White Paper Wibu Licensing

Introduction

Wibu-Systems AG is a German software company that specializes in providing license management solutions for software vendors. Wibu licensing is a form of software protection that allows software vendors to control the distribution and usage of their software.

Wibu licensing uses hardware-based protection mechanisms such as USB dongles or smart cards or a software-based protection called Smart Bind to ensure that only authorized users can access the software. This type of licensing is commonly used for high-value software applications or in industries where the protection of intellectual property is critical.

The SmartBind mechanism is a protection and licensing solution for software applications. It works by binding a software license to a unique hardware fingerprint of a computer, which is generated based on various hardware components such as the CPU, motherboard, network adapter, and hard disk drive.

When a user installs a software protected with SmartBind, the license is bound to the specific hardware configuration of that computer. This prevents users from transferring the software license to another computer, as the license will only work on the original machine with the same hardware configuration.

Wibu licensing allows software vendors to implement flexible licensing models, including node-locked licenses, floating licenses, and pay-per-use licenses, among others. These licensing models provide software vendors with greater control over the distribution and usage of their software, enabling them to generate more revenue and reduce piracy.

The CODESYS Store and single device licensing

The CODESYS Store is an online marketplace for software add-ons and plug-ins for the CODESYS development environment. It offers a wide range of software components, libraries, and add-ons that can be used to extend the functionality of the CODESYS development environment. These components include device drivers, communication protocols, visualization libraries, and many other tools and modules that can be used to build complex automation systems.

The CODESYS Store provides developers with a centralized location to find and purchase software components for their CODESYS projects. The store also provides a platform for software vendors to sell their CODESYS-compatible products to a global audience.

In addition to offering software components, the CODESYS Store also provides technical support and resources to help developers get the most out of their CODESYS development projects. This includes documentation, sample code, and tutorials that can help developers learn how to use the various components available in the store.

The CODESYS Store is a valuable resource for developers working with the CODESYS development environment, providing a wide range of software components and resources to help them build complex automation systems with ease.

Single Device Licensing is a software licensing model that allows users to license the CODESYS Control SL as well as other software functionalities for a single device. With Single Device Licensing, users can purchase a license for a single device and install it on a device. This allows them to develop and deploy their automation application on that device without any additional licensing costs.

Single Device Licensing is available for a variety of CODESYS runtime systems, including CODESYS Control for Windows, CODESYS Control for Linux, CODESYS Control for Raspberry Pi, and any CODESYS PLC from a device vendor, if the vendor decides to support single licensing. The single device licensing feature is part of the CODESYS runtime toolkit for hardware manufacturers.

The licensing process typically involves purchasing a license key and activating it on the device where the CODESYS runtime system is installed.

Single Device Licensing provides users with a cost-effective and flexible licensing option for automation applications, allowing them to develop and deploy their applications with ease. Additionally, the CODESYS development environment provides a range of tools and resources to help users develop and customize their applications to meet their specific requirements.

CmDongle vs. CmActLicense

CmDongle and CmActLicense are both methods of software licensing and protection provided by Wibu-Systems AG.

CmDongle is a physical hardware device that is plugged into a computer's USB port (alternatively Flash card ports) to act as a license key for software. The dongle contains encrypted information that is used to verify the authenticity and validity of the software license. This method of protection is often used for software that requires a high level of security or in industries where software piracy is a significant concern.

On the other hand, CmActLicense is a software-based licensing solution that does not require any additional physical hardware. Instead, it uses a unique combination of machine characteristics and a software license file to verify the authenticity and validity of the license. This method is more convenient and cost-effective for software vendors wishing to protect their software without the added expense of manufacturing and distributing hardware dongles.

In summary, CmDongle is a physical device used for software licensing and protection, while CmActLicense is a software-based licensing solution that doesn't require any hardware. CODESYS licenses support both ways of protection.

