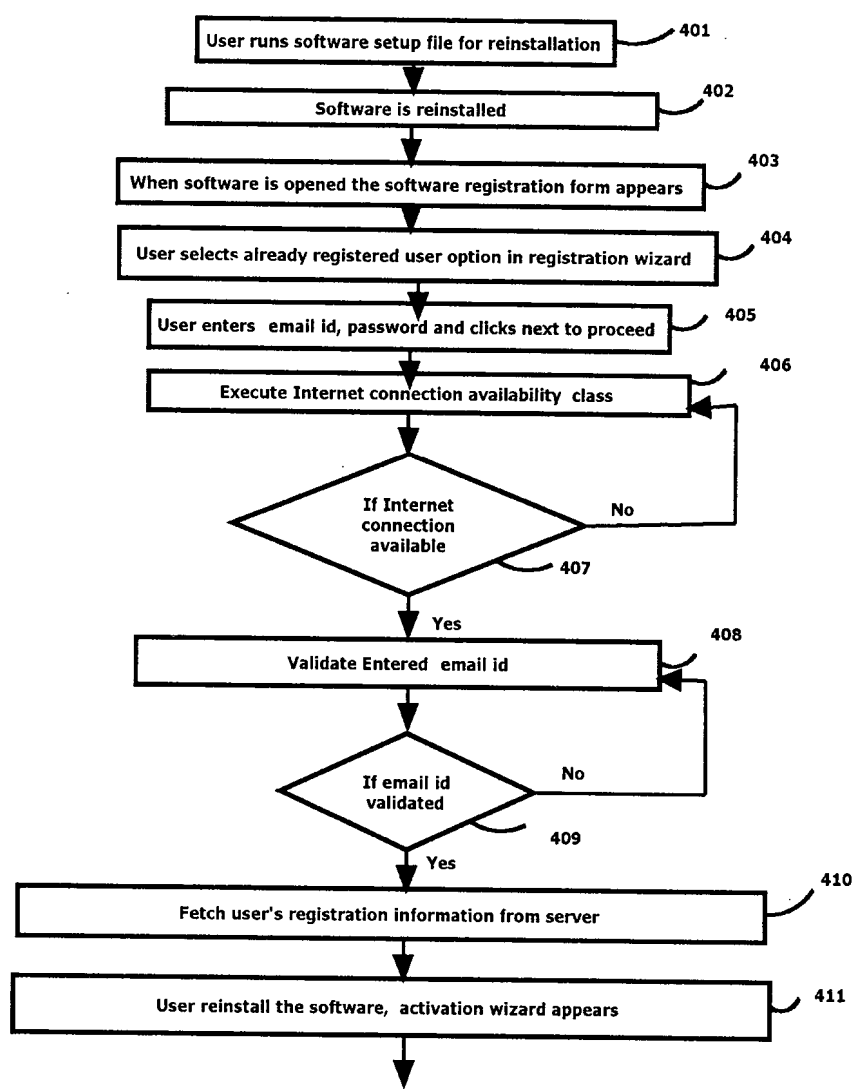


FIGURE 4a

Mandar Madhukar Patil

COMPLETE SPECIFICATION

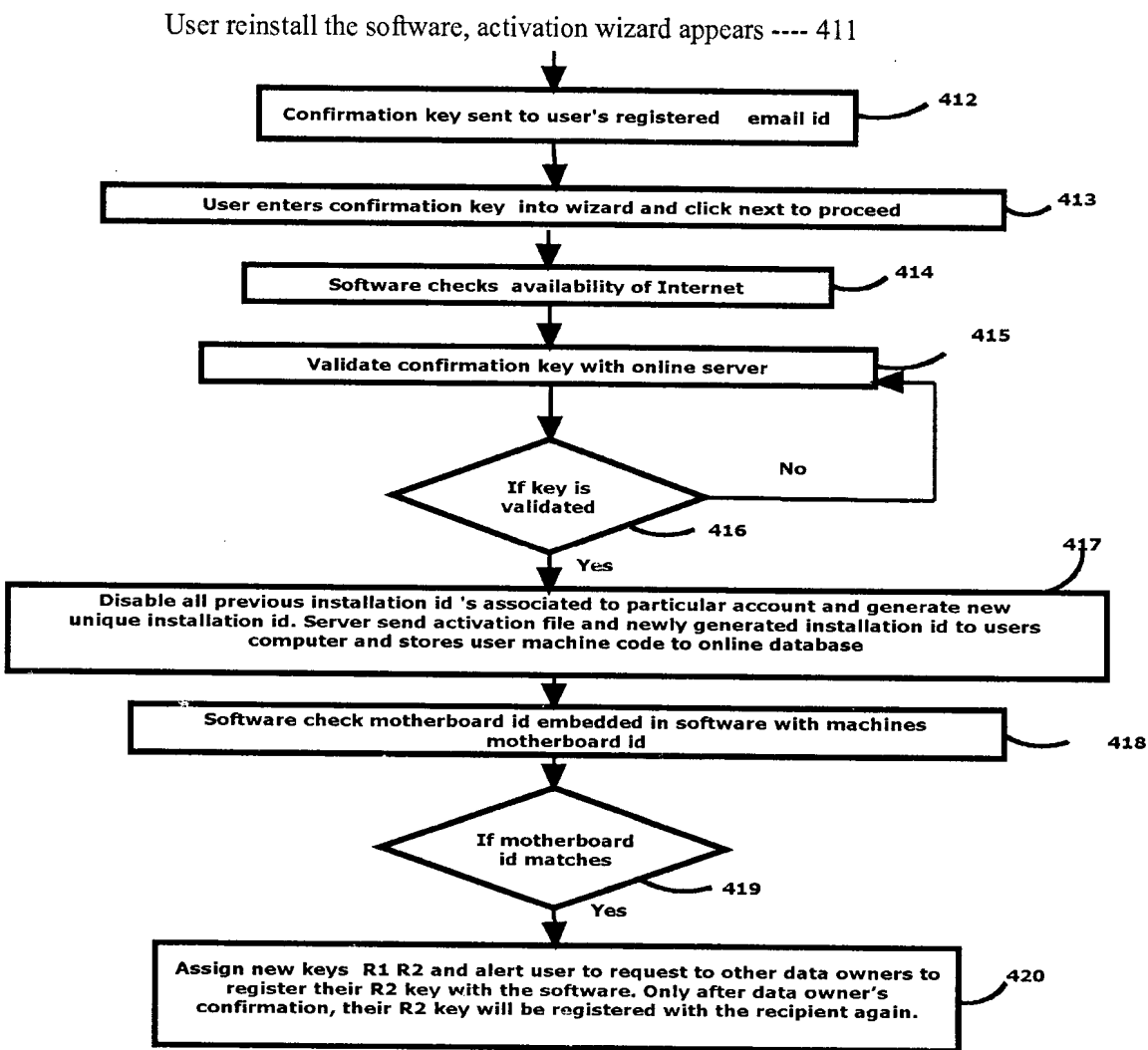


FIGURE 4b

Mandar Madhukar Patil

COMPLETE SPECIFICATION

Figure 5: Sharing of keys with various users

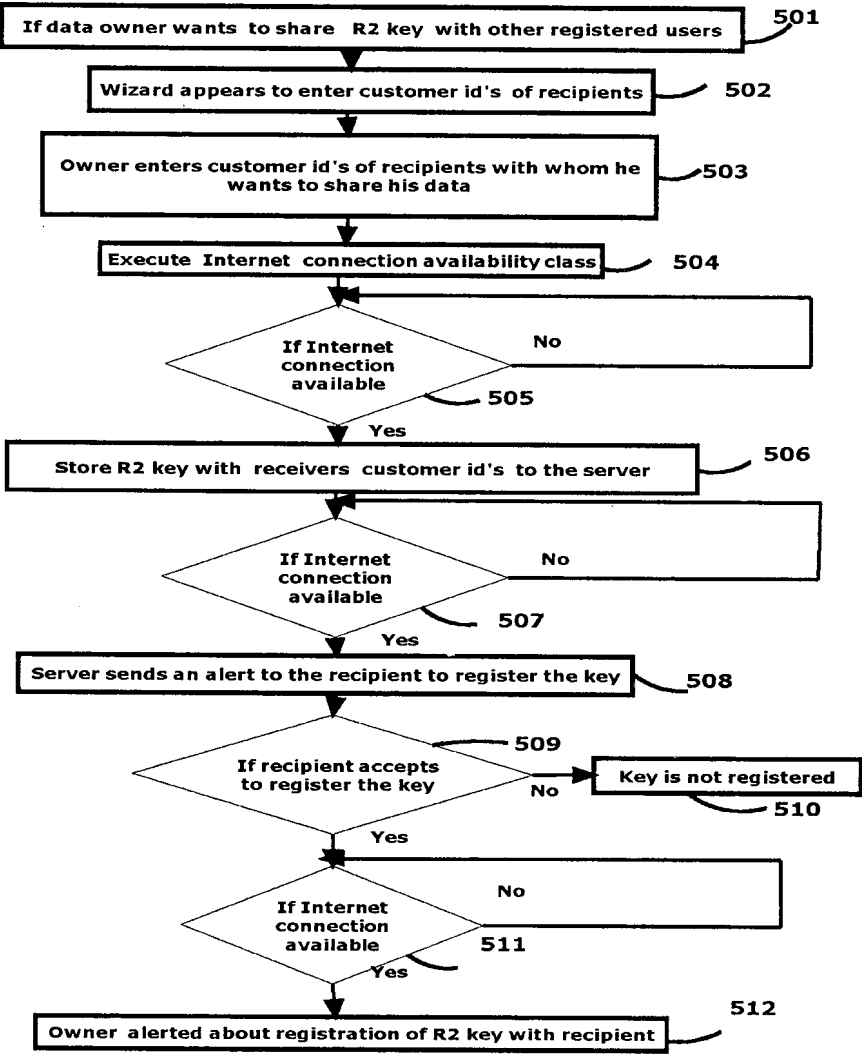


FIGURE 5

Mandar Madhukar Patil

COMPLETE SPECIFICATION

Figure 6:Revoking R2 key from recipients

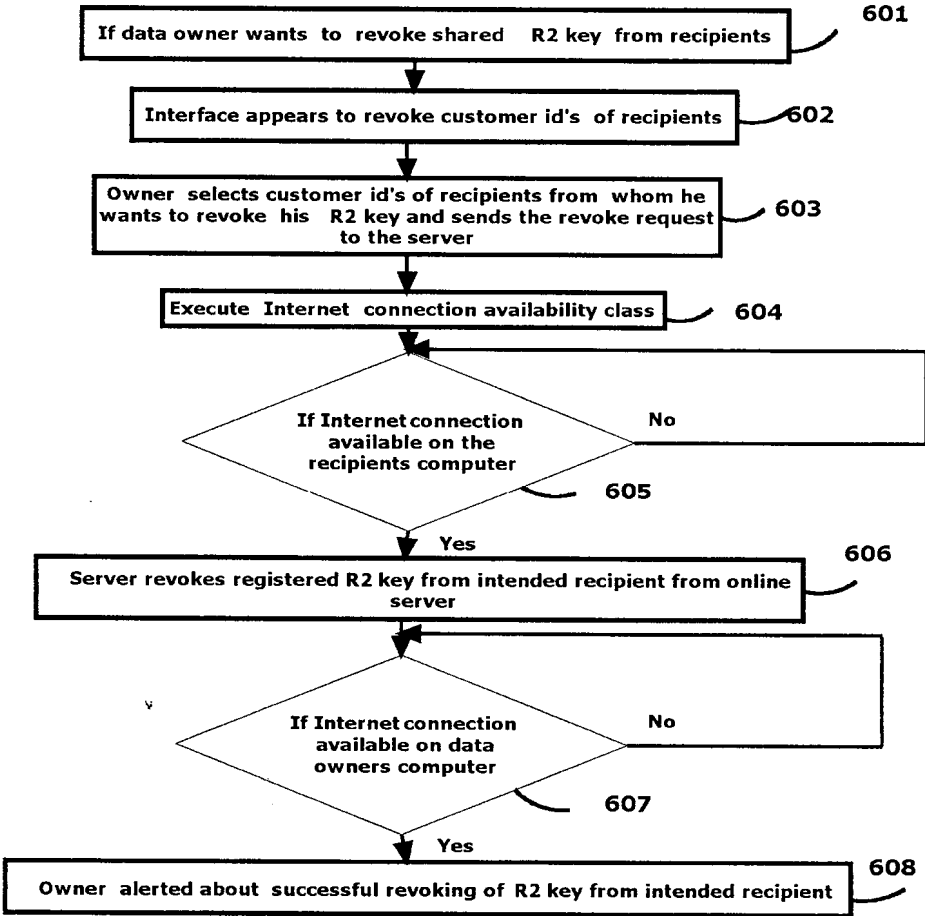


FIGURE 6

Mandar Madhukar Patil

COMPLETE SPECIFICATION

Figure 7: Authorization

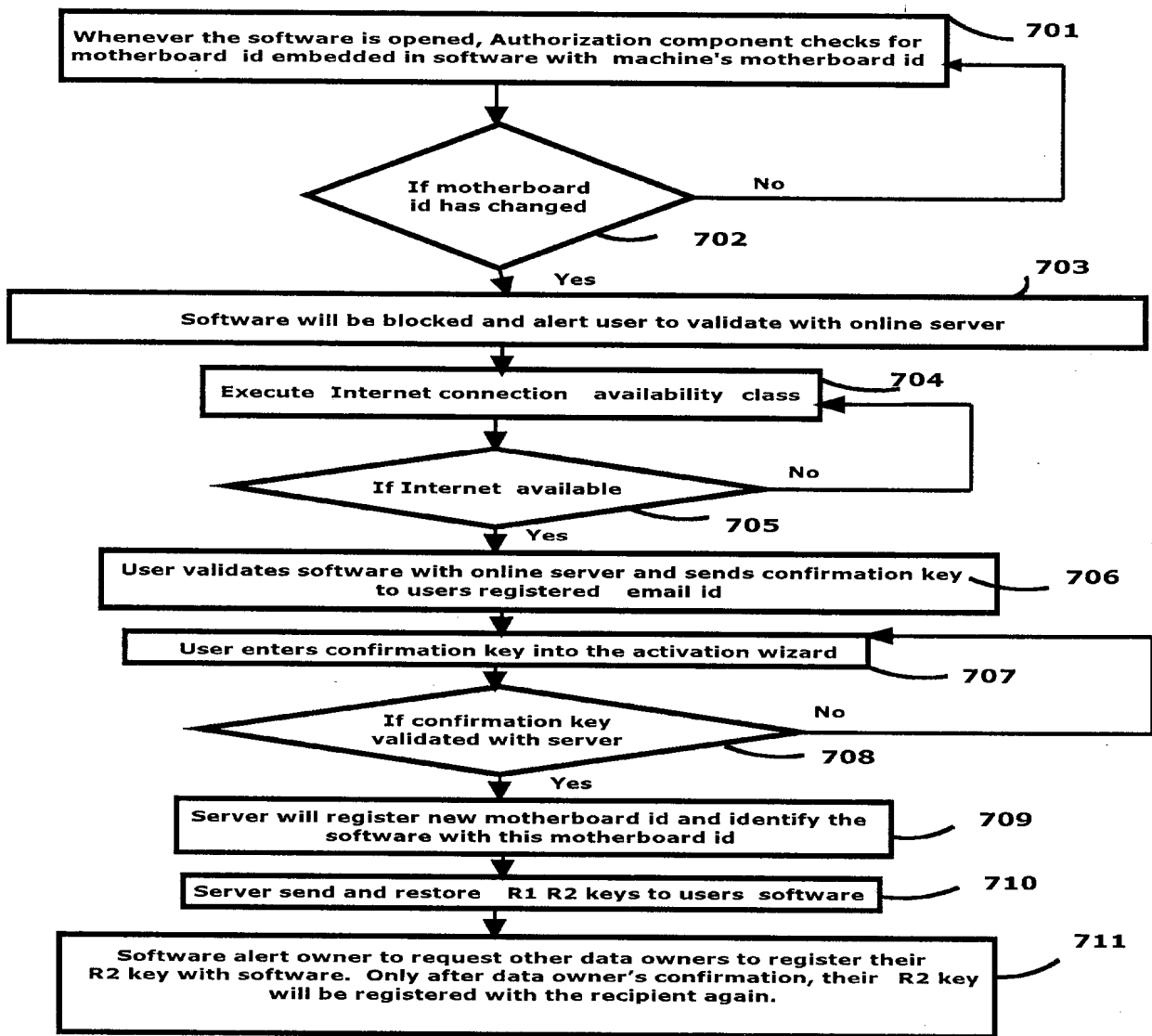


FIGURE 7

Mandar Madhukar Patil

**DOCUMENT MADE AVAILABLE UNDER THE
PATENT COOPERATION TREATY (PCT)**

International application number:	PCT/IB2010/052959
International filing date:	29 June 2010 (29.06.2010)
Document type:	Certified copy of priority document
Document details:	Country/Office: IN
	Number: 1543/MUM/2009
	Filing date: 01 July 2009 (01.07.2009)
Date of receipt at the International Bureau:	16 January 2012 (16.01.2012)

Remark: Priority document submitted or transmitted to the International Bureau but not in compliance with Rule 17.1(a),(b) or (b-bis)

16/10/52359 51

दूरभाष Tel 022-24137701

फैक्स Fax 022-24130387

Email mumbai-patent@nic.in
Website www.ipindia.nic.in



INTELLECTUAL
PROPERTY INDIA
बौद्धिक सम्पदा भारत
एकत्व / अभिकल्प / व्यापार चिन्ह /
भौगोलिक संकेत
PATENTS / DESIGNS /
TRADEMARKS /
GEOGRAPHICAL INDICATIONS



सत्यमेव जयते

भारत सरकार / GOVERNMENT OF INDIA
पेटेंट कार्यालय / THE PATENT OFFICE
बौद्धिक सम्पदा भवन, मुंबई - ४००३७
Boudhik Sampada Bhavan
Near Antop Hill Post Office, S.M. Road,
MUMBAI-400037

THE PATENTS ACT, 1970

IT IS HEREBY CERTIFIED THAT, the annex is a true copy of the Patent Application and Provisional Specification filed on 01/07/2009 in respect of Patent Application No.1543/MUM/2009 of Mr. Mandar M. Patil, Indian National at Pushkar, 269/1, E-5, Varsha Park, Baner, Near Green Park Hotel, Pune-411 045, Maharashtra, India.

This Certificate is issued under the powers vested in me under Section 147 (1) of the Patents Act, 1970.

Dated this 13th day of July, 2010.

Suneeta Betgeri

(DR. SUNEETA BETGERI)
EXAMINER OF PATENTS & DESIGNS
OFFICER IN CHARGE, RMID

1543/MUM/2009
11/7/09

EPD

FORM-1
THE PATENTS ACT, 1970
(39 of 1970)
APPLICATION FOR GRANT OF A PATENT
(See Section 5 (2), 7, 54 and 135 and rule 39)



I, Mr. Mandar M. Patil
Pushkar, 269/1, E-5, Varsha park
Baner, Near Green Park Hotel,
Pune 411045, Maharashtra, India.

1543/मुंबई/2009
CBR संख्या 6296 दि. 11/7/09
के तहत प्राप्त हुई।
रोकडिवा

An Indian national

ORIGINAL

2. hereby declare -

(a) that I am in possession of an invention titled :

**"Method and apparatus for remotely controlling and monitoring the
data Produced on and by desktop software."**

(b) that the Provisional Specification relating to this invention is filed with this application.

(c) that there is no lawful ground of objection to the grant of a patent to me

3. Further declare that the inventor for the said invention is :-

I, Mr. Mandar M. Patil
Pushkar, 269/1, E-5, Varsha park
Baner, Near Green Park Hotel,
Pune 411045, Maharashtra, India.

4. I claim the priority from the Application(s) filed in Nil convention countries, particulars of which are as follows:

- | | | |
|-----------------------------|---|----------------|
| (a) Name of the country | : | |
| (b) Application No. | : | |
| (c) Date of Application | : | |
| (d) Applicant in convention | : | NOT APPLICABLE |

1543 | मुंबई | 2009
MUM. 1 JUL 2009

53

Country.
(e) Title of the invention in the :
Convention country.

5. I state that the said invention is an improvement in or modification of the invention, the particulars of which are as follows and of which we are the applicant / patentee :

- (a) Application No. : N.A.
or Patent No.
(b) Date of Application or : N.A.
date of patent.

6. I state that the application is divided out of our application, that the particulars of which are given below and pray that this application deemed to have been filed on N.A. under Section 16 of the Act.

- (a) Application number including published : N.A.
Serial number, if any.
(b) Date of filing of Provisional Specification : N.A.
and/or Complete Specification.

And

7 That I am the assignee or legal representative/s of the true and first inventor/s.

NOT APPLICABLE

8. That my address for service in India is as follows:-

M/s. Katariya & Associates.
2 Sharada Apartments
Opp. Gate No. 5 of Abhimanshree Society
Aundh, Pune 411 007, Maharashtra, India

9. Following declaration was given by the inventors or applicants in the convention country:

I am the true and first inventor for this invention or the applicant in the convention country declare that the applicant herein is my assignee:

NOT APPLICABLE

10. That to the best of my knowledge, information and belief the facts and matters stated herein are correct and that there is no lawful ground of objection to the grant of patent to me on this application.

21 JUL 2009

54

11. Following are the attachment with the application:

- (a) Provisional Specification (2 copies)
- (b) Application fee Rs.1,000/- in cash/cheque no:
Dt.
- (c) Form 1, 2, and 3 duly signed.

I request that a patent may be granted to me for the said invention.

Dated this 1st July, 2009



(Mr. Mandar M. Patil)

To
The Controller of Patents,
PATENT OFFICE BR.,
MUMBAI-400 037

1-1 JUL 2009



FORM - 2

THE PATENTS ACT, 1970

(39 of 1970)

PROVISIONAL SPECIFICATION

(Section 10, Rule 13)

ORIGINAL

**“Method and apparatus for remotely controlling and monitoring the
data Produced on and by desktop software.”**

I, Mr. Mandar Madhukar Patil

Pushkar, 269/1, E-5, Varsha Park

Baner, Near Green Park Hotel.

Pune 411045, Maharashtra, India.

The following specification particularly describes the invention and the manner in
which it is to be performed: -

1543 | मुंबई | 2009
MUM.
JUL 2009

FIELD OF INVENTION

The invention relates to a method which restricts and controls data usage of user's software even though the user has shared data with others, using iso-data system.

The data which is created/generated using 'Iso data system' is Iso/unique/ exclusive for the same user/software by which it has been created. The data can be used by other users ONLY if the data-owner grants access/rights/permission for the same. The control of data still remains with the data-owner, even after sharing it with other users on their system/software.

More particularly, the invention relates to a method of securing control of users of data via restricting access rights and use of software data. This can be fully controlled by the original user. Data is the data which in terms of transactions user has made/created while using that software installed in that particular PC.

Even more particularly the invention relates to a method wherein data of the software can be used only by the software /system which has created it. No other user can use the original data of the software without the software owner's permission. Data also can be used restrictively/attributes which can be set by the original user like viewing, amending and saving. Registration of the software is in the vendor's online database is mandatory for usage of the iso-data system since this feature can be used by only registered, paid users of the same software . The registration system of the software and the iso-data system go hand in hand for data security. The software data can be shared by CD, pen drive or uploading data online. In this process the IR server will manage the rights and data sharing attributes of the data set by the original software user.

