Title: METHOD FOR ENABLING COMPLIANCE WITH EXPORT RESTRICTIONS

Abstract: A method and system that enables cross-border compliance with export restrictions of particular computer technology, including software loaded on a computing device. The computing device is loaded with software, and has a country location device, such as a low-end GPS device. The country location device (country locator) stores the present geographic location of the device in a location register. When the computing device is turned on or the software is activated for operation on the computing device, a security utility of the software compares the present location against a list of pre-established locations that are export-restricted. When the value matches (or falls within a range) of one of pre-established locations, the features of the software that are export restricted are automatically disabled.
Described States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published: with international search report

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

METHOD FOR ENABLING COMPLIANCE WITH EXPORT RESTRICTIONS

Technical Field

[001] The present invention relates generally to computer software and specifically to export-restricted computer software loaded onto computing devices.

Background Art

[002] Governmental entities, such as the United States Commerce Department, often place export restrictions on computer technology, both hardware and software. These restrictions are based on some determination that the particular technology is vital to national advancement in certain technological areas (such as military applications), maintaining national security, and/or beneficial to advancement of U.S. economy. Tied to these factors is a concern that certain technologies, if expected, may fall into the wrong hands and be utilized in undesirable ways that may negatively impact the economy, security, or prestige of the country.

[003] High strength encryption technology, for example, is export restricted to certain countries. With the continuing advancement of current publicly available software that includes high strength encryption and the ease with which software can be loaded onto a portable device and transported/exported to another country, government control over the export of these technologies is becoming more difficult. For example, current versions of Netscape Navigator (Netscape Navigator is a registered trademark of Netscape Communications Corporation) and Internet Explorer (IE) (Internet Explorer is a trademark of Microsoft Corporation in the United States, other countries, or both) feature high strength encryption products, which are export restricted, in addition to their low strength encryption versions that are export compliant. These very popular browser applications are loaded on a large number of desktop and portable computers.

[004] Desktops and portable computing devices that are specifically made for export are loaded with export compliant versions of software by the manufacturer. However, a large number of systems made for local (internal) use are shipped by individuals (or retailers) to other countries. Also, many individuals carry their laptops and other portable computing devices out of the country when they travel. These computing devices, made for utilization within the United States, typically have the export restricted product (e.g., high strength encryption software) loaded on the system. Additionally, with the increased globalization of the workforce, many portable computer
devices such as laptops and tablet PCs often get carried across country boundaries by business professionals.

[005] There is currently no way to stop this inadvertent (or sometimes deliberate) export of export-restricted products. The government is unable to check the software loaded on every computing device leaving the country and furthermore, most of these devices (perhaps with the exception of laptops that are screened when carried through airport terminals) are carried out without the government authorities being aware. The present invention recognizes that it would be beneficial to provide a built-in mechanism for ensuring compliance with export restrictions on computer technology.

**Disclosure of Invention**

[006] Disclosed is a method and system that enables cross-border compliance with export restrictions of particular computer technology, including software loaded on a computing device. The computing device is loaded with software, which identifies itself to the OS as export-restricted or is identified as such by the installer of the software. The computing device is provided with a country location device, such as a low-end GPS device, linked to the BIOS and the OS of the computing device. The country location device (country locator) stores the present geographic location of the computing device in a location register.

[007] When the computing device is turned on or the software is activated for operation on the computing device, a security utility of the software reads the value within the location register and compares the value against a table/list of pre-established locations that are export-restricted. When the value matches (or falls within a range of) one of the pre-established locations, the feature(s) of the software that are export restricted are automatically disabled. In one embodiment, only the particular restricted features are disabled and the remaining functions of the software are allowed to execute. Additionally, for software having both a restricted version and a similar unrestricted version (dual-purpose software), the unrestricted version is enabled by default, and access to the restricted version requires a verification that the present location is not on the list of export-restricted countries. When access to the software is limited to specific unrestricted features, the user of the computing device may receive a notification that export restrictions prevent activation of the remaining restricted features. In another embodiment, the entire software is disabled and a message sent to the user that the requested use is unauthorized in that country or violates an export restriction of the software.

[008] Various methods are provided for updating or downloading the list of export
restricted countries. In one implementation, an RFID receiver is placed within the computing device. Also, each port (sea, land, air) is equipped with an export compliance mechanism having a digitized list of export restricted countries and an RFID transmitter that broadcasts the list of export restricted countries. This list is received via the RFID receiver (within range of the transmitter) and stored in the memory (e.g., EEPROM) of the computing device.

