FALL 2013

KEYnote 26

THE WIBU-MAGAZINE

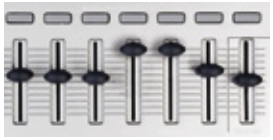
Easy Integration into Software and Processes

Topics

- Scalable Licenses with CodeMeter
- AxProtector – Simply Safer
- SmartShelter PDF: Protecting and monetizing documents

WIBU SYSTEMS

Content



Dear Clients and Partners of WIBU!

Hardly a day goes by without a mention of PRISM, Tempora, or XKeyscore in the media. Behind the acronyms, the private information of citizens is at stake – and so is industrial espionage. In business, know-how is essential for survival. It can take many forms: algorithms or software processes in IT or parts and components built into physical devices and machines. Manufacturing data, which can include invaluable intellectual property and production know-how about the complete product, is also affected. In an ever more integrated world, the 'security' of open systems has become a top priority. Governments across the world are actively investing into research in the field, be it in Europe with its ISO62443 standards, in the United States ISA99, or in Asia.

Protection against these threats needs increasingly sophisticated solutions. Licensing and monitoring are becoming more and more important in traditional IT to give users as much freedom to use their products as possible, but still allow accurate billing. In manufacturing, resilient protections have become essential in the fight against cyber-attacks and illicit manipulation. With CodeMeter, our research and development efforts cover both flanks: CmLicenseCentral has expanded modules such as retail, usage metering, and electronic software distribution functionality; our tools make integrity protection easier and more effective; and we are supporting more and more industry environments and standards. We do this to give our users a system they can depend on for the long term with solutions that fulfill their requirements both today and tomorrow.

Read this issue of KEYnote with its featured topic "Simple Integration in Software and Processes" for interesting and useful news for your applications. Our support team is always available if you have any questions about our solutions.

Before the end of the year, we will be attending many conferences and expos around the world. Come and see us – our specialists and I will be looking forward to seeing you in person! If your schedules do not allow you to meet us in the meantime, I would like to use this opportunity to wish you a great end-of-year business and a pleasant autumn and winter for you and your families.

Yours,

Oliver Winzenried (CEO)

Wibu International Partner Summit 2013

Wibu-Systems global

Wibu-Systems, founded in 1989 by Marcellus Buchheit and Oliver Winzenried, has become a global player in its industry. With subsidiaries in the United States and China, sales representatives in Belgium, France, Great Britain, the Netherlands, and Spain as well as many other distributors around the world, Wibu-Systems offers you and your international teams technical competence and delivery on site, wherever you are.

Financially independent and managed by its founders and proprietors, Wibu-Systems is committed to its medium and long-term vision: giving you, the publishers of software and makers of high-tech devices from across the globe, solutions for software licensing and product protection as well as effective means for protecting your know-how and combatting illicit manipulation and cyber-attacks.

All of our research and development activities are focused at our headquarters in Karlsruhe, with many cooperative ventures with partners and research institutions across Asia, Europe, and the United States. Our product management team is organized to respond to and match the needs of our very diverse markets around the world in the best way possible. The international patents held by Wibu-Systems are testimony to our technical competence and reduce the likelihood of infringing on the legitimate rights of others. Our company is certified according to the ISO 9001:2008 standards and has been awarded many international marks of conformity, including certification from the Underwriters Laboratories (C-UL.US) in the United States and Canada and VDE in Europe to guarantee the risk-free use of our products. Our products are also compliant with many local standards, including CE in Europe, FCC in the United States and Canada, KCC in Korea, RCM in Australia and New Zealand, and VCCI in Japan.

By choosing our production partners and components carefully and building our partnerships on a basis of trust, we are committed to fulfilling the many new requirements in the industry, such as the RoHS and REACH regulations for the removal of hazardous substances from our products, the Joint Industry Guide (JIG), and other measures to avoid the use of so-called conflict minerals. Last, but not least, export regulations are an essential topic in our industry. Users of Wibu-Systems solutions for product and know-how protection can receive the relevant clearances, such as the German non-restricted goods report (AzG) or an EAR99 and NLR (No License Required) rating from the American BIS.

All of these aspects promise you the safe and secure use of the solutions of Wibu-Systems. Guaranteeing this requires all of our expertise at our headquarters and the competence of our representatives worldwide. We offer regular training for the people in our international offices and at our distribution partners to make sure that you – and your colleagues around the world – will benefit from the best possible advice and service in your native language. Come and speak to our sales team if you have any requests or requirements concerning deliveries to specific countries or want to benefit from our global support.

Scalable Licenses with CodeMeter

"Who needs dongles?" Asked first some years ago, this question is becoming more and more frequent in times of increasing virtualization. But the question about specific types of technology or device designs is misguided. What the end user cares about is a flexible and safe means of accessing licenses, regardless of the conditions under which he is using the software in question. This article explores the many and versatile licensing options offered by CodeMeter.

Independent Software Vendors (ISVs) and their end users today have very different requirements and expectations concerning modern license management. It has to be secure and kept up-to-date with the newest advances in technology to prevent illegal copying, reverse engineering, and manipulation of their software. At the same time, the technology is expected to provide flexible licensing models, such as network licenses, feature-on-demand capabilities, pay-per-use or other time-based models in a simple and straightforward manner.

