

Software activation and copy protection method

TECHNICAL FIELD

5

[001] The present invention relates to controlling the operation of a software application on a Client Machine, particularly at the installation and activation stage in the execution of the application. Our method provides for authentication and activation to be carried out between a Client Machine and a remote Server
10 Machine via telecommunication means which may involve different categories of communication devices.

BACKGROUND ART

15

[002] In protecting software applications from illegal copying, production and use, it is typical for an application's installation to require some form of authentication by the publisher before it may be activated for continued or uninterrupted use. With the prevalence of Internet and cellular phone services,
20 such authentication and activation are often controlled centrally by a remote server via Internet or cellular network connections. There exists a number of prior art on such piracy protection and the following are representative patents on such methods.

[003] Examples of patents concerning method and system for protecting a software application from piracy may be found in PCT publication No. WO2007088384 and European Patent No. EP 1825449. Anti-piracy software protection system and method are also disclosed in PCT published application No. 5 WO 2004099952 and U.S. Patent No. 5,754,864. Other methods for controlling protecting software against unauthorized use may be found in U.S. Patent No. 5,933,497 and PCT publication No. WO 2003021403. Software registration and activation method is specifically disclosed in PCT publication no. WO 2006006017.

10 [004] More specific methods available in the art include self-authentication software or digital content disclosed in U.S. publication No. 20040225894 and No. 2004117644. A web server-based method is disclosed in Korean patent no. KR 20020016160 while U.S. publication no. 2004117663 concerns authentication of software accessed via secondary devices. Methods implemented via a 15 communications network may be found in U.S. Publication No. 2006179486. PCT published application No. WO 2006048149 and U.S. publication no. 20070238450 disclose software application security access management in mobile communication devices. Other specific aspects of such software protection methods include encryption method for register code of the software as disclosed 20 in Chinese Patent No. CN 1369809. A method involving hardware ID is disclosed in U.S. publication No. 2004059938.

[005] Generally, the prior art may be categorized into one or more of the following methods:

[006] A unique serial key is required to perform the software installation. This is the cheapest and most common method but this protection is also the most easily circumvented by using the same serial number for multiple installations. The serial numbers can also be generated by the use of customizable serial key generator programs available on the Internet once the algorithm or formulation is known.

[007] Online activation – this requires handling of registration data and serial number verification and sending it to an activation server to obtain in return a directive to activate or block the software. When the user runs the software for the first time, he is prompted for registration data. A key file uniquely identifying a user's computer is generated and sent to the Activation Server which in response would generate a license file to activate the software or switch from trial or demo mode to full functionality depending on the protection mode chosen by the developer.

[008] Phone activation allows activation without the need for Internet access or do not want the application to be connected to the activation server. In this method, the software installation generates a unique code for the user to relay to the activation center together with his serial number. The activation code is generated on the basis of user-provided data to enable the user to activate the software.

[009] Hardware dongles or locks have also been used to authenticate the

software and prevent illegal copying or installation. However, similar cracks are available for such hardware locks.

5 [010] Biometric authentication is the verification of a user's identity by means of a physical trait or behavioral characteristic such as fingerprint. This method is most reliable and would undoubtedly identify the user if he makes multiple installations of the program but would nevertheless unable to prevent such rogue user from using his registered fingerprint to install the software in multiple machines. Although it is costly as it requires biometric devices, with the
10 incorporation of fingerprint scanner in many models of laptop computers today, the cost has somewhat been defrayed by the users themselves.

SUMMARY OF DISCLOSURE

15

[011] As an alternative to the afore-discussed method, we have now proposed a method for controlling the operation of a software application to be installed and executed on a Client Machine, wherein said Client Machine is coupled with a first communication device enabled to communicate with a Server Machine which is
20 coupled with a second communication device; wherein the software application's installation procedure includes:

- (i) prompting a user to input said user's particulars;
- (ii) generating a serial key, [masking said serial key and rendering it read-only];
- (iii) encrypting said serial key and user particulars as encrypted information;

- (iv) sending said encrypted information via first communication device to said Web Server;
- (v) receiving said encrypted information at said Server Machine via second communication device;
- 5 (vi) decrypting and storing said decrypted information on a Database Server;
- (vii) examining said serial key for validity, including any one of comparing against serial keys registered with said Database in respect of other genuine copies of said software application, checking for algorithm compliance, checksum, and the like;
- 10 (viii) sending an acknowledgement message from said Web Server Machine to said Client Machine via respective second and first communication devices if said serial keys have not been previously registered with said Database;
- (ix) verifying said acknowledgement message received by said Client Machine if it has been sent from a valid source; and
- 15 (x) generating an activation code enabling activation of the software application to be enabled for execution.

