FALL 2011

KEYnote 22

THE WIBU MAGAZINE

Software licensing in the cloud

Topics

- Make or buy?
- CodeMeter SmartBind®
- Protecting CoDeSys PLC software

WIBU SYSTEMS

Contents

INFORMATION
Wibu-Systems International 3

KNOW-HOW
Make or buy? 4

PRODUCT
CodeMeter SmartBind® 6

KNOW-HOW
Licensing in the cloud 8

INTEGRATION
Secure software licensing 10

PRODUCT
Protecting PLC software using CoDeSys V3.5 and CodeMeter® 12

HIGHLIGHTS
Latest news summary 14

CUSTOMER STORY
Wincor Nixdorf customer story 15

ROADSHOW
Roadshows, trade fairs and events 16

Dear Customers and Partners,

This issue of the KEYnote magazine contains articles about new products and our development work for software licensing in the cloud and automation engineering with CoDeSys. Discover how CodeMeter SmartBind®, our new fault-tolerant and secure activation tool, works and how it benefits you and your customers.

Is it worth developing your own licensing methods if you have to constantly maintain and update them? The article entitled "Make or Buy?" offers several interesting thoughts on the matter.

"Mobility and cloud computing: the two growth generators in IT": this is the headline of the October 2011 issue of VDI News. The sector is booming and Axel Pols, chief economist at the German Information Technology Association BITKOM says "the investment backlog from the 2009 recession is now being cleared." Rainer Glatz, chairman of the Software Sector of the VDMA German Engineering Association, shares this optimism and confirms the increasing importance of IT in machine and plant production. At the same though, concerns are growing about the security of cloud computing.

This means highly secure solutions are necessary not only to protect know-how and prevent copying, but also to ensure integrity and prevent manipulation. We are working on these topics all the time. The article entitled "Secure software licensing" gives tip and tricks on how to optimally deploy our solutions. With AxProtector you can integrate complex yet secure protection methods into your software. Even the new 7.20 version now uses CodeMeter® to protect its ingenious mechanisms against reverse engineering. We don't just talk about security. We do it! For example our products are now being put to the test in the new Hackers Contest in Russia. The results will be known in a few weeks time.
There are still a few events taking place this year, for example SPS/IPC/Drives. It would be a pleasure to meet you there. As the year comes to a close I would like to take this opportunity to wish you and your families a happy and peaceful festive season.

Best regards,

Oliver Winzenried (CEO)

Wibu-Systems International

With subsidiaries in the USA and China and sales offices in England, Ireland, Spain, Belgium and the Netherlands, as well as distributors around the world, WIBU-SYSTEMS AG can truly be considered a "Real Global Player". The company's international focus means not only do Wibu customers receive support in their native language, they also benefit from quick and direct access to distribution channels in their country.

WIPS 2011

From 6th-9th July, partners and distributors from around the world were invited to attend the "Wibu-Systems International Partner Summit", also known as WIPS, which took place at headquarters in Karlsruhe. Participants attended from 16 different countries for training in the latest products.

WIPS gives participants a chance to exchange experiences they have had with customers. Important information can be fed back to R&D for use in future Wibu product developments. During the annual summit participants also receive training in how to use and integrate our software protection solutions, and could discuss the current development status of CodeMeter® product properties. Hence all members of the Wibu family learn to appreciate global customer requirements in a diversity of industries and markets. Specialist training seminars have been and still are the basis of the worldwide service offered by WIBU-SYSTEMS AG.

The round-table talks about future product development are an integral part of this summit. They ensure we continue to meet the stringent requirements of our customers who depend on Wibu-Systems for long-lasting and future-proof solutions.

This international meeting in Karlsruhe also coordinates the worldwide trade fairs, training seminars and events, such as the Hackers Contest from 9th to 24th November 2011, the Softool trade fair in Moscow, and Secure Code seminars in Shanghai, London, Brussels, Madrid, Barcelona and Amsterdam, to mention just a few locations.

Wibu-Systems International - A Global Player

Wibu-Systems International Partner Summit 2011, 7th-9th July in Karlsruhe

Supporting program

An attractive supporting program accompanied the summit. It offered our international partners the chance to learn about the cultural context of the Karlsruhe location. For example, it included a visit to the casemates beneath the Germersheim Fortification. Family members were also welcome to come along.

Summary

The Wibu-Systems International Partner Summit 2011 can be considered a success. As feedback from guests confirmed, everyone returned home well-trained in the latest know-how and newly motivated to advise customers in their country about optimal methods to protect and license software.

Make or buy?

Secure Software Licensing: Build vs. Buy. You have successfully completed development of your new software package and now it's time to go to market. In order to have a successful product launch you want to make sure you have flexible licensing that meets the market demands. And while having licensing flexibility is great, you also want to make sure it's secure so that you get paid for every copy in use.

Lastly, you want to make sure that all the new code that was developed (intellectual property) remains protected so that you don't have your competitors stealing your technology or hackers reselling your software. You go to your development team and they say "We can easily build a licensing platform and you won't need to invest in a 3rd party solution." This statement has been heard many times in many organizations. The reality is that the results of "doing it yourself" are usually marginally successful or more likely a brain drain on your developers that leads to high support costs and loss of revenue due to piracy. I hope the rest of this article provides a greater understanding of "the hidden costs of home-grown licensing" and why using the CodeMeter® technology will streamline your secure software licensing process and enhance your opportunity for greater profits.

