SPRING 2012

KEYnote 23

THE WIBU MAGAZINE

10 reasons for using CodeMeter®

Topics

- Software protection from a hacker's perspective
- CodeMeter® for newcomers
- CoDeSys application protection made easy

WIBU SYSTEMS

Contents

Dear Customers and Partners,

why does software licensing take up so much of your time? Would you like to implement new sales and business models? Do you want to deliver customers more added value? Are you on the lookout for a system with integrity protection or protection from reverse engineering and manipulation? Whatever it is you want to do, this issue of the KEYnote magazine will give you lots of interesting tips and ideas.

At the German IT Summit in December 2011, the Secretary of the Interior, Hans-Peter Friedrich, emphasized the importance of professional IT security, and the Chancellor, Angela Merkel, discussed smart grids and embedded systems and the significant security challenges they face. There is no doubt about it: governments all over the world are becoming increasingly concerned about cyber security. With our solutions for software products, instruments, machines and industrial facilities we want to help make a safer digital world for you and your customers.

What makes hackers tick and how do they work? We give you an insight into our experiences and have the results of our most recent Hacker's Contest in Russia. Get to know some of our Key Account Managers and read the 10 main reasons for using CodeMeter. Are you already maximizing the benefits? If not, the article on switching over to CodeMeter will show you how easy it can be to optimize your software licensing system. Another article explains how to integrate CodeMeter into your products to allow both dongle and software-based activation. And finally, I can't miss an opportunity to tell you a success story: our customer, Maroxx, is now using the highest level security from Wibu-Systems in their slot machines. Let us inspire you!

I hope you enjoy reading this issue of KEYnote and wish you all the very best for 2012, the year of the dragon. It would be a pleasure to meet you personally at one of the spring trade fairs or events.

Best regards,

Oliver Winzenried (CEO)

Meet the Wibu-Systems team

Our new Key Account

2011 was another successful year for Wibu-Systems. A recent study by Frost & Sullivan confirmed the upward trend of the software protection and license management market in coming years. This endorses Wibu-Systems' decision to add Key Account Management to its successful sales team.

Wibu-Systems has further expanded its talent base to provide expert advice to an ever growing number of international customers. We have recruited highly qualified staff for our district offices in the USA, China and the Netherlands, and our distributor in Russia. Since January 2012 our distributors and sales partners have been assisted by our new Senior Partner Manager, Stefan Bamberg, who brings a wealth of experience with him. We want to make sure all our customers, wherever they may be in the world, receive the local support they need, backed by know-how from headquarters in Karlsruhe.

From left to right: Stefan Bamberg, Jaqueline Fritsch, Ruediger Kuegler, Thomas Warnken

Stefan Bamberg

After studying computer science, he worked in R&D before switching over to IT project management. He was promoted to head of Sales and Key Account Management responsible for large ICT companies. Now starting as Senior Key Account & Partner Manager at Wibu this year.

Luydmilla Chekareva

finished her first diploma in french and german languages in 1999 and further on in 2011 a diploma in international diplomatic relationships in Russia. Joined Rainbow Security in May 2010 in marketing and since March 2011 is the head of marketing department.

Marcel Hartgerink

studied Electrical Engineering in Enschede and made his first software protection system for Atari-ST computers in 1988. In 1995 he joined Wibu-Systems. Today, he manages a team of security specialists and is responsible for the BeNeLux, UK, Ireland, Spain and Portugal.

Gurminder Sachdev

finished his Mtech. in Computer engineering in Moscow in 1991and has worked in backup and security software companies. Since July 2011 took over the Rainbow Security technology partnership department and works currently as Sales Director in Russia and CIS.

Marcellus Buchheit

is one of two founders of Wibu-Systems. He studied computer science at the Karlsruhe University and was the original architect behind WibuKey and CodeMeter®. He lives now in the northwest of USA, as CEO of Wibu-Systems USA, responsible for all customers in North America.

Terry Gaul

Terry Gaul is the Vice President of Sales for Wibu-Systems USA. He has spent the past 10 years selling digital rights management solutions and is currently responsible for growing business for all of North America. Terry resides in Massachusetts with his wife and 2 daughters.

Kelly Jagers

joined Wibu-Systems in 2011. She is Security & Licensing Advisor within the team responsible for sales in the Netherlands, Belgium and Luxembourg. With her recently updated knowledge of Wibu products she can translate customer needs in a fitting solution.

Dola Zou

has an academic degree in computer science and a long experience in licensing and protection of software. She has been appointed as COO for Wibu Shanghai, responsible for South and East China sales. She understands customer's aims perfectly.

10 reasons for using CodeMeter®

In a world where product piracy is becoming ever more prevalent, full protection against piracy, reverse engineering and manipulation is a must for a company's survival. Intelligent license management systems also help to boost business turnover and cut costs. This article explains the 10 most important reasons why Wibu-Systems is the right partner in all of these areas.

Global Player

1 Wibu-Systems has been offering secure hardware and software protection solutions for programs, documentation and media since 1989. With headquarters in Karlsruhe, Germany, and branch offices in the USA, China, the Netherlands, Belgium, England and Spain, the company is one of the two leading global suppliers of software protection and licensing solutions. Many years of experience and technological leadership make us a competent and reliable partner for small and medium-sized companies. Our ownership of a large number of **international patents** means customers can be sure our solutions are correctly implemented in their programs. Wibu-Systems undertakes ongoing research into market needs and technological advances to make our customers' systems even more resilient and secure. To this end we collaborate with universities and research institutes to develop the security concepts and **solutions of tomorrow.**

In-house R&D to the highest security standards

2 In the ever-changing world of IT, it is essential for software vendors to stay one step ahead of professional and well-organized hacker teams. Often used home-grown solutions are no longer able to fulfil this important demand of protection. Even commercially available products are sometimes incapable of protecting software from hackers.

The well-established **camouflage** and **deception techniques** in informational warfare can be directly deployed to protect software from potential hackers. Wibu-Systems combines its own innovative deception techniques with internationally recognized standards such as AES and ECC encryption to optimally fulfil this demand. The security of its products has been successfully demonstrated at various hacker contests around the world.