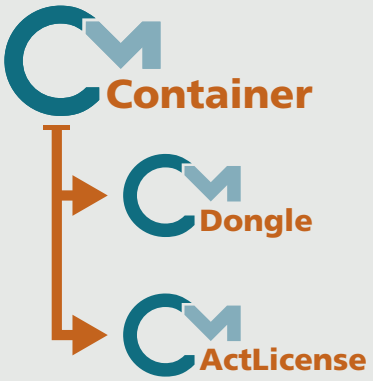
CodeMeter can provide licenses in many forms and formats under a single, unified technological roof. This is our answer to the market's seemingly conflicting requirements: Hardware-based means (CmDongle) for optimal security and flexibility as well as purely software-based activation (CmActLicenses) with an intelligent connection with the target device. Both options can work locally or in networked setups, and the range of licenses can go from unspecified demo licenses (trial licenses) to pure software encryption (protection only). The new CmWAN solution takes this a step further and manages licenses into the cloud.

What the end user wants is to be able to use the licensing model of the software developer effectively and efficiently in the chosen system environment. No vendor's software can be successful if this is not possible. CodeMeter provides a range of options for accessing licenses. The leading edge in security is guaranteed by the CmDongle in its various form factors , storing up to 6000 licenses even from diverse makers and vendors. On request, the ISV can order additional flash storage to have an immediate means of distributing the software to his end users.

CmActLicenses, by contrast, work without any hardware. The patented SmartBind technology allows a secure link with the end user's computer, while still ensuring secure use even in virtual environments

Dongle or Software Activation?

CodeMeter makes this question irrelevant. Irrespective of the eventual choice, the license management solution is integrated by the ISV into the software product. The development relies on so-called CmContainers as a transparent layer on top of the eventual choice of physical or virtual storage for the license (CmDongle or CmActLicense).



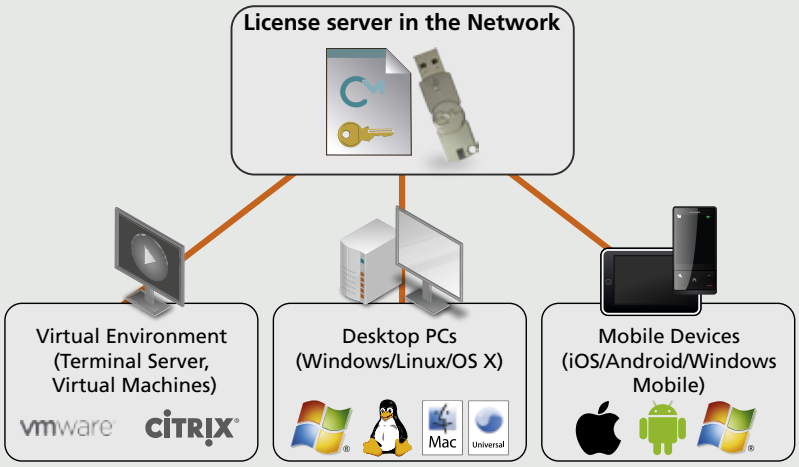
Flexible use of hardware and software-based licenses

The ISV can choose the desired use scenario when the software compiling is finished. It can be distributed with a CmDongle or CmActLicenses, or even a combination of both, giving the vendor utmost flexibility in how he chooses to distribute the software. In the end, the choice of license storage is made at the customer's location. This enables the ISV to respond to different geographic restrictions in license management.

This model is also beneficial for software maintenance. While the software itself remains actively protected by the CmActLicenses, additionally required maintenance routines can be cleared for service technicians via a dongle plugged into the system.

Licenses on Local Networks (CmLAN)

Going beyond the capabilities of locally stored licenses, network licenses promise end users even greater flexibility in the use of their software. Floating licenses (also known as concurrent licenses) are used, where the ISV gives the end user a certain number of licenses for use on a local network.



Using network licenses in mixed networks

Network licenses can be handled by CmDongles or soft CmActLicenses: Simply plug the dongle into the server, or activate the CmActLicense on the computer that will act as the network server.

The CodeMeter Runtime is installed on the chosen license server and on all devices selected for use with these licenses. This allows for as many licenses to be in use simultaneously on the network as the software vendor has provided. Every additional PC would only be allocated a license once a license has been released back into the pool.

Using such network licenses is a particularly effective means in mixed networks in which computers with different operating systems need to access a single shared license pool.

The end user can even operate multiple license servers on a single network to make all licenses in his possession ready and available in the network. This is essential for network strategies, such as effective load distribution and high reliability systems.

Licenses in the Cloud (CmWAN)

Wibu-Systems took the logical next step in the evolution of the CmLAN concept and launched the new CmWAN product with the introduction of CodeMeter 5.0. The innovative technology lets users access licenses not only on their local networks, but even in the cloud via a Wide Area Network connection.

The licenses are not restricted to software running locally either. Even applications hosted in the cloud can work with licenses stored there and take advantage of all of the flexible licensing models offered by CodeMeter. Standard CodeMeter integration makes both local and cloud-based licenses available without any need for the ISV to amend his software.

The HTTPS protocol used for CmWAN allows simple communication even with firewalls in place. The required high security is guaranteed by the client's authentication and by the encrypted connection that is formed between client and server.