The developers rallying cry: "We can build it!"

Why do software companies like building home-grown licensing? Because building software is what they do! They look at this as just another software development task. Why waste money when you can use your existing engineering resources?! They want to own the system to have complete control, because they think only they can build a licensing system that addresses all their needs. And those cost savings will be truly dramatic! No need to purchase a commercial licensing system with all those ongoing costs. "We know our software code and we know how to protect and license our software titles." The standard process is something like this: "We can create a serial number generator and each customer will receive an individual serial number for the specific name (company) and it will be protected with a cryptographic hash. And let's go one step further by binding that serial number to a specific PC. We will get the unique MAC address of the network card and we will store this in the customer specific license file. Now that license will be bound to the specific PC and cannot be installed on other PC's." It all seems so good.

The reality: Not as easy as it seems

The scenario above seems flawless at first glance. But what is the reality? First, unless your team is prepared to engage the hacker community for the long term; even a well-designed home grown system will become vulnerable after a short period of time. Second, let us not forget the support costs involved (sales operations and technical support). When looking at Secure Software Licensing you have many components to consider such as License Management, Intellectual Property Protection, Copy Protection, and Flexible Licensing Models. How will you deal with version management, license updates (upgrades and downgrades), and moving licenses from one PC to another? Will you be able to remotely update your customers without the need to "touch" each process? If you are doing software activation how will you bind the license to the PC without causing an unstable license environment (which generates support calls)? Will you be able to meet market demands for license types (perpetual, subscription, rental, trialware, concurrency/network, usage counters, checking out of licenses, etc.). Will your licensing process be streamlined and easily integrated into your ERP and CRM systems? And how will you track all the transactions that take place around your licensing process?

Lastly and most importantly:

How do you make sure you get paid for every copy of your software in use? Even though you have a staff of developers that know how to develop software, those resources are not free when building a licensing system.

Reassigning a developer (or hiring another developer) represents real costs to the company.

If this developer or developers is not working on the core business which drives revenue then this is a burden to the company's bottom line. And the developer(s) that are assigned to build and support this homegrown system certainly don't have the core expertise that you would find from a company like Wibu-Systems. This developer has a myriad of issues to concern himself/herself with such as the items discussed above and others such as platform support (all variations of Windows, MAC, and Linux), backwards compatibility issues, knowledge of encryption, integration points, etc.

A true value: The CodeMeter® licensing platform

Wibu-Systems has been doing only one thing for the past 22 years and that is providing the most flexible, reliable, and secure licensing solution to the ISV marketplace. We allow you to focus on what you do best (develop and market your software) while CodeMeter® provides the solutions that enable License Management (License Central), automatic protection (AxProtector Encryption), flexible license models, and seamless integration into your business processes. Our goal is to ensure that you get paid for every copy of your software in use and that you can meet the many demands of your customers as it relates to usage of your software. We constantly strive to stay ahead of the "hacker community" with the ongoing enhancement of our protection tools. Our development is driven by customer requirements – we listen to what you want and develop accordingly. The value we provide is that you can start using CodeMeter® today and "out of the box" it should meet your needs and going forward it will evolve as the marketplace evolves.

License Central is the license management tool that gives you the capability to organize all your sellable items (features, functions, modules, etc.) in one centralized location and the order process originates from here. License Central is a web service and can be fully integrated into your eCommerce shop, ERP, and CRM systems. When processing an order and creating a license it's at this point you can determine your binding mechanism.

CodeMeter® offers you the flexibility of binding your license to a physical device (CmDongle) or binding to the PC where your software is installed (CmActLicense). If you are looking for the strongest security because you are selling to Asia or Eastern Europe then you might consider CmDongles which offer unparalleled IP Protection and Copy Protection (we utilize a Smart Card Chip with substantial secure memory and fast processing speed, and the AES encryption engine is onboard the device). If you are selling to Western Europe or North America you might instead consider CmActLicense (same features and functionality as our devices) and bind your licenses to the PC where your software is installed.

Once your customer receives and installs your software (physical delivery or Electronic Software Distribution) they either plug in their CmDongle or go through the activation process for CmActLicense (which will bind the license to that particular PC). The license information that is generated for this particular customer is stored in your database (MySQL which we bundle with License Central, or with the SQL database you already have in place). You now have base knowledge on this license and this customer which enables all future licensing management capabilities (secure license updates, annual maintenance information, etc.).

The true costs

When making the "Build vs. Buy" decision you have to examine the true costs (tangible and intangible):

- Will it be flexible enough to meet the market demands?
- Will it be secure?
- Can I integrate this into my business processes?
- Will it be backwards compatible and forwards compatible?
- Operational costs?
- Support costs?
- End User satisfaction?

Secure Software Licensing is all we do and it's our focus and dedication to our customers that ensures we provide the most flexible, secure, and cost effective offering on the market today. We hope you give us a try!

Marcellus Buchheit
Co-Founder WIBU-SYSTEMS AG, President and CEO Wibu-Systems USA

As a software developer I know that engineers get excited to develop the next "big thing" whether that's an exciting new feature or the new release of their product. This makes sense for your next version with new features and functions where you specialize in that market segment. But in the highly specialized world of secure software licensing it makes sense to rely on a company like Wibu-Systems which has focused on this technology for over 20 years. We have an experienced and specialized team of developers whose only goal is to enhance CodeMeter and develop to meet the new market requirements (features, functions, security, new platforms such as Cloud Computing, etc.). From a business perspective it does not make sense to pull a developer(s) off your core business to try to re-invent licensing with a homegrown solution. Will that homegrown development meet your current and future needs? The bottom line: Secure Software Licensing cannot be developed as a side project. Only with a strong partner like Wibu-Systems will you achieve the results required.