[009] Export compliance functionality may be provided as a utility within the software itself or as a separate software that completes the monitoring and blocking (access) features. Computing devices that are already loaded with export-restricted software can be updated with the compliance software via Internet download or user installation.

[010] According to a first aspect, there is provided, in a computing device having a location detecting mechanism, a method for enabling compliance with export restrictions on a component of the computing device, said method comprising: identifying a current location of the computing device; determining when said current location is one of a pre-established location in which said component is not authorized to be utilized; and enforcing said export restriction on said component, wherein the component is prevented from operating within said current location.

[011] Preferably, the method further comprises: outputting a message that said component was not authorized to be utilized in said current location. More preferably, the method further comprises: detecting a request for utilization of said component; when said current location is an authorized location for utilization of said component, activating said component for utilization within said computing device. Still more preferably, said component includes a first feature that is export-restricted and a second feature that is not export restricted, wherein said enforcing step includes disabling only said export-restricted first feature of said component, wherein said second feature is automatically activated when a request for access to said component is detected.

[012] In a preferred embodiment, said component is a software application and includes a first version that is export-restricted and a second version that is not export restricted, both installed on the computing device, wherein said enforcing step includes disabling only said export-restricted first version of said software application, wherein said second version is automatically activated when a request for access to said component is detected. Preferably, said identifying step further comprises: reading the current location from the location detecting mechanism; and recording the current location within a register of said computing device. More preferably, the method further
comprises detecting a connection of said computing device to the Internet; accessing a website containing a list of export-restricted components and associated restricted countries; downloading relevant ones of said export restricted components and associated restricted countries; and storing said relevant ones within a memory of said computing device. Still more preferably, said accessing, downloading and storing steps are dynamically completed.

[013] In a preferred embodiment, the method further comprises: receiving RFID signals comprising a list of export-restricted components and associated restricted countries; storing relevant ones of said export restricted components and associated restricted countries within a memory of said computing device. Preferably, said enforcing of said export restrictions comprises one or more of: disabling the component from being activated for operation within the computing device; automatically removing said component from said computing device; and prompting for entry of access permissions prior to authorizing access to and utilization of said component, wherein said access is provided only after verification of an entered authorization code. More preferably, said identifying of a current location comprises detecting said location from an access port utilized to provide a connection at the current location by said computing device to a network. Still more preferably, the method further comprises detecting a connection of the computing device to the Internet; and automatically downloading export compliance features of specific applications on said computing device, when said specific applications are installed without said export compliance features and have not yet been updated with such features.

[014] According to a second aspect, there is provided a computer program product for execution within a computing device having a location detecting mechanism, said computer program product comprising: a computer readable medium; program code on said computer readable medium for enabling compliance with export restrictions on a component of the computing device, said program code comprising code for: identifying a current location of the computing device; determining when said current location is one of a pre-established location in which said component is not authorized to be utilized; and enforcing said export restriction on said component, wherein the component is prevented from operating within said current location.

[015] According to a third aspect, there is provided, in a computing device, a system for enabling compliance with export restrictions on a component of the computing device, said system comprising: a location detecting mechanism that identifies a current location of the computing device; and an export compliance software (ECS) utility that
includes software means for: determining when said current location is one of a pre-established location in which said component is not authorized to be utilized; and enforcing said export restriction on said component, wherein the component is prevented from operating within said current location.

[016] Preferably, said location detection mechanism includes: means for determining the current location of the device; and means for recording the current location within a register of said computing device. More preferably, said ECS utility further comprising means for: detecting a request for utilization of said component; activating said component for utilization within said computing device when said current location is an authorized location for utilization of said component; and outputting a message that said component was not authorized to be utilized in said current location when said current location is an unauthorized location for utilization of said component. Still more preferably, said component includes a first feature that is export-restricted and a second feature that is not export restricted, wherein said means for enforcing includes means for disabling only said export-restricted first feature of said component, wherein said second feature is automatically activated when a request for access to said component is detected.

[017] In a preferred embodiment, said ECS utility further comprising means for: registering a receipt of RFID signals comprising a list of export-restricted components and associated restricted countries; and storing relevant ones of said export restricted components and associated restricted countries within a memory of said computing device. In a preferred embodiment, said location detecting mechanism is a global positioning system (GPS) device.