BACKGROUND OF THE INVENTION:

Since the early days of writing, heads of state and military commanders understood that it was necessary to provide some mechanism to protect the confidentiality of written correspondence and to have some means of detecting tampering.

Julius Caesar is credited with the invention of the Caesar cipher c50 B.C., which was created in order to prevent his secret messages from being read should a message fall into the wrong hands.

World War II brought about many advancements in information security and mark the beginning of the professional field of information security.

The end of the 20th century and early years of the 21st century saw rapid advancements in telecommunications, computing hardware and software, and data encryption. The availability of smaller, more powerful and less expensive computing equipment made electronic data processing within the reach of small business and the home user. These computers quickly became interconnected through a network generically called the Internet or World Wide Web.

The rapid growth and widespread use of electronic data processing and electronic business conducted through the Internet, along with numerous occurrences of international terrorism, fueled the need for better methods of protecting the computers and the information they store, process and transmit. The academic disciplines of computer security, information security and information assurance emerged along with numerous professional organizations - all sharing the common goals of ensuring the security and reliability of information systems.

Governments, military, corporates, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers,

products, research, and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers.

Should confidential information about a businesses customers or finances or new product line fall into the hands of a competitor, such a breach of security could lead to lost business, law suits or even bankruptcy of the business. Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement.

For the individual, information security has a significant effect on privacy, which is viewed very differently in different cultures.

The field of information security has grown and evolved significantly in recent years. As a career choice there are many ways of gaining entry into the field. It offers many areas for specialization including, securing network(s) and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning and digital forensics science, to name a few.

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them.

These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms.

41 JUL 2009

Information Rights Management (IRM) technology in Microsoft® Office 2003 helps to give organizations greater control of their sensitive information. IRM is a persistent file-level technology from Microsoft that allows the user to specify permission for who can access and use documents or e-mail messages, and it helps to prevent sensitive information from being printed, forwarded, or copied by unauthorized individuals. If permission for a document or message is restricted by using this technology, the usage restrictions travel with the document or e-mail message as part of the contents of the file.

Introduction

IRM extends a Windows® platform technology called Windows Rights Management. Rights Management is a policy enforcement technology that is utilized by applications to help safeguard confidential and sensitive enterprise information — no matter where it goes. Responding to customer demand for improved content protection, Microsoft designed Rights Management as an extensible platform, capable of integration into third-party applications in addition to Office 2003 applications.

IRM is information protection technology, not network security technology, that allows documents to be shared and sent in e-mail messages while helping maintain control over who can view or edit the documents. If a document or e-mail message is protected with this technology, the access and usage restrictions are enforced no matter where the information goes, even if the file is sent outside the firewall. Because IRM protection goes with the file, usage restrictions are enforced persistently.

IRM support in Office 2003 helps organizations address two fundamental needs:

* Restricted permission for sensitive information - Most corporations today rely on firewalls, logon security-related measures, and other network technologies in an effort to help protect their sensitive intellectual property. The fundamental limitation of these technologies is that, once legitimate users have access to the information, they can share

it with unauthorized people, potentially breaching security policies. IRM helps prevent the sensitive information itself from unauthorized access and reuse.

* Information privacy, control, and integrity - Information workers often deal with confidential or sensitive information, relying on the discretion of others to keep sensitive materials in-house. IRM eliminates any temptation to forward, copy, or print confidential information by helping to disable those functions in documents and messages with restricted permission.

For information technology (IT) managers, IRM helps enable the enforcement of existing corporate policies regarding document confidentiality, workflow, and e-mail retention. For CEOs and security officers, it significantly reduces the risk of having company information in the hands of the wrong people, whether by accident, thoughtlessness, or through malicious intent.

By using IRM technology, companies can create permission policies that appear in Office 2003 applications. For example, a company might define a policy called "Company Confidential," which specifies that documents or e-mail messages using that policy can be opened only by users inside the company domain. There is no limit to the number of policies that can be created.

User workflow

IRM protection is designed to be easy to use and transparent to users. To help protect Office 2003 documents, users follow the same logical workflow they already use with digital information. The process for using IRM consists of three basic steps:

1. Creation - An author creates content in an Office 2003 application, clicks the Permission toolbar button, and enters the names of the individuals or groups who can have access, and whether they can edit, print, or only view the content. Behind the scenes, the application works with the RMS server to apply rights to the file.

2. Distribution - The author distributes the file, either by attaching it to an e-mail message, posting it to a shared folder, or distributing it on a disk. Users do not have to change the manner in which they share information to safeguard their information because IRM protection is at the file level.

3. Consumption - A recipient opens the document or file as usual. Behind the scenes, the application communicates with the RMS server to determine if the recipient has been given rights to access the file. RMS validates the user and issues a use license. The application renders the file and enforces the rights.

Rights Management Add-on for Microsoft Internet Explorer

Because permissions are granted at the application level, Office documents with restricted permission can be opened only by applications included in Office 2003 or the 2007 Microsoft Office system. However, the Rights Management Add-on for Internet Explorer allows users without Office 2003 to read content with restricted permission. The add-on plays an important role in communication with business partners, as companies choose to migrate to Office 2003 on their own time frames. With the add-on, companies that want to take advantage of IRM to create protected content can move to Office 2003 knowing that documents are still accessible to users without Office 2003. Note that the add-on can only open RM-protected documents that include an HTML representation of their contents.

Configuration

There are two ways to enable IRM functionality in Office 2003:

- * Microsoft Windows Rights Management Services for Windows Server® 2003

- * Microsoft IRM service

When enabled by an organization that uses Windows Rights Management Services (RMS) for Windows Server 2003, users of Office 2003 can easily take advantage of IRM functionality. A simple user interface based on customizable permission policies

62

(available from the File menu) makes IRM convenient and approachable. Integration with the Active Directory® directory service provides a level of convenience not possible with document-specific passwords. In addition, the Rights Management Add-on for Internet Explorer allows users of Windows — if they have the proper permission — to read e-mail messages and some documents with restricted permission whether or not they have Office 2003. For more information about Windows RMS, including licensing and pricing information, see the Windows Rights Management documentation on the Windows Server 2003 Web site.

For home users and for organizations that do not host their own Windows RMS on Windows Server 2003, users can share protected documents and e-mail messages by using Windows Live ID as the authentication mechanism instead of Active Directory. Windows Live ID accounts can be used when assigning permissions to the various users who need access to the contents of the file. However, use of Windows Live ID accounts for RMS authentication does not allow for groups of users to gain access to a file. Each user must specifically be granted permission to the file. In addition, each client workstation must have access to the Internet to access Windows Live ID servers. Note that users of the Windows Live ID service cannot create custom rights templates, such as the "Company Confidential" template described earlier. For more information about the Microsoft IRM service, see the Windows Rights Management documentation on the Windows Server 2003 Web site.

For the sake of discussing the full potential of IRM, this article assumes use of RMS within an organization.

Usage and enforcement of permissions in Office 2003

In Microsoft Office Outlook® 2003, IRM can be used to prevent forwarding, copying, editing, or printing e-mail messages. Protected messages are automatically encrypted during transit, and when rights are assigned to the message by the sender, Office Outlook 2003 disables the restricted commands. Office 2003 documents attached to protected messages are also protected automatically.

If a protected document is forwarded to unauthorized recipients, those recipients cannot view the contents of the document; if they attempt to open the document, they receive a message explaining that the document is rights-protected. The document owner has the option of providing an e-mail address for unauthorized recipients to request rights to access the document.

Note. The ability to create content or e-mail messages with restricted permission by using IRM is available only with the Microsoft Office Professional Edition 2003 version of the following applications — Office Word 2003, Office Excel 2003, Office PowerPoint 2003, and Office Outlook 2003. IRM is also available in the stand-alone versions of those applications.

Permission levels

Office 2003 bases all of its permission enforcement on the rights defined in the Windows RMS for Windows Server 2003 and a set of custom settings in the Office 2003 applications. The levels of permission are:

* Full Control - Gives the user every right subsequently listed, and the right to make changes to the permissions associated with the content. Expiration does not apply to users with Full Control.

* View - Allows the user to open and view IRM content. This maps to read access in the Office user interface.

* Edit - Allows the user to open, view, and edit the IRM content.

* Save - Allows the user to save the file.

* Extract - Allows the user to make a copy of any portion of the file and paste it into the work area of another application.

* Export - Allows the user to save the content in another location or format that might or might not support IRM.

* Print - Allows the user to print the contents of the file.

* Allow Macros - Allows the user to run macros against the contents of the file.

* Forward - Allows e-mail recipients to forward an IRM e-mail message.

* Reply - Allows e-mail recipients to reply to an IRM e-mail message.

* Reply All - Allows e-mail recipients to reply to all users in the To: and Cc: lines of an IRM e-mail message.

* View Rights - Allows users to view the rights associated with the file. Office ignores this right.

A user can specify one of several predefined groups of rights when creating IRM content:

- * Read - Users with Read permission have only the View right.
- * Do Not Forward - In Outlook, the author of an IRM e-mail message can apply the Do Not Forward permission to the users in the To:, Cc:, and Bcc: lines. This permission includes the View, Reply, and Reply All rights.
- * Change - Users with Change permission have View, Edit, Extract, Export, and Save rights.

Additional permissions in Office documents

In addition to the permission levels described earlier, specific rights can be specified in the advanced user interface of Word, Excel, and PowerPoint. Outlook always enables messages to be viewed by a browser that supports Rights Management. The following options are available in the Permission dialog box for Word, Excel, and PowerPoint:

- * This document expires on - This option allows the author to specify a date after which the IRM content becomes unreadable for everyone but users with Full Control.
- * View content in trusted browsers - This option allows the author to specify whether or not users without Office 2003 can view the content by using the Rights Management Add-on for Internet Explorer.
- * Require a connection to verify a user's permission - This option gives the author the ability to force users to connect to the Windows Rights Management server every time content is opened. This is useful if permissions to a shared document change over time and the author wants to make sure every user is verified prior to opening the document.

Technical overview of RMS and IRM

On the server, Windows RMS handles the core licensing, computer activation, enrollment, and administrative functions. RMS relies on Active Directory and uses an SQL database, such as a Microsoft SQL Server® database, to store configuration data.

On the desktop, creating or viewing rights-protected content requires an RMS-enabled application, such as Office Outlook 2003. To create rights-protected Microsoft Office documents, workbooks, presentations, and e-mail messages, Office Professional Edition 2003 is required. Other Office 2003 Editions allow designated recipients to work with rights-protected documents (but not create content) if they have been given those rights by the author. The Rights Management Add-on for Internet Explorer allows designated users to view rights-protected information if they do not have an Office 2003 application.

Architecture

RMS is a managed Web service that leverages ASP.NET implementation, HTTP simple object access protocol (SOAP) request/response protocol, and Extensible Rights Markup Language (XrML) to enable organizations to create and deploy customized information protection solutions. With high scalability, flexible topologies, straightforward administration, and ease of use, RMS was developed to meet the needs of any organization interested in information protection.

The key to Windows RMS technology is persistent usage policies, also known as usage rights and conditions. Authors can establish persistent usage policies at the file level.

After the author applies those policies to a file, they remain with that file, even when the file travels outside the corporate network.

An RMS system achieves persistent policy enforcement by establishing the following elements:

- * **Trusted entities** - Organizations can specify the entities that are trusted participants in an RMS system. This includes individuals, groups of users, computers, and applications. By establishing trusted entities, an RMS system helps protect information by enabling access only to properly authenticated participants.

- * **Usage rights and conditions** - Organizations and individuals can assign usage rights and conditions that define how a specific trusted entity can use protected information. Examples of named rights are permission to view, copy, print, save, store, forward, and modify. Usage rights can also specify when those permissions expire, and what applications and entities are excluded from accessing the protected information.

- * **Encryption** - Encryption is the process by which data is locked with electronic keys. The RMS system encrypts information, making its access and use conditional on the successful authentication of the trusted entities and the enforcement of the specified usage policies. After the information is locked, only trusted entities that were granted usage rights under the specified conditions can unlock or decrypt the information and exercise the assigned usage rights.

RMS basics

Windows RMS technology, which includes both server and client components, provides the following capabilities:

- * Creating rights-protected files and containers - Users designated as trusted entities in an RMS system can create and manage protected files by using familiar authoring programs and tools that incorporate Windows RMS technology features. For example, by using familiar application toolbars, users can assign usage rights and conditions to information such as e-mail messages and documents. In addition, RMS-enabled applications can use centrally defined and officially authorized rights policy templates to help users efficiently apply a predefined set of organizational usage policies.

- * Licensing and distributing rights-protected information - XrML-based certificates issued by an RMS system identify trusted entities that can publish rights-protected information. Users designated as trusted entities in an RMS system can assign usage rights and conditions to information they want to protect. These usage policies specify who can access and use the information.

In a process that is transparent to users, the RMS system validates the trusted entities and issues the publishing licenses that contain the specified usage rights and conditions defined by the author of the information. The information is encrypted by using the electronic keys from the applications and from the XrML-based certificates of the trusted entities. After the information is locked by this mechanism, only the trusted entities specified in the publishing licenses can unlock and use that information. Users can then distribute the rights-protected information to others in their organization or to a trusted external user via e-mail, a file share on a server, or a disk.

- * Acquiring licenses to decrypt rights-protected information and enforcing usage policies - Users who are trusted entities can open rights-protected information by using trusted clients. These clients are RMS-enabled computers and applications that allow

users to view and interact with rights-protected information, enforcing usage policies. In a process that is transparent to the recipient, the RMS server, which has the public key that was used to encrypt the information, validates the recipient's credentials and then issues a use license that contains the usage rights and conditions that were specified in the publishing license. The information is decrypted by using the electronic keys from the use license and the XrML-based certificates of the trusted entities. The usage rights and conditions are then enforced by the RMS-enabled application. The usage rights and conditions are persistent and enforceable wherever the information goes.

OBJECTIVES OF THE INVENTION:

Observed that data is sensitive. Stealing it can cause problems like misuse. When data is made unusable for some other person, its security doesn't become a problem.

Current systems protect data but data itself is very fragile.

Accordingly, it is the object of the present invention to provide a foolproof protection of software user's data i.e. data of transactions in the software, via iso-data system by giving, sharing and access permission of the software data solely in the software owner's control. Even if the data accidentally reaches unauthorized access, it can't be opened.

SUMMARY OF THE INVENTION:

At the time of installation software is registered and after that a file is generated by the server and downloaded on the client PC. This file not be known to any user. Each user will have a unique key.

Every machine 2 types keys. One key is used to encrypt and decrypt the machine's own data. The second key is used to view the other machine's data, as per the privileges provided by the data owner. Both the Keys are provided by the Iso data System server and are unique.

To illustrate further, let's consider there are 2 computers: Computer1 and Computer2. Computer1 has 2 keys i.e. Key1 (access own data) and Key2 (access other system's data). Computer2 also uses two keys i.e. Key3 (access own data) and Key4 (access other system's data).

Key 1 is used to encrypt and decrypt computer1's own data. This key is sent by the Iso-data system and is unique in nature. If Computer1 wants to share some of its data with computer2, it needs to send a request to the Server along with the privileges. Let's consider Computer1 wants Computer2 to only 'view' some of its data. The Server will generate a Key4 along with the view privilege. Computer2 will only be able to de-crypt the data sent by Computer1 using the Key4.

Similarly, If computer2 wants to view its own data, make any changes or save it, it will use a key3 which is assigned by the Iso-data system server.

Data will be encrypted with a key (reg no+server gen random no) this key is unique for each computer. Decrypt will be done by same unique key so if that key is not there then it cannot be decrypted. During registration ra and r2 two keys are generated by the server.

Iso data system helps the software owner to protect his software data from unauthorized access. The software owner can share his software data with one or many registered paid users of the same software. The software owner can set restrictions on data usage by the recipient.

User, as per his wish can make some data as iso data. In iso data system the data is encrypted into such a format where only that particular user of the software which has created the data can use it. The data cannot be used by the same software with different registration number on a different user or different PC's. The data can be only used by the same unique user from the same PC. Other user using the same software but different registration number in other PC's cannot use the same data. Though an additional facility also can be given that with consent of both the software users the same data can be used. Both users must be registered paid users of the software to share the software data. This facility is not available for a trial period user.

- 71
1. In case user 1 who is a registered user of a software wants to share his software data with user 2 who is also a registered user of the same software, the following steps are to be followed.

Case 1: Sharing Data through online server

In this case the original user of the software data select the data that is to be shared and enters the customer id of the user 2 with whom he wants to share the software data.

- a. When data goes by a cd its decrypted and given. Reciever of data will upload data on server and get the data decrypted.
- b. The original user will upload this data onto the server. The data will be in uniquely iso encrypted, so that only the intended recipient can decrypt it. This data can be used with only the authentication of the server and stored in a location separate from original location.
- c. When the user 2 opens his software and if internet connection is available, an alert will be shown to him that data from a particular user is waiting to be downloaded. This alert will be shown to him only if the data sharing permissions are still active.
- d. The user 2 will download the data and import it into the software. The software will check if the customer id entered by the original user is matching with the user2's software. Only if the customer id's match the software will decrypt the data and allow the user2 to access this decrypted data.
- e. The data will behave only in the way the display conditions have been set by the original user. For eg.
 1. the data can be used for x number of days
 2. the data can be viewed for x number of hours

3. The data can be viewed x number of times
 4. data can or cannot be amended.
 5. data can or cannot be saved.
 6. Data sharing restriction is locked with user 1. e.g. data can be shared only with original user's permission and no other user can access it.
2. Amendment of data will be shown to user 1, only if user one accepts the amendment, the data will be imported and merged. Facility will be given to user 1 to merge the data that had amended by user 2. Accept the data.
 3. Incase user 1 has given user 2 access for amending data; This amended data will have to be uploaded to server by entering user 1's customer id. User 1 will then receive an alert about the amended data once internet connection is available on his PC.
 4. The data that is to be shared, amended is kept in a separate location from the original database of the software and does not interfere in any way with the original data/records of both users software.
 5. Original user of data will be displayed all amendments. Only if he accepts the amendments
 6. Software user can share the software data with more than one registered paid user of the same software.
 7. User 1 can still keep the original copy if he wants before amending user 2's data.
 8. Same procedure will be applied if user 1 wants to share data with user 2, user3, user4, user5...any number of users.

Below is explained the Re Installation of the software. When user wants to reinstall the software, a reinstallation wizard will open. This wizard will take the input of user's customer id and an email id. If the user wants to set 2 or more email id's he can do the same. Both these details will be registered with the software vendor's online web server. After this the server will send a string to the user's email id(s). This string will be

73

valid for a decided period time. The string is valid only for one particular transaction. The user has to type the string sent to his email id(s) into this reinstallation wizard. This information will be registered with the software vendor's online web server after the strings input will match the string with the online sever. Now the server will create the encryption and decryption keys and send it back to the user's software.

DESCRIPTION OF THE INVENTION:

Online registration and activation program is a byte code program written in Microsoft .NET programming language.

The description generally provides for methods for activation of the software through desktop and registration of user to the online server.

A method for registering a user for to the online server includes receiving an initial access to desktop software by a prospective user and determining whether the user has provided valid user identification information.

If User purchases software CD, that is the purchase of the software through the software vendor where user pay and purchase the software from software vendor else user can download the software from the software download link provided to the user from website. User installs the software to his computer through purchased CD or downloaded setup by invoking function. As user successfully installs the software user is ready to use the software and user clicks on the software exe for the first time to run the software. As user use the software for first time software registration form will appear to user to register and activate the user to online server from desktop software, registration form will be displayed to user through which user can enter his information to the provided interface and register himself to activate the software. User enters the drug license number into the interface provided to the user to register himself and proceed for

registration. The internet connection availability program check's for internet connection.

If internet connection is available drug license verifier verifies the integrity of the method associated with each loaded object, If the method is successfully verified is invoked to enter the detailed information of the shop like shopkeeper's name, address, phone number, email id. User enters the shop details into and submits to register himself to the server.

If user registered to online server successfully method is invoked to transfer the unique activation file, which contains the information like drug license number, customer address, software activation date and unique customer id into from online server to user's local machine.

As user 1 who is a registered user of a software wants to share his software data with user 2 who is also a registered user of the same software, User 1 opens iso data upload wizard, user 1 uploads the data he want to share with user 2, uploaded data will be save on the server in encrypted format. User 2 get the alert i.e data is uploaded please use the data, as user 2 tries to download the encrypted data from server the software checks the validity of the user 2 by cross checking the customer Id with the uploaded customer Id. User 2 amend the data and upload back to the server by the method. User 1 gets the alert to download the amended data, as user tries to download the data user 1 get the check list of the changed data where he can select the changes which he want to download. And on that basis user 1 get the data from user 2.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference ISODATA	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/IB 10/52959	International filing date (<i>day/month/year</i>) 29 June 2010 (29.06.2010)	(Earliest) Priority Date (<i>day/month/year</i>) 01 July 2009 (01.07.2009)
Applicant PATIL, MANDAR		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

a. With regard to the language, the international search was carried out on the basis of:

- ☒ the international application in the language in which it was filed.
☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

b. ☐ This international search report has been established taking into account the rectification of an obvious mistake authorized by or notified to this Authority under Rule 91 (Rule 43.6bis(a)).

c. ☐ With regard to any nucleotide and/or amino acid sequence disclosed in the international application, see Box No. I.

2. ☐ Certain claims were found unsearchable (see Box No. II).

3. ☐ Unity of invention is lacking (see Box No. III).

4. With regard to the title,

- ☒ the text is approved as submitted by the applicant.
☐ the text has been established by this Authority to read as follows:

5. With regard to the abstract,

- ☒ the text is approved as submitted by the applicant.
☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the drawings,

- a. the figure of the drawings to be published with the abstract is Figure No. _____
☐ as suggested by the applicant.
☐ as selected by this Authority, because the applicant failed to suggest a figure.
☐ as selected by this Authority, because this figure better characterizes the invention.
- b. ☒ none of the figures is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 10/52959

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06F 21/00 (2010.01)

USPC - 705/51

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
USPC: 705/51Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 707/999.009; 707/999.104; 707/999.107; 707/E17.044 (keyword limited; terms below)Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PubWEST (USPT, PGPB, EPAB, JPAB); GoogleScholar

Search Terms Used: sharing updating sending transmission delivery controlling management usage preventing authorized unauthorized authentication ISO creation generating recipient owner sender selecting choosing chosen identifying ID identification tag access

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2009/010060 A1 (Livnat et al.) 16 April 2009 (16.04.2009), entire document, especially: para [0002], [0003], [0004], [0006], [0008], [0011], [0012], [0014], [0015], [0016], [0018], [0019], [0020], [0025], [0027], [0029], [0031], [0035], [0056], [0057], [0059], [0062], [0072], [0080], [0082], [0085], [0090], [0095], [0096], [0098], [0100], [0111], [0114], [0107], [0108], [0111], [0128], [0144], [0147], [0153], [0157], [0169], [0175], [0182], [0185], [0193], [0203], [0205], [0206], [0207], [0209], [0213], [0225], [0232], [0245], [0248], [0250], [0254], [0256], [0260], [0269], Abstract, Fig. 1	1-25
Y	US 2008/0147558 A1 (Kraus) 19 June 2008 (19.06.2008), entire document, especially: para [0025], [0045], [0046], [0060], [0066]	1-25

☐ Further documents are listed in the continuation of Box C.