From the client's point of view, using cloud-based licenses is straightforward: One simply includes the HTTPS link for the cloud license server on the server search list. The application can then access the licenses stored in the cloud directly.

Licenses – Always available!

There are many ways for ISVs to provide licenses for their end users. Whether they are hardware or software based, kept locally, in the network, or up in the cloud, Wibu-Systems has a single, fully scalable solution for all requirements. No need for end users to compromise: Their licenses are available whenever and wherever they are needed.

Secure Boot

Micro-controllers and electronic controls govern our lives. From nuclear power plants to factories and commuter trains, they are everywhere. Less than a decade ago, most control systems were innocuous little boxes with proprietary hardware and software, completely isolated from the wider world. When one stopped working, the service technician would have to physically come to the device. Time and cost constraints have forced more and more control systems to go online, where service technicians can handle multiple incidents remotely from the comfort of their workstations. This new comfort also means a new threat: **Cyber-physical attacks**.

Motivations for Attacks

Integrity: Why should people manipulate machine controls? Is this the territory of secret services and terrorist organizations? It can be, as Stuxnet has shown the world. Saboteurs? It might sound unlikely, but what is hacking unprotected control systems if not sabotage? When control systems operate offline, the saboteur needs to be physically present to cause any damage. He needs to gain access, and might be caught in the act. A system operating online minimizes the risk for the hacker using a cyber-attack. The hacker can tap into entire pools of knowledge and even work anonymously with many likeminded attackers. The motivation is irrelevant, be it a political message, an attempted extortion, or simply a hacker showing off his skills.

The facility's operators could also try to "soup up" their machines and plants. However, operating manufacturing machinery outside of its intended parameters has many risks, with more wear and tear being the least worrying scenario. The machines' original producers want ways to stop or at least prove such manipulation for warranty and liability reasons.

Confidentiality: Industrial espionage remains a risk that is too often overlooked. But the operating parameters or control concepts of manufacturing facilities are very interesting prey for competitors. Remote connections again make data theft easier. Cinema might have us believe that one could always see who is accessing what data at what time, but real-life systems often only record log-ins via protocols that are too easily manipulated. Data theft often goes by unnoticed, and the thief can analyze his "loot" leisurely offline.

How can I protect myself?

Many modern control systems use standard hardware, such as industry-grade PCs with standard operating systems like VxWorks, QNX, Windows, or Linux Embedded. Run-time environments in control systems often also employ a shared standard (such as CODESYS). Any remote network should be protected by VPNs and firewalls, but these offer no sufficient protection for the control systems themselves. Once past these hurdles, any attacker is free to do as he likes in the network, and many service technicians store the passwords or access keys for the VPNs of their clients on unprotected laptops. No chain is stronger than its weakest link, so a single absent-minded technician or a single weak password can undermine the security of the entire system.

Firewalls and VPNs can have loopholes and backdoors. Encryption keys are often too short, especially when using with RSA. Recent events

have shown that the security promised by such systems must not be seen as the ultimate ratio. The downside of the media revelations is that potential attackers now know about new weak points to exploit.

Physical separation is no protection. In any business, many different people can access control systems. Service technicians access devices right on site with their laptops. Backups of the control software and its process parameters are stored elsewhere again.

Protection therefore needs to start on the target system, that is, the controls themselves. The control system must only run code and use only such configurations and parameters that have been cleared by an authorized party.

Most control systems are field-upgradeable. New features can be added and errors remedied. Such updating capabilities are, however, a chink in the system's armor, which a malevolent attacker can use to inject his own manipulated code remotely or even right on the device. To prevent this, the system needs to boot and run in a secure environment. All of its components from the bootloader up need to be cryptographically authenticated as trustworthy. This is called a secure boot.

How does Secure Boot work?

The individual components of the control system are signed digitally by the producer or plant engineer. But who would check which components? When and where would these checks happen? A first approach is to have each layer verify whether the next layer can be started: The bootloader checks the operating system, the operating system the run-time environment, the run-time environment the application and so on. For this chain to function, the public key must never be changed at the first layer (i.e. it needs to remain authentic). That means that the first layer must be permanent and unchangeable. It is the secure anchor of the chain. The optimum in security would be a pre-bootloader, physically built in as a system-on-chip (SOC). A cheaper alternative is to use a dual bootloader whose first part cannot be updated to offer at least adequate protection against remote threats.

Is my environment safe?

Additional security requirements have each layer check whether the previous layer has been processed correctly. CodeMeter offers both means – forward and backward checks. The backward check is handled by a state engine on the CmDongle and an encrypted solution coupled with that state engine. The next layer can only be decrypted once the previous layer has been processed correctly and the right state is recorded on the CmDongle. This prevents individual parts of the software from being simulated in the attacker's lab, and it precludes any analysis of the software in the environment. Espionage becomes impossible, as does the search for possible exploits or implementation errors. The device benefits from the additional shield.

Conclusions

Secure boot and integrity protection that use signatures and encryption are a mainstay of all secure controls. They make physical attacks substantially more difficult and prevent virtually all cyber-physical attacks.

CodeMeter offers a solution that is engineered to burrow deep into the device and requires all components to verify each other. Permissions can be defined in fine detail to match the relevant use case. CodeMeter protects – against espionage, manipulation, and sabotage.