[018] The above as well as additional advantages of the present invention will become apparent in the following detailed written description.

**Brief Description of the Drawings**

[019] The novel features believed characteristic of the invention are set forth in the appended claims. The invention itself however, as well as a preferred mode of use, further objects and advantages thereof, will best be understood by reference to the following detailed description of an illustrative embodiment when read in conjunction with the accompanying drawings, wherein:

[020] **Figure 1** is a block diagram of a laptop, representing a portable computer device, within which the features of the present invention may advantageously be implemented;

[021] **Figure 2** is a block diagram of an exemplary country locator subsystem of the
computer device of Figure 1, according to one embodiment of the invention;

Figure 3A is a flow chart depicting the process by which the computing device responds to operation within an export restricted location according to one embodiment of the invention;

Figure 3B is a GPS based global network utilized for identifying a geographic location of a portable device according to one embodiment of the invention;

Figure 4 is a flow chart depicting the process by which export restrictions for software are updated according to one embodiment of the invention;

Figure 5 is another flow chart depicting the process of dynamically switching versions of an application based on a trigger such as operation within a restricted geographic location in accordance with one implementation of the invention; and

Figure 6 illustrates a wide area network, such as the Internet with computer subsystems having localized RFID transmitters at exit ports according to one implementation of the present invention;

Best Mode for Carrying Out the Invention

The present invention provides a method and system that enables dynamic cross-border compliance with export restrictions of particular computer technology, including software loaded on a computing device. The invention is described with specific reference and description of a generic computing device, which is a device capable of executing software that may be subject to export restrictions. Thus, computing device may be a laptop computer, desktop computer, handheld computer, or even a cellular phone, etc.

With reference now to the Figures and in particular to Figure 1, there are illustrated hardware (and software) components of an exemplary computing device. Computing device 100, comprises a processor (CPU) 101, which is coupled via a system bus 104 to a memory 105, input/output controller (IOC) 113, and network interface controller (NIC) 103. NIC 103 is utilized to connect computing device 100 to external networks, such as the Internet. Coupled to IOC 113 are monitor 115, user input devices (mouse, keyboard, etc.) 114, input drives (disk and/or CD drives, etc.) 116. Also coupled to IOC 113 are two wireless sensors, an RFID sensor (or receiver) 117 and a GPS sensor (or country locator device) 119. RFID sensor 117 and GPS sensor 119 are respectively utilized to complete export restricted country list updates and country location, both of which are described in greater details below.

Figure 2 illustrates an exemplary country locator subsystem of the computing device of Figure 1. Country locator subsystem 200 comprises several components
of computing device 100, specific to the functional operation of the invention. As illustrated, country locator subsystem (CLS) 200 comprises a power on/off button 207, utilized to power the computing device on and off. CLS 200 also comprises a basic input output system (BIOS) 209, which performs a power on self test (POST) operation when computing device 100 is first turned on.

[030] BIOS 209 includes a location register 211 which stores the current country location provided by the GPS sensor 119. Figure 3B illustrates a GPS network 320 in which the GPS sensor 119 of computing device 100 receives device location data/information from a satellite 323 orbiting the earth 325. In one embodiment, this GPS sensor (or other country locator) is packaged with export compliance software (ECS) (described below) or with the specific software that is export-restricted. With the latter implementation, the device must be installed along with the software before the specific restricted features of the software become functional within the computing device.

[031] Referring back to Figure 2, BIOS 209 also comprises a table 213 in which the list of export restricted software (loaded on computing device 100) and corresponding restricted countries are stored. Table 213 receives input (or updates) from RFID receiver 117 and/or Internet browser application 215 which connects to the Internet via NIC 103. Figure 3A illustrates a network 300 having the computing device 100 connected to a national export compliance server 303 via the Internet 301.

[032] Returning now to Figure 1, stored within memory 105 are software modules including operating system (OS) 107 and two versions of software application 111A and 111B for executing on the processor 101. According to one implementation of the invention, a first version 111A is export-restricted while the second version 111B is not export-restricted. Also, in the illustrative embodiment, memory 105 also comprises export compliance software (ECS) 109, by which the location monitoring, country list updating, and disabling of restricted software and related features of the invention are provided. ECS 109 may be loaded on the computing device utilizing input drives 116 or downloaded from the Internet 301 via NIC 103.