CodeMeter SmartBind®

CodeMeter SmartBind® describes the new concept to bind licenses, i.e. digital rights, to a computer or other specific device. CodeMeter SmartBind® has been developed by Wibu-System and is patent pending. Binding stands for activation. The challenge is to choose binding features which uniquely identify the computer while, at the same time, tolerating minor changes to the computer, thus ensuring high license reliability for the user.

How does it work?

Imagine you are to identify a person. Imagine further that you cannot use fingerprints since the person wears gloves or you have no fingerprint scanner at hand. In this case, you would fall back on visible features: facial form, size, weight, gender, hair color, hair length, nose width and length, shape and strength of eye-glasses, beard color and shape, etc.. If you recognize enough features then you conclude: "Yes, that's him." When there is only a short interval between the first and the next time you meet the person, most of the features will be unchanged. However, if this interval is longer, then some features may have changed more or less. And the features are of different quality. It is rather unlikely that the gender changes although possible thanks to modern surgery. Some change their hair color like they change shirts while others keep the original color throughout their lives. For adults, size is a good first exclusion criterion, while with children and teens this naturally changes.

Until meeting again with the statement "Gee, isn't that John Doe", numerous complex processes take place in the human brain. Features are compared and carefully considered before the final "yes" or "no" decision is made.

Carrying the passport photo

What does this have to do with CodeMeter SmartBind®? Nature itself has been the model case for CodeMeter SmartBind®. CodeMeter SmartBind® mathematically maps the complex recognition processes. When a license is bound to a computer, CodeMeter SmartBind® creates the fingerprint of the computer, the so-called a cryptographic key, and a list of all features found. This list is – analogous to a photo in the passport – stored on the computer. That is, the license always carries its own passport photo. The passport photo is used to identify the license. All current features are matched to those on the photo. New features, glasses in the human example, a UMTS card in the case of the computer, are negligible and do not become part of the algorithm. In contrast, in the case of classical binding, a new network card would falsify the value of the MAC address/es. Not so with CodeMeter SmartBind®. New features are not a source of error.

Dynamic feature selection

How would it be if you did actually have the fingerprint, retina scan or DNA sample of a person? Then you would of course use them. The same applies to CodeMeter SmartBind®. CodeMeter SmartBind® has no rigid scheme concerning the features it uses. The selection of features is dynamically adapted to the availability and recognition of features. CodeMeter SmartBind® is able to access a large pool of potential features. If, for example, the CPU ID and/or TPM chip is available, it will use these too.

Dynamic weighting

You definitely remember the size of a person. Children and teenagers are still growing, but size is a good and stable criterion for adults. Features are dynamically weighted by CodeMeter SmartBind® according to the available characteristics and the environment. If the CPU ID and/or TPM chip can be read, they will be given a high weighting in the binding. The components of a virtual machine differ to those of a "real" computer.

Tolerance

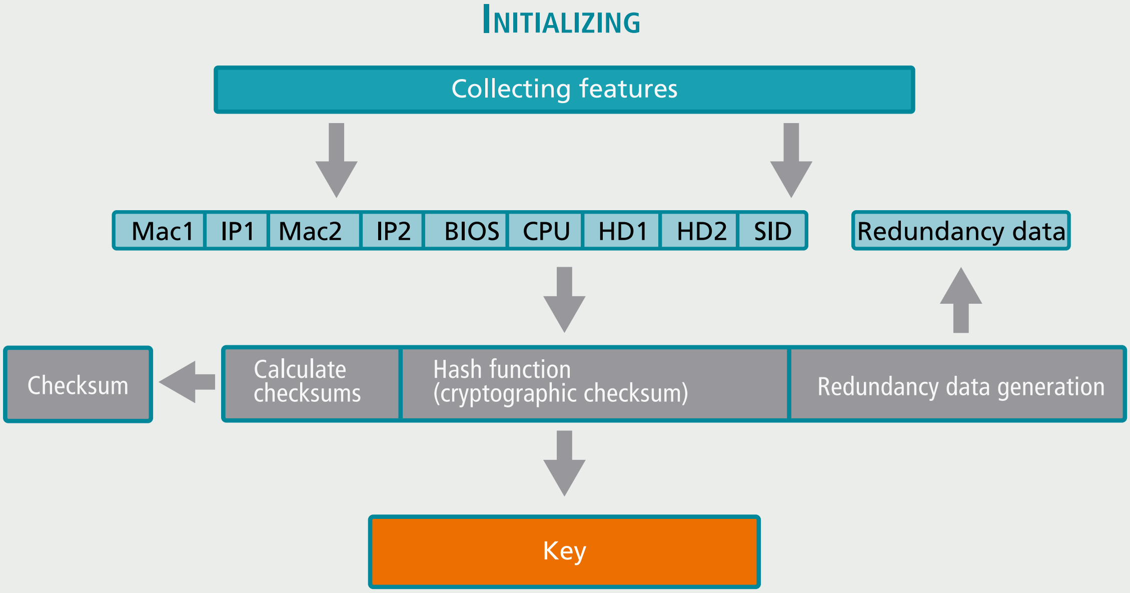
CodeMeter SmartBind® is tolerant of changing features. You set the tolerance level. If you select the "Tight" setting, the tolerance level is low; if you select the "Loose" setting, the tolerance level is high. A high tolerance level means only a few features need to be retrieved to identify the computer; a low tolerance level means many original features must be retrieved. It is not necessarily the number of features which is important, but the "overall weighting".