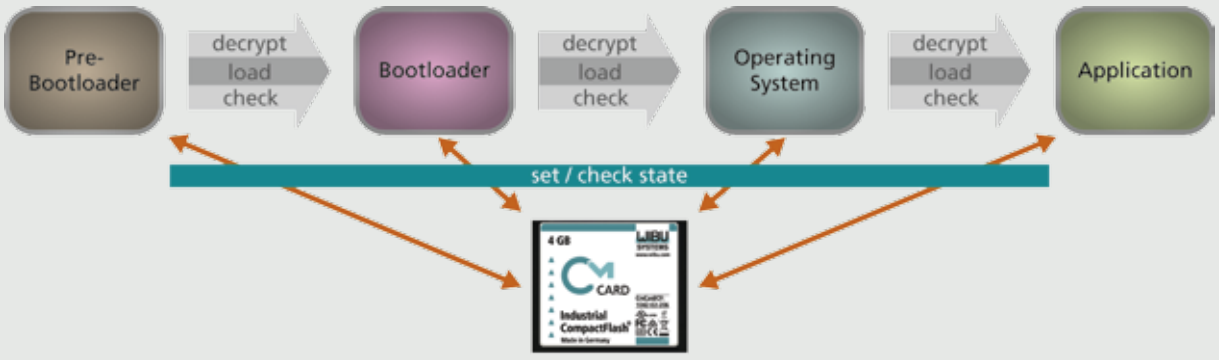
Why so complicated? Why not simply use a hash?

Any asymmetric cryptography like ECC relies on the use of a private and a public key. This makes reversing the encryption mathematically impossible – the private key cannot be recovered from the public key.

The private key is kept safe – for ideal safety, on a CodeMeter Dongle. As the name implies, the public key is available to everyone.

So why use two keys? The private key is used to create a signature, which only the key holder can do. The public key then verifies the validity of the signature, but it cannot be used to create a valid signature by itself.

A hash function with or without random salt , by contrast, uses the same key for creating and for verifying the hash value. This means that anybody who can test the hash can also create a valid hash. Signatures should never be substituted by hashes. The end result is only a deceptive sense of security.



AxProtector – Simply Safer

Protecting software should be simple and secure. Two mutually exclusive goals? They do not have to be. Learn how to integrate fraud protection easily into software and embed the protection system seamlessly into existing processes with Wibu-Systems' AxProtector.

Protecting intellectual property and making sure that only legitimate license holders use their products are just two of the many challenges faced by software developers and vendors. Software products are distributed in many forms and ways, as executable programs or libraries. Whether the software is meant for Windows, Mac, or Linux systems, the answer to these software protection challenges is AxProtector.

The term AxProtector (Automatic Executable Protection) refers to tools for the automated protection of compiled programs of varying types, ranging from "true" binaries (e.g. scripted in C/C++ or Delphi) to pre-compiled code for .NET for Windows or cross-platform Java. All of these program types can be protected with the versatile means offered by AxProtector.

A Unified Interface

Once AxProtector is started, the user chooses application type. This leads to an interface that guides the user through the process of turning an unprotected program into a fully encrypted program in a few simple steps. No complex instructions are needed. AxProtector supports multiple licensing systems, which means that a single program can be encrypted for use with different licenses (e.g. hardware-based CmDongles or activation-based CmActLicenses). Both options can be allowed concurrently, and the program itself finds the right license upon launching. A simple setting determines how the license for the protected software is counted (e.g. once per launch of the program or only once per computer). Setting whether and how often the license should be verified is just one or many setting options, which are already preset with a reasonable default value.

Protecting against Attacks

The protected software learns to recognize manipulation or attacks attempted by hackers. Such incidents immediately lead to the license in question being locked down. Your intellectual property is safe and future attacks are prevented. In addition to the keys stored in the licenses, there is a variable key on the software side to make the encryption unpredictable. AxProtector also checks whether the software has been tampered since its original encryption and prevents it from running if any manipulations are identified.

More Protection - IxProtector

The high level of security promised by automated encryption can be improved even further by adding function-level encryptions. Specially selected functions are encrypted separately and only decrypted into executable code when they are required. We call this protection technology IxProtector. It is just as easy as AxProtector to integrate into a software product - marking the function in question, add a simple API for requesting decryption, and flag the function in the settings – that is all there is to it.

The different formats used in .NET and Java applications mean that protection generally happens via method or class-level encryption, which is decrypted automatically as required during operation.

Few steps are required to include modular protection and the reading and use of license details. The interface can define additional licenses (e.g. for separately licensed modules). The Wibu Universal Protection Interface (WUPI) can verify whether these additional licenses are available while the application is running, and the function-level encryption allows the modules in question to be shielded as necessary.

Comfortable Notifications

When neither basic nor additional licenses are available, a flexible error handling system springs into action. The AxProtector settings and the so-called UserMessage library allow customized responses and notifications for the user. The application can display a custom error message or a protected service can record the incident in a secure log file.

Simple Process Integration

The protection should be embedded deep into standardized processes to make sure the software is protected during its original testing. The encryption of applications or libraries can be integrated readily into the build process. All parameters defined via the AxProtector interface can be exported to a configuration file at the click of a button to allow automatic encryption via a simple command line entry.

Protecting Your Investment

Wibu-Systems regularly publishes new versions of AxProtector with new and improved security mechanisms. These free updates improve the security of your products without any additional efforts on your part and maintain your head start in the race against potential attackers.