[033] In the described embodiment, a separate export compliance software package (ECS) is provided. This export compliance software is separate from the actual software that is being monitored for export compliance. This embodiment allows computing devices that are already loaded with the export-restricted software to be provided with the checking mechanism. This embodiment also provides a user with customizable software to assist the users in complying with export/import regulations.
Users who frequently travel in and out of the country are able to customize the ECS based on the countries to which they travel and/or the software loaded on the computing device, and other user preferences, including what actions should be taken once the potential import/export violation is detected. Possible actions may include (1) notifying the user of potential violation, (2) disabling the software for a temporary duration with an ability to re-enable, (3) automatically removing the software upon detection from the device, and/or (4) launching a compliant version in the destination country instead of the non-compliant version. Also, these responses may be implemented at the detection time or at the occurrence of some other trigger event.  

With ECS, when the geographic location is found in the list of export restricted locations, the compliance software detects which software products are potential export violations. In one embodiment, the software dials out and downloads the latest import/export compliance regulations on a periodic basis. Then, based on latest set of regulations, the software scans the computing device for pieces of software that would result in compliance violations to various countries. Depending on the type of software found, the compliance software then takes the action programmed by the user or software manufacturer. These actions range from warning/notifying the user, disabling the software (with a facility to re-enable it for later use), automatic removal of software, etc. These actions may occur at the detection time or upon some other event such as a first use of the software in the destination country. In one embodiment, detection of the location of the computing device may be determined by the port at which the computing device connects to the Internet or other network. The port is determined when the computing device connects to the phone/DSL/ISDN or LAN or Wireless LAN, etc., in the destination country.  

In one implementation, the export compliance software is packaged as an add-on to the computing device software (OS and/or applications) along with the country locator device. In another embodiment, the export compliance software is automatically downloaded from the website of the restricted software into the computing device when the computing device is connected to the Internet. This latter implementation works best with browser-type applications (e.g., Netscape and IE), where the compliance software is packaged as an upgrade, similarly to the methods currently utilized to upgrade browsers and Internet-based applications.  

**Figure 5** illustrates the process by which the dynamic detection and deactivation of export-restricted software is completed. Prior to that process, however, the computing device is first loaded with software, which identifies itself to the OS as
export-restricted or is identified as such by the installer of the software. The computing
device is manufactured with or enhanced with a country location device, such as a
low-end GPS device, linked to the BIOS and the OS of the computing device.

Referring now to the figure, the country location device (hereinafter “country
locator”) detects and stores the present geographic location of the computing device
in the location register as indicated at block 501. The computing device is turned on and/or
the software is selected for operation on the computing device as shown at block
503. ECS (and/or the OS) reads the value within the location register and, as depicted
at block 505, compares the value against the table of pre-established locations/
countries that are export-restricted for that software. A determination is made at block
507 whether the current location is on the export restricted list. Notably, this list may
be a set of geographic coordinates or the actual name of the country. The exact form in
which the information is presented and check is not limiting on the invention. When
coordinates are utilized, however, the checking involves mapping the current value
within a range of values and is thus more cumbersome to execute.

Notably, for extremely sensitive technology with extensive restrictions, the verification may simply compare the present location/country against a short list of un-
restricted countries, rather than checking against the countries not authorized for the
software. Where the country of origin retains exclusive access to the technology (e.g.,
restricted to use in the USA only), a simpler response would be to deactivate the
software as soon as the computing device passes through an exit port.

Also, following an activation of the software in an export-restricted location,
additional checks are provided by the software to ensure that subsequent activation is
indeed within a restricted location, and this may require the user to enter particular in-
formation in response to a query generated by the software. This internal checking
ensures that a user does not attempt to fool the system by tampering with the GPS
device. In another related implementation, tampering with the GPS device or opening
the computing device cover sets flag, which forces additional compliance checks when
the user later attempts to activate the software.

Returning to Figure 5, if the software has no export restrictions and/or the export
restriction does not apply to the current location, full access is provided to the software
as indicated at block 509. However, when the current location is a restricted location, a
second check is made at block 508 whether the software has an unrestricted version
or whether there are some features of the software which are not restricted. When the
entire software is restricted, all access to the software is automatically blocked as
shown at block 510. The entire software is disabled and a message sent to the user that the requested use is unauthorized in that country or violates an export restriction of the software.