Security

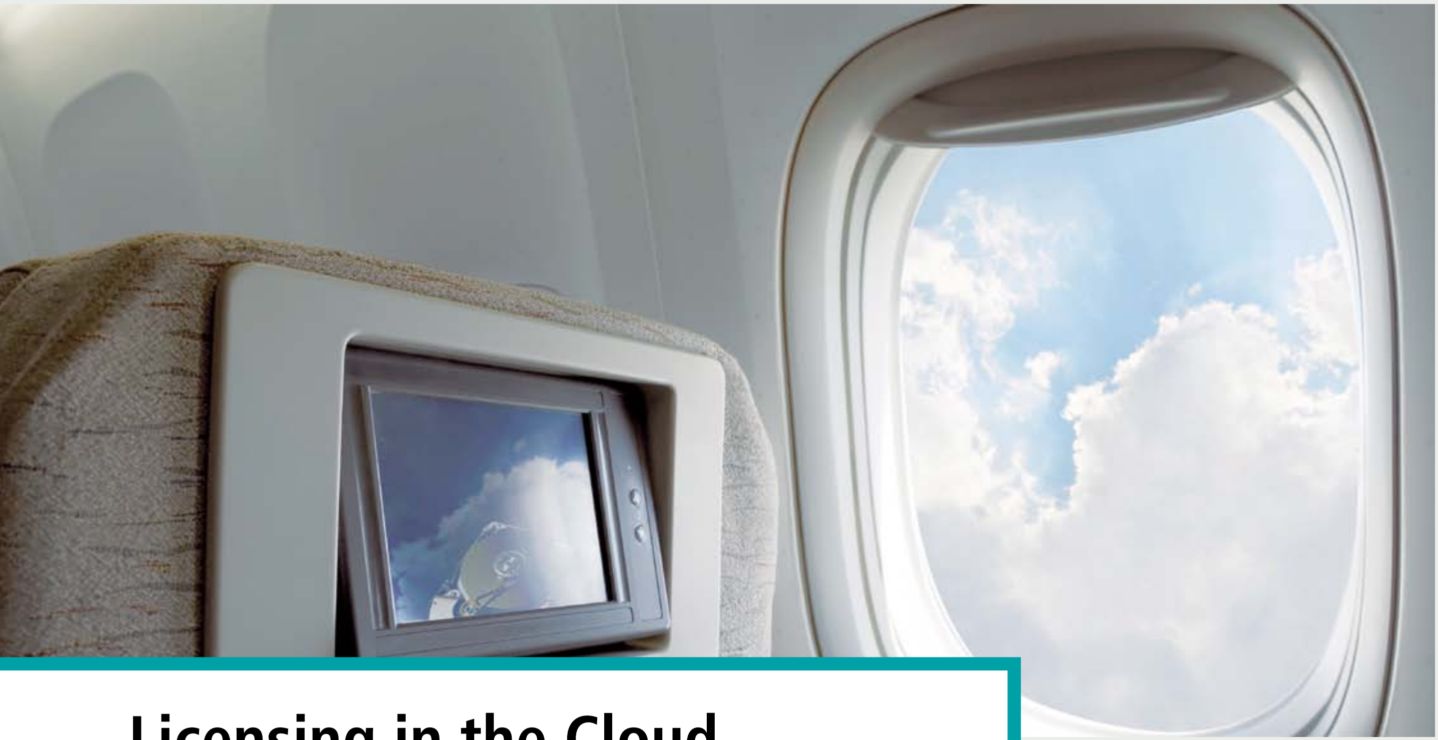
Doesn't a passport photo then present a security risk? A particularly fine example here is provided by the advertising poster of a security services company which showed the bit of a key belonging to the company. The picture was enough to allow the key to be copied. This couldn't happen with SmartBind® as features are not stored in plain text in the passport photo. The information in the passport photo only says this feature existed when the license was activated but does not allow the feature itself to be reconstructed.

Conclusion

CodeMeter SmartBind® provides an easy and secure way to bind a license to a computer. Using a variety of dynamically selected features, CodeMeter SmartBind® provides both reliability and security preventing manipulation. Let us go back to our comparison with recognizing a person. If I take off my glasses I will still be recognized. A colleague who puts on my glasses though will not succeed in pretending to be me. The license does not become invalid and require reactivation until several features have changed.



Calculating the CodeMeter SmartBind® key



Licensing in the Cloud

At the turn of the century, ASP (Application Service Providing) was all the rage. "Customers won't buy and download software in the future, instead they will lease it online". With ASP, software such as Microsoft Office runs on a terminal server and customers only need a client to use it. The concept never caught on. Lack of confidence in user data security, service availability and the blurry situation of software vendor and software licensing are some of the reasons which explain its rejection. Now the same idea is back under a new name - cloud computing. The time is now right for it and the technology has matured.

Who uses the cloud?