AxProtector protects the following types of programs:

- Windows applications (32-bit, 64-bit)
- Windows libraries (32-bit, 64-bit)
- Mac OS X applications (32-bit, 64-bit)
- Mac OS X libraries (32-bit, 64-bit)
- Linux applications (32-bit, 64-bit)
- Linux libraries (32-bit, 64-bit)
- .NET Assembly
- Java applications
- Java Servlet

Simple & Secure

AxProtector allows you to give your applications or libraries double protection in a few simple steps. The software is protected both against piracy and against the malicious analysis of your code. Protect your revenue stream and secure your invaluable know-how at the same time.

AxProtector Embedded Systems can guard applications on the following platforms:

- Linux ARM
- Windows Embedded
- Android
- VxWorks

SmartShelter PDF: Protecting and Monetizing Documents

Protection against piracy is a proposition which has been around for a long time in the software development arena and is very familiar to most software vendors. But, what about document licensing and protection? How can revenues be guaranteed or even multiplied from sale and accurate management of documents? Does this topic need to be dealt with differently because the finer details are more complex than with standard software? The article explains similarities of the two scenarios and peculiarities of secure document handling from a business oriented point of view.

The exchange of information is a fundamental part of our communication culture. Nevertheless, it shouldn't always be possible to duplicate information or grant free access to it. Know-how within a company should be protected, with access only granted to particular groups of people such as service technicians in order to hinder industrial espionage. In this day and age of globally networked systems, managers need to think about digital documents in a completely new dimension and implement the necessary measures to protect them. In line with the motto "One Technology fits All", with CodeMeter® Wibu-Systems offers a comprehensive solution which does not only fulfill the requirements of document files, but also those of traditional PC market, industrial devices and cloud-based infrastructures.

Easy document protection

Back in the early nineties the software company Adobe® introduced PDF, an exchange format for digital content. Today this format is recognized as an international standard. The functional scope of Adobe® Acrobat® includes a document protection system based on password assignment. However, there are two fundamental problems with passwords; first there's no way to prevent them from being passed on, and secondly, they are often far too short and obvious which makes them easy to crack.

The basic idea behind passwords is in principle correct but in practice the security they offer is usually worse than bad, to say the least. Long and cryptic passwords are not the solution either as they are not practical for everyday use. A better solution would be to generate passwords automatically and store them immediately in a secure hardware dongle or software license.

Plugin controls encryption and licensing

Wibu-Systems' approach to the solution makes use of Adobe Acrobat's encryption technology. Following installation, SmartShelter PDF® nests itself into the program as a plugin and provides the user with various functions for generating protected documents. The plugin is available for both Windows and Apple Macintosh. A globally unique Firm Code generated directly for the user by Wibu-Systems and an arbitrary Product Code form the backbone of the security concept. Combined together, the result is a use license for the document which can be stored in either a hardware dongle (CmDongle) or a soft license (CmActLicense).

Before the document can be encrypted, the SmartShelter PDF plugin must be started. The publisher of the document enters the required Product Code. The SmartShelter PDF plugin encrypts the document and generates an extremely secure password which it safely

stores in the dongle or soft license. The user never comes into contact with the password again. If the procedure described above is used extensively in an automated environment, SmartShelter PDF can be implemented as a command line tool.

SmartShelter PDF Plug-in

Options for document use

Document usage, such as printing or editing, can be controlled by granting or denying permissions. It is also possible to restrict use of the document to the Acrobat Reader only. Protection can be tightened even further, e.g. screen shot capturing can be disabled and a debugger check can be activated to close the document as soon as it detects a debugger running.

The customer only needs to install a SmartShelter PDF plugin for the freely available Acrobat Reader®. If he owns a CmDongle or CmActLicense with the correct firm code and product code combination, he can now open the encrypted document.

Flexible license models facilitate monetization

The CodeMeter technology used by SmartShelter PDF not only provides protection functionality for documents, but also allows flexible license models. The possibilities range from time-limited licenses through pay per use to network license models, and include any combination thereof. Hence new models for generating revenues from the sale or use of documents can be defined. The concept of arbitrary product codes permits a role-based permissions strategy for protecting documents.

License distribution made easy

There are a number of ways to distribute licenses. If a permissions system has been implemented, CmDongles and CmActLicenses with the corresponding permissions levels (licenses) can be pre-manufactured and shipped to the user as and when required.

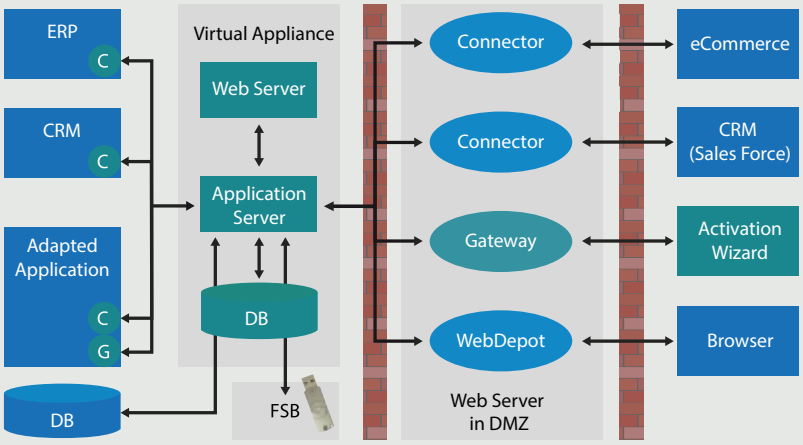
On the other hand, online activation, as provided by CmLicenseCentral Internet, offers greater flexibility for both the publisher and the user. In this case licenses are not generated in advance, but are fetched online directly by the user from the publisher's server. This means a web shop, for example, can sell and distribute licenses worldwide, 24 hours a day, 7 days a week.