* Special categories of cited documents:	
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"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
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
08 December 2010 (08.12.2010)

Date of mailing of the international search report

27 DEC 2010

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450
Facsimile No. 571-273-3201Authorized officer:
Lee W. YoungPCT Helpdesk: 571-272-4300
PCT OSP: 571-272-7774

27

PATENT COOPERATION TREATY

From the **Asig 34005** ^① ICG AUTHORITY

PCT

NOTIFICATION OF RECEIPT
OF SEARCH COPY

(PCT Rule 25.1)

To:
MANDAR PATIL
SURVEY NUMBER 118 TO 124, PLOT NUMBER
85, NATIONAL
SOCIETY, AUNDH, PUNE 411007
MAHARASHTRA, 411007
INDIA

PALM Tracking Number = 51090481

Date of mailing
(day/month/year) 24 Aug 2010

Applicant's or agent's file reference ISODATA		IMPORTANT NOTIFICATION
International application No. PCT/IB10/52959	International filing date (day/month/year) 29 Jun 2010	Priority date (day/month/year) 01 Jul 2009
Applicant PATIL, MANDAR		

1. Where the International Searching Authority and the receiving Office are not the same Office:
The applicant is hereby notified that the search copy of the international application was received by this International Searching Authority on the date indicated below. 18 AUGUST 2010

Where the International Searching Authority and the receiving Office are the same Office:
The applicant is hereby notified that the search copy of the international application was received on the date indicated below.

(date of receipt)

2. ☐ The search copy was accompanied by a nucleotide and/or amino acid sequence listing in electronic form.

3. ☐ The search copy contained a nucleotide and/or amino acid sequence listing in electronic form.

4. Time limit for establishment of international search report and written opinion of the International Searching Authority
The applicant is informed that the time limit for establishing the international search report and the written opinion of the International Searching Authority is three months from the date of receipt indicated above or nine months from the priority date, whichever time limit expires later (Rules 42.1 and 43bis.1(a)).

A copy of this Notification has been sent to the International Bureau and, where the first sentence of paragraph 1 applies, to the receiving Office.

Name and mailing address of the ISA/ Mail Stop PCT, Commissioner for Patents P.O. Box 1450, Alexandria, VA 22313-1450 Facsimile No. 571-273-3201	Authorized officer Susan Nguyen Telephone No.
---	---

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: MANDAR PATIL
SURVEY NUMBER 118 TO 124, PLOT
NUMBER 85, NATIONALSOCIETY,
AUNDH, PUNE 411007
MAHARASHTRA, INDIA.
411007 PUNE
INDIA

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Date of mailing
(day/month/year)

27 DEC 2010

Applicant's or agent's file reference
ISODATA

FOR FURTHER ACTION

See paragraph 2 below

International application No.

PCT/IB 10/52959

International filing date (day/month/year)

29 June 2010 (29.06.2010)

Priority date (day/month/year)

01 July 2009 (01.07.2009)

International Patent Classification (IPC) or both national classification and IPC

IPC(8) - G06F 21/00 (2010.01)

USPC - 705/51

Applicant PATIL, MANDAR

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450
Facsimile No. 571-273-3201

Date of completion of this opinion

08 December 2010 (08.12.2010)

Authorized officer:

Lee W. Young

PCT Helpdesk: 571-272-4300
PCT OSP: 571-272-7774

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITYInternational application No.
PCT/IB 10/52959

Box No. I	Basis of this opinion
1.	With regard to the language, this opinion has been established on the basis of: ☒ the international application in the language in which it was filed. ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).
2.	☐ This opinion has been established taking into account the rectification of an obvious mistake authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a)).
3.	With regard to any nucleotide and/or amino acid sequence disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished: a. (means) ☐ on paper ☐ in electronic form b. (time) ☐ in the international application as filed ☐ together with the international application in electronic form ☐ subsequently to this Authority for the purposes of search
4.	☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
5.	Additional comments:

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/IB 10/52959

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-25	YES
	Claims	None	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-25	NO
Industrial applicability (IA)	Claims	1-25	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-25 lack an inventive step under PCT Article 33(3) as being obvious over US 2009/0100060 A1 to Livnat et al. (hereinafter "Livnat") in view of US 20080147558 A1 (Kraus).

Regarding claim 1, Livnat teaches a method of controlling usage (para [0080] - controlling the operation of applications 156 and/or 157, e.g., to restrict the utilization of content presented by applications 156) of data (para [0256] - secure web application 154 (FIG. 1) may "cover", "hide" and/or obfuscate the contents of the protected file) and prevent unauthorized usage of data (para [0090] - tracked and control is maintained so that permissions may be updated in the future) which is generated by software (abstract - generating a web-application file including the content in a format presentable by a secure web application), using system (see fig. 1 for system). Livnat fails to explicitly teach sharing of ISO data. However, Kraus does teach sharing (para [0045] - allow users to interact and share information over the network(s); also see para [0046] - computer that accesses shared network resources provided by another computer, e.g., a server) of ISO data (para [0025] - video file...ISO; also see para [0060] - sharing with others who might be interested in audio tracks on the play list; and para [0066] - owner has authorized another). It would have been obvious to one of ordinary skill in the art to combine the securely sharing of file of Livnat with the teaching of Kraus in order to have more compatibility of the system by supporting sharing of ISO data.

Regarding claim 2, Livnat teaches data can be used only (abstract - presenting the content of the protected file to the user via the secure web application, only if the user is an allowed user of the allowed users) on the computer which has created (para [0029] - generate a web-application file including the content) it using system (see fig. 1 for system); to use said data on another computer (para [0003] - only authorized users are allowed to access the files only according to predefined permissions), data owner must authorize a recipient (abstract - presenting the content of the protected file to the user via the secure web application, only if the user is an allowed user of the allowed users), using the same system on another computer (para [0011] - allow a user ("the file owner") to define one or more permissions identifying who can and/or who cannot gain access to one or more files "owned" by the user; also see fig. 2). Kraus further teaches sharing (para [0045] - allow users to interact and share information over the network(s); also see para [0046] - computer that accesses shared network resources provided by another computer, e.g., a server) of ISO data (para [0025] - video file...ISO; also see para [0060] - sharing with others who might be interested in audio tracks on the play list; and para [0066] - owner has authorized another). It would have been obvious to one of ordinary skill in the art to combine the securely sharing of file of Livnat with the teaching of Kraus in order to have more compatibility of the system by supporting sharing of ISO data.

Regarding claim 3, Livnat teaches selecting the data to be shared (para [0004] - selectively share files with clients, partners and/or suppliers) and embedding (para [0209] - embed the link [links for owner's info] as part of the protected file) data owner's customer id (para [0025] - identifying the linked device [owner's device ID]); identifying (para [0011] - identifying who can and/or who cannot gain access to one or more files "owned" by the user) and authorizing at least one recipient (para [0011] - to define one or more utilization-restrictions to be selectively applied on one or more of the users which are allowed to access the owned file) with whom the data is to be shared (para [0011] - applied [input or entering the allowed user info] on one or more of the users which are allowed to access the owned file) by entering the recipient's customer id (para [0085] - identify a user of system 100 based on an email address associated with the user [customer identification]); identifying each set of data (para [0018] - file identifier to identify the web-application file) being shared by a unique data id (para [0019] - generating...the file identifier) generated by the data owner's system (para [0019] - file identifier in association with the permission information corresponding to the web-application file) where in the access permissions to each set of data are associated with each particular data id (para [0019] - file identifier in association with the permission information corresponding to the web-application file); issuing required access permissions (para [0027] - sending to the electronic mail address an electronic mail message including first authentication information) to authorized recipient to use the data (para [0011] - identifying who can and/or who cannot gain access to one or more files "owned" by the user); using appropriate data sharing methods i.e. sharing via uploading the data to the online server or by copying the data to any external storage device (para [0029] - server to receive the content of a file to be protected and permission information representing one or more allowed users [data is sharing by uploading data to online server]).

-----continued in Supplemental Box-----

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/IB 10/52959

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:
Box V.2. Citations and explanations:

Regarding claim 4, Livnat teaches during software activation (para [0254] - activation...function of the internal playable file; also see para [0006] - installation of special client software on each user's computer), the vendors' online server sends two keys (para [0016] - decrypting the encrypted web-application file at the secure web application using the file encryption key) namely R1 (para [0020] - encrypting the web-application file using a file key to generate an encrypted web-application file) and R2 to the software (para [0100] - public keys 153 assigned; also see plurality of keys may be use such as 155, 157 as shown in fig. 1). Key R1 is used to encrypt owner's data to protect it (para [0020] - encrypting the web-application file using a file key to generate an encrypted web-application file) from unauthorized usage of this data on any other computer (para [0004] - prohibiting the sharing of the content with unauthorized people). When data is created in the software it is automatically (para [0095] - automatically allowing...access a protected file) encrypted with the R1 key (para [0020] - encrypting the web-application file using a file key to generate an encrypted web-application file) and stored in this encrypted form (para [0019] - storing the web-application file). Key R2 is used to protect the data (para [0100] - public keys 153 assigned; also see plurality of keys may be use such as 155, 157 as shown in fig. 1) that is to be shared with one or more intended recipients (abstract - protected file to the user via the secure web application) on their computer system (abstract - file to be protected and permission information representing one or more allowed user). Ra and Rb are the private (para [0100] - public keys 153 assigned; also see plurality of keys may be use such as 155, 157 as shown in fig. 1) and public keys of the recipient (para [0157] - server application 104 (FIG. 1) may generate and provide a private key).

Regarding claim 5, Livnat teaches data owner can share the data with the recipient via uploading the data to the online server or by transferring data to an external storage device and sharing this device with the recipient (para [0029] - server to receive the content of a file to be protected and permission information representing one or more allowed users [data is sharing by uploading data to online server]).

Regarding claim 6, Livnat teaches incase the recipient has not yet (para [0153] - authentication information was not included[have not registered]) registered (para [0144] - register add-in) the data owner's R2 key (para [0157] - key 150 (FIG. 1) to client application) and data to be shared is uploaded to the online server (para [0203] - transfer the encrypted file to server application), data is first decrypted using the data owner's R1 key (para [0203] - decrypt the file; also see para [0203] - decrypt the permission information of the protected file, e.g., using any private keys) and then encrypted with the data owner's R2 key (para [0035] - encrypt the web-application file using a file key). This data is uploaded to the server (para [0203] - transfer the encrypted file to server application) where it is decrypted with data owner's R2 key (para [0203] - decrypt the file; also see para [0203] - decrypt the permission information of the protected file, e.g., using any private keys) and again encrypted with the recipient's Rb key (para [0035] - encrypt the web-application file using a file key). Recipient downloads this data (para [0248] - downloading a byte stream including the encrypted web-application file to the secure web application) and uses it with his Rb key (para [0250] - application 154 (FIG. 1) may decrypt the byte stream representing web-application file...decryption file key).

Regarding claim 7, Livnat teaches incase the recipient has not yet (para [0153] - authentication information was not included[have not registered]) registered (para [0144] - register add-in) the data owner's R2 key (para [0157] - key 150 (FIG. 1) to client application) and data to be shared is sent to the recipient (para [0072] - share one or more files while ensuring the confidentiality of the shared files) via an external storage device (para [0269] - "external" operations which may be performed [via external device]; also see para [0100] - suitable storage 106, the information of the linked), data is -first decrypted using the data owner's R1 key (para [0203] - decrypt the file; also see para [0203] - decrypt the permission information of the protected file, e.g., using any private keys) and then encrypted with the data owner's R2 key (para [0035] - encrypt the web-application file using a file key). This data transferred (para [0062] - sending at least part of the content) to the external storage device (para [0269] - "external" operations which may be performed [via external device]; also see para [0100] - suitable storage 106, the information of the linked) and shared with the recipient (para [0096] - send the protected file to the other user). The recipient uploads this data to the online server (para [0205] - uploading the content of the file...transfer the copy to server application) and incase the data owner has given sufficient permissions (para [0207] - permission information corresponding to the protected web-application file; also see para [0029] - only if the user is an allowed user of the allowed users), the server decrypts this data with the data owner's R2 key (para [0203] - decrypt the file; also see para [0203] - decrypt the permission information of the protected file, e.g., using any private keys) and encrypts this data with the recipients Rb key (para [0035] - encrypt the web-application file using a file key) after which recipient can download and use this data with his Rb key (para [0250] - application 154 (FIG. 1) may decrypt the byte stream representing web-application file...decryption file key).

Regarding claim 8, Livnat teaches incase the recipient (see 132 of fig. 1) has previously registered (para [0144] - register) the data owner's R2 key (para [0157] - key 150 (FIG. 1) to client application) and data to be shared is uploaded to the online server (para [0205] - uploading the content of the file...transfer the copy to server application), data is first decrypted using the data owner's R1 key (para [0203] - decrypt the file; also see para [0203] - decrypt the permission information of the protected file, e.g., using any private keys) and then encrypted with the data owner's R2 key (para [0020] - encrypting the web-application file using a file key to generate an encrypted web-application file). This data is uploaded to the server (para [0205] - uploading the content of the file...transfer the copy to server application), the recipient downloads this data from the server (para [0248] - downloading a byte stream including the encrypted web-application file to the secure web application) and decrypts and uses the data with the data owner's R2 key (para [0016] - decrypting the encrypted web-application file at the secure web application using the file encryption key).

-----continued in Supplemental Box-----

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/IB 10/52959

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:
Box V.2. Citations and explanations:

Regarding claim 9, Livnat teaches incase the recipient (see 132 of fig. 1) has registered (para [0144] - register) the data owner's R2 key (para [0157] - key 150 (FIG. 1) to client application) and data is shared (para [0072] - share one or more files while ensuring the confidentiality of the shared files) via an external storage device (para [0269] - "external" operations which may be performed [via external device]; also see para [0100] - suitable storage 106, the information of the linked), data is first decrypted using the data owner's R1 key (para [0203] - decrypt the file; also see para [0203] - decrypt the permission information of the protected file, e.g., using any private keys) and then encrypted with the data owner's R2 key (para [0020] - encrypting the web-application file using a file key to generate an encrypted web-application file). This data is transferred (para [0072] - share one or more files while ensuring the confidentiality of the shared files) to the external storage device (para [0269] - "external" operations which may be performed [via external device]; also see para [0100] - suitable storage 106, the information of the linked) and shared with the recipient (para [0248] - downloading a byte stream including the encrypted web-application file to the secure web application). Recipient downloads this data (para [0248] - downloading a byte stream including the encrypted web-application file to the secure web application) from the storage device (para [0100] - suitable storage 106, the information of the linked) and decrypts and uses the data with the data owner's R2 key (para [0016] - decrypting the encrypted web-application file at the secure web application using the file encryption key).

Regarding claim 10, Livnat teaches system can be used to protect any data (abstract - presenting the content of the protected file to the user via the secure web application, only if the user is an allowed user of the allowed users) on the data owner's computer/system (para [0011] - allow a user ("the file owner") to define one or more permissions identifying who can and/or who cannot gain access to one or more files "owned" by the user; also see fig. 2; also see 110 of fig. 1). Kraus further teaches sharing (para [0045] - allow users to interact and share information over the network(s); also see para [0046] - computer that accesses shared network resources provided by another computer, e.g., a server) of ISO data (para [0025] - video file...ISO; also see para [0060] - sharing with others who might be interested in audio tracks on the play list; and para [0066] - owner has authorized another). It would have been obvious to one of ordinary skill in the art to combine the securely sharing of file of Livnat with the teaching of Kraus in order to have more compatibility of the system by supporting sharing of ISO data.

Regarding claim 11, Livnat teaches the data downloaded by the authorized (para [0011] - allow a user ("the file owner") to define one or more permissions identifying who can and/or who cannot gain access to one or more files "owned" by the user; also see fig. 2) and designated recipient is bound by certain access rights issued by the data owner (para [0003] - only authorized users are allowed to access the files only according to predefined permissions); said data can be used by the recipient only as per the access rights set (para [0003] - permission to view the content of the document), where said set access rights are viewing (para [0003] - permission to view the content of the document), amending (para [0011] - editing the file), printing (para [0011] - printing the file) and saving (para [0114] - save the contents of the file).

Regarding claim 12, Livnat teaches the authorized recipient can amend the data (para [0003] - only authorized users are allowed to access the files only according to predefined permissions; also see para [0011] - editing the file) and send it back to the data owner (para [0096] - send the protected file to the other user) if needed (para [0111] - back to server application). This amended data (para [0012] - edited the file) will be recognized (para [0175] - recognized email address) using a new data id (para [0018] - file identifier to identify the web-application file). The data is encrypted with Rb key (para [0020] - encrypting the web-application file using a file key to generate an encrypted web-application file) and uploaded to the server (para [0205] - uploading the content of the file...transfer the copy to server application) where it is decrypted with the Rb key (para [0203] - decrypt the file; also see para [0203] - decrypt the permission information of the protected file, e.g., using any private keys) and again encrypted with the data owner's R2 key (para [0035] - encrypt the web-application file using a file key). Owner can download this data (para [0248] - downloading a byte stream including the encrypted web-application file to the secure web application) and convert it back (para [0206] - convert the received file...format presentable by secure application) to the R1 key (para [0250] - decrypt the byte stream representing web-application file...decryption file key) and use it (para [0016] - using the file encryption key).

Regarding claim 13, Livnat teaches recipient can amend the data (para [0011] - editing the file) shared by the data owner (para [0003] - only authorized users are allowed to access the files only according to predefined permissions), if needed, and send amended data back (para [0111] - back to server application) to the data owner (para [0096] - send the protected file to the other user) either via uploading the data to the online server or by transferring data to an external storage device and sharing this device with the data owner (para [0029] - server to receive the content of a file to be protected and permission information representing one or more allowed users [data is sharing by uploading data to online server]).

Regarding claim 14, Livnat teaches incase the recipient has not yet (para [0153] - authentication information was not included [have not registered]) registered (para [0144] - register) the data owner's R2 key (para [0157] - key 150 (FIG. 1) to client application). Amended data to be shared (para [0011] - editing the file) is encrypted with recipient's Rb key (para [0031] - encrypted web-application file using the file encryption key) and uploaded to the online server (para [0205] - uploading the content of the file...transfer the copy to server application), where it is decrypted with the recipient's Rb key (para [0203] - decrypt the file; also see para [0203] - decrypt the permission information of the protected file, e.g., using any private keys) and later encrypted with the data owner's R2 key (para [0035] - encrypt the web-application file using a file key). Data owner downloads this data (para [0248] - downloading a byte stream including the encrypted web-application file to the secure web application) and converts it from (para [0206] - convert the received file...format presentable by secure application) R2 to his R1 key (para [0250] - decrypt the byte stream representing web-application file...decryption file key) and then uses it (para [0016] - using the file encryption key).

-----continued in Supplemental Box-----

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/IB 10/52959

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:
Box V.2. Citations and explanations:

Regarding claim 15, Livnat teaches incase the recipient has not yet (para [0153] - authentication information was not included[have not registered]) registered (para [0144] - register 0 the data owner's R2 key (para [0157] - key 150 (FIG. 1) to client application) and amended data (para [0011] - editing the file) to be shared is sent to the data owner (para [0096] - send the protected file to the other user) via an external storage device (para [0100] - suitable storage 106, the information of the linked), data is encrypted using the recipient's Rb key (para [0035] - encrypt the web-application file using a file key) transferred to the external storage device (para [0269] - "external" operations which may be performed [via external device]) and shared with the data owner (para [0072] - share one or more files while ensuring the confidentiality of the shared files; also see 110 of fig. 1). The data owner uploads this data to the online server (para [0205] - uploading the content of the file...transfer the copy to server application) and incase the recipient has given sufficient permissions (para [0207] - permission information corresponding to the protected web-application file), the server decrypts this data with the recipient's Rb key (para [0203] - decrypt the file; also see para [0203] - decrypt the permission information of the protected file, e.g., using any private keys) and encrypts this data with the data owner's R2 key (para [0035] - encrypt the web-application file using a file key) after which data owner can download this data (para [0248] - downloading a byte stream including the encrypted web-application file to the secure web application), convert it from the R2 key (para [0206] - convert the received file) to R1key (para [0250] - decrypt the byte stream representing web-application file...decryption file key; keys 155, 157 as shown in fig. 1) and use it (para [0016] - using the file encryption key).

Regarding claim 16, Livnat teaches incase the recipient (see 132 of fig. 1) has previously registered (para [0144] - register) the data owner's R2 key (para [0157] - key 150 (FIG. 1) to client application) and amended data (para [0011] - editing the file) to be shared (para [0096] - send the protected file to the other user) is uploaded to the online server (para [0205] - uploading the content of the file...transfer the copy to server application), data owner downloads this data (para [0248] - downloading a byte stream including the encrypted web-application file to the secure web application) and decrypts it using his R2 key (para [0016] - decrypting the encrypted web-application file at the secure web application using the file encryption key). Said data can be converted (para [0206] - convert the received file...format presentable by secure application) from the R2 key to R1 key (para [0250] - decrypt the byte stream representing web-application file...decryption file key; keys 155, 157 as shown in fig. 1) and then used (para [0016] - using the file encryption key).

Regarding claim 17, Livnat teaches incase the recipient (see 132 of fig. 1) has previously registered add-in the data owner's R2 key (para [0157] - key 150 (FIG. 1) to client application) and shares the amended data (para [0011] - editing the file) via an (para [0096] - send the protected file to the other user) external storage device (para [0269] - "external" operations which may be performed [via external device]; also see para [0100] - suitable storage 106, the information of the linked), data owner downloads this data (para [0248] - downloading a byte stream including the encrypted web-application file to the secure web application) from the storage device (para [0269] - "external" operations which may be performed [via external device]; also see para [0100] - suitable storage 106, the information of the linked) and decrypts it using his R2 key (para [0016] - decrypting the encrypted web-application file at the secure web application using the file encryption key). Said data can be converted (para [0206] - convert the received file) from the R2 key (para [0206] - convert the received file...format presentable by secure application) to R1 key (para [0250] - decrypt the byte stream representing web-application file...decryption file key; keys 155, 157 as shown in fig. 1) and then used (para [0016] - using the file encryption key).

Regarding claim 18, Livnat teaches process (para [0018] - process for managing) and storage of original data (para [0019] - storing the web-application file) and data which is received for sharing (para [0029] - receive the content of a file to be protected [for sharing]), are processed (para [0018] - process for managing) through two different and mutually exclusive sub systems (see 106, 102, 120, 110, 132 of fig. 1) and are at two separate locations in the same computer system (106, 102, 120, 110, 132 are located remotely from each other with in the same communication network as shown in fig. 1).

Regarding claim 19, Livnat teaches the data owner is alerted (para [0169] - alert may be generated) about the (para [0185] - verification notification to the user) amendment done by the authorized recipient (para [0012] - who edited the file and when) in the shared data (para [0003] - authorized users are allowed to access the files) and can merge it (para [0056] - being stored, transferred, combined) into the original data if required (para [0059] - suitable electronic file).

Regarding claim 20, Livnat teaches the data owner (para [0144] - server 102 (FIG. 1), and register) can register his R2 key (para [0157] - key 150 (FIG. 1) to client application) with other recipients for secured data (para [0185] - protected file to the user, e.g., via secure web application) sharing purpose by sending the server (para [0003] - authorized users are allowed to access the files) an instruction to do so (para [0225] - updated permission instructions [to server]) and entering both customer's (para [0011] - applied [input or entering the allowed user info] on one or more of the users which are allowed to access the owned file) as well as data owner's customer id (para [0209] - embed the link [links for owner's info] as part of the protected file). The registration of this key can be revoked at any time by either parties (para [0108] - file owner may decide to revoke access to one or more or even all of these users), by sending an instruction to the vendor's online server about the same (para [0225] - updated permission instructions [to server]).