The cloud is anything online and includes software and services. Hence the cloud is much more than just Application Service Providing. Use of the cloud can be divided into the following categories:

Infrastructure Vendor: provides the hardware (and the operating system software) in the cloud. He is responsible for availability and backup.

Service Vendor: provides the software or service. He is responsible for his own application.

Corporate User: uses the infrastructure, software and services in the cloud for business purposes. He has a special status as he himself installs the software in the cloud and manages his staff's access to it.

Private User: uses the cloud privately. He is a consumer of software and services and mainly uses the cloud to store data or play online gambling games.

The classical Application Service Provider which offers third-party software such as Microsoft Office hardly exists anymore. The provider has a similar status to that of the Corporate User i.e. he operates third-party software in the cloud.

Software Vendor: is not actually present in the cloud. The Corporate User and Application Service Provider use his software though in the cloud.

What is the cloud?

The following types of services are available in the cloud:

Infrastructure as a Service (IaaS): the Infrastructure Vendor provides a basic structure (hardware only or hardware plus operating system). The Corporate User normally leases the infrastructure (a virtual computer). He installs, distributes and starts instances of programs (any software from any software vendor) on this computer. A typical example here is the Amazon computer center.

Software as a Service (SaaS): the Service Vendor operates his software and services in the cloud. Either he is an Infrastructure Vendor himself or he buys the services. The Corporate User and Private User are online consumers of his products. Typical examples here include Google Maps and CRM System Sales Force.

Platform as a Service (PaaS): this service is similar to SaaS. The only difference is that the Service Vendor allows the user (normally the Corporate User)to optionally define the business logic. Other providers can extend the functionality. CRM System Sales Force and SaaS belong to this category.

Webspace: the Infrastructure Vendor allows the Private User to store his data in the cloud. Examples of this are the PlayStation Network (PSN) from Sony which allows players to store the current state of their games online, and the Telekom cloud.

Protection interests of providers

Regardless of whether your concern is Private User data in the webspace or the sales figures in a hosted ERP application, security is an important issue. There has been a succession of bad news recently: data relating to millions of users stolen from Sony, or security breaches at a mail-order company operating online prize games. Who wants to protect what in the cloud and how can Wibu-Systems help?

It is in the interest of the Infrastructure Vendor to limit physical access to his computing center. The protection interests of the Service Vendor depend on his business model; some provide their services for free and earn money via advertising. Others bill customers depending on how often and how long they use their service. In this case, protecting access directly makes money. The Service Vendor has an indirect interest in protecting data on his server as this increases customer acceptance of his service.

The protection interests of the Private User are obvious. He wants to be sure his access data is protected against misuse and that his data is stored securely in the cloud. Just like the Private User, the Corporate User also wants his access data and own data securely stored in the cloud. Wibu-Systems has numerous products to meet these interests e.g. CodeMeter® Password Manager, CodeMeter Identity, a PKCS#11 middleware and a powerful encryption API. The password manager allows the user, be it the Private User or the Corporate User, to choose good strong passwords and to securely store them in a CmDongle. By using CodeMeter Identity and the encryption API the Service Vendor can integrate personalized security into his solution. The PKCS#11 middleware transforms a CmDongle into a standard token which can be integrated into the existing architecture of the Corporate User.

Protection and licensing for the Software Vendor

Although he didn't originally want to be, the Software Vendor is present in the cloud. The Application Service Provider or Corporate User upload their software to the cloud which can then be used by their own users or customers. Two requirements co-exist:

- The software should never be resold and can be used as often as necessary.
- It is difficult to license the software as tying it to a computer or dongle contradicts the philosophy of the cloud. The software doesn't run on a specific computer in the conventional sense. The Infrastructure Vendor can modify the hardware during operation without prior notice, or move the service to a completely new hardware.

The time is now ripe for a new strategy which the Software Vendor can and must pursue. One option is to migrate to a pay-per-use model. What implications does this have for the Software Vendor? Wibu-Systems can help him to develop a special cloud-ready version of his software which can run anywhere at any time but which only processes the entered data associated with a specific license. The Software Vendor integrates the license into the application with the aid of the CodeMeter® API.

But isn't this unsafe? "If the software runs anywhere at any time, can't I then modify the software to run without a license? As a software vendor, the protection offered up till now by AxProtector was very important to me." No problem: you can still use AxProtector; indeed it is an important part of the protection concept. The cloud-ready version of your software is encrypted using AxProtector which means it is impossible to detect where the API verifies the license. Hence manipulation is ruled out. By using a special untied CmActLicense you guarantee your software runs everywhere immediately, in other words on any computer in the cloud, while still being sure it is protected against reverse engineering and manipulation.

How can the license and the entered data be linked to each other? Initially the user's data exists locally. His purchased license or pay-per-use units are also located locally. A special local client from the Software Vendor uses the license to sign the data. This can only be done by the license owner as only this person has the private key for the signature which is securely stored in the CmDongle or a CmActLicense. An important aspect here is that the client deducts the pay-per-use units in accordance with the data. You don't have any local data to upload? No problem! Our Professional Services team will help you implement your individual solution.

When the cloud-ready version of your software starts, it checks the data signature is correct. If it is, the software executes the corresponding action or uses the entered data for the calculation. AxProtector thus guarantees your software is protected against manipulation. The software only contains the public key needed to verify the signature. Even if this key is extracted, it does not contain enough information to generate a valid signature.