Scalable solutions under one umbrella

3 All available CodeMeter® products share a common construction type and have identical functionality. They are integrated into the customer's software via a standard API. This method is also used by CmActLicense. In this case time- limited licenses must be used which can be managed via the network.

Regardless of whether a customer prefers a hardware dongle or a soft license, the integration procedure and functionality are the same. It is even possible to use both methods in a single application. This means customers can **adapt their license models** at any time to regional market needs without modifying their applications. A standard concept helps software vendors familiarize themselves more quickly with the look and feel of the product, and hence lowers the cost of investment.

Comprehensive license management

A major benefit of the Wibu-System concept is that it allows a wide range of **flexible licenses** to be deployed in **a variety of situations**. Licenses can be generated in either a dongle or a license file. In the latter case the license is then tied to a specific computer. License types range from single-user or network licenses through time limited "pay per use" licenses to "feature on demand" concepts which allow modules to be combined as required.

Back-office integration

One of the most important aspects beside the actual protection of the application is the management of the licenses used by persons operating the protected application. To this end Wibu-Systems provides its customers with a powerful database tool called **CodeMeter® License Central**. This is a unified solution for sales, product management and shipment. The real benefit of CodeMeter® License Central lies in its flexible integration into exisiting ERP and shop systems using special connectors. It only then requires a gateway to directly activate the licenses via the Internet.

Investment security for customers

Anyone investing in the protection of their software wants to be sure their investment is **sustainable and adaptable to future needs.** Customers often need to quickly adapt their licensing strategies to deal with new technical requirements or changes in the market. Solutions from Wibu-Systems are downward compatible and licenses are easily updated on or offline via a remote file. No expensive or time-consuming replacement of hardware is necessary. Because the firmware can be updated, new functionality can be added at any time to hardware already in use.

The right type of construction

No matter how the product is used, Wibu-Systems has the right hardware solution. The classic CmStick comes in a plastic or precious metal housing and connects to the USB port. Options include a high quality industrial flash memory card and a **battery-backed clock** in addition to the standard internal clock. Our latest product highlight is the extremely small and compact CmStick/C which only protrudes a few millimeters from the USB port. Suitable construction types are also available for compact flash, PC card, express card, secure digital and microSD interfaces, all of which deploy Wibu's tried and tested protection technology. The CmStick/I and CmASIC chip have been designed for use in embedded systems and are therefore easily integrated into a hardware environment.

Multi-platform support during development

Wibu-Systems protection solutions cover a wide range of operating systems. Regardless of whether the protected software runs on Windows 32/64 bit or .NET, Linux 32/64 bit or Mac OS, the API used to integrate the Wibu solution into the customer's software is always the same. Wibu-Systems' security and license features have been fully integrated into the CoDeSys V3.5 development environment which is used to develop programmable controllers for **embedded systems.** Software protection and licensing solutions are also available for VxWorks and Windows CE.

Straightforward integration and user-specific GUIs

A central development environment with an extensive Help function and many useful examples exists for the integration of all Wibu-Systems products into customer products. **AxProtector** quickly and simply protects programs without needing to access the source code. Customer-specific solutions with special security and licensing needs should use **IxProtector**. This tool allows parts of the program to be encrypted. The flexible design of user dialogs is of significant benefit to customers as they **allow individualised information** and error messages to be displayed in the protected software application.

Services

Wibu-Systems' product range is supplemented by a wide assortment of business services to ensure products are optimally deployed in tailor-made systems. Prior to purchase, our team of **security experts** are at hand to help you design the right concept. Our **Professional Services** team help to adapt the solution to your special needs. The **Training Services** team are skilled specialists with a wealth of practical knowledge to support the implementation of the software protection and licensing strategy chosen by the customer. Make sure you benefit from our knowledge and experience, and save yourself time and money with the implementation. And for your end users, **Support Services** is there to give quick and comprehensive assistance whenever needed. You may also be interested in using our **Wibu Operating Services** to host your CodeMeter® License Central in the secure Wibu Cloud.

CodeMeter® with 10-way protection: software-based or in different construction types

Software protection from a hacker's perspective

Мы должны знать намерения своих врагов. "You need to know the arguments of your enemies" replied an aristocratic landowner in a Russian novel when asked why he had books by Karl Marx on his shelves. This is not unlike the world of software protection where good protection is only possible if you know the methods and tools used by your hackers.

Let's pretend I'm a hacker, but only theoretically, of course. Why do I hack software? Mainly because I can and it's fun. But most importantly I earn money from it. I don't just let anybody use my hacks in the Internet. I sell them. I'm not politically motivated like hacker groups who compromise online systems and bring down the websites of public authorities and governmental organizations.

Who am I dealing with?

Before I begin, I try to get as much information as possible about the protected software. What anti-piracy system does it use? Is it a commercially available product or a homegrown solution? How's it integrated into the software? Via an API or a wrapper? Does it have a dongle or is the license tied to a computer? Will my client supply me an executable version or do I have to work without a license? And finally: what pitfalls can I expect to encounter?

I divide my hacks into two categories: trivial ones which don't need a license and challenges which do. In the latter case, I act like Rambo at the end of the first book. No, not the film, but the book. I take my time and am very careful, as I am not sure what fatal traps my license faces. With CodeMeter® for example you can expect lots of nasty things. I've managed to destroy many of their dongles because the lads from Wibu are always coming up with new ideas. If I switch sides one day, I'll go there.

Crack without license

First I examine the software to see whether the executable code is encrypted. There are people around who think they can scare me off by using a packer like UPX. As far as I'm concerned, compressed software is just like unencrypted software. The properties of the application allow me to recognize very quickly which packer or encryption tool has been used. The section names give it away immediately.

If the application is unencrypted I analyze it using a disassembler. IDA Pro is a very good one for native applications. For .NET applications I like to use Reflector, even if you now have to pay for it. The disassembler takes a while to do its job, so I sit at my PlayStation 3 for a couple of hours. But it's worth waiting. Afterwards you get a diagram of the program flow, and a list of functions names and linked libraries. Now I want to change the program and very quickly find the best place to redirect a jump i.e. where to change a JNZ to a JZ so the program jumps if the license isn't found. This is not actually the type of hack I like at all as you can't make money from it. How do I control its distribution and stop other hackers from giving it away? Usually I distribute my trivial hacks for free, my motto being "He who makes no effort deserves to be stolen from."