[012] In a first aspect of our method, the first and second communication devices include any one or in combination of a modem and/or telephone
20 employing wired or wireless telecommunication means. Preferably, the wired telecommunication means includes any one or in combination of a PSTN, ISDN, DSL (ADSL, HDSL, etc.) and like services while the wireless telecommunication means includes any one or in combination of a SIM-based cellular radio network, including GSM, CDMA, UTMS and data services such as GPRS/EDGE, HSPA

(HSDPA/HSUPA). Preferably, the first and second communication devices are able to transmit via the Internet.

[013] In a second aspect of our invention, the serial key generated is further
5 masked and/or its file attribute is switched to read-only. The encryption may further comprise automatic encrypting at least one unique identifier from the Client Machine and/or first communication devices, including any one of processor serial number, motherboard serial number, SIM phone number, IMSI number, IMEI number, product ID, UUID, Contact/Contactless Smart card ID, RFID tag and the
10 like.

[014] In a third aspect, the transmission between the first and second communication devices include intermediary gateways, proxy servers, routers and networks. Moreover, the software application may comprise at least the following
15 subroutines or layers for performing each specific task in a sequential manner:

- (i) a user Interface layer for inputting of user details and other related information;
- (ii) a communication layer for establishing data flow between first communication device and Client Machine, and from said first
20 communication device to second communication device;
- (iii) an authentication layer for checking if the serial key is valid; and
- (iv) an activation layer for generating activation code upon successful authentication.

[015] Preferably, the communication layer further includes encryption subroutine and is capable of invoking modem query commands. The layers, subroutines or modules are preferably distributed between the Client Machine, Server Machine and optionally a remote database server.

5

[016] In a fourth aspect, the acknowledgement message generated by the Server Machine is encoded with a Server Machine identifier enabling the Client Machine to identify and validate that said acknowledgement message originates from a valid source.

10

[017] In a fifth aspect, our method may be embodied as a subroutine or instruction set in said software application's installation and activation module or procedure. Preferably, the installation and/or activation program execution is split into a 2-part procedure wherein the first part is resident upon the Client Machine and the second part is resident upon the first communication device. More preferably, the parameters necessary for the installation and/or activation program execution is retrievably stored in 2 parts wherein the first part is stored in the Client Machine and the second part is stored in the first communication device.

15

20

[018] Nevertheless, the complete execution of the installation and/or activation program is preferably performed on the Client Machine upon retrieval of the 2-part executable files and/or parameters each from said Client Machine and first communication device. As a preferred embodiment, the first communication device is a cellular phone and the second part is stored in any one of the SIM card

and cellular phone or modem's memory. Another preferred embodiment of the 2-part execution procedure is to adapt it to provide for encryption and decryption of digital contents transferred between a Server Machine and a Client Machine, wherein a public key is hosted on the Server Machine on the first part and a
5 private key is generated using the first communication device connected to the Client Machine on the second part.

[019] In a sixth aspect, the activation code is generated or encoded as a sequence comprising text, image (including barcode or 2D barcode), audio or
10 sound tones and like machine-readable parameters, or encoded as an executable file essential for completing the installation.

[020] In relation to reinstallation of the software application, the uniqueness of the serial key is maintained by requiring a previously registered user seeking to
15 reinstall the software application to uninstall said application and remove previously registered serial key and user records from the database before verifying reinstallation-generated serial key.

[021] In respect of the various implementation of our method, one specific use
20 may be as a substitute for secure system login by a user. Another use would be in the downloading of updates, patches and fixes of said software application.