However, when there are portions of the software that are unrestricted, the restricted features of the software are deactivated as shown at block 511. A message is then generated and sent to the user as indicated at block 513. The exact message depends on the ECS and user customizing of the ECS. Then, the features of the software that are not export restricted are activated and limited access is provided to that part of the software as shown at block 515. Then the process ends as indicated at block 517. When only particular restricted features are disabled and the remaining functions of the software are allowed to execute, the user of the computing device may receive a notification of the export restriction of the particular restricted features.

Because the list of export restricted software and associated restricted countries may change after the software is bought and/or loaded on the computing device, the invention provides two different implementations by which the list of export restricted countries (or geographic locations) is updated. The first implementation is illustrated by the flow chart of Figure 6. The ECS and/or the installed (export restricted) software include a country update utility that monitors for connection to the Internet. Thus, the computing device is connected to the Internet as indicated at block 601. The ECS or country update utility automatically accesses an established national export regulation website (e.g., a commerce department import/export repository) once the Internet connection is established, as shown at block 603. When implemented via the country update utility, the utility then downloads the list of export restricted countries relevant for that software as indicated at block 605. When implemented via the ECS, however, the ECS downloads updates for all export restricted software loaded on the computing device. Since only a small number of software applications are export-restricted, this download may not involve a substantial amount of time or memory and processor resources. Once downloaded, the list of countries is stored within the table as indicated at block 607.

Notably, the country-update utility may either automatically download the list of countries during each internet connection or may download the list only when an update flag is placed on the website. That is updates to the list of countries for that software are made by the government personnel and a flag is automatically set on the site once that update is completed. In another implementation, the country update utility may download the current list based on a detected change in the value stored within
the location register (i.e., indicating the computing device has been moved to another geographic location). With this implementation, one embodiment may provide the country update utility with the functionality to dial out and/or connect to the particular web site as required.

[044] In one implementation, a monitoring feature is provided with the software and allows the software to register the locations in which the software has been utilized. During subsequent access to the web site, information about use within export-restricted locations may be provided anonymously. This enables the government or software manufacturer to track the extent of the use of the software in the export restricted locations.

[045] Figure 4 illustrates a different method by which the list of export restricted countries are provided or updated within the computing device. This second implementation involves the utilization of RFID (radio frequency identification) technology and/or other short range wireless technology. An RFID receiver is placed within the computing device (laptop) 100 as described above. This is a common implementation for current portable computing devices and thus requires little change to existing hardware. Each exit port (sea, land, air) 401 is equipped with an RFID transmitter 403, which is connected to an export compliance control subsystem that includes a computer subsystem 407 connected to the national export compliance server 303 via the Internet 301. The RFID transmitter 403 transmits the list of export restricted software and associated countries at the exit port 401. This list is received by the RFID receiver and stored in the memory (e.g., EEPROM) of the computing device 100.

[046] One extension of the features of the invention is provided for software that is packaged with both an export restricted version and a non-restricted version. Figure 7 illustrates a flow chart of the selection process for executing such software applications. The features provided may also be applicable to software that comprises both a restricted feature and a restricted feature that may be implemented independently of each other (i.e., dual-functionality software). With such software, a logical assumption is that the restricted version provides more features and is the preferred version. A user wishes to default to the restricted version whenever that version is available, based on compliance checks against export restrictions, etc. The implementation provides a single selection point (e.g., selectable icon on the GUI) for the software (i.e., both accessed via the same icon). As shown at block 701, the user selects the software icon for execution of the software.

[047] A background determination is made at block 703 whether the computing device
is in a restricted location for that software. When the computing device is not in a restricted location, the complete (export regulated) version of the software is implemented as indicated at block 705. However, when the computing device is in a restricted location, only the non-regulated version of the software is provided as shown at block 707. Notably, the user may not be aware of the reasons why one version is provided versus another. For example, the Internet Explorer® browser may be opened without the encryption package and provide all other features. The software may provide a message that the encryption package is unavailable if he/she attempts to access that feature.

[048] One embodiment of the invention may also allow the user to deactivate the export restricted version or features of the software, so that the selection defaults to the non-restricted version. This implementation would then allow the user to have provide a password to enable access the export-regulated features, where the password is obtained after signing a license agreement that includes language about prosecution for unauthorized export of the export-regulated version of the software.