Regarding claim 21, Livnat teaches the data owner (see 110 of fig. 1) can block the access rights to the data shared with a recipient (para [0232] - blocking the sequence of events of certain operations [accessing]), by instructing the server to block (para [0225] - updated permission instructions [to server]) or delete the data sent to the recipient (para [0245] - blocking one or more user actions based on the content-utilization restriction).

Regarding claim 22, Livnat teaches even if the data from the recipients computer (para [0248] - downloading a byte stream [on recipient's device]), is used on any other computer (para [0082] - other form of utilizing the protected file, while a second allowed user), it cannot be accessed (para [0082] - user may not be permitted to perform any of copy-pasting the content of the protected file), used or processed (para [0003] - not allowing the first user to copy, print and/or save the content), due to lack of permissions from the data owner (para [0082] - who cannot gain access to the protected file; and/or to define one or more utilization-restrictions to be selectively applied on one or more of the users).

-----continued in Supplemental Box-----

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/IB 10/52959

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:
Box V.2. Citations and explanations:

Regarding claim 23, Livnat teaches in case the software (para [0006] - restricts and/or prohibits the installation of client software) is required to be reinstalled (para [0006] - require the installation of special client software on each user's computer), an easy method (para [0008] - methods of file-utilization management) of reinstallation is provided (para [0098] - install client application 140, and may use the installed client application 140 to verify) to the software user (para [0015] - downloading the secure web application to the computing device) and the server sends (para [0016] - providing a file encryption key to the secure web application) the encryption and decryption keys (para [0100] - public keys 153 assigned; also see plurality of keys may be use such as 155, 157 as shown in fig. 1) again to the software (para [0016] - providing a file encryption key to the secure web application) after activation (para [0254] - activation...function of the internal playable file). It also sends (para [0016] - providing a file encryption key to the secure web application) the previously registered (para [0144] - register) R2 keys (para [0157] - key 150 (FIG. 1) to client application) of other user's into the software (para [0128] - installed client application 140 (FIG. 1)).

Regarding claim 24, Livnat teaches incase during reinstallation (para [0111] - report the detected action) or each time the software is opened (para [0111] - report the detected action back to server application), it is detected (para [0147] - detecting the authentication) that there is the motherboard id (para [0182] - detecting a received response including second authentication information (identification info)) of the computer has changed (para [0107] - tag [hardware ID] provided by the computing device is not valid; also see para [0213] - detect the change in the permissions), then the software will have to be revalidated (156 of fig. 1) with the server (para [0260] - validation, integrity checking) and also the R2 keys (para [0016] - providing a file encryption key) will have to be revalidated (para [0260] - validation, integrity checking) again by the data owners (110 of fig. 1) only then the data sharing from these owners can occur (para [0072] - share one or more files while ensuring the confidentiality of the shared files).

Regarding claim 25, Livnat teaches the system can also be used as an independent (para [0193] - include encrypting the file using an encryption key to generate a protected file including the encrypted file; also see fig. 1) encryption module (para [0002] - protecting and/or securing information) to secure (para [0003] - securing and/or protecting electronic organizational files) data storage (para [0057] - memories or other information storage medium; also see 106 of fig. 1). Kraus further teaches sharing (para [0045] - allow users to interact and share information over the network(s); also see para [0046] - computer that accesses shared network resources provided by another computer, e.g., a server) of ISO data (para [0025] - video file...ISO; also see para [0060] - sharing with others who might be interested in audio tracks on the play list; and para [0066] - owner has authorized another). It would have been obvious to one of ordinary skill in the art to combine the securely sharing of file of Livnat with the teaching of Kraus in order to have more compatibility of the system by supporting sharing of ISO data.

Claims 1-25 have industrial applicability as defined by PCT Article 33(4), because the subject matter can be made or used in industry.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44bis)

Applicant's or agent's file reference isodata	FOR FURTHER ACTION See item 4 below	
International application No. PCT/IB2010/052959	International filing date (day/month/year) 29 June 2010 (29.06.2010)	Priority date (day/month/year) 01 July 2009 (01.07.2009)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant PATIL, Mandar		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 bis.1(a).

2. This REPORT consists of a total of 8 sheets, including this cover sheet.

In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

- | | | |
|-------------------------------------|--------------|---|
| ☒ | Box No. I | Basis of the report |
| ☐ | Box No. II | Priority |
| ☐ | Box No. III | Non-establishment of opinion with regard to novelty, inventive step and industrial applicability |
| ☐ | Box No. IV | Lack of unity of invention |
| ☒ | Box No. V | Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement |
| ☐ | Box No. VI | Certain documents cited |
| ☐ | Box No. VII | Certain defects in the international application |
| ☐ | Box No. VIII | Certain observations on the international application |

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44bis.3(c) and 93bis.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44bis .2).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Date of issuance of this report 04 January 2012 (04.01.2012)
	Authorized officer Cécile Chatel e-mail: ro.ib@wipo.int

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: MANDAR PATIL
SURVEY NUMBER 118 TO 124, PLOT
NUMBER 85, NATIONAL SOCIETY,
AUNDH, PUNE 411007
MAHARASHTRA, INDIA.
411007 PUNE
INDIA

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Date of mailing
(day/month/year)

27 DEC 2010

Applicant's or agent's file reference
ISODATA

FOR FURTHER ACTION

See paragraph 2 below

International application No.

PCT/IB 10/52959

International filing date (day/month/year)

29 June 2010 (29.06.2010)

Priority date (day/month/year)

01 July 2009 (01.07.2009)

International Patent Classification (IPC) or both national classification and IPC

IPC(8) - G06F 21/00 (2010.01)

USPC - 705/51

Applicant PATIL, MANDAR

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450
Facsimile No. 571-273-3201

Date of completion of this opinion

08 December 2010 (08.12.2010)

Authorized officer:

Lee W. Young

PCT Helpdesk: 571-272-4300
PCT OSP: 571-272-7774

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITYInternational application No.
PCT/IB 10/52959

Box No. I	Basis of this opinion
1.	With regard to the language, this opinion has been established on the basis of: ☒ the international application in the language in which it was filed. ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).
2.	☐ This opinion has been established taking into account the rectification of an obvious mistake authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a)).
3.	With regard to any nucleotide and/or amino acid sequence disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished: a. (means) ☐ on paper ☐ in electronic form b. (time) ☐ in the international application as filed ☐ together with the international application in electronic form ☐ subsequently to this Authority for the purposes of search
4.	☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
5.	Additional comments:

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/IB 10/52959

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-25	YES
	Claims	None	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-25	NO
Industrial applicability (IA)	Claims	1-25	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-25 lack an inventive step under PCT Article 33(3) as being obvious over US 2009/0100060 A1 to Livnat et al. (hereinafter 'Livnat') in view of US 20080147558 A1 (Kraus).

Regarding claim 1, Livnat teaches a method of controlling usage (para [0080] - controlling the operation of applications 156 and/or 157, e.g., to restrict the utilization of content presented by applications 156) of data (para [0256] - secure web application 154 (FIG. 1) may "cover", "hide" and/or obfuscate the contents of the protected file) and prevent unauthorized usage of data (para [0090] - tracked and control is maintained so that permissions may be updated in the future) which is generated by software (abstract - generating a web-application file including the content in a format presentable by a secure web application), using system (see fig. 1 for system). Livnat fails to explicitly teach sharing of ISO data. However, Kraus does teach sharing (para [0045] - allow users to interact and share information over the network(s); also see para [0046] - computer that accesses shared network resources provided by another computer, e.g., a server) of ISO data (para [0025] - video file...ISO; also see para [0060] - sharing with others who might be interested in audio tracks on the play list; and para [0066] - owner has authorized another). It would have been obvious to one of ordinary skill in the art to combine the securely sharing of file of Livnat with the teaching of Kraus in order to have more compatibility of the system by supporting sharing of ISO data.

Regarding claim 2, Livnat teaches data can be used only (abstract - presenting the content of the protected file to the user via the secure web application, only if the user is an allowed user of the allowed users) on the computer which has created (para [0029] - generate a web-application file including the content) it using system (see fig. 1 for system); to use said data on another computer (para [0003] - only authorized users are allowed to access the files only according to predefined permissions), data owner must authorize a recipient (abstract - presenting the content of the protected file to the user via the secure web application, only if the user is an allowed user of the allowed users), using the same system on another computer (para [0011] - allow a user ("the file owner") to define one or more permissions identifying who can and/or who cannot gain access to one or more files "owned" by the user; also see fig. 2). Kraus further teaches sharing (para [0045] - allow users to interact and share information over the network(s); also see para [0046] - computer that accesses shared network resources provided by another computer, e.g., a server) of ISO data (para [0025] - video file...ISO; also see para [0060] - sharing with others who might be interested in audio tracks on the play list; and para [0066] - owner has authorized another). It would have been obvious to one of ordinary skill in the art to combine the securely sharing of file of Livnat with the teaching of Kraus in order to have more compatibility of the system by supporting sharing of ISO data.

Regarding claim 3, Livnat teaches selecting the data to be shared (para [0004] - selectively share files with clients, partners and/or suppliers) and embedding (para [0209] - embed the link [links for owner's info] as part of the protected file) data owner's customer id (para [0025] - identifying the linked device [owner's device ID]); identifying (para [0011] - identifying who can and/or who cannot gain access to one or more files "owned" by the user) and authorizing at least one recipient (para [0011] - to define one or more utilization-restrictions to be selectively applied on one or more of the users which are allowed to access the owned file) with whom the data is to be shared (para [0011] - applied [input or entering the allowed user info] on one or more of the users which are allowed to access the owned file) by entering the recipient's customer id (para [0085] - identify a user of system 100 based on an email address associated with the user [customer identification]); identifying each set of data (para [0018] - file identifier to identify the web-application file) being shared by a unique data id (para [0019] - generating...the file identifier) generated by the data owner's system (para [0019] - file identifier in association with the permission information corresponding to the web-application file) where in the access permissions to each set of data are associated with each particular data id (para [0019] - file identifier in association with the permission information corresponding to the web-application file); issuing required access permissions (para [0027] - sending to the electronic mail address an electronic mail message including first authentication information) to authorized recipient to use the data (para [0011] - identifying who can and/or who cannot gain access to one or more files "owned" by the user); using appropriate data sharing methods i.e. sharing via uploading the data to the online server or by copying the data to any external storage device (para [0029] - server to receive the content of a file to be protected and permission information representing one or more allowed users [data is sharing by uploading data to online server]).

-----continued in Supplemental Box-----

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/IB 10/52959

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:
Box V.2. Citations and explanations:

Regarding claim 4, Livnat teaches during software activation (para [0254] - activation...function of the internal playable file; also see para [0006] - installation of special client software on each user's computer), the vendors' online server sends two keys (para [0016] - decrypting the encrypted web-application file at the secure web application using the file encryption key) namely R1 (para [0020] - encrypting the web-application file using a file key to generate an encrypted web-application file) and R2 to the software (para [0100] - public keys 153 assigned; also see plurality of keys may be use such as 155, 157 as shown in fig. 1). Key R1 is used to encrypt owner's data to protect it (para [0020] - encrypting the web-application file using a file key to generate an encrypted web-application file) from unauthorized usage of this data on any other computer (para [0004] - prohibiting the sharing of the content with unauthorized people). When data is created in the software it is automatically (para [0095] - automatically allowing...access a protected file) encrypted with the R1 key (para [0020] - encrypting the web-application file using a file key to generate an encrypted web-application file) and stored in this encrypted form (para [0019] - storing the web-application file). Key R2 is used to protect the data (para [0100] - public keys 153 assigned; also see plurality of keys may be use such as 155, 157 as shown in fig. 1) that is to be shared with one or more intended recipients (abstract - protected file to the user via the secure web application) on their computer system (abstract - file to be protected and permission information representing one or more allowed user). Ra and Rb are the private (para [0100] - public keys 153 assigned; also see plurality of keys may be use such as 155, 157 as shown in fig. 1) and public keys of the recipient (para [0157] - server application 104 (FIG. 1) may generate and provide a private key).

Regarding claim 5, Livnat teaches data owner can share the data with the recipient via uploading the data to the online server or by transferring data to an external storage device and sharing this device with the recipient (para [0029] - server to receive the content of a file to be protected and permission information representing one or more allowed users [data is sharing by uploading data to online server]).

Regarding claim 6, Livnat teaches incase the recipient has not yet (para [0153] - authentication information was not included[have not registered]) registered (para [0144] - register add-in) the data owner's R2 key (para [0157] - key 150 (FIG. 1) to client application) and data to be shared is uploaded to the online server (para [0203] - transfer the encrypted file to server application), data is first decrypted using the data owner's R1 key (para [0203] - decrypt the file; also see para [0203] - decrypt the permission information of the protected file, e.g., using any private keys) and then encrypted with the data owner's R2 key (para [0035] - encrypt the web-application file using a file key). This data is uploaded to the server (para [0203] - transfer the encrypted file to server application) where it is decrypted with data owner's R2 key (para [0203] - decrypt the file; also see para [0203] - decrypt the permission information of the protected file, e.g., using any private keys) and again encrypted with the recipient's Rb key (para [0035] - encrypt the web-application file using a file key). Recipient downloads this data (para [0248] - downloading a byte stream including the encrypted web-application file to the secure web application) and uses it with his Rb key (para [0250] - application 154 (FIG. 1) may decrypt the byte stream representing web-application file...decryption file key).

Regarding claim 7, Livnat teaches incase the recipient has not yet (para [0153] - authentication information was not included[have not registered]) registered (para [0144] - register add-in) the data owner's R2 key (para [0157] - key 150 (FIG. 1) to client application) and data to be shared is sent to the recipient (para [0072] - share one or more files while ensuring the confidentiality of the shared files) via an external storage device (para [0269] - "external" operations which may be performed [via external device]; also see para [0100] - suitable storage 106, the information of the linked), data is -first decrypted using the data owner's R1 key (para [0203] - decrypt the file; also see para [0203] - decrypt the permission information of the protected file, e.g., using any private keys) and then encrypted with the data owner's R2 key (para [0035] - encrypt the web-application file using a file key). This data transferred (para [0062] - sending at least part of the content) to the external storage device (para [0269] - "external" operations which may be performed [via external device]; also see para [0100] - suitable storage 106, the information of the linked) and shared with the recipient (para [0096] - send the protected file to the other user). The recipient uploads this data to the online server (para [0205] - uploading the content of the file...transfer the copy to server application) and incase the data owner has given sufficient permissions (para [0207] - permission information corresponding to the protected web-application file; also see para [0029] - only if the user is an allowed user of the allowed users), the server decrypts this data with the data owner's R2 key (para [0203] - decrypt the file; also see para [0203] - decrypt the permission information of the protected file, e.g., using any private keys) and encrypts this data with the recipients Rb key (para [0035] - encrypt the web-application file using a file key) after which recipient can download and use this data with his Rb key (para [0250] - application 154 (FIG. 1) may decrypt the byte stream representing web-application file...decryption file key).

Regarding claim 8, Livnat teaches incase the recipient (see 132 of fig. 1) has previously registered (para [0144] - register) the data owner's R2 key (para [0157] - key 150 (FIG. 1) to client application) and data to be shared is uploaded to the online server (para [0205] - uploading the content of the file...transfer the copy to server application), data is first decrypted using the data owner's R1 key (para [0203] - decrypt the file; also see para [0203] - decrypt the permission information of the protected file, e.g., using any private keys) and then encrypted with the data owner's R2 key (para [0020] - encrypting the web-application file using a file key to generate an encrypted web-application file). This data is uploaded to the server (para [0205] - uploading the content of the file...transfer the copy to server application), the recipient downloads this data from the server (para [0248] - downloading a byte stream including the encrypted web-application file to the secure web application) and decrypts and uses the data with the data owner's R2 key (para [0016] - decrypting the encrypted web-application file at the secure web application using the file encryption key).

-----continued in Supplemental Box-----

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/IB 10/52959

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:
Box V.2. Citations and explanations:

Regarding claim 9, Livnat teaches incase the recipient (see 132 of fig. 1) has registered (para [0144] - register) the data owner's R2 key (para [0157] - key 150 (FIG. 1) to client application)and data is shared (para [0072] - share one or more files while ensuring the confidentiality of the shared files)via an external storage device (para [0269] - "external" operations which may be performed [via external device]; also see para [0100] - suitable storage 106, the information of the linked), data is first decrypted using the data owner's R1key (para [0203] - decrypt the file; also see para [0203] - decrypt the permission information of the protected file, e.g., using any private keys) and then encrypted with the data owner's R2 key (para [0020] - encrypting the web-application file using a file key to generate an encrypted web-application file). This data is transferred (para [0072] - share one or more files while ensuring the confidentiality of the shared files) to the external storage device (para [0269] - "external" operations which may be performed [via external device]; also see para [0100] - suitable storage 106, the information of the linked) and shared with the recipient (para [0248] - downloading a byte stream including the encrypted web-application file to the secure web application). Recipient downloads this data (para [0248] - downloading a byte stream including the encrypted web-application file to the secure web application) from the storage device (para [0100] - suitable storage 106, the information of the linked)and decrypts and uses the data with the data owner's R2 key (para [0016] - decrypting the encrypted web-application file at the secure web application using the file encryption key).

Regarding claim 10, Livnat teaches system can be used to protect any data (abstract - presenting the content of the protected file to the user via the secure web application, only if the user is an allowed user of the allowed users) on the data owner's computer/system (para [0011] - allow a user ("the file owner") to define one or more permissions identifying who can and/or who cannot gain access to one or more files "owned" by the user; also see fig. 2; also see 110 of fig. 1).Kraus further teaches sharing (para [0045] - allow users to interact and share information over the network(s); also see para [0046] - computer that accesses shared network resources provided by another computer, e.g., a server) of ISO data (para [0025] - video file...ISO; also see para [0060] - sharing with others who might be interested in audio tracks on the play list; and para [0066] - owner has authorized another). It would have been obvious to one of ordinary skill in the art to combine the securely sharing of file of Livnat with the teaching of Kraus in order to have more compatibility of the system by supporting sharing of ISO data.

Regarding claim 11, Livnat teaches the data downloaded by the authorized (para [0011] - allow a user ("the file owner") to define one or more permissions identifying who can and/or who cannot gain access to one or more files "owned" by the user; also see fig. 2) and designated recipient is bound by certain access rights issued by the data owner (para [0003] - only authorized users are allowed to access the files only according to predefined permissions); said data can be used by the recipient only as per the access rights set (para [0003] - permission to view the content of the document), where said set access rights are viewing (para [0003] - permission to view the content of the document), amending (para [0011] - editing the file), printing (para [0011] - printing the file)and saving (para [0114] - save the contents of the file).

Regarding claim 12, Livnat teaches the authorized recipient can amend the data (para [0003] - only authorized users are allowed to access the files only according to predefined permissions; also see para [0011] - editing the file) and send it back to the data owner (para [0096] - send the protected file to the other user) if needed (para [0111] - back to server application). This amended data (para [0012] - edited the file) will be recognized (para [0175] - recognized email address) using a new data id (para [0018] - file identifier to identify the web-application file). The data is encrypted with Rb key (para [0020] - encrypting the web-application file using a file key to generate an encrypted web-application file) and uploaded to the server (para [0205] - uploading the content of the file...transfer the copy to server application) where it is decrypted with the Rb key (para [0203] - decrypt the file; also see para [0203] - decrypt the permission information of the protected file, e.g., using any private keys) and again encrypted with the data owner's R2 key (para [0035] - encrypt the web-application file using a file key). Owner can download this data (para [0248] - downloading a byte stream including the encrypted web-application file to the secure web application) and convert it back (para [0206] - convert the received file...format presentable by secure application) to the R1 key (para [0250] - decrypt the byte stream representing web-application file...decryption file key) and use it (para [0016] - using the file encryption key).

Regarding claim 13, Livnat teaches recipient can amend the data (para [0011] - editing the file) shared by the data owner (para [0003] - only authorized users are allowed to access the files only according to predefined permissions), if needed, and send amended data back (para [0111] - back to server application) to the data owner (para [0096] - send the protected file to the other user) either via uploading the data to the online server or by transferring data to an external storage device and sharing this device with the data owner (para [0029] - server to receive the content of a file to be protected and permission information representing one or more allowed users [data is sharing by uploading data to online server]).

Regarding claim 14, Livnat teaches incase the recipient has not yet (para [0153] - authentication information was not included[have not registered]) registered (para [0144] - register) the data owner's R2 key (para [0157] - key 150 (FIG. 1) to client application). Amended data to be shared (para [0011] - editing the file) is encrypted with recipient's Rb key (para [0031] - encrypted web-application file using the file encryption key) and uploaded to the online server (para [0205] - uploading the content of the file...transfer the copy to server application), where it is decrypted with the recipient's Rb key (para [0203] - decrypt the file; also see para [0203] - decrypt the permission information of the protected file, e.g., using any private keys) and later encrypted with the data owner's R2 key (para [0035] - encrypt the web-application file using a file key). Data owner downloads this data (para [0248] - downloading a byte stream including the encrypted web-application file to the secure web application) and converts it from (para [0206] - convert the received file...format presentable by secure application) R2 to his R1 key (para [0250] - decrypt the byte stream representing web-application file...decryption file key) and then uses it (para [0016] - using the file encryption key).

-----continued in Supplemental Box-----

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/IB 10/52959

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:
Box V.2. Citations and explanations:

Regarding claim 15, Livnat teaches incase the recipient has not yet (para [0153] - authentication information was not included[have not registered]) registered (para [0144] - register 0 the data owner's R2 key (para [0157] - key 150 (FIG. 1) to client application) and amended data (para [0011] - editing the file) to be shared is sent to the data owner (para [0096] - send the protected file to the other user) via an external storage device (para [0100] - suitable storage 106, the information of the linked), data is encrypted using the recipient's Rb key (para [0035] - encrypt the web-application file using a file key) transferred to the external storage device (para [0269] - "external" operations which may be performed [via external device]) and shared with the data owner (para [0072] - share one or more files while ensuring the confidentiality of the shared files; also see 110 of fig. 1). The data owner uploads this data to the online server (para [0205] - uploading the content of the file...transfer the copy to server application) and incase the recipient has given sufficient permissions (para [0207] - permission information corresponding to the protected web-application file), the server decrypts this data with the recipient's Rb key (para [0203] - decrypt the file; also see para [0203] - decrypt the permission information of the protected file, e.g., using any private keys) and encrypts this data with the data owner's R2 key (para [0035] - encrypt the web-application file using a file key) after which data owner can download this data (para [0248] - downloading a byte stream including the encrypted web-application file to the secure web application), convert it from the R2 key (para [0206] - convert the received file) to R1key (para [0250] - decrypt the byte stream representing web-application file...decryption file key; keys 155, 157 as shown in fig. 1) and use it (para [0016] - using the file encryption key).

Regarding claim 16, Livnat teaches incase the recipient (see 132 of fig. 1) has previously registered (para [0144] - register) the data owner's R2 key (para [0157] - key 150 (FIG. 1) to client application) and amended data (para [0011] - editing the file) to be shared (para [0096] - send the protected file to the other user) is uploaded to the online server (para [0205] - uploading the content of the file...transfer the copy to server application), data owner downloads this data (para [0248] - downloading a byte stream including the encrypted web-application file to the secure web application) and decrypts it using his R2 key (para [0016] - decrypting the encrypted web-application file at the secure web application using the file encryption key). Said data can be converted (para [0206] - convert the received file...format presentable by secure application) from the R2 key to R1 key (para [0250] - decrypt the byte stream representing web-application file...decryption file key; keys 155, 157 as shown in fig. 1) and then used (para [0016] - using the file encryption key).