LIST OF ACCOMPANYING DRAWINGS

[022] The following drawings have been included for ease of understanding of our invention, by way of reference to exemplary, non-limiting embodiments with
5 the detailed description that follows, in which:

[023] FIGURE 1 shows a general scheme of our method in which our installation program's multi-layers or subroutines are listed;

10 [024] FIGURE 2 illustrates the process of sending serial key to the Server Machine according to our invention in a flowchart or logic diagram;

[025] FIGURE 3 depicts the activation code generation process according to our invention in a flowchart or logic diagram;

15

[026] FIGURE 4 exemplifies in a flowchart or logic diagram the process of verification in our invention;

[027] FIGURE 5 portrays in a flowchart or logic diagram the process of
20 uninstallation according to one aspect of our invention;

[028] FIGURE 6 represents in a flowchart or logic diagram the splitting of executable files in another aspect of our invention; and

[029] FIGURE 7 portrays in a flowchart or logic diagram the execution of the split executable files of FIG. 6 in one embodiment of our invention.

5 DETAILED DESCRIPTION OF SPECIFIC EMBODIMENTS

[030] Whilst our invention endeavours to provide a means to protect software (which covers all forms of software including computer applications, downloadable digital content, games, etc., and to prevent piracy of the software, it does not alter
10 the existing distribution channels, i.e. whether they are distributed through secondary storage medium or multimedia disk (e.g. CD or DVD) or downloaded through Internet, cellular network, etc. The user may install the software application from the CD or DVD on a computer as usual. Depending on the publisher, a grace period (e.g. 10 days or 30 days) may be provided for the user to
15 try the software without activation. To activate the software according to our invention, we shall describe specific embodiments in the following.

[031] The crux of our method for preventing software piracy, through controlled authentication and activation of the software, lies in using hardware or firmware
20 that are prevalent and pervasive as personal communication devices such that a user or customer of the software application is very likely to be in possession of such hardware (e.g. cellular phone) or firmware (Subscriber Identity Module or SIM card) without limiting to these examples. Accordingly, our invention takes advantage of the unique and secure encoding based on these personal hardware

or devices without the need for investing in further hardware keys for authentication. It is to be noted that our proposed activation procedure may or may not rely on having Internet connection to complete the activation.

5 [032] Our invention thus makes use of such personal communication devices and their cellular communications network (e.g. PCM/GSM, GPRS/EDGE, 3G and 3.5G networks) in order to establish transmission between a Client Machine (i.e. where the software is to be installed and executed or operated on) and a Server machine (i.e. which undertakes the authentication and activation decisions). By
10 employing existing unique identity or data from such personal communication devices, user input and conventional use of the software's serial number, which is also known as "Product Key" may be eliminated during installation, authentication and activation process.

15 [033] The general embodiment of our invention may be schematically shown in FIGURE 1. Basically, our invention provides for a method for controlling the operation of a software application to be installed and executed on a Client Machine wherein the Client Machine is coupled with a first communication device enabled to communicate with a Server Machine which is coupled with a second
20 communication device. The term "**Client Machine**" is employed in this specification to mean any device including a computer capable of being installed with a software application which is the subject of protection of the invention herein, and to operate or execute that application.

[034] The term “**Server Machine**” is employed in this specification as to mean the conventional server, i.e. it may be a device or application that performs services for connected clients as part of a client-server architecture which connection to its clients may or may not be based on the Internet. Hence, the term “**Web Server**” may be used interchangeably with “Server Machine” in this specification to also cover a server that is not Web-based.

[035] Specifically, our software application’s installation procedure includes the following steps:

- 10 (i) prompting a user to input said user’s particulars;
- (ii) generating a serial key;
- (iii) encrypting said serial key and user particulars as encrypted information;
- (iv) sending said encrypted information via first communication device to said Web Server;
- 15 (v) receiving said encrypted information at said Web Server Machine via second communication device;
- (vi) decrypting and storing said decrypted information on a Database;
- (vii) examining said serial key for validity, including any one of comparing against serial keys registered with said Database in respect of other
- 20 genuine copies of said software application, checking for algorithm compliance, checksum, and the like;
- (viii) sending an acknowledgement message from said Web Server Machine to said Client Machine via respective second and first communication devices if said serial keys have not been previously registered with said

Database;

- (ix) verifying said acknowledgement message received by said Client Machine if it has been sent from a valid source; and
- (x) generating an activation code enabling activation of the software application to be enabled for execution.

