## Contact Information

Publications@ipcg.com

ipCapital Group, Inc.
400 Cornerstone Drive, Suite 325
Williston, VT 05495
United States of America
(802) 872-3200 x214

## Title of the Invention

SYSTEM AND METHOD FOR INSTALLING AND VERIFYING A DIGITAL RIGHTS MANAGEMENT OPERATING SYSTEM

## Description of the Invention

The Operating System is initially installed without any Digital Rights Management capabilities. Each license of the Operating System requires a license-unique version of the DRM Subsystem, and so piracy of the Operating System for use with DRM content is prevented. At the same time, due to the Operating System's unique nature, it is easily identified and discerned from a non-DRM Operating System running on the same machine.

### *Problem/Opportunity*

On a daily basis, large amounts of rights-sensitive information are transferred over the Internet. An Operating System (OS), such as Linux, with a digital rights management (DRM) system would allow media rights holders to restrict and monitor who is eligible to access, copy, and distribute such digital media. However, such an operating system also creates a new problem in how such an OS with DRM capabilities can be installed without risking the piracy of the operating system software itself. Also, there is the issue of discerning such an operating system from other operating systems running under a virtual machine on the same system.

### *Detailed Description of the Invention*

This invention provides for a system for installing and verifying an Operating System with DRM capabilities while preventing the piracy of the operating system itself.

The invention begins with the "install process" which involves two separate phases.

The first phase (Figure 2) is comprised of the end user installing the non-DRM Operating System components and creating an account with the OS developer.

The second phase (Figure 3) is comprised of using information from the account registration process to generate and install a license code specific version of the DRM Subsystem of the OS, in a process involving a series of communications between the user's operating system and the OS Maintenance Server.

The DRM components of the operating system (shown in Figure 1) are specific to the license key of a given OS, and they are executable only on the given licensed operating system. Therefore, discerning the DRM operating system from non-DRM operating systems is achieved in this invention as the DRM media file can be opened by the OS since it will be inferred that the OS accessing the file necessarily has the DRM Subsystem installed; otherwise the file would not open. The same case would hold true for Operating Systems running under a virtual machine, since such an operating system would need DRM components to access protected files.

Figure 1 shows the structure of the system. The system involves a User Machine (1.1), which consists of a processing device such as a PC, with network connectivity. This user machine contains a non-DRM operating system (1.2). This non-DRM Operating System has a DRM Installation subroutine (1.3), which can use the license key constant (1.4) of the non-DRM Operating System to install the DRM Subsystem (1.5). To install the DRM Subsystem, there is also a remote OS Maintenance Server (1.6) located on the Internet (1.7) that contains a DRM component generation program (1.8) and a User Database (1.9).

As shown in Figure 2, the system begins with the OS developer generating a license key and coding it into the non-DRM Operating System installer as a system constant (2.1). In this way, each installer file or disc for the OS is unique and traceable to the vendor and end user. At the same time, it also prevents the end user from modifying their license key to exploit the security of the DRM subsystem, as the key is located in the software itself as opposed to in memory. Next, the user proceeds to install the non-DRM Operating System (2.2), where they are required to enter this key. Once the installer verifies the key, it installs the non-DRM Operating System. Next, the user must set up an account with the OS developer on the OS Maintenance Server (2.3), again using the provided license key. Next, the user is prompted as to whether or not they would like to install the DRM Subsystem (2.4). The user has the option to not activate the DRM Subsystem of the operating system, but doing so prevents any DRM content from being accessed, viewed, or copied (2.5). Should the user choose to install the DRM Subsystem, the user machine would proceed to run the DRM Installation subroutine (2.6).