To begin with, the publisher stores the licenses for sale as products in CmLicenseCentral. When a user purchases a particular product, the license publisher sends him a ticket by email. The ticket can be redeemed for the licenses at the publisher's web portal. The licenses are then transferred to the CmDongle or activated in the CmActLicense immediately.

CmLicenseCentral Internet can also be integrated into the publisher's existing processes. This can be accomplished using web interfaces. In this case, connection is possible to existing internal or external ERP or CRM systems which directly accept customer orders and generate the corresponding tickets. An alternative is the direct integration into a publisher's shop system.

Summary

If you desire a system which simultaneously protects your documents and implements appropriate license models for your users, then SmartShelter PDF is the ideal solution. Not only does it protect documents, it also allows you to generate and distribute licenses for the documents. So SmartShelter PDF is on the one hand the right choice for editors, who want to get paid for each copy and on the other hand for companies that want to distribute chargeable content or want to protect their manuals, patents and legal documents. In doing so it optimally fulfills the requirements of small business solutions as well as those of complex document management systems.



Flexible integration of CmLicenseCentral Internet into existing processes

Customer Portal

As an Independent Software Vendor (ISV), you might be wondering: "Why do I need a customer portal?" The answer is simple: "Because you want to **sell more** and **save internal process costs**!" You can do this with a licensing, protection, and security solution like CodeMeter. The customer portal is only one of many means of achieving your objective. This article shows you how a customer portal can help you and presents other options it has to offer.

What is a customer portal?

A customer portal is a web application that enables users to see and manage the licenses they own. Your user simply logs into the portal with his user name and password or a dedicated license key – the ticket. Once he is logged in, the user gets an overview of which licenses and software products he owns. He can see which licenses have been retrieved or activated, activate licenses right there, and download the software that goes with the license. Additional deactivation and reactivation functionality can be offered as an option. The portal allows the user to even register licenses acquired via a reseller.

In short, you and the user get a one-stop place to see all of the licenses bought by a single client.

How does this help me sell more?

Up-selling and cross-selling to established clients is easier and more cost-effective than acquiring new clients. Doing so efficiently means knowing which licenses the client already owns. Software products and their licenses are often sold via resellers, and few ISVs know their end users personally. You can offer your clients the opportunity to register all of their licenses via the customer portal. Incentives like discounts on additional modules or access to exclusive online content can help motivate the user to do so.

The benefits are substantial for you and your clients. You are given an overview of the licenses held by the user and can pick and mix the right packages for him. The customer portal also gives you a great canvas for showcasing your new offers, whether they be updates to existing products, upgrades with new and exciting functions, or completely new products that might fit the user's tastes and needs. In addition to targeting the user via the portal, the data also helps you mix and match your newsletter effectively.

How does the user benefit?

Registration via the customer portal offers benefits not only for you as the ISV, but also provides advantages to the user. The time of lost licenses has ended. No more looking for license keys bought years ago when the operating system is reinstalled or software needs to be migrated to a new computer. No user likes to lose the software he has become familiar with. The customer portal gives the user access to all of the licenses he owns. All he needs is his email address to get his password renewed if he forgets it in the meantime.

The user will also find up-to-date information about whether and which updates are available for his products. Updating software is often inevitable to ensure it is functioning correctly, especially when a new operating system has been installed.

How can I save costs?

Depending on the target group, the typical end users will change computers or reinstall their systems every one to five years. With licenses kept on a dongle or CmStick, no new activation would be required after such a system change. The case is different with soft licenses like a CmActLicense, which require the new device to be activated. Current legislation means that the user is entitled to use the license. Typically, binding a license to one machine and deleting it when that machine has reached the end of its life is not allowed. Requiring a new activation cuts both ways: The user is required to do it, and you as the ISV are required to provide the means to allow him to.

This is where the customer portal comes into play. You define the rules for deactivation and reactivation to match your specific product and its target group. For instance, you can state that the user can deactivate a license at any time and reactivate it on a new machine once it has been cleared again. In cases in which deactivation is not possible, you can allow a defined number of initial reactivations – including "no more" reactivations – and a point at which the customer would be allowed to reactivate the license – e.g. "after one year". These options enable the user to manage and transfer licenses himself via the customer portal, but within the framework defined by you. Support would only need to intervene in cases that go beyond that framework. You stay in control of the licenses you have sold, but minimize the need for support resources substantially.

Who uses my software for how long?

As an ISV, you are naturally interested in knowing how frequently and for how long your users employ a specific version of your software. Again, a customer portal can be the answer: With automatic registration capabilities built into your software, your customer portal can receive detailed usage data whenever the software is used. Giving the end user access to exclusive online content can be an incentive for allowing such monitoring. At the same time, the system can check and verify whether the user's license is still valid.