[036] FIGURE 2 shows a flowchart of the installation up to registration of the user at the Web Server. Based on the scenario that a user is installing the software application on his computer and is seeking to activate it, the user may be prompted to input his particulars in the course of the installation. A user interface may be used such as a dialog box display on a computer screen during the execution of the installation routine or subroutine of the software application. By “**user interface**” we also mean any other form of prompting such as a audio sounds or voice commands for the user to follow through with the input. For example, the user may have to input user details such as Name, Email, Mobile number, and other related information.

[037] In generating a serial key, a further step in masking the serial key and/or rendering it read-only may be made for additional security so that the user is not able to modify or change it. The resultant serial key, whether it is further masked and/or rendered read-only, is then transmitted to the Web Server. As additional security, the resultant serial key may be encrypted together with the user’s particulars before being transmitted.

[038] The transmission is done via a first communication device which may be a modem coupled to the computer. It should be clarified that in the event that Internet activation is not chosen and the user instead opt for telephone activation, then the user's hand phone is considered as the equivalent of the "first communication device" and the proximity and use of the hand phone in contacting the Web Server by the user is to be considered as being coupled to the computer as the Client Machine.

[039] If the first communication device is not, for example, a modem coupled to the computer such as in the case of a hand phone, then it should be understood that data transmission may be established via infrared, Bluetooth, data cable or other conventional data transmission means.

[040] In order that the user is not burdened with submitting technical details that is required to generate a unique code as part of identifying the user and his hardware (i.e. the computer or hand phone), commands may be built-in to the user interface to automatically retrieve such information and include it in the information to be transmitted to the Web Server. For example, the computer's processor serial number may be gleaned from the operating system's System Information and transmitted along with user particulars. As another example, the International Mobile Equipment Identity (IMEI) number may be obtained by dialing "*#06#" which sequence may be included in the activation instructions to the user or in the user interface. The resultant combined identity may thus be included in a text message (Short Messaging Service, SMS) sent to the Web Server.

[041] The encryption step may thus further comprise automatic encrypting at least one unique identifier from the Client Machine and/or first communication devices, including any one of the computer processor serial number, motherboard serial number, SIM phone number, International Mobile Subscriber ID (IMSI) number, the aforesaid IMEI number, product ID (also known as Product Key), Universally Unique Identifier (UUID) and the like. Although we have used the example of the communication device as being a cellular or GSM phone, it is obvious that transmission over other related services such as GPRS/EDGE (2.5G), CDMA/UTMS (3G) and HSPA (HSDPA/HSUPA or 3.5G) networks is also possible, and that apart from the use of mobile phones, the use of camera phones, Smart phones, PDA phones, etc. are also possible. Moreover, if the Client Machine is installed or coupled with Smart Card, or RFID tag reader, the use of contact or contactless Smart card, RFID tag, etc. are also possible.

15

[042] For the Web Server to be able to receive the information from the user sending it via his hand phone, the Web Server will have a second communication device coupled to it such as a compatible hand set. The Web Server, upon receiving the information from the user, will be able to recognize the format of the string of alphanumerical data or, if it is encrypted, will be able to decrypt it and parse the decrypted information according to its predetermined format in order to identify the unique hardware or firmware code, user particulars, software application's details, etc.

20

[043] The decrypted and/or parsed the information may then be stored in a database which may be hosted by the Web Server. The database may be provided in the form of a text-based file such as .DAT or .XML file. The database may also be hosted remote from the Web Server in which case a third
5 communication device may be required for the Web Server to store and retrieve information on the users from the remote Database Server if the Web Server's second communication device is to be dedicated for user authentication and activation.