[049] The ECS thus completes the following processes: (1) checks the geographic location against the list of export-restricted locations; (2) detect whether a requested application/product is a potential export violation; and (3) launch only a compliant version in the destination country (rather than the non-compliant version). These actions may occur at the detection time or upon some other trigger event, such as (1) opening the software in the destination country or (2) connecting the computing device to the phone or LAN or some other network for the first time in the destination country, for example.

[050] Also, it is important to note that while the present invention has been described in the context of a fully functional data processing system, those skilled in the art will appreciate that the mechanism of the present invention is capable of being distributed in the form of a computer readable medium of instructions in a variety of forms, and that the present invention applies equally, regardless of the particular type of signal bearing media utilized to actually carry out the distribution. Examples of computer readable media include: nonvolatile, hard-coded type media such as Read Only Memories (ROMs) or Erasable, Electrically Programmable Read Only Memories (EEPROMs), recordable type media such as floppy disks, hard disk drives and CD-ROMs, and transmission type media such as digital and analog communication links.

[051] While the invention has been particularly shown and described with reference to a preferred embodiment, it will be understood by those skilled in the art that various
changes in form and detail may be made therein without departing from the scope of the invention.
Claims

[001] In a computing device having a location detecting mechanism, a method for enabling compliance with export restrictions on a component of the computing device, said method comprising: identifying a current location of the computing device; determining when said current location is one of a pre-established location in which said component is not authorized to be utilized; and enforcing said export restriction on said component, wherein the component is prevented from operating within said current location.

[002] The method of Claim 1, further comprising: outputting a message that said component was not authorized to be utilized in said current location.

[003] The method of Claim 1 or Claim 2, further comprising: detecting a request for utilization of said component; when said current location is an authorized location for utilization of said component, activating said component for utilization within said computing device.

[004] The method of Claim 3, wherein said component includes a first feature that is export-restricted and a second feature that is not export restricted, wherein said enforcing step includes disabling only said export-restricted first feature of said component, wherein said second feature is automatically activated when a request for access to said component is detected.

[005] The method of any preceding claim, wherein said component is a software application and wherein said software application includes a first version that is export-restricted and a second version that is not export restricted, both installed on the computing device, wherein said enforcing step includes disabling only said export-restricted first version of said software application, wherein said second version is automatically activated when a request for access to said component is detected.

[006] The method of any preceding claim, wherein said identifying step further comprises: reading the current location from the location detecting mechanism; and recording the current location within a register of said computing device.

[007] The method of any preceding claim, further comprising: detecting a connection of said computing device to the Internet; accessing a website containing a list of export-restricted components and associated restricted countries; downloading relevant ones of said export restricted components and associated restricted countries; and storing said relevant ones within a memory of said computing
device.

[008] The method of Claim 7, wherein said accessing, downloading and storing steps are dynamically completed.

[009] The method of any preceding claim, further comprising: receiving RFID signals comprising a list of export-restricted components and associated restricted countries; storing relevant ones of said export restricted components and associated restricted countries within a memory of said computing device.

[010] The method of any preceding claim, wherein said enforcing of said export restrictions comprises one or more of: disabling the component from being activated for operation within the computing device automatically removing said component from said computing device; and prompting for entry of access permissions prior to authorizing access to and utilization of said component, wherein said access is provided only after verification of an entered authorization code.

[011] The method of any preceding claim, wherein said identifying of a current location comprises detecting said location from an access port utilized to provide a connection at the current location by said computing device to a network.

[012] The method of any preceding claim, further comprising: detecting a connection of the computing device to the Internet; and automatically downloading export compliance features of specific applications on said computing device, when said specific applications are initially installed without said export compliance features and have not yet been updated with such features.

[013] A computer program product for execution within a computing device having a location detecting mechanism, said computer program product comprising: a computer readable medium; program code on said computer readable medium for enabling compliance with export restrictions on a component of the computing device, said program code comprising code for: identifying a current location of the computing device; determining when said current location is one of a pre-established location in which said component is not authorized to be utilized; and enforcing said export restriction on said component, wherein the component is prevented from operating within said current location.

[014] The computer program product of Claim 13, further comprising program code for: detecting a request for utilization of said component; activating said component for utilization within said computing device when said current location is an authorized location for utilization of said component; and
outputting a message that said component was not authorized to be utilized in
said current location when said current location is an unauthorized location for
utilization of said component.

[015] The computer program product of Claim 14, wherein said component includes a
first feature that is export-restricted and a second feature that is not export
restricted, wherein said program code for completing said enforcing step
includes code for disabling only said export-restricted first feature of said
component, wherein said second feature is automatically activated when a
request for access to said component is detected.