As shown in Figure 3, the DRM Installation subroutine proceeds by first connecting to the OS Maintenance Server. The OS Maintenance Server must then authenticate the login of the user machine (2.7), and reads the license key from the OS. Using the license key, it can then bring up the user account associated with that license. The system can then check the user's login credentials against the registered license key, and assuming they match the user's registration records, the Maintenance Server will then compile and send a license specific version of the DRM Subsystem to the User Machines OS for installation (2.8). Upon completion of the installation, the Maintenance Server then modifies the users account to make sure that their license key cannot be used again for a second install of DRM critical components. Should authentication of the user fail (2.9), the OS Maintenance Server would notify the user machine that they do not have proper login credentials, and return the user to the non-DRM Operating System.

In operation, the verification process for the install works as shown in Figure 3:

3.1: The User Machine (1.1) establishes a secure connection to an OS Maintenance Server (1.6) over the Internet (1.7).
3.2: Using the login information from the non-DRM OS (1.2) installation process, the user is prompted for their login information by the OS Maintenance Server (1.6).
3.3: The OS Maintenance Server (1.6) verifies the login information of the user. Assuming the login information is correct, the OS Maintenance Server (1.6) would then request the License Key (1.4) from the OS (1.2).
3.4: The DRM Installation sub-routine (1.3) accesses the OS License Key (1.4), stored as a constant in the OS (1.2), and returns it to the OS Maintenance Server (1.6).
3.5: The OS Maintenance Server (1.6) uses the given OS License Key (1.4) to generate an installer for the DRM Subsystem (1.5) based on the OS License Key (1.4) that will run only with that particular license of the non-DRM OS (1.2). When the DRM Subsystem has been compiled by the DRM Component Generator (1.8) program, the OS Maintenance Server (1.6)signals the OS on the user machine.
3.6: The OS (1.2) prompts the user with an on-screen dialog box to agree to the conditions of the install, and then initiates the download.
3.7: The OS Maintenance Server (1.6) now records the beginning time of the download in the user's account.
3.8: Upon completion, the OS (1.2) notifies the OS Maintenance Server (1.6) of the completion of the download.
3.9: The OS Maintenance Server (1.6) records the completion time of the download, and flags the user account in the User DB (1.9) so that the DRM Subsystem can not be downloaded again for that license key without prior approval.
3.10: The OS (1.2) proceeds to install the DRM Subsystem (1.5) onto the user machine (1.1).