10 [044] Reference will now be made in respect of FIGURE 3 which illustrates the procedure from checking the serial key's authenticity up to generating an activation code. One embodiment of our method for checking if the serial key that is being sent by a user attempting to activate the software has previously been used is to check it against the database table in which previous authenticated
15 users of genuine software have been registered and stored or tabulated in the database. If the serial key that is being submitted has not been previously registered, then the Client Machine will send an acknowledgement message via the second communication device to the Client Machine via the first communication device (which may be, for example, the user's hand phone or the
20 Client Machine's modem). One way of maintaining the uniqueness of the serial key is to require a previously registered user seeking to reinstall the software application to uninstall the application and thus remove previously registered serial key and user records from the database before verifying the reinstalled software and the reinstallation-generated serial key.

[045] The installation procedure at the Client Machine has been preprogrammed to recognize if an acknowledgement message received originates from a valid source, i.e. the Web Server. One way enabling the Client Machine to discriminate if the acknowledgement message is valid or comes from the Web Server is to
5 encode the message with a Server Machine identifier. If the acknowledgement message is valid, the installation procedure would then generate an activation code which would enable the software application to be activated for continuous or uninterrupted use.

10 [046] In a preferred embodiment, the activation code may be generated or encoded as a sequence comprising text, image (including barcode or 2D barcode), audio or sound tones and like machine-readable parameters, or encoded as an executable file essential for completing the installation. For example, if a user has indicated in the user information sent to the Web Server that the hand phone
15 model used is a particular camera phone model, the Web Server may in turn send the acknowledgement message to include a 2D barcode (also known as "matrix code") which the user may print out and capture with his camera phone. Examples of such 2D codes include:

20 [047] - bCODE (developed by the Australian company, bcode.com) which is sent as an SMS message to hand phones and displayed on the phone's screen to be read electronically such as that used presently in mobile ticketing systems, mobile vouchers, security passes, etc.

[048] - InterCode (by IconLab, Inc.) which is the standard 2D barcode in Korea. All 3 Korean mobile carriers put the scanner program of this code into their handsets to access mobile internet, as a default embedded program.

5 [049] - mCode (developed by Nextcode Corporation) specifically for camera phone scanning applications. It is Designed to enable advanced cell mobile applications with standard camera phones.

[050] It would also be apparent that depending on the capability of the camera
10 phone model, 2D, graphical or other matrix codes may also be send as a multimedia message (MMS) or extended message service (EMS). For smartphones or PDA phones, the options and functionality are greatly increased.

[051] As shown in FIG. 1, the software's installation or setup file may have an
15 architecture comprising multiple layers. Each layer is a subsystem that performs a specific task or provides a specific set of services (including communication procedure calls). As could be seen in FIG. 1, the setup file for the Client Machine may comprise of at least the following subroutines or layers for performing each specific task in a sequential manner:

- 20 (i) a **user Interface layer** (previously described) for inputting of user details and other related information;
- (ii) a communication layer for establishing data flow between first communication device and Client Machine, and from said first communication device to second communication device;

- (iii) an authentication layer for checking if the serial key is valid; and
- (iv) an activation layer for generating activation code upon successful authentication.

5 [052] The **communication layer** comprises program codes for establishing connection between the communication device and the Client Machine. Preferably, the communication layer further includes subroutines for encryption, modem querying and commands. Program codes are also provided to retrieve and update data either stored in the memory of the communication device (e.g.
10 phone memory) or on the SIM card.

[053] The **authentication layer** comprises program codes to check if the serial key sent by the user is valid or not. Authentication will be performed at least once during the installation of the software. The **activation layer** comprises program
15 codes that generate and check the acknowledgement code received from the Web Server. In a successful activation, an activation code is generated using the serial key and/or user details.

[054] For the Web Server, the setup file may contain the following layers or
20 subroutines as shown in FIG. 1:

[055] The **communication layer** comprises program codes which are able to establish connection between the communication device and the Web Server. The program codes are also able to retrieve and update data either stored in the

memory of the communication device or on the SIM card, and to send and receive data to and from other communication device. The communication layer contains program codes that may use AT commands if the Web Server is coupled with a modem and also contains methods to encrypt and decrypt data. It should be noted that where the user chooses online activation and the Web Server provides a secure computing website (<https://>), the encryption and decryption functions of the communication layer above would be redundant. As such, our encryption and decryption steps should be interpreted accordingly under such secured computing domains.