Regarding claim 17, Livnat teaches incase the recipient (see 132 of fig. 1) has previously registered add-in) the data owner's R2 key (para [0157] - key 150 (FIG. 1) to client application) and shares the amended data (para [0011] - editing the file) via an (para [0096] - send the protected file to the other user) external storage device (para [0269] - "external" operations which may be performed [via external device]; also see para [0100] - suitable storage 106, the information of the linked), data owner downloads this data (para [0248] - downloading a byte stream including the encrypted web-application file to the secure web application) from the storage device (para [0269] - "external" operations which may be performed [via external device]; also see para [0100] - suitable storage 106, the information of the linked) and decrypts it using his R2 key (para [0016] - decrypting the encrypted web-application file at the secure web application using the file encryption key). Said data can be converted (para [0206] - convert the received file) from the R2 key (para [0206] - convert the received file...format presentable by secure application) to R1 key (para [0250] - decrypt the byte stream representing web-application file...decryption file key; keys 155, 157 as shown in fig. 1) and then used (para [0016] - using the file encryption key).

Regarding claim 18, Livnat teaches process (para [0018] - process for managing) and storage of original data (para [0019] - storing the web-application file) and data which is received for sharing (para [0029] - receive the content of a file to be protected [for sharing]), are processed (para [0018] - process for managing) through two-different and mutually exclusive sub systems (see 106, 102, 120, 110, 132 of fig. 1) and are at two separate locations in the same computer system (106, 102, 120, 110, 132 are located remotely from each other with in the same communication network as shown in fig. 1).

Regarding claim 19, Livnat teaches the data owner is alerted (para [0169] - alert may be generated) about the (para [0185] - verification notification to the user) amendment done by the authorized recipient (para [0012] - who edited the file and when) in the shared data (para [0003] - authorized users are allowed to access the files) and can merge it (para [0056] - being stored, transferred, combined) into the original data if required (para [0059] - suitable electronic file).

Regarding claim 20, Livnat teaches the data owner (para [0144] - server 102 (FIG. 1), and register) can register his R2 key (para [0157] - key 150 (FIG. 1) to client application) with other recipients for secured data (para [0185] - protected file to the user, e.g., via secure web application) sharing purpose by sending the server (para [0003] - authorized users are allowed to access the files) an instruction to do so (para [0225] - updated permission instructions [to server]) and entering both customer's (para [0011] - applied [input or entering the allowed user info] on one or more of the users which are allowed to access the owned file) as well as data owner's customer id (para [0209] - embed the link [links for owner's info] as part of the protected file). The registration of this key can be revoked at any time by either parties (para [0108] - file owner may decide to revoke access to one or more or even all of these users), by sending an instruction to the vendor's online server about the same (para [0225] - updated permission instructions [to server]).

Regarding claim 21, Livnat teaches the data owner (see 110 of fig. 1) can block the access rights to the data shared with a recipient (para [0232] - blocking the sequence of events of certain operations [accessing]), by instructing the server to block (para [0225] - updated permission instructions [to server]) or delete the data sent to the recipient (para [0245] - blocking one or more user actions based on the content-utilization restriction).

Regarding claim 22, Livnat teaches even if the data from the recipients computer (para [0248] - downloading a byte stream [on recipient's device]), is used on any other computer (para [0082] - other form of utilizing the protected file, while a second allowed user), it cannot be accessed (para [0082] - user may not be permitted to perform any of copy-pasting the content of the protected file), used or processed (para [0003] - not allowing the first user to copy, print and/or save the content), due to lack of permissions from the data owner (para [0082] - who cannot gain access to the protected file; and/or to define one or more utilization-restrictions to be selectively applied on one or more of the users).

-----continued in Supplemental Box-----

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/IB 10/52959

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:
Box V.2. Citations and explanations:

Regarding claim 23, Livnat teaches in case the software (para [0006] - restricts and/or prohibits the installation of client software) is required to be reinstalled (para [0006] - require the installation of special client software on each user's computer), an easy method (para [0008] - methods of file-utilization management) of reinstallation is provided (para [0098] - install client application 140, and may use the installed client application 140 to verify) to the software user (para [0015] - downloading the secure web application to the computing device) and the server sends (para [0016] - providing a file encryption key to the secure web application) the encryption and decryption keys (para [0100] - public keys 153 assigned; also see plurality of keys may be use such as 155, 157 as shown in fig. 1) again to the software (para [0016] - providing a file encryption key to the secure web application) after activation (para [0254] - activation...function of the internal playable file). It also sends (para [0016] - providing a file encryption key to the secure web application) the previously registered (para [0144] - register) R2 keys (para [0157] - key 150 (FIG. 1) to client application) of other user's into the software (para [0128] - installed client application 140 (FIG. 1)).

Regarding claim 24, Livnat teaches incase during reinstallation (para [0111] - report the detected action) or each time the software is opened (para [0111] - report the detected action back to server application), it is detected (para [0147] - detecting the authentication) that there is the motherboard id (para [0182] - detecting a received response including second authentication information (identification info) of the computer has changed (para [0107] - tag [hardware ID] provided by the computing device is not valid; also see para [0213] - detect the change in the permissions), then the software will have to be revalidated (156 of fig. 1) with the server (para [0260] - validation, integrity checking) and also the R2 keys (para [0016] - providing a file encryption key) will have to be revalidated (para [0260] - validation, integrity checking) again by the data owners (110 of fig. 1) only then the data sharing from these owners can occur (para [0072] - share one or more files while ensuring the confidentiality of the shared files).

Regarding claim 25, Livnat teaches the system can also be used as an independent (para [0193] - include encrypting the file using an encryption key to generate a protected file including the encrypted file; also see fig. 1) encryption module (para [0002] - protecting and/or securing information) to secure (para [0003] - securing and/or protecting electronic organizational files) data storage (para [0057] - memories or other information storage medium; also see 106 of fig. 1). Kraus further teaches sharing (para [0045] - allow users to interact and share information over the network(s); also see para [0046] - computer that accesses shared network resources provided by another computer, e.g., a server) of ISO data (para [0025] - video file...ISO; also see para [0060] - sharing with others who might be interested in audio tracks on the play list; and para [0066] - owner has authorized another). It would have been obvious to one of ordinary skill in the art to combine the securely sharing of file of Livnat with the teaching of Kraus in order to have more compatibility of the system by supporting sharing of ISO data.

Claims 1-25 have industrial applicability as defined by PCT Article 33(4), because the subject matter can be made or used in industry.