By the way, you can contract me as a consultant. I would then analyze your software as a good guy, like Robert Redford in Sneakers. When I get a contract job from a company, the first I hear are stories about all the great things the R&D engineers have built into the software in attempts to confuse me. Actually what confuses me most is that my JNZ patch doesn't seem to have any effect.

Memory dumping

I have two approaches for encrypted software, and both of them need a license. In the first approach I start the software and wait untill it's sitting unencrypted in memory. I then do a memory dump and reconstruct the software from it.

By the way, did I mention I hate CodeMeter®? I hate it because it only lets part of the software sit unencrypted in memory. The dump is then like a puzzle but without any type of pattern. My biggest challenge is to get the software to run so that all parts are eventually decrypted. I have to use the software intensively to do this. Unfortunately, I'm not an expert user of boring geology software. And even if I were, how would I know if every function's been run at least once? The best test plans of a manufacturer only manage to test about 80% of the software. If I managed 100% I would make a fortune selling test tools. I would then be sitting under a sun umbrella on a Caribbean beach sipping cocktails every day. Or maybe I'd buy a villa in Baden Baden.

I don't really like this type of hack either. For one thing, I have to protect it somehow if I want to sell it, and then I have to repeat the hack each time a new version of the software is released. How am I supposed to get rich if I can't automate anything?

I decide to change the hack and write my own tools to automatically remove the protective encryption wrap. This means I only have to press a button when a new version is released or when I come across a piece of software with the same protection. Up till now I've seldom had to change anything to cope with new releases. These tools give me an edge over my competitors. By the way, did I mention I hate CodeMeter®? CodeMeter® inserts encrypted traps into the software. If I fall into one of them the license is deactivated. And so far I haven't managed to detect them all. I guess they must have spent of lot of time designing them. For today, I think I'll do the hacks with the other two dongles. I'll look at the CodeMeter® dongle some time next week when I have nothing else to do.

Record Playback / Emulation

My favorite hack is the emulation or record/playback hack. I hook up between the software and the dongle. There are people around who think they can stop me by encrypting their communications data. It might work with most people but not with me. Here again I have a competitive edge over all those wannabe hackers.

Just as I expected: CodeMeter®'s encrypted their communications data. At first glance, it's just like other decent dongles do. The fact that CodeMeter® uses an open source driver (USB flash driver) rather than a proprietary one doensn't help me or hinder me. I spend ages battling with CodeMeter®'s anti-debug measures. Other dongles are child's play in comparison.

I now listen in on the traffic flowing between the dongle and software, and produce a simulation, emulation or playback driver. It's both easy to sell and protect from piracy. And generally speaking it's scalable for future versions. It's my money printing press. I don't even have to listen in any more on some older dongles. I just need some data from the dongle and I have enough information to fully emulate it. A homegrown algorithm was never a good idea. Unfortunately, so many people use AES, now that this type of hack hardly works anymore. By the way, CodeMeter® was one of the first dongles to use AES. Even the old WibuKey used the standardized FEAL algorithm, which was a real tough nut to crack but thanks to the 40 bit export control I managed it eventually. The new WibuKey uses 64 bit FEAL which neither I nor my rivals have managed to crack. A well-implemented standard is, and always will be, the hacker's enemy.

My record/playback doesn't work either with CodeMeter®. They use a method called P-RID (RID = Required Information Decryption). The required data is multiply stored in the software. Different sequences are randomly fetched (random in terms of time and computer, P = Probabilistic). I'm nowhere near understanding it yet, though there does seem to be an encryption layer within the encrypted channel. It appears to extend from the protected application to the CmDongle. I can't find anything about it in either the manual or the user API. What's for sure though is that the Wibu concept has three layers of protection during communication: the outer (simple) encryption, the inner encryption and the random components.

By the way, did I tell you I hate CodeMeter®? I'm giving up on it for now. Maybe I'll have a look at it again next week. For the time being though, I'll concentrate on my other hacks.

Summary

Of course the world isn't just black and white, and I have to combine a number of approaches to get my hack right. As I earn my money from my hacks, I make sure they are protected and try to use scalable solutions. Once you get it working, you can make money from it all the time. When CodeMeter®'s involved though, it's like doing a puzzle. I more or less have to start all over again every time a new version is released. And the number of licenses, or better said, client licenses I've managed to kill; they weren't too pleased about it.

I like a sporting challenge, but with CodeMeter® it's nothing but a load of sequences and the same old boring, tiresome analysis. I hate it. I'm never sure I've got the full solution. Of course there are differences here too. I've come across software with lousy CodeMeter® integration. Such software is then easy to crack.

If I give my client a memory dump of a software where CodeMeter® has been skillfully integrated, it won't be long before I hear complaints. It doesn't work anymore, or the hack computes the wrong results. The problem is, I don't really understand the software. I might be a very good hacker, but at the end of day, I'm just a hacker.

Result of the 2011 Hacker's Contest in Russia

A Hacker's contest was held by Wibu-Systems for the first time in Russia from November 23 to December 8, 2011.

The reward of the Hacker's contest was 20 000 Euro. 114 participants were registered in the contest. The main objective of the Hacker's contest was to run the software, protected by a Wibu hardware key CmStick without a security key.

However, Wibu hardware solutions have been so resistant to cracking, that neither party could overcome their defense, and the hefty amount of 20 000 Euro remains in the Wibu coffers.

The hacker's contest in Russia reconfirms the highest level of protection provided by the solutions from Wibu-Systems.

Russia is famous for its ingenious hackers and outstanding professionals in the field of encryption. This is an accepted fact! But even the originality and ingenuity of our professionals has not helped them to break the solutions of Wibu-Systems. The results of the Hacker's contest show that software developers can be absolutely confident in the safety of their intellectual property using solutions from Wibu-Systems.