Wibu-Systems will be happy to help you implement your own protection concept in the cloud-ready version of your software.

And finally one last word

The cloud covers everything which does not run locally on your computer. The benefit for the user is that he doesn't have to invest in or maintain any local computing power. Instead he uses the computing power of the cloud and only pays for what he actually uses, and that he can use anywhere and everywhere.

If the concept is applied to software, migration to a pay-per-use model is necessary.

CodeMeter® provides a framework for easy and individualized migration. A CmDongle or CmActLicense can contain several thousand counters which allows precise billing of each client in the cloud.

When the security aspects are solved, cloud computing offers excellent opportunities. We are working on standard solutions for the cloud which involve participation in research projects such as S4Cloud and MimoSecco in conjunction with research institutions and other companies.

What are your cloud requirements? Talk to us about them and we'll find a solution together. We are ready for the cloud!

Secure software licensing

How good is good software protection? As a software developer what do I need to think about during development to make sure my software is as perfect as possible? How long should good software protection last? The Egyptian Pyramids are a classic example of good protection. Many fatal accidents of varying nature made sure no attacker had a chance to attack again. Of course progress in the world continued and thanks to X-ray equipment, the internal workings of the pyramids are no longer a secret. It has always been a good idea to protect one's property, and the pyramids certainly were well protected by the standards of the time. If they hadn't been, it is questionable whether they would today enjoy the fame they do.

Why protection is sensible

The same principle applies to software protection today. If everything can eventually be cracked, is it worth protecting software at all? Isn't it a waste of time and effort? This may be true in a few cases, but in general the benefit of software protection is greater than the cost. Honest customers can't accidentally violate license terms and use more licenses than they have paid for. Your competitors can't just copy and plagiarize your methods. Hence you keep your competitive edge in the market. If the Egyptians had just buried their pharaohs in a field, they probably wouldn't have earned their place in history. They were protected so well that they are now on exhibition in museums around the world. Hence they achieved their desire for immortality.

Reading out data

The simple "is there a license?" question provides the most primitive type of protection. Accidental multiple use of the software is thus avoided, but this simple question does not protect it against hackers who professionally copy the software or use reverse engineering to find out your methodology. The hackers also read the data in the license e.g. activated modules or flow control data.

This type of protection requires a yes/no decision in the code. A disassembler can locate the question and replace it with code which ensures the question is always answered with "yes". Alternatively, the hacker can imitate the right answer. It makes no different whether this is done in a self-written statically linked library or in an external copy protection system.

Encrypting random data

If more sophisticated protection is required, cryptography can be used. The "what do I encrypt when?" strategy is important here.

Encrypting random data is slightly more reliable than reading out data. The data is decoded later and the license is only correctly verified if the two values match. However, this type of protection also requires a simple yes/no decision in the code. This type of encryption can also be simulated by another encryption e.g. an XOR.

Encrypting required data

A more suitable method is to encrypt data or, better still, the executable code required by the application. The data is encrypted and embedded in the software prior to release. It is subsequently decoded by the copy protection system, for example a dongle. If the license is missing, the required key is missing and hence the data cannot be decoded or used.

A hacker can try to change the question so that the checksum comparison always returns "yes". The software calculates an incorrect value and hence will not run correctly or, in the worst case, crashes. Hence it is almost impossible to crack the software without the relevant license. The hacker would have to guess the encrypted data. Unfortunately this type of protection has a major drawback: it can be cracked by eavesdropping on the transmission between the software and copy protection. The only solution is to build lots of encrypted secrets into the software at different places.

More than one key

In particular, CodeMeter® improves encryption of the necessary data as it allows more than one key to be used. As a consequence the same data can be encrypted with different keys and embedded in different places in the software. At runtime you randomly select which key to use. It is now much more difficult for the hacker to locate all the questions.

This method makes it extremely difficult and therefore expensive to crack existing licenses. You can further improve protection by NOT randomly choosing the random key. Instead you should couple it to the date and the computer data. The hacker thinks he has found a hack which works, but he will soon discover it doesn't work later on or for his "customers".

Challenge-response

Not only does CodeMeter® offer AES-based encryption, it can optionally generate signatures. You generate a random number, the so-called challenge, which you let the CmDongle sign. You then receive the response. The corresponding private signature key is securely stored in a secret or hidden data field in the CmDongle. You verify the signature in the software using the matching public key which you have embedded in your software. This key is only used for verification. Even if the hacker manages to extract it from the software, he can't use it to generate a valid signature.

Challenge-response requires a yes/no decision in the software, but it cannot be simulated using XOR. Compared to AES encryption, signature generation is very slow. It takes approximately 300 ms which means the mechanism should be used sparingly.

Integrity protection

Alongside simulation of the copy protection by the hacker, the second weak point is the modification of the protected application. The hacker changes the code in the application. For example, he replaces a JNZ ("jump if not zero") command with a JZ ("jump if zero") command. You can prevent this by monitoring your software for changes i.e. by building checksums and hash values over certain sections of the software and checking them at runtime. The saying "the more the better" certainly applies here. A high level of nesting is also helpful. An even better solution is to use checksums as jump addresses. Integrating these manually into the code is a time consuming and an error-prone job though.