[016] The computer program product of any of Claims 13 to 15, wherein said
component is a software application that includes a first version that is export-
restricted and a second version that is not export restricted, both installed on the
computing device, wherein said program code for said enforcing step includes
code for disabling only said export-restricted first version of said software ap-
lication, wherein said second version is automatically activated when a request
for access to said component is detected.

[017] The computer program product of any of Claims 13 to 16, further comprising
program code for: detecting a connection of said computing device to the
Internet; automatically accessing a website containing a list of export-restricted
components and associated restricted countries; dynamically downloading
relevant ones of said export restricted components and associated restricted
countries; and storing said relevant ones within a memory of said computing
device.

[018] The computer program product of any of Claims 13 to 17, further comprising
program code for: registering a receipt of RFID signals comprising a list of
export-restricted components and associated restricted countries; and storing
relevant ones of said export restricted components and associated restricted
countries within a memory of said computing device.

[019] The computer program product of any of Claims 13 to 18, wherein said program
code for enforcing of said export restrictions comprises program code for
completing one or more of: disabling the component from being activated for
operation within the computing device automatically removing said component
from said computing device; and prompting for entry of access permissions prior
to authorizing access to and utilization of said component, wherein said access is
provided only after verification of an entered authorization code.
The computer program product of any of Claims 13 to 19, wherein said program code for identifying a current location comprises code for detecting said location from an access port utilized to provide a connection at the current location by said computing device to a network.

The computer program product of any of Claims 13 to 20, further comprising program code for: detecting a connection of the computing device to the Internet; and automatically downloading export compliance features of specific applications on said computing device, when said specific applications are initially installed without said export compliance features and have not yet been updated with such features.

In a computing device, a system for enabling compliance with export restrictions on a component of the computing device, said system comprising: a location detecting mechanism that identifies a current location of the computing device; and an export compliance software (ECS) utility that includes software means for: determining when said current location is one of a pre-established location in which said component is not authorized to be utilized; and enforcing said export restriction on said component, wherein the component is prevented from operating within said current location.

The system of Claim 22, wherein said location detection mechanism includes: means for determining the current location of the device; and means for recording the current location within a register of said computing device.

The system of Claim 22 or Claim 23, said ECS utility further comprising means for: detecting a request for utilization of said component; activating said component for utilization within said computing device when said current location is an authorized location for utilization of said component; and outputting a message that said component was not authorized to be utilized in said current location when said current location is an unauthorized location for utilization of said component.

The system of Claim 25, wherein said component includes a first feature that is export-restricted and a second feature that is not export restricted, wherein said means for enforcing includes means for disabling only said export-restricted first feature of said component, wherein said second feature is automatically activated when a request for access to said component is detected.

The system of any of Claims 22 to 25, wherein said component is a software application that includes a first version that is export-restricted and a second
version that is not export restricted, both installed on the computing device, wherein said means for enforcing includes means for disabling only said export-restricted first version of said software application, wherein said second version is automatically activated when a request for access to said component is detected.

[027] The system of any of Claims 22 to 26, said ECS utility further comprising means for: detecting a connection of said computing device to the Internet; automatically accessing a website containing a list of export-restricted components and associated restricted countries; dynamically downloading relevant ones of said export restricted components and associated restricted countries; and storing said relevant ones within a memory of said computing device.

[028] The system of any of Claims 22 to 27, said ECS utility further comprising means for: registering a receipt of RFID signals comprising a list of export-restricted components and associated restricted countries; and storing relevant ones of said export restricted components and associated restricted countries within a memory of said computing device.

[029] The system of any of Claims 22 to 28, wherein said means for enforcing of said export restrictions comprises means for completing one or more of: disabling the component from being activated for operation within the computing device automatically removing said component from said computing device; and prompting for entry of access permissions prior to authorizing access to and utilization of said component, wherein said access is provided only after verification of an entered authorization code.

[030] The system of any of Claims 22 to 29, wherein said means for identifying a current location comprises means for detecting said location from an access port utilized to provide a connection at the current location by said computing device to a network.

[031] The system of any of Claims 22 to 30, further comprising program code for: detecting a connection of the computing device to the Internet; and automatically downloading export compliance features of specific applications on said computing device, when said specific applications are initially installed without said export compliance features and have not yet been updated with such features.