CodeMeter® for newcomers

You are about to release a new version of your software which contains innovative ideas and state-of-the-art technology. However your protection and license management system is old-fashioned and out of date. This is probably because you're not sure whether your software can cope with a new security concept and you've no idea how long it will take and how much it will cost to implement.

A new year brings new challenges! Are you planning a new version of your software? Have you rewritten most of your code for .NET only to discover that your current protection technology can't encrypt it? Are you annoyed that the intern working in Consulting needed only 30 minutes using Reflector and Reflexil to delete the code you painstakingly spent hours writing to check if the dongle is attached, even though you've spent even more money buying an obfuscator? Do you want to give key customers a license with software activation, or send customers with notebooks a mini dongle or SD card? Or maybe you only expect a healthy long-term collaboration with your supplier? If so, it's now time to fundamentally rethink your software protection concept.

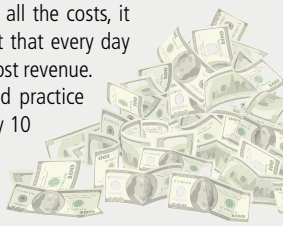
Wibu-Systems concentrates on its core business of software protection and licensing. "We are always focused on the customer. Solutions must suit the customer, and the benefits must outweigh the costs otherwise we aren't offering anything," explains Rüdiger Kügler, Vice President Sales. "We help our customers to increase their profits by reducing losses from piracy and lowering licensing costs through the use of automation and integration. Our support of innovative sales and licensing models means they also gain new customer segments."

The economic side

The main reason most people don't implement new software protection models is the effort involved. It takes time to get used to a new system and define new processes, and it requires heavy investment in new dongles. But look at it another way. How much is it costing you to keep the old system going? How much money are you losing because of poor license management? Although customers may honestly claim not to do so, they are often unknowingly using illegal copies. They do not realize they are infringing license terms, duplicating licenses via terminal servers, or purchasing licenses from illegal resellers. The experience of a Germany company specializing in construction software illustrates the point perfectly. The company wanted to gain a foothold in the South American market prior to the World Cup in Brazil. They soon discovered though they were already market leaders there. Bad luck for them: The company didn't know they had a reseller in Brazil. The outcome of the lawsuit is still pending.

How much money is wasted by non-optimal processes? Do you generate your licenses manually? An R&D engineer who spends 50% of his time programming dongles doesn't run up any extra costs, of course. However a new R&D engineer hired to relieve the "dongle programmer" of his duties because he only has 50% of his time left to do his other work, generates expenditure which is theoretically fully attributable to licensing. And this doesn't even take into account disgruntled customers in the USA or Asia who have to wait 24 hours for their licenses. Or is your "dongle programmer" on 24 hour standby?

How much potential business are you losing because you don't offer innovative license models such as software rental or "lite" versions? If you were to add up all the costs, it would soon become apparent that every day of procrastination is a day of lost revenue. Generally speaking, it is good practice to review your processes every 10



years and adapt them to new requirements, circumstances and increasing globalization. This review would be the ideal opportunity to implement a new protection and licensing system, although of course it shouldn't be the only reason for the review.

The technical view

But let's look more closely at the business of dongle replacement. Is it worth the effort? What would new dongles cost, and does this include shipment and logistics costs? Wouldn't it be better to keep the old dongles and let the new system run parallel to the old one? In other systems this would mean you would have to build an "if-then-else" construct into the software via the API to check which dongle type is attached and then start the software as soon as a valid license is detected in either the new or old system. This has two significant drawbacks though: even the smallest patch might destroy the protection, and you have to keep both license systems running.

Not so with CodeMeter®! CodeMeter® is the only system available which lets you keep your old dongles while offering improved security and standardized license production. The solution is known as **CodeMeter® Binding Extension**. You create a license file (CmActLicense) which your software and your licensing tool (CodeMeter® License Central) handle like a virtual CmDongle which means you can use all the security functions of CodeMeter®. For example, you can use AxProtector to automatically protect your software from reverse engineering and piracy, while IxProtector licenses individual functions which are decrypted at runtime to improve security. CodeMeter® License Central provides you with a uniform tool for creating, managing and shipping licenses.

You tie the license file to your old dongle. Of course, for your key customers, you may prefer to create a license file which is tied to their computer. In this case, CodeMeter SmartBind® from Wibu-Systems delivers an intelligent automated solution. A fingerprint is created from a large set of computer parameters. The exact ingredients of the recipe used for the fingerprint (i.e. the weighting of each parameter on each system) is Wibu-Systems' trade secret, and a patent application has been filed. You can select the tolerance level (Strict, Medium or Loose) to fix the sensitivity with which the system reacts to changes in the various hardware components.

It is also possible to define configurations supporting virtual machines. In this case the recipe differs to the one used for real computers, as the significance of parameters depends on the environment in which they exist. CodeMeter SmartBind® has an ingenious method for taking this into account. There are other methods beside CodeMeter SmartBind® for tying your licenses to computers.

And the great thing is that, it doesn't make any difference to your software how it is tied to your customer's computer: you can give your customer a CmDongle, tie the software to the old dongle using Binding Extension, or use a CmActLicense tied in some other way. It's up to you to decide what method you want to use. Wibu-Systems calls this maximum flexibility. But let's look more closely at CodeMeter® Binding Extension. You create a dll to fetch a unique feature from your old dongle such as the serial number. You probably already see the weak point here in the system. And the overall system is only as secure as its weakest link. You may have used AxProtector to protect your code from reverse engineering but if a full emulator of your old dongle exists on the black market, it would work here too. A further improvement in security is only achievable if each and every dongle is replaced. The decision to do so is yours and yours only. Wibu-Systems can only advise you. We leave it to you to choose.

You create a fingerprint of the unique feature. We recommend you use a secret "salt" value to create a HASH of the fetched feature and transfer this to CodeMeter® as the fingerprint. You give the binding dll a name and sign it with a private key in your FSB. This ensures no tampering takes place when CodeMeter® assigns the name, DLL and firm code.