Even without automatic registration, tracking the number and distribution of activation and reactivation incidents allows you to estimate the average lifespan of a PC or software product in your target group.

How can CmLicenseCentral help me achieve this?

CmLicenseCentral helps you implement a customer portal. With the Web Depot, CmLicenseCentral includes a compact stand-alone solution that is ready for use out of the box. You simply change the layout to match your corporate design and define the rules for deactivating and reactivating licenses, providing immediate relief for your support personnel. The Web Depot comes with the following functionality:

- Online license activation and deactivation
- Offline license activation and deactivation
- Automated reactivation

Depending on your established infrastructure, the Web Depot's modular design allows its expansion into a full-service customer portal and integration with existing systems. The following modules are included as standard:

- Customer login (stand-alone)
- Customer login (integrated as single sign-on)
- License overview
- Customer registration
- License / Ticket registration
- Ordering and creation of trial licenses
- Creation of emergency licenses

With these modules at your disposal, you can tailor your customer portal to match your requirements and integrate it with your established systems. You can integrate the CmLicenseCentral functionality directly into existing portals via web services (SOAP). CmLicenseCentral delivers optimum flexibility and complete integration.

Latest News Summary

World Premiere: CmCard/CFast

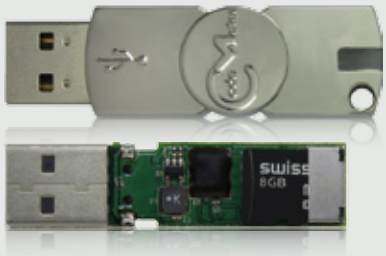
The CmCard/CFast combines the CodeMeter smart card chip and high-reliability SLC flash memory with a fast SATA II interface. SMART monitoring, power fail protection, and fixed BOM are among the many new features of the card (available from 2 to 16 GB).

Internal CmStick/IV

Wibu-Systems CmStick/IV for integration into computers or other devices is increasingly popular with users. Designed for compact mainboard layouts, the new CmStick/IV (internal vertical) model completes the CmStick/I and CmStick/CI line-up.

New CmStick/M

CodeMeter functionality, hardware-based AES encryption, and top storage flexibility are the marquee features of the CmStick/M 1011-03. The new model will be available in Q1 2014 with industrial-level SLC flash memory (128 MB to 16 GB) for greater temperature ranges or MLC (8 GB to 128 GB).



WHQL Certification

The CmCard/SD (4 GB) and CmStick for USB interfaces have completed the Microsoft Windows Hardware Quality Lab test as part of Wibu-Systems' regular compatibility testing in the first half of 2013. This guarantees trouble- and hassle-free use for our clients.

Microsoft Partner

Gold OEM

New RCM Mark

Wibu-Systems is fully registered with the Australian authorities. All products of the company have now also received the new Radio Compliance Mark (RCM).

Oliver Winzenried Confirmed in Industry Association Roles

Wibu-Systems is committed to working in industry associations to stay in touch with the needs and requirements of software publishers and industrial users. Oliver Winzenried is proud to have been confirmed as a member of BITKOM's governing board and elected as Chairman of the "Protect-ing" Working Group of the VDMA.

Expanded Qualification Tests

The test range in the preliminary qualification of CodeMeter hardware has been expanded with a dedicated climatic test cabinet for temperature and humidity tests.

Successful Webinar Course

Adding to our acclaimed workshops and seminars, our regular webinars have gained great popularity among clients and many other interested participants. Our webinars hosted in cooperation with specialists like Wind River, 3S-Smart Software Solutions, or charismathics offer interesting insights into many new perspectives. Register now – It is worth it!

CodeMeter SDK 5.10

The new runtime 5.10 allows the quick integration of remote updates in CmDongles, especially for cases with multiple product items. A new interface has been developed to enable Java-free in-browser use. AxProtector .NET 9.0 can now obfuscate methods, deploy traps, and configure caching for unencrypted methods. For more details about the changes, see the release notes.

Customer Satisfaction Survey

Working with TNS Custom Research, we have again asked our clients for their opinions about Wibu-Systems. We thank all of our customers for their interesting insights. Beyond the individual responses, the survey revealed a strong wish for top security, even if it comes at a cost. Our clients appreciate our cross-platform solutions with CmActLicense activation and the versatile range of CmDongles just as much as our flexible means for the back-end integration of our CmLicenseCentral with their sales processes.

Congratulations to Jens Kopf, Product Manager at Pilz GmbH & Co. KG! He was chosen at random from the survey respondents as the winner of a special "Dinner for Two".

Propellerhead Success Story

propellerhead

Formed in 1994, Propellerhead Software is a privately owned company based in Stockholm, Sweden. Renowned for its musician-centric approach, Propellerhead has created some of the world's most innovative music software applications, mobile apps and technology standards.

Musicians, producers and the media have praised Reason, ReCycle and ReBirth applications for being inspiring, great sounding and of superior quality. The music making iOS app Figure won Apple's App of the Year in several markets in 2012. Technologies such as ReWire and the REX file format are de-facto industry standards, implemented in all major music software.

Today, Propellerhead's products are used all over the world by hundreds of thousands of professionals and enthusiasts for all kinds of music making.