[056] The **authentication layer** comprises program codes to check if the serial key is valid or not. Authentication will be performed at least once during the installation of the software. Where the user downloads the installation software from Website, i.e. the Client Machine is connected to Internet, most of the steps as described previously are applicable, except for the encryption/decryption steps, particularly where the publisher provides the Web Server in a secure computing domain (<https://>). Furthermore, the functions of communication layer, authentication layer and activation layer may also be performed through the Web Server.

[057] The **activation layer** comprises program codes that generate the activation code. The activation code is generated using the serial key and/or user details.

[058] A **re-activation layer** may also be provided for the setup file on the Web Server. Subsequent activation can be performed on regular intervals, or if there is an update for the software, or whenever there is a crack found for the software on the Internet (a set of program codes can determine if a crack is found for the software based on querying Web search engines and if it returns relevant results, the results could be forwarded to the respective department who can take a decision if re-activation should be done), or depending on the publisher's policy.

[059] The variation in verification before allowing for re-activation procedure is illustrated in FIGURE 4. It can be noted here that any attempt to use the same serial key to install the software will fail as the Web Server will block the generation of activation code. Moreover it will help to identify the pirate since relevant information is stored on the Web Server. The steps involved in the uninstallation of the software application before the user is allowed to reinstall is outlined in FIGURE 5.

[060] As a preferred embodiment, as shown in FIGURE 6, our installation and/or activation program execution may be split into a 2-part procedure wherein the first part is resident upon the Client Machine and the second part is resident upon the first communication device. In this 2-part procedure, the parameters necessary for the installation and/or activation program execution is retrievably stored in 2 parts wherein the first part is stored or resident in the Client Machine or computer for execution at the computer, while the second part is stored in the first communication device (i.e. the modem coupled to the computer, or phone memory

or SIM card storage of the cellular phone used for the activation process).

[061] In this arrangement, as shown in FIGURE 7, the complete execution of the installation and/or activation program is preferably performed on the Client Machine upon retrieval of the 2-part executable files and/or parameters each from said Client Machine and first communication device. Admittedly, an ordinary phone and SIM card would have limited memory for effectively loading an executable or library (e.g. DLL) file; hence, we have used the term “**parameter**” to cover any code or argument that may serve as a local or isolated copy of the parameter to enable a subroutine to complete its execution when called at runtime.

[062] In one embodiment, the 2nd part may be provided as a parameter to be saved on the SIM card or device’s memory storage, i.e. whether internal or external memory. Where the device may not be adapted to execute a program, the 2nd part may be provided as a parameter, message, phone book entry, etc. to suit the capability of the second device. AT commands may be used to write the contents to the SIM card or internal memory of the device. For external memory, the 2nd part may be written directly thereunto.

[063] As an alternative, the 2-part execution procedure may also be adapted to provide for encryption and decryption of digital contents transferred between a Server Machine and a Client Machine, wherein a public key may be hosted on the Server Machine on the first part and a private key is generated using the first communication device connected to the Client Machine on the second part. This

arrangement will enable digital content downloading such as audio files, multimedia files, games, etc. to be downloaded directly to the Client Machine and activated. As such, the use of our invention for purchase of licensing of software or digital content on a pay-per-use basis may be securely implemented by way of
5 sending an SMS to the paying phone number.

[064] It will be appreciated by a skilled person that, upon understanding the teachings herein, that variations, modifications and adaptations of the various components or parts of our invention disclosed herein may be implemented in
10 many ways. For example, the activation code can be stored on the client machine, Web Server, SIM or phone memory. Moreover, our method may be embodied as subroutines or instruction sets in existing software application's installation and activation module or procedure since none of our components or procedure is hardware-specific or limited to a particular type of ID. Hence, it is
15 possible to adopt a "mix-and-match" approach in implementing our invention.