Flexible license models

Before you can generate the license, you need to create a license information file. This file can be viewed as an empty cover for storing the subsequent CmActLicense. The most important information contained in the file is the name of your binding DLL and your firm code, and it has the same format for all customers. The CodeMeter® runtime accesses it during activation to get the name of the signed tamper-resistant bindling dll prior to loading it. Your fingerprint is now used to generate the remote context file from this CmActLicense. Of course only the public key is copied to the remote context file and not the fingerprint itself. This file is then used to generate a remote update file which contains information about the software module being activated. The fingerprint is used to decrypt the remote update file when the software is installed on the customer's computer. The fingerprint is verified each time CodeMeter® Runtime starts. You can retrigger a verification of the fingerprint at any time via a special API command (CmRevalidateBox).

All license types are handled in the same way by CodeMeter® License Central. It doesn't matter if you decide for a license file tied to the old dongle, a CmDongle or a CmActLicense with SmartBind. In all cases you have a standardized, well organized licensing system to manage your generated licenses.

Prior to changing protection systems, it's often very important to consider those customers with maintenance contracts. Have you been generating large numbers of activation files to send to customers with maintenance contracts whenever new software was released? If so, you won't need to do this anymore! With CodeMeter® you just enter the maintenance period in the license, and whenever a release is available the license automatically recognizes whether a customer has a maintenance contract or not. A change to the license is only required when the customer buys or pays for something. The maintenance period in the license is updated whenever the customer extends the maintenance contract. And it makes no difference if you sell licenses on a calendar year basis in Germany or on a twelve month basis in the USA. CodeMeter® helps you to optimize your processes and saves you cold hard cash.

Switch over to CodeMeter® and enjoy the following benefits:

- Many ways to switch over using Binding Extensions
- Powerful development API
- Flexible license models
- Combination of dongles and software-based activation
- Comprehensive license management
- Diverse range of construction types

For further information, please call your country specific vendor or vist our website - www.wibu.com.

CodeMeter® for everyone

CodeMeter® is driverless but we recommend you install the CodeMeter® runtime with administrator rights. How does this fit together?

Driverless isn't really driverless

From a purely technical viewpoint, a driverless product can't exist: without a driver, a hardware device can't be accessed. However, there are driver classes available which devices can use instead. The manufacturer doesn't supply the core driver though, which means it must be installed separately. Examples of available driver classes include Human Interface Devices (HID) such as a mouse, and Mass Storage Devices such as a USB memory stick. CodeMeter® uses the **Mass Storage Devices** driver which is why it is described as driverless.

Driverless benefits

By using the available Mass Storage Device driver, CodeMeter® gives you **maximum protection** of investment. A dongle with a proprietary driver makes you dependent on the good will of your supplier: when a new operating system is released, it's up to the supplier to decide whether to update the driver or not. Not so with CodeMeter®. Be it Windows XP Service Pack 2, Windows Vista or Windows 7 in the past, or Windows 8 in the future, it's like the classic tale of the tortoise and the hare: CodeMeter® wins every time because Wibu-Systems can always say "we got there first".

CodeMeter® also provides a major benefit during installation. You can attach a CmDongle to any computer and use it straightaway without administrator rights. This means you can start your software directly from CD or install a mobile version of it on a CmDongle with flash memory. Your software and license are then stored on the same device. And you can configure the CodeMeter® runtime not to leave anything behind on the computer you've used.

How is the CmDongle accessed?

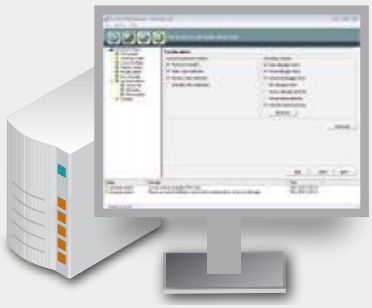
A runtime called CodeMeter.exe manages access to the CmDongle. CodeMeter.exe is usually installed on the PC as a service. If you are using a mobile version, your application can also automatically start CodeMeter.exe in user space (without administrator rights). In this case CodeMeter.exe must be stored together with a configuration file in the same directory as the protected application.

You might want to know why you can't directly access the CmDongle. There's probably no reason why you can't if this is the only application on the PC and you've configured it and are sure no other user installs any other software on the computer. This is generally the situation with embedded devices, and for these we provide a CodeMeter® compact driver.

For a standard Windows PC though, the preferred choice is usually the CodeMeter® runtime which offers the following functionality:

- Encrypted communication
- Simultaneous access
- Software-based licenses
- License counting on a terminal server
- Network client
- Network server
- Multiplatform functionality
- Compatibility with new construction types

Encrypted communication



CodeMeter® provides **two security shells** to protect your software from record/playback driver level hacks. P-RID (Probabilistic Required Information Decryption) weaves random data into the encryption of the inner wrapping making it impossible to create a fully functional hack from a single recording of the software traffic. A hacker doesn't usually get this far though as CodeMeter.exe encrypts the communication with the CmDongle to stop data being recorded.

A single CmDongle can protect several applications at a time. This could be an application (exe) and library (dll), or applications from different software vendors. CodeMeter.exe builds an encrypted channel to the CmDongle and assigns the licenses to applications. An important security feature **only allows one simultaneous encrypted communication channel** to the CmDongle. The number of times this channel can reinitialized within a short period is restricted. CodeMeter.exe prevents anyone from listening in on your encrypted data.

Software-based licenses

CodeMeter.exe also takes over management of software-based licenses (CmActLicenses). If your software allows both software-based CmActLicenses and CmDongles, CodeMeter.exe automatically checks which method is used to store the license.

If a CmActLicense is used, CodeMeter.exe must run as a service to make sure the license activation information is hidden on the PC. It must also run as a service to read and evaluate the fingerprint which ties the license to the computer. Administrator rights are only required to install the CodeMeter® runtime. Your protected software also starts in user space and the CodeMeter® checks it is licensed to run on the hardware.

If a CmDongle is used, CodeMeter.exe can either be installed as a service (recommended) or started automatically in user space by the protected application.