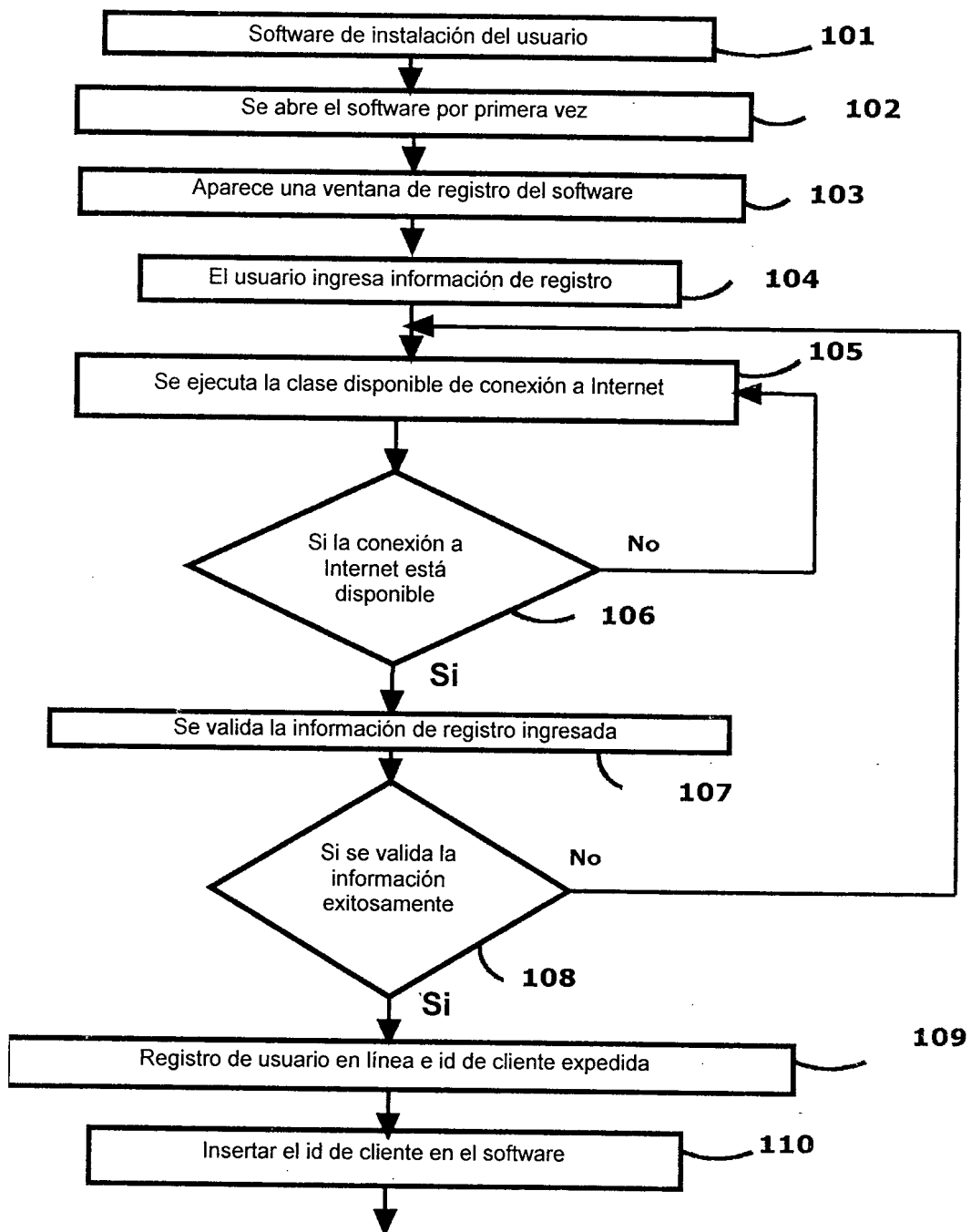


FIGURA 1a

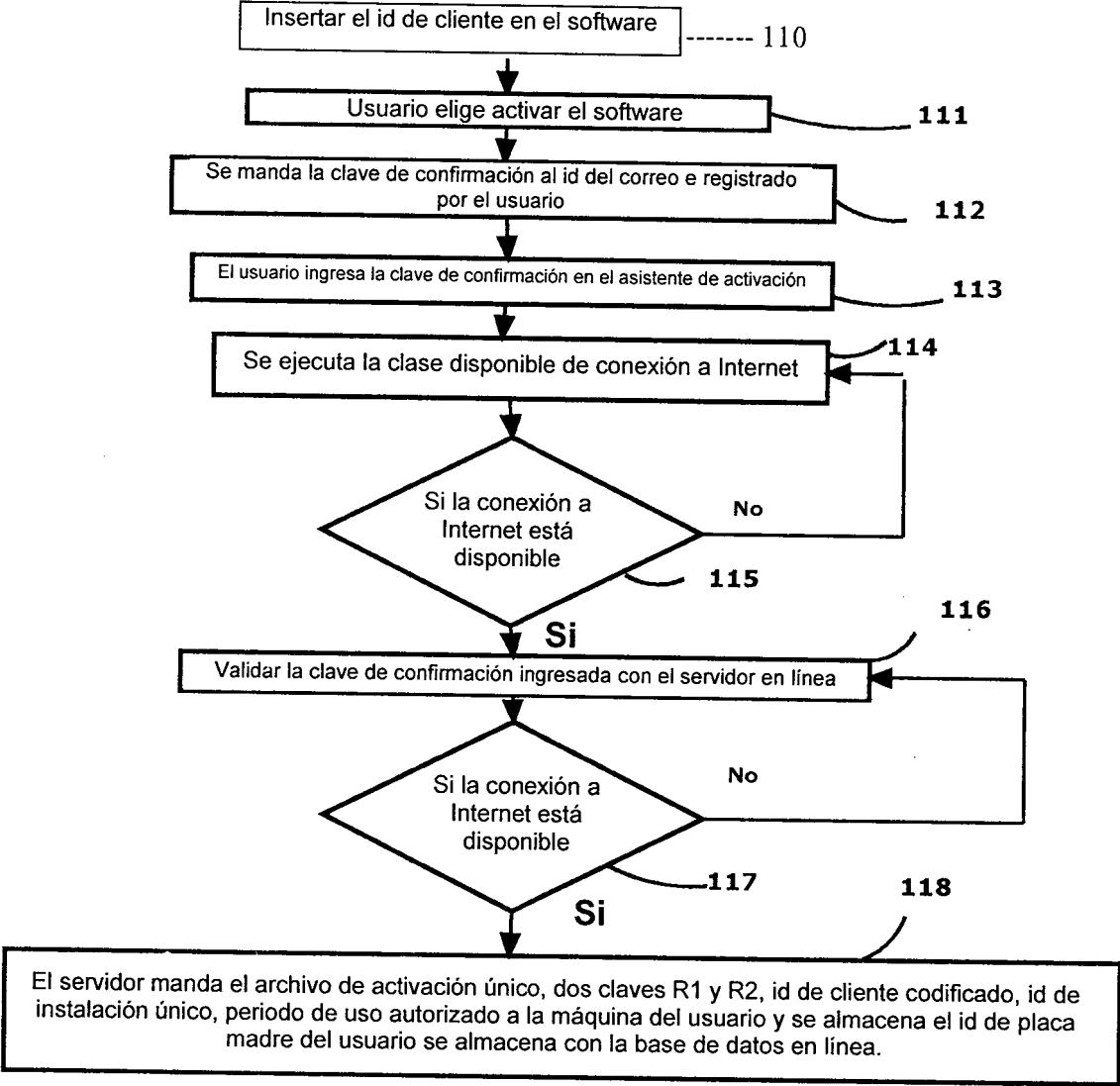


FIGURA 1b

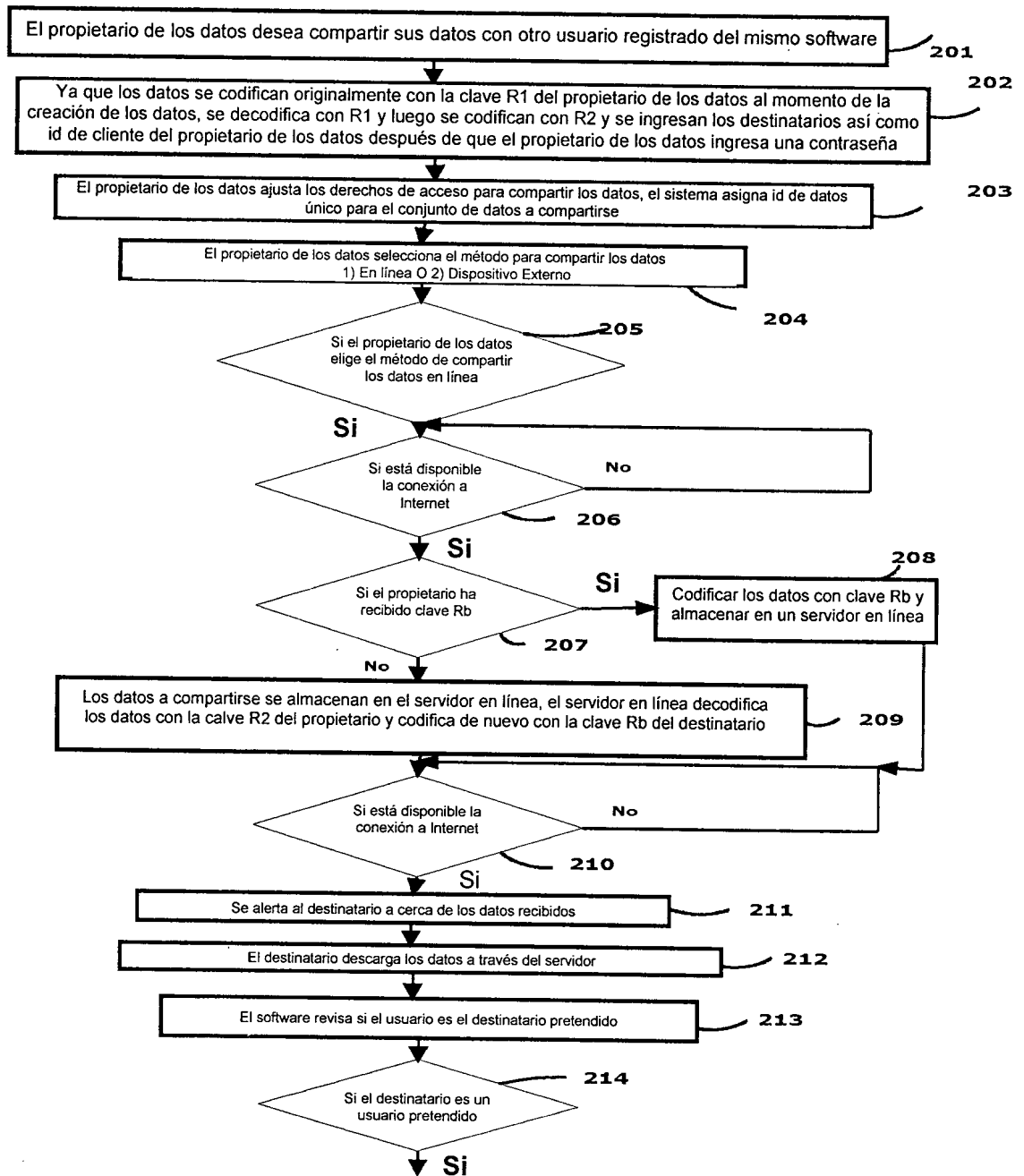


FIGURA 2a

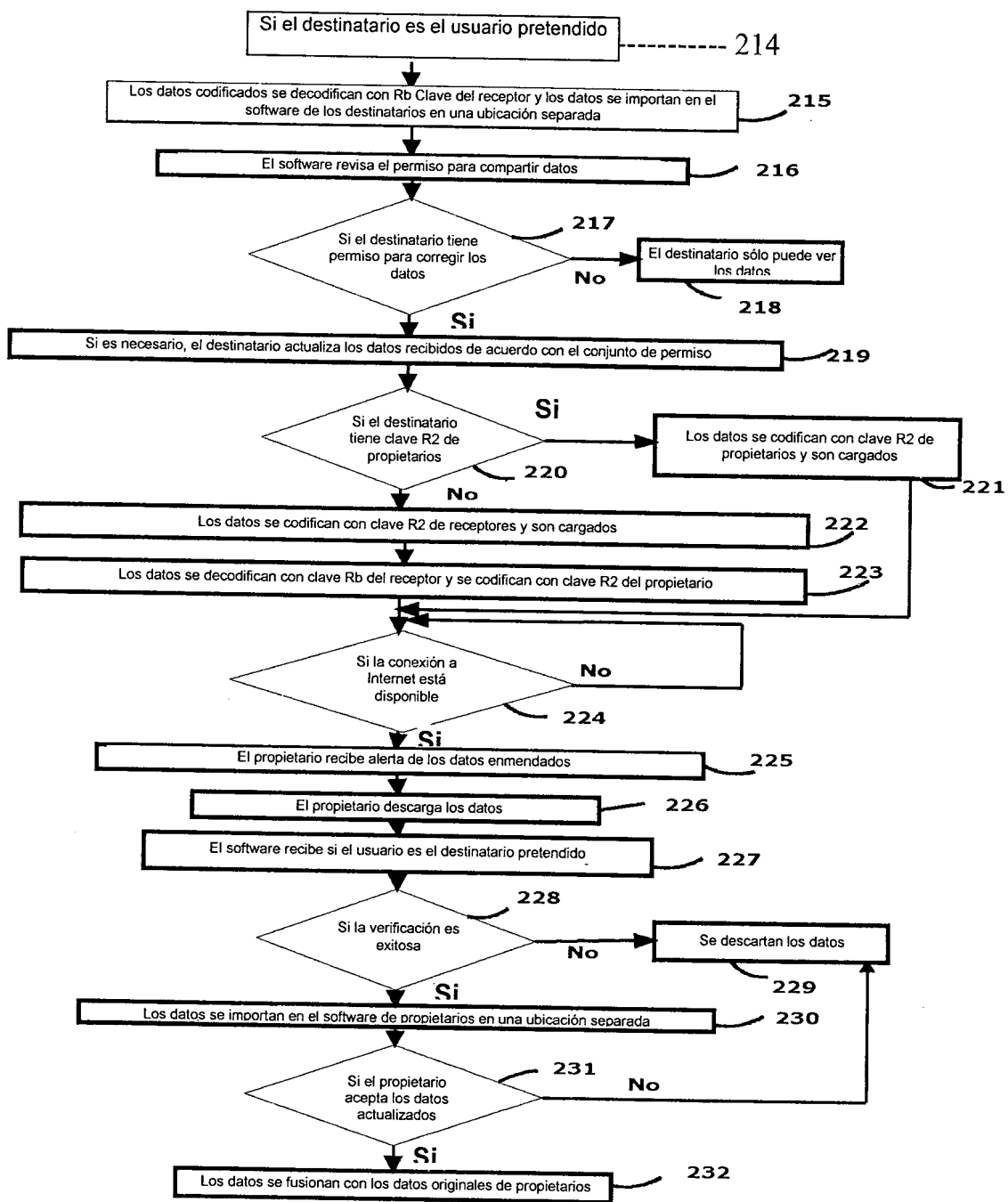


FIGURA 2b

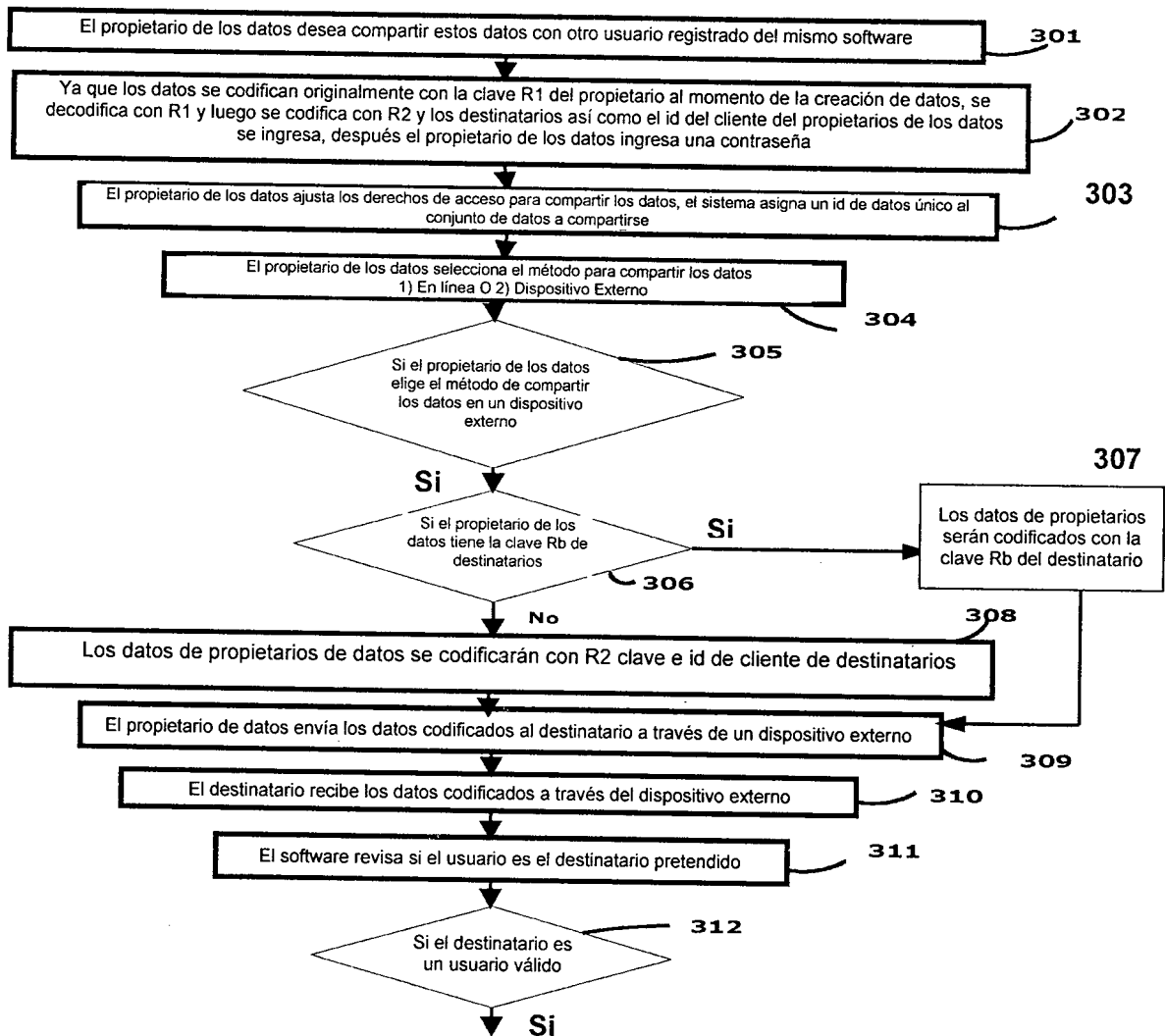


FIGURA 3a

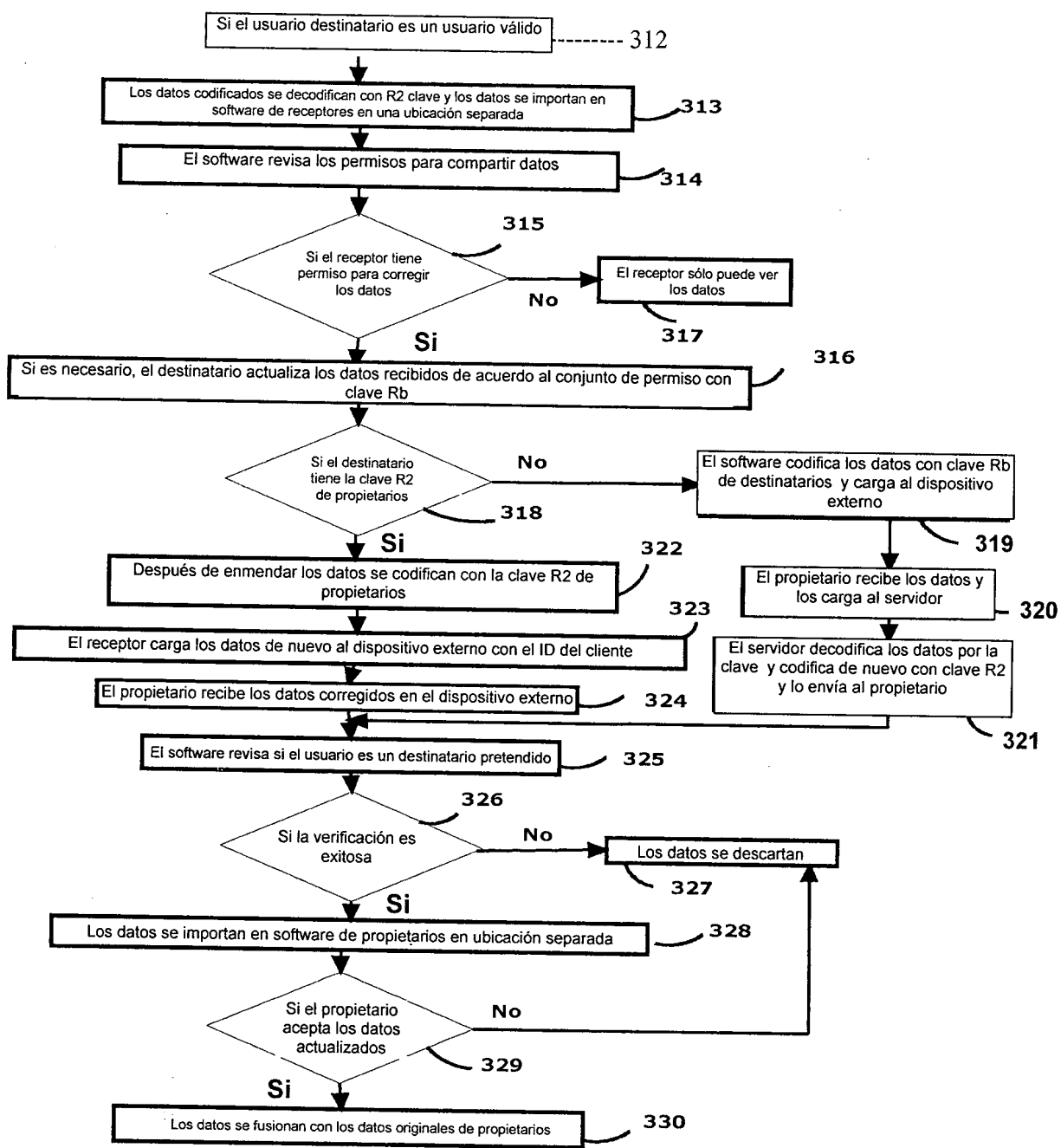


FIGURA 3b

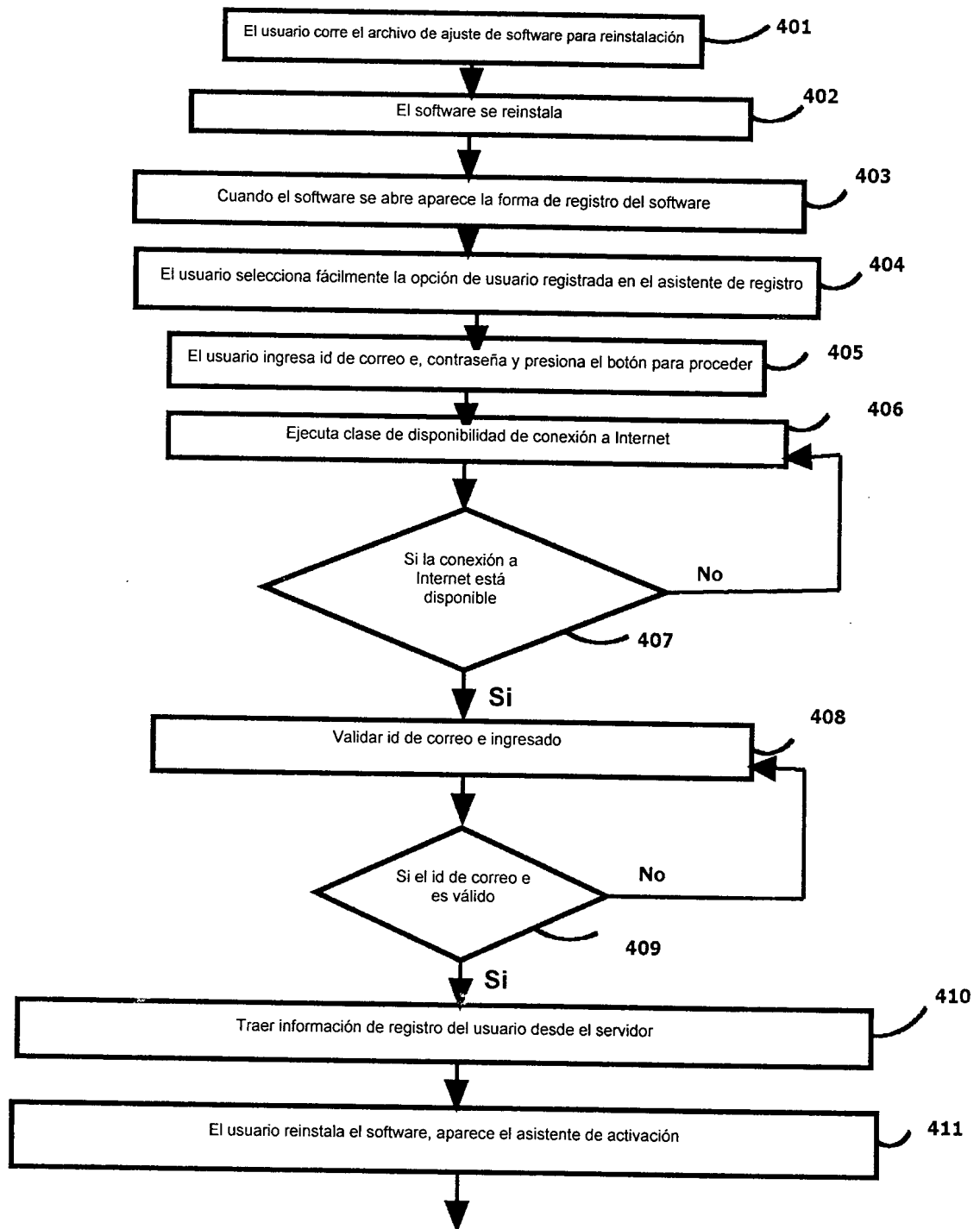


FIGURA 4a

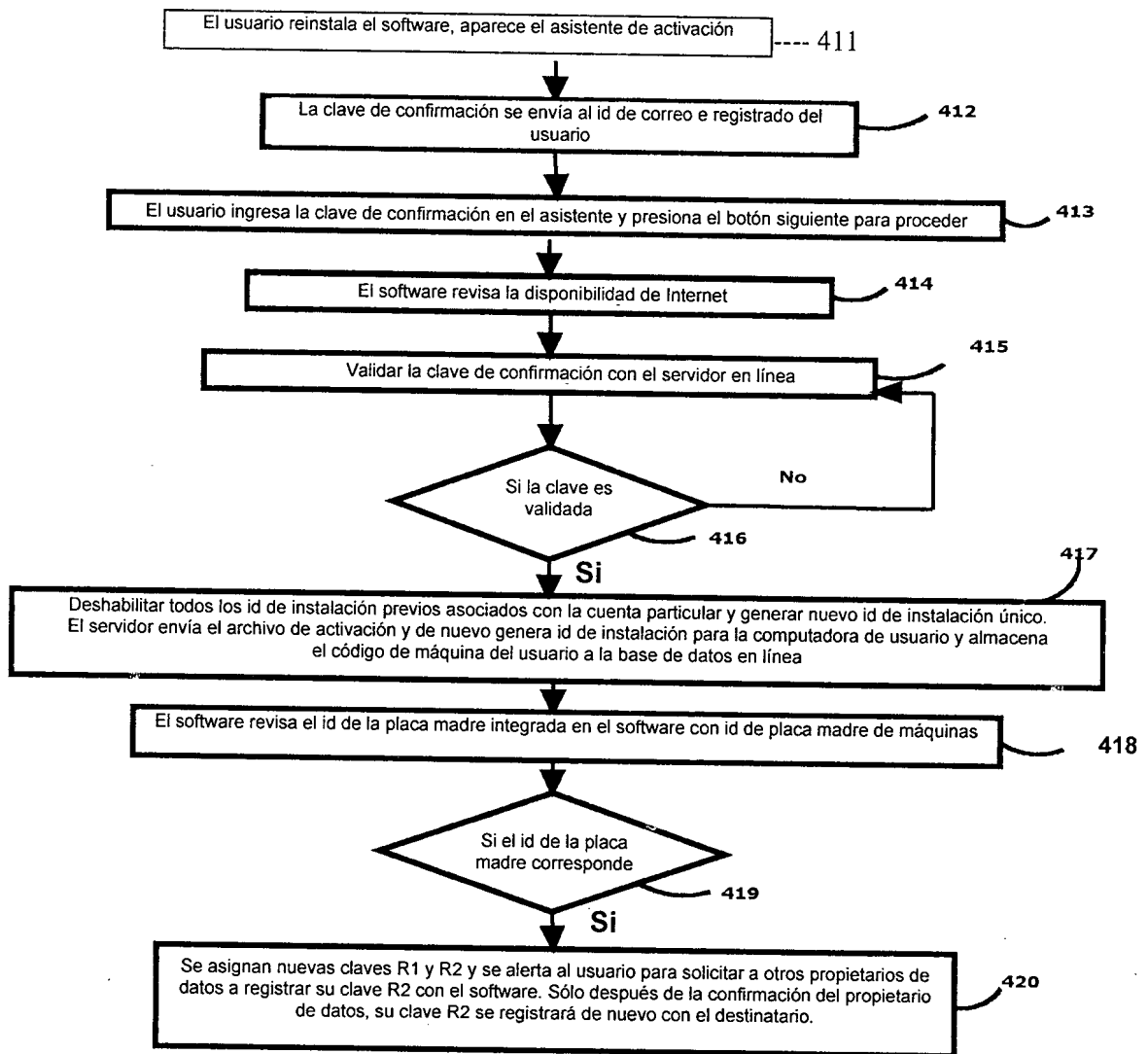


FIGURA 4b

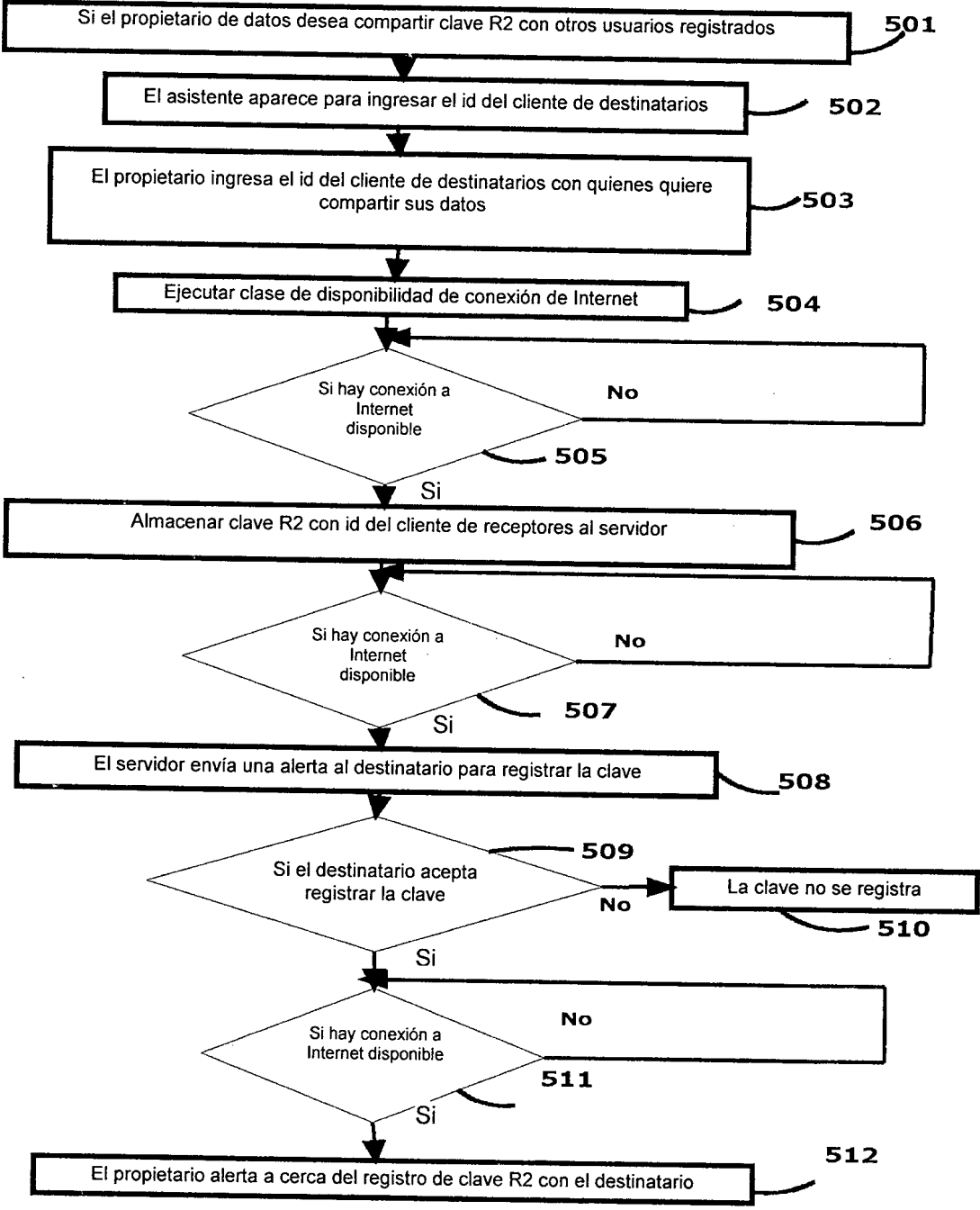


FIGURA 5

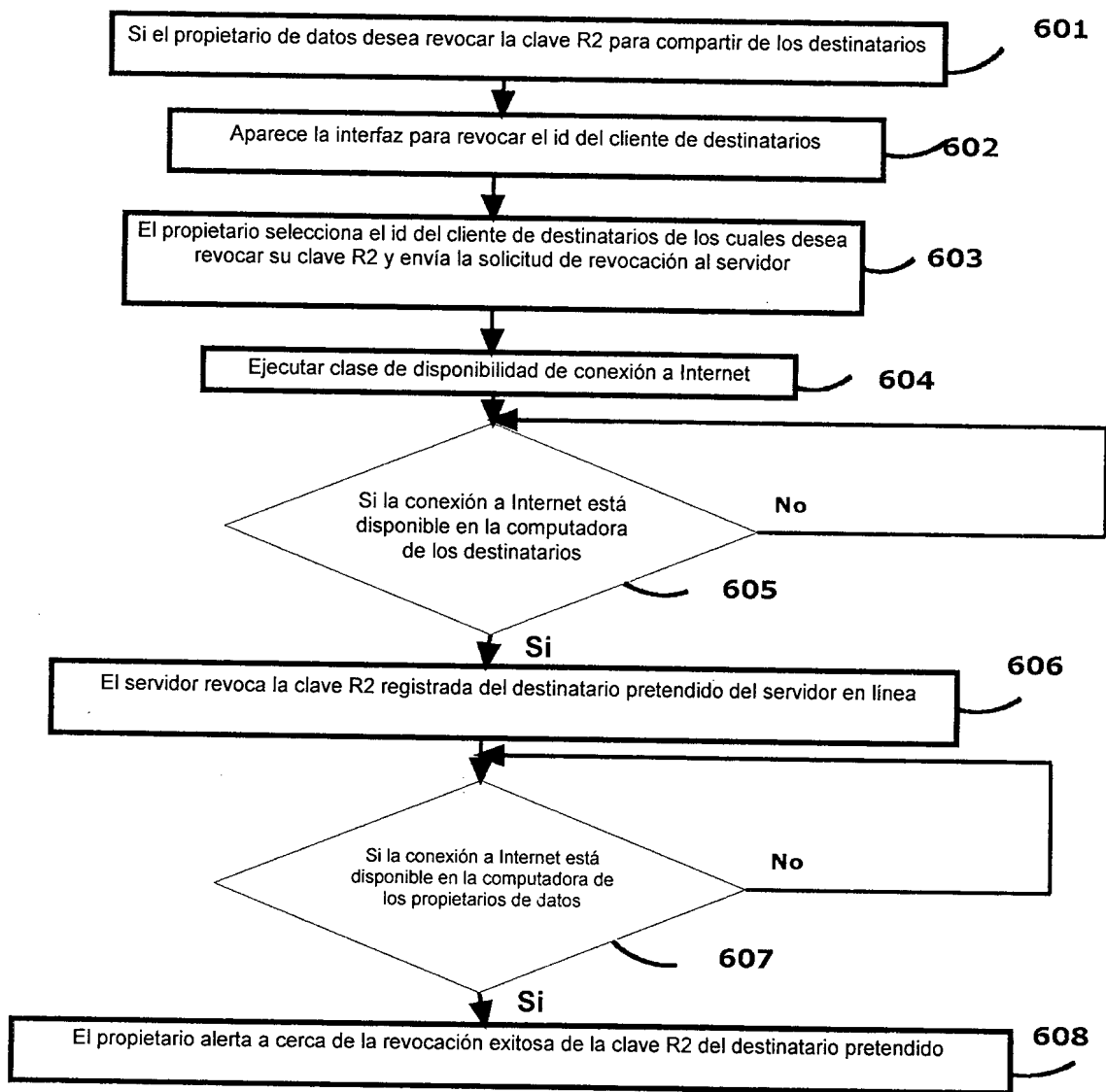


FIGURA 6

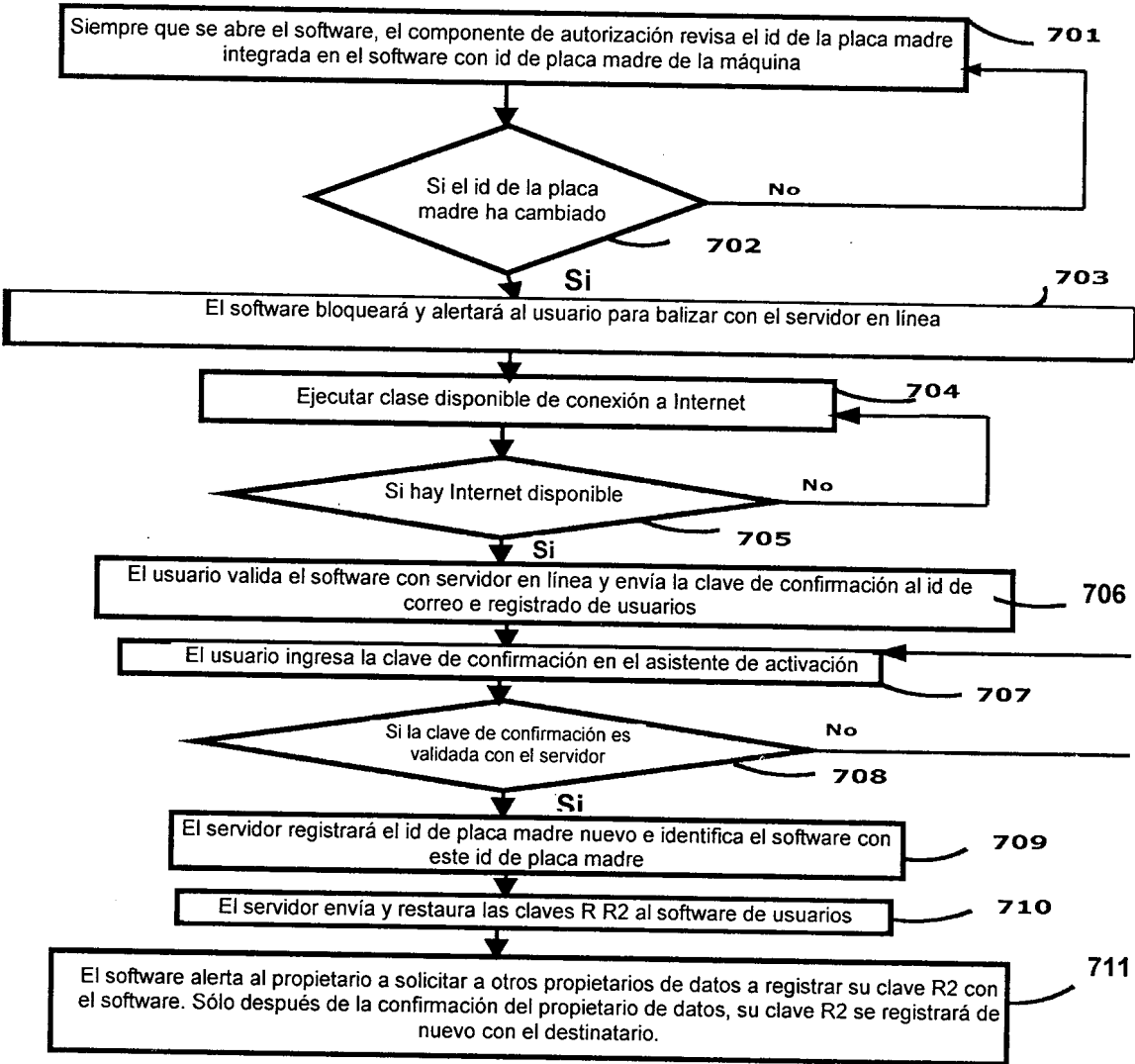


FIGURA 7

MÉTODO PARA CONTROLAR Y SUPERVISAR REMOTAMENTE LOS DATOS

PRODUCIDOS EN UN SOFTWARE DE ESCRITORIO

CAMPO DE LA INVENCION

5 Esta invención se refiere a un método, particularmente a un sistema de datos ISO, que proporciona un mecanismo de protección para salvaguardar del uso no autorizado los datos generados por cualquier software usando el sistema de datos ISO.