Use of CmDongle

CmDongles work without any adaptations, as long as the device provides USB ports, SD or micro SD ports to plug in the CmDongle device. The following devices are supported by CODESYS:

- All variants of Wibu CmSticks

Other devices on request:

- Wibu CodeMeter ASIC
- All variants of Wibu CmCard
- Swissbit CmReady devices

How to support the Single Device Licensing feature for CmActLicense

(Hier kommt ein Bild, bitte aus Confluence entnehmen: https://confluence.codesys.com/pages/resumedraft.action?draftId=203718797&draftShareId=589bc6a9-f597-4056-9bd2-49951bc9b5b5&)

CODESYS-encrypted runtime

CODESYS provides the option to encrypt the CODESYS runtime for device vendors with the Wibu Ax IP protection mechanism.

Ax IP Protection is designed to prevent the unauthorized use or distribution of software applications by protecting the intellectual property (IP) of the software vendor.

Ax IP Protection uses a combination of software and hardware protection mechanisms to safeguard the software application against reverse engineering, tampering, and piracy. The solution works by encrypting the software code and binding it to a specific hardware device or dongle.

In addition to protecting the software code, Ax IP Protection also includes licensing and activation mechanisms that enable software vendors to control the distribution and usage of their software applications. This allows vendors to enforce license compliance and prevent unauthorized use of their software.

Overall, Ax IP Protection is a comprehensive software protection solution that provides strong security and flexibility for software vendors looking to protect their intellectual property and ensure that their software applications are used only as intended.

Wibu Container Files

A Wibu container file is a file to store and manage license information for CODESYS software products. The Wibu container file typically has the extension ".WibuCmLif" and contains encrypted license data.

The container file is used to generate a Wibu container, which is able to receive the Wibu license. Depending on how the licenses shall be bound to the hardware (Smart Bind or Binding extension) different container files have to be used.

Wibu container files are designed to be highly secure and difficult to tamper with, in order to prevent software piracy and unauthorized use of protected software products.

Wibu Smart Bind

Wibu Smart Bind is a software protection mechanism that binds a license to a specific computer hardware configuration, such as the hard disk, CPU, or network adapter.

This binding ensures that the licensed software can only be used on the authorized machine and cannot be transferred or copied to other computers, thereby preventing unauthorized usage and software piracy. Smart Bind also provides additional security features such as tamper-proof protection and encryption of the licensed software.

In summary, Wibu Smart Bind is a security technology that helps software vendors protect their intellectual property by binding software licenses to specific hardware configurations, ensuring that the software is used only by authorized users and devices.

Wibu Binding Extension

When Wibu Smart Bind fails on a specific hardware, the most probable reason is that there were not enough hardware criteria to bind the license to. Wibu is continuously expanding the number of binding criteria for Smart Bind, but this is not generically possible for any hardware and firmware without side effects. This is where the Binding Extension comes into play.

The Wibu Binding Extension is an interface for the CodeMeter Runtime. With the use of the interface, the device vendor can implement the binding of licenses to the hardware by himself. CODESYS then reviews and assesses the implementation to be as tamper-proof as possible, and then the Binding extension gets signed by CODESYS.

Once the Binding extension is signed by CODESYS, single device licenses from the CODESYS Store can be installed on that device.

Overall, the Wibu Binding Extension provides a robust and flexible solution for software protection and licensing, and is used by many software vendors across various industries.

CODESYS SysTargetGetSerialNumber_Secure

Whenever the CodeMeter runtime does not run on a device because the OS is not supported or a supported OS is not able to execute the CodeMeter runtime due to missing system libraries (sometimes the case with Yocto linux versions), the CmEmbedded implementation can be used.

The CmEmbedded is already integrated in the CODESYS runtime system as a core component and can be added to the runtime on delivery by CODESYS (upon customer request). When this is done, the function SysTargetGetSerialNumber_Secure of component SysTarget needs to be implemented by the device vendor.

The function has to return a unique and tamper-proof ID of the system. The implementation of the device vendor needs to be assessed by CODESYS as part of the runtime system adaptation. Once this is done, single device licenses from the CODESYS Store can be installed on that device.