Network licenses

CodeMeter® also takes over network license management on both the client and the server. Your software first asks the local CodeMeter.exe if a license exists on the client. If it doesn't (and you've configured network licenses), CodeMeter.exe automatically searches the network for a license server.

CodeMeter.exe automatically allocates the network licenses on the license server if you must have previously installed the CodeMeter® runtime on the server and enabled the "release licenses to network" function (Option: "Run as server"). Of course, only licenses which are network licenses can be activated. Single user licenses (License Quantity = 0), for example, can only be used on the local computer.

The true strength of CodeMeter® is demonstrated by a **terminal server**. If CodeMeter.exe is running locally, a terminal server can count the number of licenses either by counting the number of launched applications or the number of sessions (i.e. connected computers). CodeMeter.exe automatically ensures no license violations occur due to the terminal server.

What happens when your software crashes? The customer restarts it. This might cause problems though if the license is still active. Here too, CodeMeter.exe offers automatic assistance. It monitors the relevant processes and deactivates the licenses when the corresponding processes crash. It doesn't matter if the licenses are local or on the network.

CodeMeter® is **multiplatform**. Even if your software runs on Windows only, the user can set up a license server on a Linux machine. The Windows CodeMeter.exe is fully compatible with the CodeMeterLin daemon on Linux, and the Mac OS and Sun Solaris versions of CodeMeter®.

New construction types

CodeMeter® is undergoing constant development. The CmDongle is currently available in SD or CF card format. Nobody can say today which additional construction types and interfaces CodeMeter® will support in 5 years time. Nevertheless, CodeMeter® provides full investment protection here too: All you need to do to use another construction type is update the CodeMeter® runtime (and this might not even be necessary). Your software doesn't have to be recompiled at all.

CodeMeter® compact driver

Wibu-Systems provides a CodeMeter® compact driver for large volume **embedded devices**. The CodeMeter® compact driver replaces the CodeMeter® runtime allowing you to directly access the CmDongle from your application or CmActLicense. The API is fully compatible with the CodeMeter® runtime but only a subset of the functions can be used.

The CodeMeter® compact driver is available as ANSI C source code which you can compile for your target system. An important feature of the CodeMeter® compact driver from Wibu-Systems is its modular design which allows it to be streamlined to your project. When installed on your own operating system or an embedded operating system, it is the ideal alternative to the CodeMeter® runtime.

A version with simultaneous operation of the CodeMeter® runtime and CodeMeter® compact driver on a PC is planned.

CoDeSys application protection made easy

In 2010 Wibu-Systems signed a cooperation agreement with 3S-Smart Software Solutions to integrate its protection technology into the CoDeSys V3.5 development environment used to develop industrial controller applications. This article shows how easy it is to implement the important protection features offered by the CoDeSys environment.

Are you one of those people who have discovered fake versions of their machines or systems at a trade fair? In a survey carried out in 2010 by VDMA (German Engineering Federation), 50% of those questioned replied in the affirmative. The resulting **loss in turnover** is reported to be **several billion dollars**. Protection technology from Wibu-Systems makes the reverse engineering of equipment, control systems and machines considerably more difficult by encrypting the embedded source code and hence protecting it from piracy and manipulation.

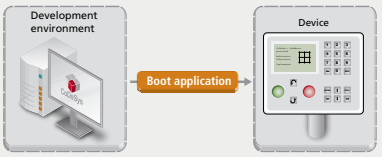
The tried and tested CodeMeter® technology from Wibu-Systems has been seamlessly integrated into the latest version of the **CoDeSys V3.5** development environment allowing software to be easily and effectively encrypted during development. The end results are PLC-based industrial applications with sustainable and secure protection.

The fundamental principle is straightforward. The source code is encrypted and the corresponding key is stored in a dongle so that the protected software is tied to a particular device or controller. The same principle is used to protect the embedded software in PLCs. The entire source code is stored on the target system in encrypted format to prevent it from being disassembled and decompiled by an analyzer. The code cannot be decrypted without the corresponding license.

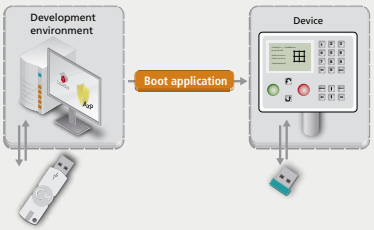
CoDeSys V3.5 and CodeMeter®

CodeMeter® protection technology has been integrated into CoDeSys since version 3.5 of the development environment. An automation manufacturer uses CoDeSys to develop a controller application and encrypt it before downloading it to the controller. Here it is stored in the memory of the controller and can only be decrypted and executed if the corresponding license exists on a CmStick. The CoDeSys runtime decrypts the software in controller memory automatically and protects it from piracy and unauthorized reverse engineering.

Controller software development takes place in two stages. First the source code is written on the computer on which the CoDeSys development environment is installed. A **boot application** with the executable code is then generated and downloaded to the PLC via a gateway.



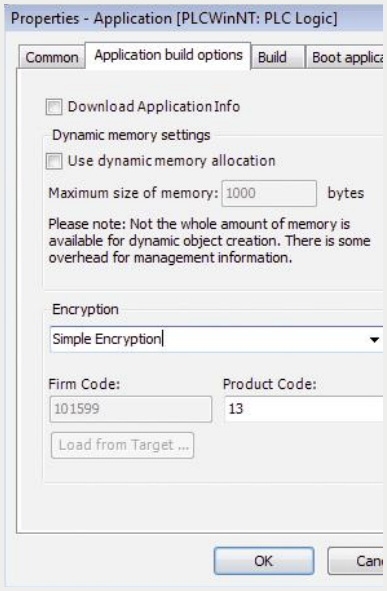
At this stage the generated code on both the development PC and the controller can still be read and could be copied or manipulated. CoDeSys Version 3.5 can prevent this by placing an encryption wrap around the application, in the same way that **AxProtector** does.



The encryption features are best explained by way of example. The properties used to encrypt the application are shown by clicking the right mouse button on the "Application" item of the list in the Devices window.