10 En particular, el sistema de datos ISO es un método en el cual los datos creados usando el sistema son únicos y exclusivos para el software instalado en una computadora en particular. Los datos se pueden usar solamente en la computadora que los ha creado. Para usar estos datos en otra
15 computadora, se deben proporcionar por el propietario permisos de acceso suficientes para los datos.

ANTECEDENTES DE LA INVENCION

 Muchas veces, los datos son confidenciales en
20 carácter. El mal uso de los datos puede conducir a serias pérdidas debido a lo cual es muy importante protegerlos. La protección de datos comprende tres elementos principales, Confidencialidad, Integridad y Accesibilidad. Confidencialidad significa proteger los datos del acceso no
25 autorizado. Integridad significa que los datos se puedan

modificar solamente si se proporcionan por el propietario de los datos permisos y autorización apropiados. Disponibilidad significa simplemente que los datos puedan estar disponibles cuando se requiera. Las soluciones actuales están disponibles en la seguridad de datos están usando contraseñas, candados de hardware, encriptados y clases similares.

TÉCNICA ANTERIOR

La solicitud de Patente de EUA no. 20090259512 describe un método para controlar el acceso a un dispositivo de almacenamiento de medios para almacenar una pluralidad de objetos de medios, en donde el método incluye recibir los primeros datos que identifican el dispositivo de almacenamiento de medios, y segundos datos que identifican una lista que comprende por lo menos un destinatario autorizado del dispositivo de almacenamiento de medios; almacenar los primeros datos en asociación con los segundos datos; expedir el dispositivo de almacenamiento de medios a por lo menos un destinatario en la lista; usar un identificador de sesión de entrega para establecer una sesión de entrega para el dispositivo de almacenamiento de medios expedido con un sistema de identificación de usuario que corresponde a destinatarios asociados con los segundos datos; y luego actualizar los segundos datos sobre la base de los datos recibidos del sistema de identificación de usuario y el

identificador de sesión de entrega, para modificar en consecuencia la lista de destinatarios autorizados del dispositivo de almacenamiento de medios.

Además también se proporciona un sistema de control
5 de acceso de distribución que controla el acceso a un dispositivo de almacenamiento de medios, el dispositivo de almacenamiento de medios almacena una pluralidad de objetos de medios, el sistema de control de acceso distribuido en donde una interfaz arreglada para recibir los primeros datos
10 que identifican el dispositivo de almacenamiento de medios y los segundos datos que identifican una lista comprende por lo menos un destinatario autorizado del dispositivo de almacenamiento de medios; se proporciona un sistema de almacenamiento arreglado para almacenar los primeros datos en
15 asociación con los segundos datos; y un sistema de expedición de dispositivos arreglado para expedir un dispositivo de almacenamiento de medios a por lo menos un destinatario en la lista. El sistema de expedición de dispositivos se arregla para crear un identificador de sesión de entrega para
20 establecer una sesión de entrega para el dispositivo de almacenamiento de medios expedido con un sistema de identificación de usuario que corresponde por lo menos a un destinatario asociado con los segundos datos, y un sistema de almacenamiento se arregla para actualizar los segundos datos
25 sobre la base de la sesión de entrega y los datos recibidos

del sistema de identificación de usuario, para modificar en consecuencia la lista de destinatarios autorizados del dispositivo de almacenamiento de medios expedido.

5 OBJETIVOS DE LA INVENCION

Mal uso de datos significa acceso y uso no autorizado de datos. Cuando los datos se hacen no utilizables para destinatarios no autorizados, su seguridad ya no sigue siendo un problema. Los sistemas actuales no tienen métodos exhaustivos e infalibles para proteger los datos. Es un objetivo de la presente invención proporcionar un método infalible para protección, acceso y uso de datos por destinatarios no autorizados. Aún si los datos alcanzan accidentalmente un acceso no autorizado, no se pueden usar y procesar. Los datos creados en una computadora particular no se pueden usar en cualquier otra computadora, a menos que el propietario de los datos haya concedido los permisos requeridos para cada computadora en la cual desea que estos datos se compartan. La presente invención también proporciona un sistema de reinstalación de software automatizado, fácil y sin problemas para el usuario.

SUMARIO DE LA INVENCION

El registro del software en el servidor en línea del vendedor es obligatorio para el uso del sistema de datos

ISO, puesto que esta característica se puede usar solamente por usuarios registrados del software. El sistema de registro del software y el sistema de datos ISO van de la mano para la seguridad de datos. Después del registro exitoso del software con el servidor en línea del vendedor, se expide una identificación (id) para el cliente, permanente, única para cada software registrado. Este id del cliente es único e importante y se usa para identificar al usuario del software particular instalado en una computadora particular. Durante la activación del software, es generado un archivo por el servidor. Este archivo se envía al software. Este archivo es desconocido para el usuario y contiene las claves R1 y R2. El servidor genera estas claves y las almacena permanentemente. La función de estas claves es para proteger los datos del software de uso no autorizado. Estas claves se usan para encriptado y desencriptado en etapas requeridas. Tanto R1 como R2 son claves permanentes, únicas para cada software registrado y se asocian con un id del cliente único particular con el servidor en línea del vendedor y con el software instalado único particular. La clave R1 se usa para proteger los datos del software instalados en la computadora particular que son los datos del propietario. La clave R1 no se comparte con ningún otro usuario. Por omisión, los datos creados por el software particular siempre se encriptan y se almacenan con la clave R1 en la computadora en la cual el

software se instala. Es una clave privada. R2 es la clave que se puede registrar con otros usuarios en otras computadoras, si es necesario, con el permiso del propietario y se usa para proteger los datos que están siendo compartidos. Es una clave pública de aquel software único particular.

Ra y Rb son la claves privada y pública del destinatario, respectivamente. Las claves públicas y las claves privadas son confidenciales y no se usarán o se compartirán sin un propósito. El propietario de los datos puede registrar su clave R2 con tantos destinatarios como lo necesite. Estos pueden ser destinatarios a quienes el propietario puede necesitar enviar frecuentemente datos. El propietario de los datos enviará una instrucción al servidor para registrar su clave R2 con los destinatarios, al ingresar los id del cliente del destinatario. También esta instrucción contendrá el id del cliente del propietario de los datos. Cuando el destinatario se conecta al servidor en línea, se mostrará una alerta requiriendo que el destinatario registre la clave R2 del propietario de los datos. Le corresponde al destinatario registrar la clave o no. En cualquier punto de tiempo el propietario de los datos puede revocar el registro de su clave R2 con los otros destinatarios al instruir al servidor hacerlo. El servidor no necesitará el permiso del destinatario para revocar la clave R2 del propietario de los datos registrada con un destinatario particular.

Los datos son información creada mientras se usa el software. Los datos del software se pueden compartir al usar cualquier dispositivo de almacenamiento externo o al subir los datos en línea al servidor del vendedor desde donde los
5 puede descargar el destinatario. El propietario puede establecer permisos de acceso totales o parciales por ejemplo, examinar, leer, imprimir, guardar y enmendar. El control de datos permanece con el propietario de los datos, aún después de compartirlos con otros usuarios. Cada vez que
10 el destinatario autorizado accede a los datos compartidos, el estado de los permisos de acceso se verificará con el servidor en línea, si es necesario. Solamente si aún están activos los permisos de acceso, el destinatario puede acceder a los datos si no, el destinatario será alertado de que los
15 permisos de acceso de los datos ya no son válidos. El propietario de los datos también puede enviar una instrucción al servidor en línea para suprimir los datos si es necesario, que ha compartido de la computadora del destinatario autorizado. El proceso y almacenamiento de los datos
20 originales y los datos que se reciben para compartir, se procesan a través de dos subsistemas diferentes y mutuamente exclusivos que soportan el sistema de encriptado respectivamente, y los datos se almacenan en dos ubicaciones separadas en la misma computadora/sistema respectivamente.
25 Los datos se pueden proteger del uso no autorizado, usando el

sistema de datos ISO. El proceso para asegurar el uso autorizado de los datos, usando el sistema de datos ISO, se explica adicionalmente. En la presente modalidad, el medio ambiente contiene un propietario de datos, un destinatario
5 con quien el propietario de datos necesita compartir los datos y un servidor en línea. El propietario puede compartir datos con otros usuario registrados. El destinatario puede o no tener la clave R2 del propietario de datos registrada con el mismo. En ambos casos, el intercambio de datos se puede
10 hacer por dos métodos, ya sea al subir el conjunto/paquete de datos que se comparten al servidor en línea, o al copiar los datos a ser compartidos en cualquier dispositivo de almacenamiento externo y compartir este dispositivo con el destinatario propuesto.

15 Considérese que el destinatario no tiene la clave R2 del propietario de datos y el propietario de datos desea compartir los datos al subirlos al servidor en línea. Puesto que los datos a ser compartidos ya están en una forma encriptada con la clave R1 del propietario de datos, se
20 descripta por la misma clave R1 y luego se encripta usando la clave R2 en la computadora del propietario de datos que se controla por un mecanismo de contraseña estándar cada vez.

También el id de cliente del destinatario así como también el remitente se ingresan en estos datos. Cada
25 conjunto/paquete de datos compartido por el propietario de

datos contendrá un id de datos particular generado por el sistema del propietario de los datos. El id de los datos determinará la especificidad de cada conjunto de datos enviados a ser compartidos y también ayudará en el manejo de los datos. Los permisos de acceso y la información correspondiente de cada conjunto de datos se asocian con su id de los datos. El servidor mantendrá un registro de todos los conjuntos/paquetes de datos, todos los atributos asociados con sus id de los datos correspondientes. Estos datos luego se suben al servidor en línea donde se desenscriptan nuevamente usando la clave R2 del propietario de los datos y se convierten en forma normal/original. Estos datos luego se encriptan con la clave Rb del destinatario. El servidor en línea envía una alerta al destinatario que ciertos datos están esperando a ser compartidos. El destinatario luego descarga estos datos y los desenscripta usando la clave Rb del destinatario de los datos.

Los mismos datos se pueden proporcionar a través de un dispositivo de almacenamiento externo al destinatario. En este caso el destinatario subirá estos datos al servidor en línea. El servidor verificará si el propietario de los datos, ha establecido el permiso para el destinatario particular, el id del cliente que ha subido los datos y solamente si los permisos se establecen los datos serán procesados y se enviarán de nuevo al destinatario. Si los permisos no se

conceden por el propietario de los datos, el servidor en línea suprimirá los datos de la computadora del destinatario. Cuando el usuario sube estos datos al servidor en línea se llevará a cabo el desenscriptado y encriptado como se explica en lo anterior y cuando el destinatario se conecta al servidor en línea puede descargar y usar estos datos. Se considera ahora que el destinatario tiene la clave R2 del propietario de los datos registrada con el mismo. Nuevamente el propietario de los datos puede compartir los datos al subirlos al servidor en línea o al almacenar los datos a un dispositivo de almacenamiento externo y compartir este dispositivo con el destinatario. En este caso los datos encriptados se desenscriptan usando la misma clave R1 y se encriptan nuevamente usando la clave R2 del propietario de los datos. El destinatario puede ya sea descargar estos datos del servidor o del dispositivo de almacenamiento externo; sin embargo el propietario de los datos los ha enviado. Puesto que el destinatario ya tiene la R2 del propietario de los datos registrada, los datos se pueden desenscriptar usando la clave Rb del propietario y usarlos.

Aún si los datos alcanzan accidentalmente el software no autorizado que tiene la clave R2 del propietario de los datos, los datos no serán accedidos ya que el ID del cliente del software en el cual los datos están siendo

abiertos diferirán con el id del cliente instruido en la autorización.

Los datos compartidos se pueden usar solamente con la autenticación del servidor y se almacenan en una ubicación
5 separada de la ubicación original. El destinatario descargará los datos y los importará en el software. Los datos se pueden usar como para los derechos de acceso proporcionados con los datos. Los derechos de acceso podrían ser de dos tipos, uno es la revisión solamente de donde los datos se pueden revisar
10 solamente, no guardar y segundo es acceso total o parcial para usar o cambiar los datos. Los datos se comportarán solamente en la forma en que el acceso de datos y los permisos de uso se han establecido por el propietario de los datos. Por ejemplo, los datos se pueden usar para x número de
15 días, x número de horas, x número de veces, los datos pueden o no ser enmendados, los datos pueden o no ser guardados, los datos pueden o no ser impresos.

En caso de que el destinatario enmiende los datos y desee compartirlos de nuevo con el propietario de los datos,
20 lo mismo se puede hacer por medio de cuatro métodos. En el método 1, a considerar, el destinatario no tuvo la clave R2 del propietario de los datos. El destinatario encriptará los datos que se envían de nuevo al propietario con su clave Rb. Estos datos que se pueden enviar al propietario de los datos
25 a través de dos métodos; uno mediante el cual el destinatario

sube los datos al servidor en línea en donde el servidor convierte los datos encriptados con la clave Rb a la clave R2 del propietario de los datos y envía estos datos al propietario de los datos en su conexión con el servidor en
5 línea. El propietario de los datos descarga estos datos y los convierte de clave R2 a clave R1 a fin de usarlos. El destinatario puede adoptar un segundo método para proporcionar los datos encriptados con la clave Rb que se comparte con un dispositivo de almacenamiento externo. En
10 este caso, el propietario de los datos recibirá el dispositivo de almacenamiento externo y subirá estos datos recibidos al servidor en línea donde el servidor convertirá los datos de clave Rb a clave R2 y el propietario de los datos puede descargar estos datos y convertir los datos de
15 clave R2 a clave R1 y usar los datos.

En el método 2, se considera que el destinatario tiene la clave R2 del propietario de los datos; en este caso, nuevamente el destinatario puede enviar los datos enmendados de nuevo al propietario de los datos a través de un
20 dispositivo de almacenamiento externo o a través de subir los datos a ser compartidos al servidor en línea. En ambos casos los datos se encriptan usando la clave R2 del propietario de los datos y se envían. El propietario de los datos puede descargar estos datos a través del servidor en línea o del
25 dispositivo de almacenamiento externo sin embargo el

destinatario ha enviado y convertido los datos de R2 a R1 y usa los mismos.

La enmienda de los datos se mostrará al propietario de los datos, solamente si acepta la enmienda, los datos se
5 importarán y se fusionarán. Se le proporcionará una facilidad al propietario de los datos para fusionar los datos que se han enmendado por el destinatario. Los datos que van a ser compartidos, enmendados se mantienen en una ubicación separada de la ubicación original del software y no
10 interfieren de ninguna manera con los datos/registros originales de ambos software del usuario hasta que se proporcione una instrucción de hacerlo. El propietario de los datos puede mantener la copia original si es requerido antes del amalgamado/integración de los cambios del destinatario.
15 Se aplicará el mismo procedimiento si el propietario de los datos desea compartir los datos con más de un destinatario.

En caso de que surja una necesidad para que el usuario reinstale el software, se abrirá un asistente de reinstalación. Este asistente tomará la entrada del id del
20 correo electrónico del usuario. Después de la verificación, los detalles de la cuenta serán descargados del servidor y el software se reinstalará. El servidor enviará una clave de confirmación al id del correo electrónico registrado del usuario. La clave de confirmación es válida solamente para
25 una transacción particular y se asocia con el archivo de

activación de ese software. El usuario tiene que ingresar la clave de confirmación enviada al id del correo electrónico registrado, dentro de este asistente de activación después de lo cual se envía un archivo de activación al software del servidor. En caso de que los id de la tarjeta madre de la computadora se igualen con el id de la tarjeta madre registrado con el servidor en línea cuando el software se registró, las claves R1, R2 se restaurarán por el servidor en el software. El usuario tendrá que enviar una petición de nuevo a los otros usuarios para volver a registrar sus claves R2 con su software. En caso de que el id de la tarjeta madre de la computadora difiera durante el tiempo de la instalación, el software se instalará pero las claves R2 registradas previamente con el servidor no se registrarán nuevamente debido a la discrepancia encontrada en el id de la tarjeta madre y el software también alertará al usuario para que envíe nuevamente la petición a los diversos propietarios de los datos para el nuevo registro de sus claves R2 con el software.

20 Cada vez que el software se abre, un componente de autorización iguala el id de la tarjeta madre incrustado en el software con el id de la tarjeta madre de la computadora. En caso de que se encuentre una discrepancia en el id de la tarjeta madre, el software se bloqueará y alertará al usuario a validarse con el servidor en línea. Una vez que el usuario

se valida con el servidor en línea, se enviará una clave de confirmación al id del correo electrónico registrado del usuario después de lo cual las claves R1 y R2 se enviarán y se restaurarán al software. El software también alertará al usuario de enviar nuevamente la petición a los diversos propietarios de los datos para un nuevo registro de su clave R2 con el software. Solamente después de la confirmación del propietario de los datos, su clave R2 se registrará con el destinatario nuevamente. Cada vez que la computadora se conecta en internet, el servidor verificará el estado de la clave R2 que se registra con el software. Si el servidor observa que la clave R2 de un propietario de los datos particular, ha sido revocada, revocará el registro de esta clave R2 con el destinatario. Similarmente, el destinatario también puede remover el registro de una clave R2 particular al informar al servidor. En este caso el propietario de los datos será alertado acerca de su clave R2 que no se registra por un destinatario particular.

20 **VENTAJAS Y APLICACIONES**

El sistema de datos ISO del método de la presente invención ayuda al propietario del software a proteger sus datos de software de acceso no autorizado. El propietario del software puede establecer restricciones en el uso de datos por el destinatario. Los datos se pueden compartir mediante

cualquier disco duro externo o al subirlos al servidor en línea.

En vista de la amplia variedad de modalidades a las cuales se pueden aplicar los principios de la presente invención, se debe entender que las modalidades ilustradas son ejemplares solamente. Las modalidades ilustradas no se deben tomar como limitantes del alcance de la presente invención. Aunque varios elementos de las modalidades preferidas se han descrito por ser implementadas, otras implicaciones de las modalidades se pueden usar alternativamente y viceversa.

BREVE DESCRIPCIÓN DE LA FIGURAS

La Figuras 1a y 1b ilustran el proceso de registro del software y uso de datos por el propietario.

Las Figuras 2a y 2b ilustran el procedimiento para el intercambio de datos en línea.

Las Figuras 3a y 3b ilustran el proceso de intercambio de datos usando un disco duro externo similar a un disco compacto.

Las Figuras 4a y 4b ilustran el proceso de software de reinstalación y reasignación de claves.

La Figura 5 ilustra el proceso de compartir la clave R2 con varios destinatarios potenciales.

La Figura 6 ilustra el proceso de revocar la clave R2 de destinatarios potenciales.

La Figura 7 ilustra el proceso de autorización.

5

DESCRIPCIÓN DETALLADA DE LA INVENCION

El programa de sistema de datos ISO es un programa de código de bites escrito en el lenguaje de programación de Microsoft.NET.

La descripción proporciona en general un método
10 para proteger los datos del usuario de acceso no autorizado. Un método para registrar un usuario al servidor en línea incluye recibir un acceso inicial al software de escritorio por un usuario prospectivo, y determinar si el usuario ha proporcionado información de identificación del usuario
15 válida. Con referencia a la Figura 1a, el usuario instala el software a su computadora al ejecutar la función 101, en la instalación exitosa el usuario está listo para usar el software. El usuario hace clic sobre el software ejecutable por primera vez para ejecutar el software, el método 102 se
20 activa. Cuando el propietario usa el software por primera vez, aparecerá la ventana de registro de software 103 para registrar al usuario al servidor en línea del vendedor desde el software de escritorio. El propietario ingresa la información de registro a través del 104 en el asistente de
25 registro 103. Si la conexión a internet 105 está disponible

verifica la integridad del método 105 asociado con cada objeto cargado, si el método 106 se ejecuta exitosamente el método 107 valida la información del usuario en la activación exitosa de 108, el usuario se registra al servidor en línea
5 del vendedor al activar el método 109 y el servidor expide un id del cliente único al usuario e incluye el id del cliente en el software al ejecutar el método 110. El método 111 (como es referido en la Figura 1b) se activa para mostrar el asistente de activación, el usuario selecciona la opción de
10 suscripción, es decir, el método de prueba o suscripción 112 se activa para enviar la clave de confirmación al id del correo electrónico registrado del usuario. El usuario ingresa la clave de confirmación en el asistente de activación al ejecutar la función 113, el software ejecuta la clase de
15 disponibilidad de conexión a internet 114 para verificar la conexión de internet si el internet está disponible, entonces la función 116 ejecuta para validar la clave de confirmación con la base de datos en línea al ejecutar la clase de disponibilidad de internet 117. Con la validación exitosa el
20 servidor envía el archivo de activación con el id del cliente encriptado 118, este archivo de activación también contiene dos claves únicas R1 y R2 para encriptado y desencriptado de los datos de software, id de instalación, período de uso autorizado transferido del servidor en línea a la máquina del
25 usuario y almacenar el id de la tarjeta madre del usuario a

la base de datos en línea. El software crea la base de datos encriptada con la clave R1 del propietario.