Traps destroy the license

How were the pyramids protected so well? They contained deadly traps! CodeMeter® is the modern day version of these traps. When you detect a manipulation, for example an invalid hash value, a locking sequence is sent to the CmDongle. This detects and subsequently locks all of your licenses so they can't be used any more. Any data which has not yet been decoded is now permanently out of reach of the attacker. You can of course reactivate your licenses at any time via a remote update file. The licenses are not permanently destroyed; on the contrary, they are always under your control. Incidentally, the remote update file can only be transferred to and used once by the dedicated CmDongle. If the attacker falls into the next trap, the procedure is repeated.

Conclusion

CodeMeter® offers an extensive framework for state-of-the-art software protection. When correctly integrated into the depths of your software, the protection may not last several thousands of years as it did for the pyramids, but it will certainly last several thousand days. Instead of using a hammer and axe for the integration,

Wibu-Systems offers you AxProtector and, more importantly, IxProtector. AxProtector fully encrypts your software using different keys and implements traps to lock the license.

IxProtector is needed to subsequently decode the individual parts of your application.

You don't have to make any decisions about what to encrypt. Just use the executable code with IxProtector. Without this tool, the software won't run properly.

The hacker has to execute all of the software to discover all of the secrets. The longer he executes and analyses the software, the more traps he will fall into.

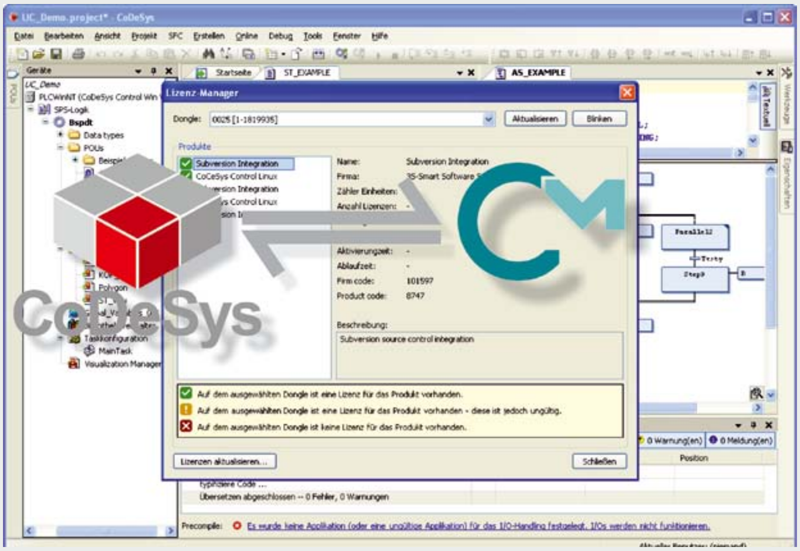
Some of the recently discovered individual hacks demonstrate how incredibly important it is to integrate the protection deeply within the product. None of the analyzed hacked software was protected by IxProtector and none had simple questions built in. For good protection we recommended using AxProtector and IxProtector. Enable as many of the anti-debug features as possible in AxProtector. Our Professional Services team will also be happy to support you with the individualized integration into your software.

Hacker's Contest in Russia 23.11. – 8.12.2011

The opening of the Wibu-Systems Hacker's Contest was announced this year at the "Softool" trade fair in Moscow which took place from 25.10 to 28.10.11.

Protecting PLC software using CoDeSys V3.5 and CodeMeter®

Software protection is not only relevant to PC software. There are also important reasons for protecting PLC software: machines and plants, and the know-how in embedded software in them, need to be protected against reverse engineering. It also allows new business models to be implemented and guarantees system integrity. **Oliver Winzenried, chief executive of Wibu-Systems, explains what's possible today.**



Dongle: 0025 [1-1819935]

- Subversion Integration
- CoDeSys Control Linux

Name: Subversion Integration
Firma: 3S-Smart Software
Zähler Einheiten:
Anzahl Lizenzen: -
Aktivierungzeit: -
Ablaufzeit: -
Firm code: 101597
Product code: 8747
Beschreibung: Subversion source control integration

Auf dem ausgewählten Dongle ist eine Lizenz für das Produkt vorhanden.
Auf dem ausgewählten Dongle ist eine Lizenz für das Produkt vorhanden - diese ist jedoch ungültig.
Auf dem ausgewählten Dongle ist keine Lizenz für das Produkt vorhanden.

Übersetzen abgeschlossen -- 0 Fehler, 0 Warnungen

Precompile: Es wurde keine Applikation (oder eine ungültige Applikation) für das I/O-Handling festgelegt. I/Os werden nicht funktionieren.

CoDeSys Security Key

Has the Stuxnet incident made manufacturers and users more aware of the dangers posed by viruses etc., and have they taken the necessary steps to protect themselves?

Users and machine designers are now more aware of the need for security in automation and embedded systems than they were before the Stuxnet incident. Many governments have started programs and set up "cyber defense centers" to protect critical infrastructure such as traffic guidance systems or energy and water utilities which must be protected against attacks from both terrorists and hackers. In the 23.10.2011 edition of the "Frankfurter Allgemeinen" Sunday newspaper, Michael Hange, president of the German Federal Office for Information Security, BSI, called upon industry to report attacks by the Duqu worm. Symantec first warned about this worm which has many similarities to the Stuxnet worm.

At the same time, unauthorized manipulation is becoming more and more of a problem. An example: manufacturers of wind power plants are anxious to prevent operators from tuning their wind turbines to generate more energy than specified. This will increase the wear and tear of parts still under guarantee which the manufacturer will then have to replace.