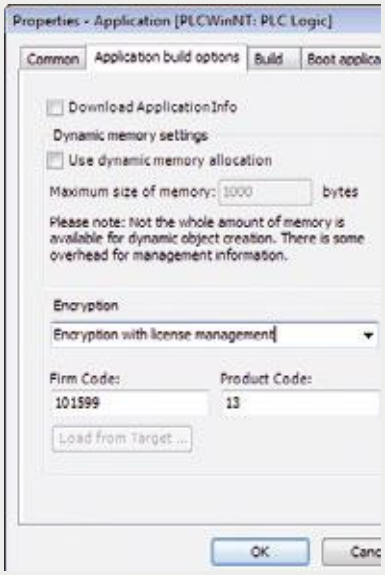
A dialog box appears containing a tab called "Application build options." This tab is used to set the parameters of the used dongle. The controller application manufacturer can choose between two types of encryption:

1. Simple encryption



The manufacturer can purchase a pre-programmed **CoDeSys Security Key** (dongle) from 3S-Smart Software Solutions for this type of encryption. The dongle is shipped together with the manufacturer's application to the customer. The dongle contains a globally unique key which is stored as a firm code and product code. The product code must be entered in the corresponding input field of the application when requested. If the controller is already connected to the network, the product code can be fetched directly from the connected dongle by pressing the "Load from target ..." button.

2. Encryption with license management



A new feature, soon to be released, is encryption with license management which allows for much greater flexibility. For example, the controller application manufacturer can **create and manage licenses himself**. He uses his master dongle to program Wibu-Systems' CmDongles with the required license parameters (firm code and product code). The values of these parameters are entered in the input fields during encryption and are the values used by the person later operating the encrypted software. Whereas simple encryption creates an individual application for each device, this type of encryption allows a manufacturer to generate identical controller applications in batches of a hundred, for example.

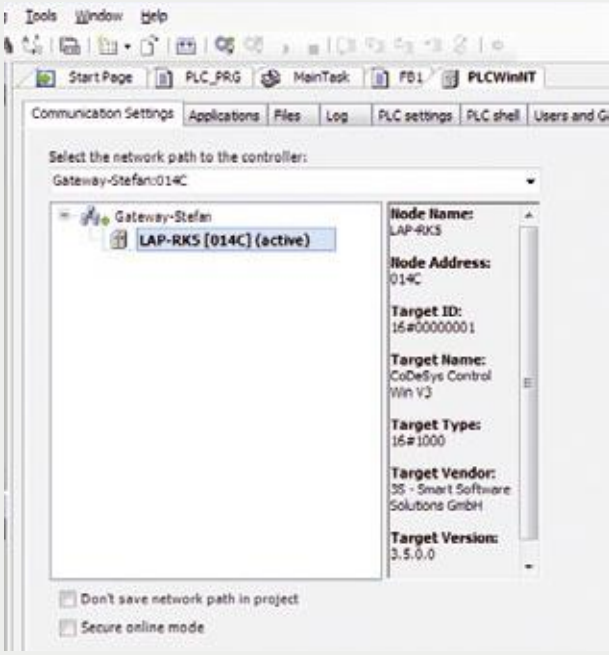
The current version of CoDeSys, version 3.5, only allows use of the encryption options if the development environment and the controller emulation run on different computers. The CodeMeter® runtime must not run on the target computer used to emulate the controller!

The application's communication settings connect the controller (known here as the device) to the network: (see screenshot on the right).

The CodeMeter® runtime CmDongle which encrypts the application must be connected to the computer on which the controller is installed. If this is the case, all the conditions have now been fulfilled to successfully encrypt and download the application to the controller. Here the CoDeSys runtime verifies the encrypted application and then decrypts it prior to launching. This is the only time the check is carried out, ensuring that encryption does not negatively impact the performance of the controller during operation.

Wibu-Systems technology has been directly integrated into the CodeSys V3.5 development environment. This means a special developer's dongle can be used to encrypt projects within the development environment to protect them from unauthorized access.

The combined development environment and encryption tool solution provides developers of embedded systems with an easy-to-use and effective way of writing software with integrated protection from product piracy, reverse engineering and manipulation.



Latest news summary

ISO 9001:2008 recertification

2012 kicked off to a good start for Wibu-Systems with successful ISO 9001 recertification in all departments – namely R&D, product management, manufacturing, support, finance, sales and executive management. Once again we have demonstrated our compliance with the ISO9001:2008 quality management system, a system that helps us to meet the needs of our customers and fulfil our legal obligations. The recertification confirms the well-structured organization of our company and its use of mandatory processes, reinforcing our status as a reliable partner for small and middle-sized industry.

Current software versions:

- CodeMeter® SDK 4.40, 2011-12-20
- CodeMeter License Central 1.50, 2012-02-xx
- CmIdentity 4.40, 2011-12-20
- WibuKey SDK 6.0f, 2012-01-27
- AxProtector 8.00, 2011-12-20
- SmartShelter PDF 6.0, 2011-06-16

Current firmware:

- CmStick, CmStick/M: 1.18
- CmCard/µSD, /SD, /CF: 1.18

The latest software versions give you the benefit of new improvements; the latest firmware offers you high stability and new functionality.
Please update regularly.

License Central 1.5 expands supported database products

In addition to the original MySQL database connection, the new version of Wibu-Systems' powerful and intelligent license management tool, License Central 1.5, now supports the popular database products from Microsoft (MSSQL) and Oracle. This is a reflection of the fact that many companies already operate solutions based on these products. The solutions are integrated into the IT landscape in accordance with the company guidelines for backup, reliability and performance. License Central 1.5 thus makes efficient use of existing resources and cuts investment costs.

CmStick/C with design protection

The ultracompact CmStick/C from Wibu-Systems was presented with the "Most Successful Design Award 2011" in recognition of its innovative design. It has also been granted international design protection, a type of industrial design right allowing Wibu-Systems exclusive use of the ornamental characteristics such as design, color and shape for the next 25 years. This will provide protection from imitations by competitors and allow us to defend ourselves against piracy. For you, it means your product can boast a dongle with a unique design.