Con referencia a la Figura 2a, si el propietario de los datos desea compartir sus datos con otro destinatario registrado al ejecutar el método 201, ya que los datos se encriptaron originalmente con la clave R1 del propietario de los datos en el momento de la creación de los datos, los datos del software se desencriptan con la clave R1 del propietario de los datos y luego se encriptan usando la clave R2 del propietario de los datos después de que el propietario de los datos ingresa una contraseña y el id del cliente se ingresa al ejecutar el método 202; el propietario establece los permisos de acceso de datos, el sistema asigna un id de los datos a este conjunto de datos al ejecutar la función 203. El usuario necesita seleccionar el método para compartir los datos 204. Si el usuario selecciona el método de intercambio de datos en línea al ejecutar el método 204, y si la conexión de internet está disponible, el software verifica la integridad del método 206 asociado con cada objeto cargado. Si el método 206 se ejecuta exitosamente, se activa 207 para verificar si el propietario tiene la clave Rb del destinatario, si el propietario tiene la clave Rb del destinatario entonces la función 208 se ejecuta para encriptar los datos con la clave Rb y los almacena en el servidor en línea si no el método 209 se ejecuta para

almacenar los datos en el servidor en línea con la clave R2, el servidor en línea descripta los datos con la clave R2 del propietario de los datos y encripta los datos nuevamente con la clave Rb del destinatario. Si la conexión a internet está disponible el verificador de software 210 verifica la integridad del método 210 asociado con cada objeto cargado, si el método 210 se verifica exitosamente se activa 211 para alertar al destinatario acerca de los datos. El destinatario descarga los datos del propietario a través del servidor al ejecutar el método 212. Si el método 214 se verifica exitosamente se activa 215 (como es referido en la Figura 2b) para descriptar los datos con la clave Rb del receptor y los importa en el software del receptor en una ubicación separada. El verificador de software 216 verifica el permiso de intercambio de datos, el software verifica si el destinatario tiene permiso para enmendar los datos al ejecutar 217; si el método 217 se ejecuta exitosamente, entonces el método 219 se activa para enmendar los datos de acuerdo con el permiso establecido. Si el permiso se niega para enmendar los datos, el destinatario solamente puede observar los datos 218.

Después de la terminación de la enmienda de los datos; la función 220 verifica si el destinatario tiene la clave R2 del propietario si 220 se ejecuta exitosamente, el método 221 se activa para encriptar los datos con la clave R2

del propietario y los sube al servidor en línea, si no los datos enmendados se encriptan con la clave Rb del destinatario y suben los datos de nuevo al servidor al ejecutar el método 222. En el servidor, los datos se
5 desenscriptan con la clave Rb del destinatario y se encriptan nuevamente con la clave R2 del propietario de los datos al ejecutar el método 223. Después de esto el propietario obtendrá la alerta de datos enmendados por el método 225, si la conexión a internet está disponible el verificador de
10 software 224 verifica la integridad del método 224 asociado con cada objeto cargado, si el método 225 logra alertar al propietario, el método 226 se activa para descargar los datos. El software verifica si el usuario es el destinatario propuesto al ejecutar el método 227 y si la verificación del
15 usuario es correcta entonces el verificador 228 verifica la integridad del método 228 asociado con cada objeto cargado, si el método 228 se verifica exitosamente se activa 230 por el propietario para importar los datos en el software en una ubicación separada y si la verificación no se logra entonces
20 los datos se eliminan al ejecutar el método 229. Si el propietario acepta los datos al ejecutar el método 231, el método 232 se activa para fusionar los datos en los datos originales.

Con referencia a la Figura 3a, si el propietario de
25 los datos desea compartir sus datos con otros destinatarios

registrados al ejecutar el método 301, puesto que los datos se encriptan originalmente con la clave R1 del propietario de los datos en el momento de la creación de los datos, el software desencripta los datos usando la clave R1 y luego

5 encripta los datos usando la clave R2 al ejecutar el método 302; esto se lleva a cabo solamente después de que el propietario de los datos ingresa una contraseña para ejecutar esta transacción. El propietario establece los permisos para enmendar los datos y se asigna un id de los datos únicos a

10 este conjunto de datos al ejecutar la función 303. El propietario selecciona el método para compartir los datos 304, es decir, a través del método en línea o a través de un disco externo. Si el propietario de los datos selecciona el método de intercambio de datos a través del disco externo al

15 ejecutar el método 305, la función 306 se activa para verificar si el propietario tiene la clave Rb del destinatario si el propietario tiene la clave Rb del destinatario entonces la función 307 se ejecuta para encriptar los datos con la clave Rb y los almacena en el

20 servidor en línea si no, el método 308 se ejecuta para encriptar los datos con la clave R2 y los detalles del receptor. El propietario envía los datos encriptados al destinatario a través del disco externo al ejecutar el método 309. El receptor acepta los datos al ejecutar el método 310.

25 El software verifica la validez del usuario al cotejarse con

el id del cliente al ejecutar el método 311, el verificador de software 312 verifica la integridad del método 312 asociado con cada objeto cargado, si el método 312 se verifica exitosamente se activa 313 (como es referido en la

5 Figura 3b) para descriptar los datos e importarlos en el software del destinatario. El verificador 314 verifica el permiso establecido para la enmienda de los datos, si el destinatario tiene permiso para enmendar los datos al ejecutar 315, si el método 315 se ejecuta exitosamente

10 entonces el método 316 se activa para descriptar los datos con la clave Ra asociada con el receptor si no, el receptor puede observar solamente los datos al ejecutar el método 317. Con esto el destinatario actualiza los datos del propietario de acuerdo con el permiso establecido al ejecutar el método

15 316, después de la terminación de la enmienda de los datos; la función 318 verifica si el destinatario tiene la clave R2 del propietario, si 318 se ejecuta exitosamente los datos actualizados se encriptan con la clave R2 del propietario al ejecutar los métodos 322. El destinatario sube los datos

20 nuevamente al disco duro externo al ejecutar la función 323, el propietario obtendrá el disco duro de los datos actualizados por el método 324. Si no el software encripta los datos con la clave Rb del destinatario y los sube nuevamente al disco externo al ejecutar el método 319, el

25 propietario recibe los datos y los sube al servidor al

ejecutar el método 320, al final del servidor en línea descripta los datos con la clave Rb y los encripta nuevamente con la clave R2 y los envía al propietario al ejecutar el método 321. El software verifica si el usuario es
5 el destinatario propuesto al ejecutar el método 325 y si la verificación del destinatario es correcta entonces el verificador 326 verifica la integridad del método 326 asociado con cada objeto cargado, si el método 326 se verifica exitosamente se activa 328 por el propietario para
10 importar los datos en el software y si la verificación falla, los datos se eliminan al ejecutar el método 327. Si el propietario acepta los datos al ejecutar el método 329, se activa el método 330 para fusionar los datos recibidos en los datos originales del propietario. De acuerdo con este
15 escenario los datos proporcionados se protegen de acceso no autorizado.

Con referencia a la Figura 4a, si el usuario necesita reinstalar el software debido a cualquier razón se activa el método 401. El usuario reinstala el software al
20 ejecuta la función 402. El método 403 se ejecuta mientras el usuario hace clic para activar el software, aparecerá la ventana de registro de software 404, el usuario ingresa el id del correo electrónico registrado y la contraseña y hace clic en siguiente, continua al ejecutar la función 405. Si la
25 conexión a internet está disponible 406 verifica la

integridad del método 406 asociado con cada objeto cargado, si el método 407 se verifica exitosamente, se activa 408 para verificar la información de registro ingresada con la base de datos del servidor en línea del vendedor si la información del registro se valida exitosamente, 409 verifica su integridad asociada con cada objeto cargado, si el método 409 se verifica exitosamente se activa 410 para descargar toda la información del cliente quien ya se ha registrado al servidor en línea. El método 411 reinstala el software y activa el método 412 (como es referido en la Figura 4b) para enviar la clave de confirmación al id del correo electrónico registrado del usuario, el método ingresa la clave de confirmación y hace clic en siguiente al ejecutar el método 413. El software valida la clave de confirmación 415 con la base de datos en línea, si la clave se valida por 416 entonces desactiva todos los id de instalación previos para el usuario particular y genera un nuevo id de instalación único, la máquina de almacenamiento codifica la base de datos en línea al ejecutar la función 417. El software verifica el id de la tarjeta madre incluido en el software con el id de la tarjeta madre de la máquina al ejecutar el método 418. El verificador 419 verifica exitosamente el id de la tarjeta madre se ejecuta la función 420 para asignar nuevas claves R1 y R2 al usuario y alertar al usuario de enviar nuevamente la petición a los diversos propietarios de los datos para el nuevo registro de

su clave R2 con el software. Solamente después de la confirmación del propietario de los datos, su clave R2 se registrará otra vez con el nuevo destinatario.

Con referencia a la Figura 5, si el propietario
5 desea compartir la clave R2 con otros usuarios registrados se activa el método 501. El asistente 502 se presenta para ingresar el id del cliente de los destinatarios. El propietario ingresa el id del cliente de los destinatarios con quienes desea compartir sus datos al ejecutar la función
10 503, si la conexión a internet está disponible el verificador de conexión 504 verifica la integridad del método 505 asociado con cada objeto cargado, si el método 505 se verifica exitosamente se activa 506 para almacenar la clave R2 con el id del cliente del receptor al servidor en línea.
15 Si la conexión a internet está disponible el verificador de conexión 507 verifica su integridad asociada con cada objeto cargado, si el método 507 se verifica exitosamente se activa 508 para alertar al destinatario para registrar la clave. Ahora si el usuario acepta registrar la clave al ejecutar la
20 función 509, entonces si la conexión a internet está disponible el verificador de conexión 511 verifica la integridad del método 511 asociado con cada objeto cargado, si el método 511 se verifica exitosamente se activa 512 para alertar al propietario acerca del registro de la clave R2 con

el destinatario. Si el usuario no acepta 510, la clave no se registra.

Con referencia a la Figura 6, si el propietario de los datos desea revocar la clave R2 compartida con otros usuarios se activa el método 601. La interfaz 602 aparece con la lista de los id del cliente con quienes la clave R2 del propietario de los datos se registra. El propietario selecciona el id del cliente de los destinatarios de quien desea revocar su clave R2 y envía esta petición al servidor en línea al ejecutar la función 603, si la conexión a internet está disponible en la computadora del destinatario el verificador de conexión 604 verifica la integridad del método 605 asociado con cada objeto cargado, si el método 605 se verifica exitosamente se activa 606 para revocar la clave R2 registrada del destinatario propuesto del servidor en línea. Si la conexión a internet está disponible en la computadora del propietario de los datos, el verificador de conexión 607 verifica su integridad asociada con cada objeto cargado, si el método 607 se verifica exitosamente se ejecuta 608 para alertar al propietario acerca de la revocación exitosa de la clave R2 del destinatario propuesto.

Con referencia a la Figura 7, cuando el software se abre, el componente de autorización 701 verifica el id de la tarjeta madre incluido en el software con el id de la tarjeta madre de la máquina. La función 702 verifica si los id de la

tarjeta madre han cambiado, entonces la función 703 se ejecutará para bloquear el software y alertará al usuario para validarse con el servidor en línea. Si la conexión a internet está disponible el verificador de conexión 704
5 verifica la integridad del método 705 asociado con cada objeto cargado, si el método 705 se verifica exitosamente se activa 706 para validar el software con el servidor en línea y envía la clave de confirmación al id del correo electrónico registrado del usuario. El usuario ingresa la clave de
10 confirmación en el asistente de activación al ejecutar la función 707. Si el verificador 708 valida la clave de confirmación con el servidor en línea, entonces la función 709 se ejecuta para registrar el nuevo id de la tarjeta madre con el servidor e identifica el software con este id de la
15 tarjeta madre. La función 710 se ejecuta para enviar y restaurar las claves R1, R2 al software del usuario. La función 711 se ejecutará para alertar al propietario para pedir a los otros propietarios de los datos registrar su clave R2 con el software. Solamente después de la
20 confirmación del propietario de los datos, su clave R2 se registrará con el destinatario nuevamente.

REIVINDICACIONES

1. Un método para controlar el uso de datos y prevenir el uso no autorizado de datos que se generan por el software, caracterizado porque usa el sistema de datos ISO.

5 2. El método de conformidad con la reivindicación 1, caracterizado porque se pueden usar los datos solamente en la computadora que los ha creado usando el sistema de datos ISO; para usar los datos en otra computadora, el propietario de los datos debe autorizar a un destinatario, usando el
10 mismo sistema de datos ISO en otra computadora.

3. El método de conformidad con la reivindicación 1, caracterizado porque comprende:

seleccionar los datos a ser compartidos e incluir el id del cliente del propietario de los datos;

15 identificar y autorizar por lo menos a un destinatario con quien los datos van a ser compartidos al ingresar el id del cliente del destinatario;

identificar cada conjunto de datos que se comparten por un id de los datos único generado por el sistema del
20 propietario de los datos, donde los permisos de acceso a cada conjunto de datos se asocian con cada id de los datos particulares;

expedir permisos de acceso requeridos al destinatario autorizado para usar los datos;

usar los métodos de intercambio de datos apropiados es decir compartir a través de la subida de datos al servidor en línea o al copiar los datos a cualquier dispositivo de almacenamiento externo.

5 4. El método de conformidad con la reivindicación 1, caracterizado porque durante la activación del software, el servidor en línea del vendedor envía dos claves particularmente R1 y R2 al software. La clave R1 se usa para encriptar los datos del propietario para protegerlos el uso
10 no autorizado de estos datos en cualquier otra computadora. Cuando los datos se crean en el software se encriptan con la clave R1 y se almacenan en esta forma encriptada. La clave R2 se usa para proteger los datos que van a ser compartidos con uno o más destinatarios propuestos en su sistema de
15 computadora. Ra y Rb son las claves privadas y públicas del destinatario.

5. El método de conformidad con la reivindicación 3, caracterizado porque el propietario de los datos puede compartir los datos con el destinatario a través de la subida
20 de datos al servidor en línea, o al transferir los datos a un dispositivo de almacenamiento externo y al compartir este dispositivo con el destinatario.

6. El método de conformidad con la reivindicación 3, caracterizado porque en caso de que el destinatario
25 todavía no haya registrado la clave R2 del propietario de los

datos y los datos a ser compartidos se suban al servidor en línea, los datos primero se desenscriptan usando la clave R1 del propietario de los datos y luego se encriptan con la clave R2 del propietario de los datos. Estos datos se suben
5 al servidor donde se desenscriptan con la clave R2 del propietario de los datos y se encriptan nuevamente con la clave Rb del destinatario. El destinatario descarga estos datos y los usa con su clave Rb.

7. El método de conformidad con la reivindicación
10 3, caracterizado porque en caso de que el destinatario todavía no haya registrado la clave R2 del propietario de los datos y los datos a ser compartidos se envíen al destinatario a través de un dispositivo de almacenamiento externo, los datos primero se desenscriptan usando la clave R1 del
15 propietario de los datos y luego se encriptan con la clave R2 del propietario de los datos. Estos datos se transfieren al dispositivo de almacenamiento externo y se comparten con el destinatario. El destinatario sube estos datos al servidor en línea y en caso de que el propietario de los datos haya dado
20 permisos suficientes, el servidor desenscripta estos datos con la clave R2 del propietario de los datos y encripta estos datos con la clave Rb del destinatario después de lo cual el destinatario puede descargar y usar estos datos con su clave Rb.

8. El método de conformidad con la reivindicación 3, caracterizado porque en caso de que el destinatario haya registrado previamente la clave R2 del propietario de los datos y los datos a ser compartidos se suban al servidor en línea, los datos primero se desenscriptan usando la clave R1 del propietario de los datos y luego se encriptan con la clave R2 del propietario de los datos. Estos datos se suben al servidor, el destinatario descarga estos datos del servidor y desenscripta y usa los datos con la clave R2 del propietario de los datos.

9. El método de conformidad con la reivindicación 3, caracterizado porque en caso de que el destinatario haya registrado la clave R2 del propietario de los datos y los datos a ser compartidos a través de un dispositivo de almacenamiento externo, los datos primero se desenscriptan usando la clave R1 del propietario de los datos y luego se encriptan con la clave R2 del propietario de los datos. Estos datos se transfieren al dispositivo de almacenamiento externo y se comparten con el destinatario. El destinatario descarga estos datos del dispositivo de almacenamiento y desenscripta y usa los datos con la clave R2 del propietario de los datos.

10. El método de conformidad con la reivindicación 1, caracterizado porque el sistema de datos ISO se puede usar para proteger cualquier dato en la computadora/sistema del propietario de los datos.

11. El método de conformidad con la reivindicación 3, caracterizado porque los datos descargados por el destinatario autorizado y designado se unen por ciertos derechos de acceso expedidos por el propietario de los datos; 5 los datos se pueden usar por el destinatario solamente como por los derechos de acceso establecidos, donde los derechos de acceso establecidos son observar, enmendar, imprimir y guardar.

12. El método de conformidad con la reivindicación 10 3, caracterizado porque el destinatario autorizado puede enmendar los datos y enviarlos de nuevo al propietario de los datos si es necesario. Estos datos enmendados se reconocerán usando un nuevo id de los datos. Los datos se encriptan con la clave Rb y se suben al servidor donde se desencriptan con 15 la clave Rb y se encriptan nuevamente con la clave R2 del propietario de los datos. El propietario puede descargar estos datos y convertirlos nuevamente a la clave R1 y usarlos.

13. El método de conformidad con la reivindicación 20 12, caracterizado porque el destinatario puede enmendar los datos compartidos por el propietario de los datos, si es necesario, y enviar los datos enmendados nuevamente al propietario de los datos ya sea a través de subir los datos al servidor en línea o al transferir los datos a un

dispositivo de almacenamiento externo y compartir este dispositivo con el propietario de los datos.

14. El método de conformidad con la reivindicación 12, caracterizado porque en caso de que el destinatario no
5 haya registrado todavía la clave R2 del propietario de los datos, los datos enmendados a ser compartidos se encriptan con la clave Rb del destinatario y se suben al servidor en línea, donde se desencriptan con la clave Rb del destinatario y después se encriptan con la clave R2 del propietario de los
10 datos. El propietario de los datos descarga estos datos y los convierte de R2 a su clave R1 y luego los usa.

15. El método de conformidad con la reivindicación 12, caracterizado porque en caso de que el destinatario todavía no haya registrado la clave R2 del propietario de los
15 datos y los datos enmendados a ser compartidos se envíen al propietario de los datos a través de un dispositivo de almacenamiento externo, los datos se encriptan usando la clave Rb del destinatario transferida al dispositivo de almacenamiento externo y compartida con el propietario de los
20 datos. El propietario de los datos sube estos datos al servidor en línea y en caso de que el destinatario haya dado suficientes permisos, el servidor desencripta estos datos con la clave Rb del destinatario y encripta estos datos con la clave R2 del propietario de los datos después de lo cual el

propietario de los datos puede descargar estos datos, convertirlos de la clave R2 a la clave R1 y usarlos.

16. El método de conformidad con la reivindicación 12, caracterizado porque en caso de que el destinatario haya
5 registrado previamente la clave R2 del propietario de los datos y los datos enmendados a ser compartidos se suban al servidor en línea, el propietario de los datos descarga estos datos y los desencripta usando su clave R2. Los datos se pueden convertir de la clave R2 a la clave R1 y luego usar.

10 17. El método de conformidad con la reivindicación 12, caracterizado porque en caso de que el destinatario haya registrado previamente la clave R2 del propietario de los datos y comparta los datos enmendados a través de un dispositivo de almacenamiento externo, el propietario de los
15 datos descarga estos datos del dispositivo de almacenamiento y los desencripta usando su clave R2. Los datos se pueden convertir de la clave R2 a la clave R1 y luego usar.

18. El método de conformidad con la reivindicación 3, caracterizado porque el proceso y almacenamiento de los
20 datos originales y los datos que se reciben para intercambio, se procesan a través de dos subsistemas diferentes y mutuamente exclusivos y están en dos ubicaciones separadas en la misma computadora/sistema.

19. El método de conformidad con la reivindicación
25 12, caracterizado porque el propietario de los datos es

alertado acerca de la enmienda hecha por el destinatario autorizado en los datos compartidos y puede fusionarlos en los datos originales si es requerido.

20. El método de conformidad con la reivindicación
5 1, caracterizado porque el propietario de los datos puede registrar su clave R2 con otros destinatarios para el propósito de intercambiar datos seguros al enviar al servidor una instrucción para hacerlo de esta manera e ingresar el id del cliente así como también el id del cliente del
10 propietario de los datos. El registro de esta clave se puede revocar en cualquier momento por cualquiera de las partes, al enviar una instrucción al servidor en línea del vendedor acerca del mismo.

21. El método de conformidad con la reivindicación
15 3, caracterizado porque el propietario de los datos puede bloquear los derechos de acceso a los datos compartidos con un destinatario, al instruir al servidor bloquear o suprimir los datos enviados al destinatario.

22. El método de conformidad con la reivindicación
20 3, caracterizado porque aún si los datos de la computadora del destinatario, se usa en cualquier otra computadora, no se puede acceder, usar o procesar, debido a la falta de permisos del propietario de los datos.

23. El método de conformidad con la reivindicación
25 1, caracterizado porque en caso de que el software sea

requerido a ser instalado, se proporciona un fácil método de
reinstalación al usuario del software y el servidor envía las
claves de encriptado y desencriptado nuevamente al software
después de la activación. También envía las claves R2
5 previamente registradas de otro usuario en el software.

24. El método de conformidad con la reivindicación
16, caracterizado porque en caso que durante la instalación o
cada vez que el software se abra, se detecta que el id de la
tarjeta madre de la computadora ha cambiado, entonces el
10 software tendrá que ser revalidado con el servidor y también
las claves R2 tendrán que ser revalidadas nuevamente por los
propietarios de los datos, solamente entonces el intercambio
de datos de estos propietarios puede llevarse a cabo.

25. El método de conformidad con la reivindicación
15 1, caracterizado porque el sistema de datos ISO también se
puede usar como un módulo de encriptado independiente para
asegurar el almacenamiento de datos.

RESUMEN DE LA INVENCION

De acuerdo con esta invención se proporciona un método para controlar el uso de datos y prevenir el uso no autorizado de datos que se generan por el software usando el
5 sistema de datos ISO donde los datos se pueden usar solamente en la computadora que ha creado los datos o usar y/o acceder a los datos en otras computadoras solamente si el propietario de estos datos ha dado acceso/permiso a estos datos.

☐ Indicación que se solicita una patente.

☐ Datos de identificación del solicitante o de la persona que presenta la solicitud

☐ Descripción de la invención

☐ Dibujos de ser estos pertinentes

☐ Comprobante de pago de las tasas establecidas (De ser el caso formato de descuento)

Completa ☐ Incompleta ☐

PATENTE DE INVENCION PCT ☒ MODELO DE UTILIDAD PCT ☐ Art.33 Decisión 486/00, Circular Única

☒ Indicación que se solicita una PCT

☒ Copia de la solicitud en español, tal como fue presentada inicialmente (capítulo descriptivo, reivindicatorio, resumen)

☒ Dibujos de ser estos pertinentes.

☒ Comprobante de pago de las tasas establecidas (de ser el caso formato de descuento)

Completa ☒ Incompleta ☐

DISEÑO INDUSTRIAL ☐ (Art. 119 Decisión 486/00)

☐ Indicación que se solicita Diseño industrial

☐ Datos de identificación del solicitante o de la persona que presenta la solicitud

☐ Representación gráfica y fotográfica del Diseño industrial o muestra del material que incorpora el diseño

☐ Comprobante de pago de las tasas establecidas

Completa ☐ Incompleta ☐

ESQUEMA DE TRAZADO ☐ (Art. 92 Decisión 486/00)

☐ Indicación que se solicita un esquema de trazado

☐ Datos de identificación del solicitante o de la persona que presenta la solicitud

☐ Representación gráfica de un esquema de trazado

☐ Comprobante de pago de las tasas establecidas

Completa ☐ Incompleta ☐