**Figures:**

**Figure 1: System Diagram**

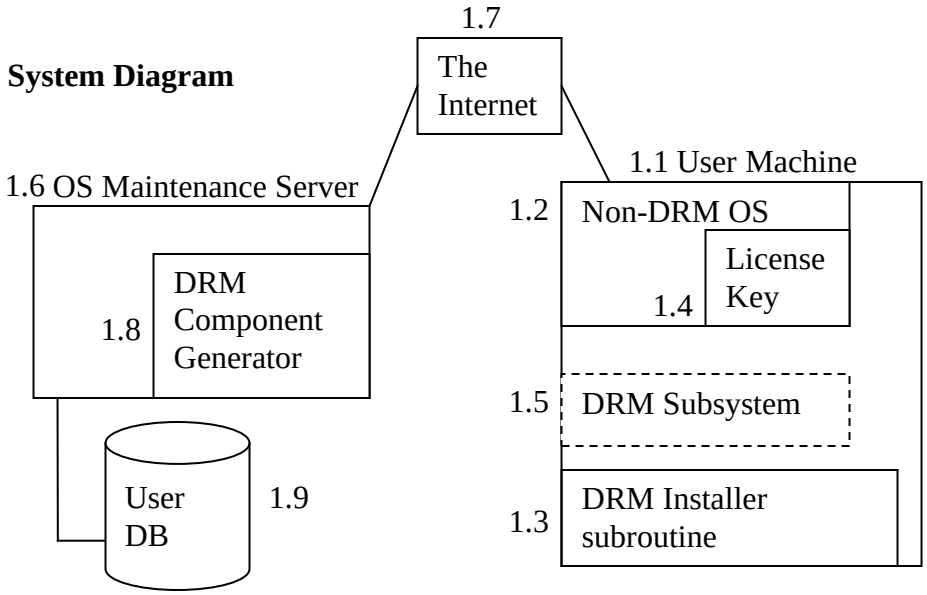

**Figure 2: Flowchart Illustrating OS Install Process**

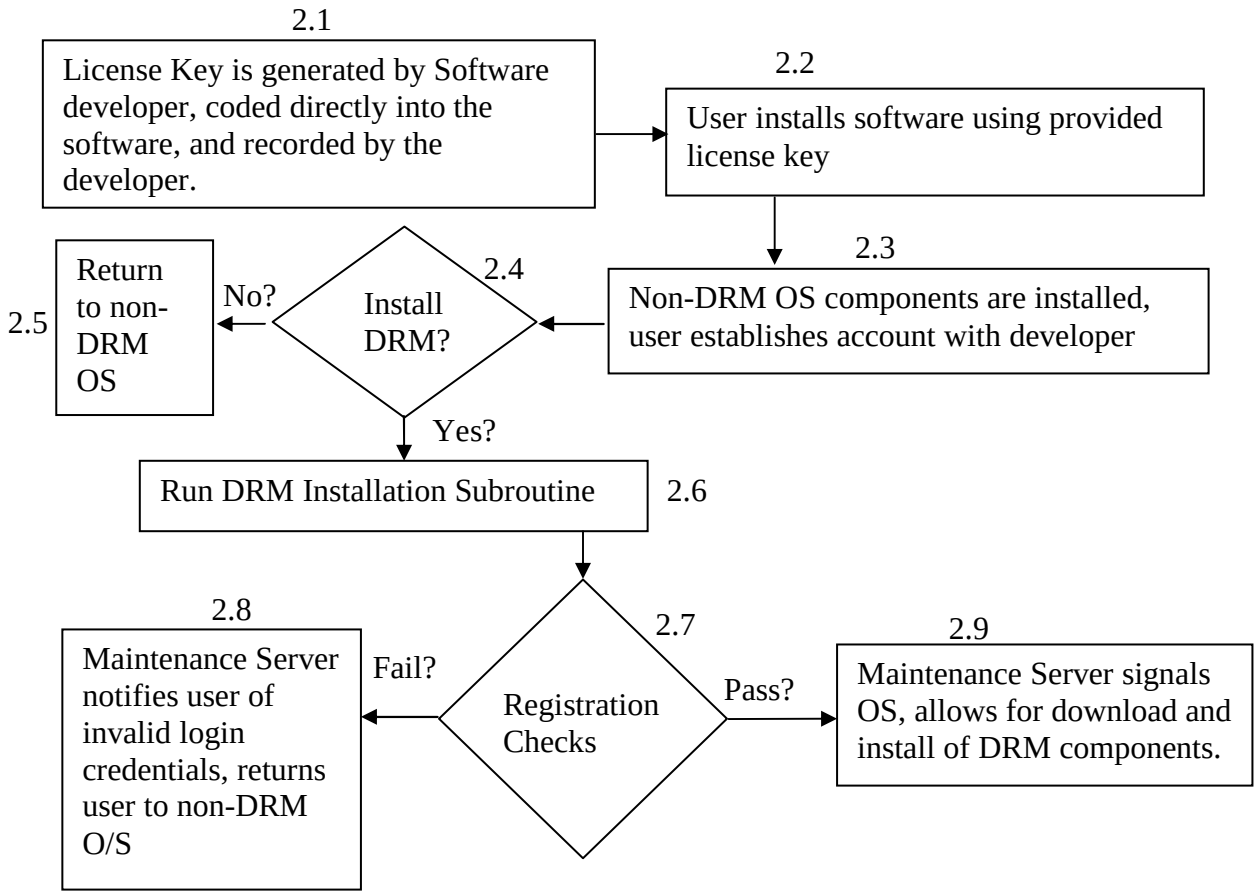

**Figure 3: DRM installation process**