New patents for Wibu-Systems

Patents are of great significance to small and middle-sized companies. Collaborations with international organizations are necessary to achieve mass-market penetration, but such collaborations will only work in the long term if products and ideas are protected by patents. Wibu-Systems owns a large number of international patents, including a patent in the USA for driverless communication between software and hardware. It has also been granted a patent in China for a concept called "Intrusion Detection & Prevention" which automatically detects and blocks attacks on the CodeMeter® runtime or license container. A patent application has been filed for the SmartBind mechanism, an intelligent and flexible system to tie licenses to hardware. As a customer you can be confident Wibu-Systems has settled all patent-related issues, and that you are not infringing any patents when using Wibu licensing products.

Frost & Sullivan Market Study

Wibu-Systems was included in the "Hot Vendor Watchlist" of the N9FA-70 "Global Software License Management Market" study published in December 2011. This prestigious award offers technology and growth opportunities, and proves that Wibu-Systems is the right partner for your software licensing solution.

Newsflash

+++ SmartShelter plugin compatible with Adobe Acrobat X +++ AxProtector Mixed Mode to launch at CeBIT +++ 64 bit release of IxProtector and WUPI with Shared Objects scheduled for Q2 +++ Compact Driver 1.3 under development +++ CodeMeter® now ready for IPv6 +++ CodeMeter® PasswordManager plugin for Firefox 10 released +++

MAROXX customer story

MAROXX SOFTWARE GmbH

Let the game begin ...

... with high-tech system solutions from MAROXX and security from Wibu-Systems.

For many years MAROXX has been one of the most popular international companies specializing in gambling software. Our well thought-out strategy has enabled us to firmly establish ourselves in many European countries. With more than 20 years of experience in the gambling business, we guarantee our long-standing customers above average profits.

The word "recession" does not exist in MAROXX's vocabulary: our order books are overflowing and have been for many years. MAROXX is an entirely Austrian company, financed by cash flow from its business. We attach great importance to our independence, fix the value of the company ourselves and do not depend on any bank or stock exchange.

Our state-of-the-art hardware and software create trends in computing, individuality, graphics and sound. MAROXX gambling software sets new standards, which is exactly what we expect from our partners. With Wibu-Systems we have found a partner who perfectly complements our philosophy.

Our intensive collaboration with Wibu-Systems has enabled us to develop a product which lives up to our high demands and is the most modern of its type.

Unfortunately the gambling sector operates in an environment with difficult security challenges which makes MAROXX products susceptible to manipulation attacks. As we strive for perfection, this means we are committed to offering our customers the highest levels of security.

In our endeavours to achieve this, Wibu-Systems has proved to be the perfect partner. The company supplies industrial compact flash cards with CmDongles which represents the ideal combination of storage device and integrated software protection. The result of our collaboration has been the seamless integration of Wibu-Systems protection technology into our system. The fact that we have successfully adapted both products to function together smoothly means there is no negative impact on performance during usage, which is a very important customer requirement.

Maximilian Stromer
Managing Director MAROXX
"Wibu-Systems has proved to be the perfect partner. Together we have managed to achieve high levels of synergy which benefit both us and our end users, and hence positions us even further ahead of our competitors."

Roadshows, trade fairs and events

Join us at the following trade fairs and conferences:

Microsoft Tech Days 2012
16.02. – 17.02.2012
Device Area, World Forum, The Hague

Embedded World
28.02. – 01.03.2012
Hall 5, Booth 340, Messe Nürnberg

BASTA! SPRING 2012
28.02. – 01.03.2012
Maritim Rhein-Main Hotel, Darmstadt

CeBIT
06.03. – 10.03.2012
Hall 12, Booth B59, Messe Hannover

Bouw & ict
21.03. – 22.03.2012
Hall 2, Booth A035,Royal Dutch Jaarbeurs Utrecht

HMI
23.04. – 27.04.2012
Hall 7, Booth F48, Messe Hannover

ACCU Conference 2012
25.04. – 28.04.2012
Booth 1, Barcelo Hotel, Oxford, UK

Secure Code Seminar .NET (SCS)

Secure protection of .NET-Assemblies against piracy and reverse engineering, including license management

Our successful series of Secure Code Seminars have been brought up to date and will be taking place somewhere near you.

You will discover how to protect your .NET applications against piracy and reverse engineering in just a few minutes. New to the seminar is the modular protection of .NET applications using Wibu Universal Protection Interface (WUPI). WUPI combines license management with protection at the method level.

The .NET Secure Code seminar is aimed at the product manager who wants to know how to use CodeMeter® to implement his license models, and at the developer who wants to know how to integrate CodeMeter® into .NET-Assemblies.

Forthcoming events

14 March 2012	SCS Madrid, Spain
29 March 2012	SCS Karlsruhe, Germany
04 April 2012	SCS Milton Keynes, UK
17 April 2012	SCS Gent, Belgium
01 May 2012	SCS Amsterdam, The Netherlands
08 May 2012	SCS Berlin, Germany
09 May 2012	SCS Brussels, Belgium
09 May 2012	SCS Hamburg, Germany

The current dates of our Secure Code Seminars can be found on our website.
Germany, Austria & Switzerland: www.wibu.com/de/training-schutz-reverse-engineering.html
Spain & Portugal: www.wibu.com/es/proteccion-ingenieria-inversa.html
Netherlands & Belgium: www.wibu.com/nl/training-beveiliging-reverse-engineering.html
UK & Ireland: www.wibu.com/uk/training-reverse-engineering-protection.html

5060-002-02/20120207

Imprint
KEYnote
23rd edition, spring 2012

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

Responsible for the content:
Oliver Winzenried

Editors:
Marcellus Buchheit
Stefan Bamberg
Terry Gaul
Marcel Hartgerink
Rüdiger Kügler
Gurminder Sachdev
Maximilian Stromer
Thomas Warnken
Oliver Winzenried

Design and Production
Markus Quintus

Print
E&B engelhardt und bauer, Karlsruhe

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 KEYnote23 and leading article:
©iStockphoto.com/DNY59
Leading image page 8
©iStockphoto.com/Andreas Weber
Leading image page 10:
©iStockphoto.com/Steve Cukrovbild
All remaining images:
©Wibu-Systems