The challenge

Our challenge was to find a solution that was safe and cost effective, that had enough infrastructure around it for us to integrate it with our licensing and distribution systems, but at the same time was open and accessible enough for us to be able to minimize long term dependency risk.

The solution

CodeMeter allows us to provide multiple licensing options for the end user, which they really appreciate, since they have different needs. Case in point is that we can scale the same solution from single private customers all the way up to site licenses that involved

hundreds of seats, and the solution works equally well in all cases. The API's also allowed our engineers to make a low level integration between the encryption mechanisms and our software, that allows for an unparalleled security

The success

So far, Wibu have provided a very reliable solution for us, both in terms of technology and support. A customized CmStick as "Ignition Key", the embedded variant CmStick/CI and the activation based solution CmActLicense give us highest flexibility and benefits.

Ernst Nathorst-Böös
CEO Propellerhead:
"Using Wibu's world class software protection technology, Propellerhead have been able to create a licensing solution that makes perfect sense for the end user and that not only protects our interests, but also those of our partners, that are creating add-on products for our platform. Without this system I doubt that Rack Extensions would have been anywhere near as successful as they are."

Product training

Wibu-Systems organizes several product training sessions each year for the implementation of software protection, software licensing, document protection, media protection, and access control.

You can register for an open training or a special in-house session with an unlimited amount of participants from your company. The open trainings start at 09.00 a.m.; the maximum amount of participants is 6. The sessions can be held in English, Dutch, or Spanish. In-house training can be adapted to meet your specific requirements.

Training location	Protection & Licensing of Software, 1 day, £ 373 / € 399 per participant	CmLicenseCentral Desktop, 1 morning, £ 186 / € 199 per participant	CmLicenseCentral Internet & Back office Int., 1 day, £ 373 / € 399 per participant
Antwerp (B)	05 November 2013	06 November 2013	06 November 2013
Paris (FR)	20 November 2013	21 November 2013	21 November 2013
Driebergen (NL)	26 November 2013	27 November 2013	27 November 2013
Hengelo (NL)	21 January 2014 2	2 January 2014	22 January 2014
Milton Keynes (UK)	19 February 2014	20 February 2014	20 February 2014
Madrid (ES)	05 March 2014	06 March 2014	06 March 2014

Masterclasses
Smart & secure software licensing

Wibu-Systems offers you the opportunity to participate in one of the special seminars about:

- Code protection against illegal use & reverse engineering
- Licensing of software, with hardware or software-based keys (SmartBind)
- Solutions for embedded software in systems or cloud applications
- Back office integration

Training location	Date	Time
Utrecht	28 Nov 2013	11.00-15.00 hour
Office Antwerp (President Building)	4 Dec 2013	11.00-15.00 hour
Rotterdam	4 Feb 2014	11.00-15.00 hour
Office Paris (Near Gare du Nord & Est)	18 Mrt 2014	11.00-15.00 hour

Contact your local sales representative for details		
United Kingdom / Ireland	+44 (0)2031474727	sales@wibu.co.uk
Netherlands	+31 (0)747501495	sales@wibu-systems.nl
Spain / Portugal	+34 (0)914148768	sales@wibu.es
Belgium / Luxembourg	+32 (0)34000314	sales@wibu.be
France	+33 (0)173030491	sakes@wibu.fr

WIND RIVER
Developer Conference China

05. November – Shenzhen, JW Marriott Hotel
06. November – Shanghai, Sheraton Pudong Hotel
08. November – Beijing, Marriott Northeast Hotel

MEDICA 2013
11-1pm, TechForum Hall 12
22. November 2013
Duesseldorf, Germany

Bits & Chips 2013 Embedded Systems
November 07, 2013
Stand 22
Brabanthallen 's-Hertogenbosch, NL

sps/ipc/drives 2013
November 26-28, 2013
Hall 7, Stand 640
Nuremberg, Germany

Imprint
KEYnote
26th edition, Fall 2013

Publisher:
WIBU-SYSTEMS AG
Rüppurrer Straße 52-54
76137 Karlsruhe
Tel. +49 721 93172-0
Fax +49 721 93172-22
info@wibu.com
www.wibu.com

Responsible for the content:
Oliver Winzenried

Editors:
Stefan Bamberg
Marco Blume
Rüdiger Kügler
Wolfgang Völker
Oliver Winzenried

Design
Markus Quintus

Print
E&B engelhardt und bauer, Karlsruhe, Germany, EMAS III & ISO 14001 certified

Letters are always welcome. We will protect the confidentiality of sources. Third party articles do not necessarily reflect the opinion of the editorial office. Write us at global-marketing@wibu.com

Picture credits:
Cover KEYnote24:
©iStockphoto.com/alxpin
Article page 4:
©iStockphoto.com/LuisPortugal
Article page 6:
Chemical plant: ©iStockphoto.com/CaraMaria
Agent: ©iStockphoto.com/swilmor
Article page 8:
©lassedesignen-Fotolia.com
Armored car: image by Krzysztof Szkurlatowski; 12frames.eu
Article page 10:
©iStockphoto.com/Cristian_Baitg
Article page 12:
©iStockphoto.com/Alina_Vincent_Photography
Page 16:
©iStockphoto.com/nailzchap
All remaining images are copyrighted by their owner.

MEDIA
ACCESS
PERFECTION IN SOFTWARE PROTECTION
DOCUMENT

WIBU SYSTEMS