[065] For example, a Near Field Communication (NFC) capable hand phone may be used in our invention whereby the 2nd part parameter may be written to the NFC hand phone's radio-frequency identity (RFID) tag embedded in the phone.
20 As another example, instead of using a GSM mobile phones described above as the first communication device, an IP or VoIP phone with direct connection to the Internet may be used instead. Furthermore, stand-alone card readers (such as RFID tag readers) connected to the Client Machine can also be used. In such cases, information could be sent by Internet to the server machine directly.

[066] In terms of applications, our method may also be used in substitution of a security clearing system instead of the conventional secure system login by a user. It is also possible for a software publisher to extend our invention to cover software support whereby the downloading of future updates, patches and software fixes to require such authentication and activation of the software updates or patches. This category of application in software support may also include broadcast tool to announce the release of updates, patches and fixes using the transmission mode established between the user or Client Machine and Web Server.

[067] Instant error reporting tool from the client machine with the help of communication device (E.g. sending of error messages originating for the use of the software). The communication device attached to Web Server could forward the message to the support department through the communication device, hence enabling quicker response time in time critical applications. Another possible implementation is the use as a statistical tool (e.g. which country, state or district has the highest number of a particular software application installed, highest number of unlicensed or multiple installations, etc.).

[068] It will also be obvious to a skilled person that, although the foregoing description is simplified in terms of transmission between the first communication device and the second communication device in that it is to be understood that over a distributed wide area network such as the Internet, such transmission is

likely to involve intermediary gateways, proxy servers, routers and sub-networks although they are not specifically mentioned.

[069] In respect of the architecture outlined above, for example, the aforesaid
5 software layers, subroutines, modules or software components may be distributed between the Client Machine and Web Server, and optionally a remote database server. It is therefore to be noted that these components need not be hosted within a single territory covered by a patent but may be configured with innumerable combinations and permutations, and distributed far and wide as the
10 present global Internet connection would allow.

[070] In the same vein, as the implementation of our invention may occur over territorial jurisdictions or cross-boundaries, it is to be understood that some of our claims hereinafter may be directed to specific components or devices such as the
15 Client Machine and Web Server, with or without their respective communication devices. All these are to be considered as equivalents to our invention, or corresponding equivalent parts thereof which are to be interpreted as falling within the scope and letter of the following claims.

CLAIMS

1. A method for controlling the operation of a software application to be installed and executed on a Client Machine, wherein said Client Machine is
5 coupled with a first communication device enabled to communicate with a Server Machine which is coupled with a second communication device; wherein the software application's installation procedure includes:
- (i) prompting a user to input said user's particulars;
 - (ii) generating a serial key, masking said serial key and rendering it read-only;
 - 10 (iii) encrypting said serial key and user particulars as encrypted information;
 - (iv) sending said encrypted information via first communication device to said Web Server;
 - (v) receiving said encrypted information at said Server Machine via second communication device;
 - 15 (vi) decrypting and storing said decrypted information on a Database;
 - (vii) examining said serial key for validity, including any one of comparing against serial keys registered with said Database in respect of other genuine copies of said software application, checking for algorithm compliance, checksum, and the like;
 - 20 (viii) sending an acknowledgement message from said Server Machine to said Client Machine via respective second and first communication devices if said serial keys have not been previously registered with said Database;
 - (ix) verifying said acknowledgement message received by said Client Machine if it has been sent from a valid source; and

(x) generating an activation code enabling activation of the software application to be enabled for execution.

2. A method for controlling the operation of a software application according to
5 Claim 1 wherein the first and second communication devices include any one or in combination of a modem and/or telephone employing wired or wireless telecommunication means.

3. A method for controlling the operation of a software application according to
10 Claim 2 wherein the wired telecommunication means includes any one or in combination of a PSTN, ISDN, DSL (ADSL, HDSL, etc.) and like services.

4. A method for controlling the operation of a software application according to
Claim 2 wherein the wireless telecommunication means includes any one or in
15 combination of a SIM-based cellular radio network, including GSM, CDMA, UTMS and data services such as GPRS/EDGE, HSPA (HSDPA/HSUPA).