[032] The system of any of Claims 22 to 31, wherein said location detecting mechanism is a global positioning system (GPS) device.
Figure 1
Figure 4
LOCATION OF DEVICE DETECTED AND STORED 501

SOFTWARE SELECTED FOR ACTIVATION 503

BLOCK ALL ACCESS 510

NO

DUAL-VERSION SW: SOME FEATURES OK 508

YES

OS CHECKS LOCATION AGAINST PRE-ESTABLISHED LIST 505

MATCH? 507

NO

ALLOW FULL ACCESS TO SW 509

YES

DEACTIVATE REGULATED FEATURES FROM SW. 511

MESSAGE EXPORT REG. PROBLEM 513

ALLOW LIMITED ACCESS TO SW 516

END 517

Figure 5
Figure 6

CONNECT TO INTERNET 801

ACCESS NATIONAL SITE WITH LIST 803

DOWNLOAD NEW LIST TO COMPUTER 805

SAVE LIST ON COMPUTER 807

Figure 7

USER SELECTS SOFTWARE ICON 701

RESTRICTION APPLICABLE? 703

IMPLEMENT NON-RESTRICTED VERSION 707

IMPLEMENT FULL EXPORT-REGULATED VERSION 705
**INTERNATIONAL SEARCH REPORT**

**A. CLASSIFICATION OF SUBJECT MATTER**

IPC 7  G06F17/60  G06F1/00

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)

IPC 7  G08G  H04M  G06F  G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>EP 0 769 751 A (SEGA ENTERPRISES, LTD) 23 April 1997 (1997-04-23)</td>
<td>1-32</td>
</tr>
<tr>
<td></td>
<td>abstract column 1, lines 5-13 column 2, line 44 - column 4, line 50</td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>US 6 166 688 A (CROMER ET AL) 26 December 2000 (2000-12-26)</td>
<td>1-32</td>
</tr>
<tr>
<td></td>
<td>abstract column 2, lines 32-49 column 4, lines 17-42; figure 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>column 5, paragraph 24-67; figure 2 column 7, line 32 - column 8, line 12;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>figures 4-6</td>
<td></td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

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

"*" 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

"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

"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.

"*" document member of the same patent family

Date of the actual completion of the international search

2 March 2005

Date of mailing of the international search report

11/03/2005

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk
Tel: (+31-70) 340-2040, Tx. 31 651 epc nl, Fac: (+31-70) 340-3016

Authorized officer

Dedek, F
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>WO 03/034192 A (ENUVIS, INC) 24 April 2003 (2003-04-24)</td>
<td>2, 7, 11, 12, 17, 20, 21, 27, 30, 31</td>
</tr>
<tr>
<td></td>
<td>abstract page 4, lines 9-12 page 5, line 14 - page 6, line 23; figure 1 page 8, lines 29-26 page 14, lines 9-13</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>US 2003/188199 A1 (TADANO TOORU ET AL) 2 October 2003 (2003-10-02)</td>
<td>9, 18, 28</td>
</tr>
<tr>
<td></td>
<td>abstract paragraphs '0030!' - '0032!'; figure 3 paragraphs '0050!' - '0053!'; figure 8b</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>US 2003/184474 A1 (BAJIKAR SUNDEEP M) 2 October 2003 (2003-10-02)</td>
<td>1, 13, 22</td>
</tr>
<tr>
<td></td>
<td>abstract paragraphs '0014!' - '0016!'</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>EP 0 997 808 A (DATUM, INC) 3 May 2000 (2000-05-03)</td>
<td>1, 13, 22</td>
</tr>
<tr>
<td></td>
<td>abstract</td>
<td></td>
</tr>
<tr>
<td></td>
<td>abstract paragraphs '0016!' - '0018!'</td>
<td></td>
</tr>
<tr>
<td>Patent document cited in search report</td>
<td>Publication date</td>
<td>Patent family member(s)</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 6035400 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 1152366 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 9635186 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 6272638 B1</td>
</tr>
<tr>
<td>US 6166688 A</td>
<td>26-12-2000</td>
<td>NONE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2004205194 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 5401599 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BR 9904979 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2287596 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 0997808 A2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2000163379 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KR 2000035093 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ZA 9906799 A</td>
</tr>
<tr>
<td>US 2003105971 A1</td>
<td>05-06-2003</td>
<td>NONE</td>
</tr>
</tbody>
</table>