5. A method for controlling the operation of a software application according to
Claim 2 wherein at least at one of said first and second communication devices
20 are able to transmit via the Internet.

6. A method for controlling the operation of a software application according to
Claim 1 wherein the serial key generated is further masked and/or its file attribute is switched to read-only.

7. A method for controlling the operation of a software application according to Claim 1 wherein the encryption step further comprising automatic encrypting at least one unique identifier from the Client Machine and/or first communication
5 devices, including any one of processor serial number, motherboard serial number, SIM phone number, IMSI number, IMEI number, product ID, UUID, RFID tag and the like.

8. A method for controlling the operation of a software application according to
10 Claim 1 wherein the transmission between the first and second communication devices include intermediary gateways, proxy servers, routers and networks.

9. A method for controlling the operation of a software application according to Claim 1 wherein said software application comprises at least the following
15 subroutines or layers for performing each specific task in a sequential manner:

- (i) a user Interface layer for inputting of user details and other related information;
- (ii) a communication layer for establishing data flow between first communication device and Client Machine, and from said first
20 communication device to second communication device;
- (iii) an authentication layer for checking if the serial key is valid; and
- (iv) an activation layer for generating activation code upon successful authentication.

10. A method for controlling the operation of a software application according to Claim 9 wherein the communication layer further includes encryption subroutine.

12. A method for controlling the operation of a software application according to
5 Claim 9 wherein the layers, subroutines or modules are distributed between the Client Machine, Server Machine and optionally a remote database server.

13. A method for controlling the operation of a software application according to Claim 1 wherein the acknowledgement message generated by the Server Machine
10 is encoded with a Server Machine identifier enabling the Client Machine to identify and validate that said acknowledgement message originates from a valid source.

14. A method for controlling the operation of a software application according to any one of the preceding claims embodied as a subroutine or instruction set in
15 said software application's installation and activation module or procedure.

15. A method for controlling the operation of a software application according to any one of Claims 1, 9, and 12 wherein the installation and/or activation program execution is split into a 2-part procedure wherein the first part is resident upon the
20 Client Machine and the second part is resident upon the first communication device.

16. A method for controlling the operation of a software application according to any one of Claims 1, 9, and 12 wherein the parameters necessary for the installation and/or activation program execution is retrievably stored in 2 parts

wherein the first part is stored in the Client Machine and the second part is stored in the first communication device.

17. A method for controlling the operation of a software application according to
5 any one of Claims 15 – 16 wherein the complete execution of the installation and/or activation program is performed on the Client Machine upon retrieval of the 2-part executable files and/or parameters each from said Client Machine and first communication device.

10 18. A method for controlling the operation of a software application according to any one of Claims 15 – 17 wherein the first communication device is a cellular phone and the second part is stored in any one of the SIM card, cellular phone, modem's memory, RFID tag and the like.

15 19. A method for controlling the operation of a software application according to any one of Claims 15 - 18 wherein the 2-part execution procedure is adapted to provide for encryption and decryption of digital contents transferred between a Server Machine and a Client Machine, wherein a public key is hosted on the Server Machine on the first part and a private key is generated using the first
20 communication device connected to the Client Machine on the second part.

20. A method for controlling the operation of a software application according to Claim 1 wherein the activation code is generated or encoded as a sequence comprising text, image (including barcode or 2D barcode), audio or sound tones

and like machine-readable parameters, or encoded as an executable file essential for completing the installation.

21. A method for controlling the operation of a software application according to
5 Claim 1 wherein the uniqueness of the serial key is maintained by requiring a previously registered user seeking to reinstall the software application to uninstall said application and remove previously registered serial key and user records from the database before verifying reinstallation-generated serial key.

10 22. A method for controlling the operation of a software application according to Claim 1 used in substitution for secure system login by a user.

23. A method for controlling the operation of a software application according to Claim 1 implemented in the downloading of updates, patches and fixes of said
15 software application.

24. A Client Machine implementing or having implemented a method according to any one of Claims 1 – 23.

20 25. A Server Machine implementing or having implemented a method according to any one of Claims 1 – 23.