How can automation systems be effectively protected against manipulation?

Technical protection systems make it difficult to reverse engineer equipment, control systems and machines. The embedded software is effectively protected if the program code is encrypted. The encryption key is securely stored in either a dongle or in software which then activates and ties the key to a specific device or control system. Protection against reverse engineering is achieved by storing the program code in the target system in encrypted format as this prevents a disassembler from statically analyzing it. There are also mechanisms for detecting an "attack" which immediately cause the license to be locked and hence stop more software from being decoded.

The manufacturer digitally signs the program code to prevent it from being manipulated or modified without permission. The protection mechanism on the target system only allows correctly signed program components to be loaded and executed. Or put another way: a manipulated program won't run.

Wibu-Systems and 3S-Smart Software Solutions have been working together since 2010 to integrate CodeMeter® technology into the CoDeSys PLC programming and runtime system. What is the situation at the moment?

3S is rolling out version 3.5 of CoDeSys at SPS/IPC/Drives this year. CodeMeter® technology – known here as CoDeSys Security Key – is fully integrated into this version. You only need to tick the relevant box to generate protected code from within the development environment. The code can then be executed when a CoDeSys Security Key is connected to the target system.

The new security concept helps to stop valuable know-how from being copied or transferred to other control systems. Other security functions such as "signed application" and "encrypted communication" between the programming PC and PLC will satisfy the demand for integrity protection. The integrated user management, which protects access to projects or source code, effectively prevents third party manipulation of control systems.

Wasn't this possible before?
Up till now the CoDeSys development system only contained password protection. PLC programs in the target systems weren't protected. It wasn't possible to use CmDongles as they need a runtime software which wasn't available. New in version 3.5 of CoDeSys: by using the right dongle, program code can now be protected on any platform.
The deep level of integration in CoDeSys opens up new possibilities. Individual software components no longer have to be licensed immediately. This functionality, known as Feature-on-Demand, means functions present in the software can be "enabled" as and when required. They can be enabled via the Internet or offline via a license file after the software has been distributed. The machine manufacturer can thus use Feature-on-Demand to individually sell the features of his machines, both before and after shipment. For example he can offer a cheap starter model to compete with low cost foreign suppliers and a high-end one with lots of extras. Control system suppliers can sell a fixed number of licenses for target systems on a pay-per-use basis. The machine or plant engineer can then activate the licenses in his control systems as required. The manufacturer can also use pay-per-use mechanisms to lease his machines and bill customers according to usage. This will ensure he gets paid!
And last but not least, this method can also be used by the machine or plant engineer to protect his source code. He can choose which parts can be seen and modified by his customers (the end user), and which parts appear as a black box i.e. they can be used but not modified.

How are all these functions or features managed?
License management is integrated into the sales process i.e. licenses are given "part numbers" just like the mechanical components of a machine. The number appears in the parts lists of the ERP system. The ERP system, for example SAP, is connected to the License Central via a web interface so that licenses can be generated automatically. They are transferred to the machine's control system either online or offline using a file.

Are the security functions described above always available in CoDeSys?
Yes they will be but you will need a CoDeSys Security Key to use them. The key is available from 3S. Similar types of Security Keys are also available for the target platforms. All CodeMeter® hardware variants can be used as Security Keys, for example the USB CmStick/M or CmCards in MicroSD, SD or CF card format. They only cost a little more than normal industrial memory cards.

Beside the collaboration with 3S, are there similar cooperations with, for example, control system manufacturers?
3S has done pioneering work with the deep integration of CodeMeter® in CoDeSys. It is the first supplier in the PLC industry to offer such a solution. The Research Center for Information Technology (FZI) in Karlsruhe is currently developing a protection profile and is evaluating security functions. A protection profile is a sort of criteria catalogue which can be used to objectively test which of our products offer protection from which attacks. The project is partly financed by the BMWi (German Federal Ministry of Economics and Technology).

We are also involved in talks with other suppliers in Europe, USA and Asia. I would like to mention here one collaboration in particular: Wibu-Systems is a Validated Partner of Wind River, a 100% subsidiary of Intel. VxWorks has made Wind River one of the leading global suppliers of real time operating systems. Our CodeMeter Compact Runtime has been integrated into VxWorks which means RTP (Real Time Process) and DKM (Downloadable Kernel Module) components can be securely downloaded and program code is protected. Full integration into the Eclipse-based VxWorks Workbench development environment is under way.

Security is also a basic prerequisite for meeting safety requirements. What does this mean?
Safety standards and measures guarantee that machines and plants do not present a hazard to humans, the environment or property. This can only be guaranteed though if the manipulation of safety-critical systems is made impossible. The appropriate security solutions protect the safety solutions against attacks from outside, for example against unauthorized execution of program code or unauthorized modifications.
Safety can only be achieved using security.

Dieter Hess
CEO of 3S-Smart Software Solutions GmbH

"CoDeSys Security makes it easy for automation engineers to effectively protect their applications. It is based on tried and tested CodeMeter technology. Because this technology is fully integrated into CoDeSys it only takes a few mouse clicks to activate the protection. There is no need to familiarize oneself with the technology. The concept doesn't exist in any other PLC programming system at the moment."

Latest news summary

Premiere at the fair SPS/IPC/DRIVES 2011:

WIBU-SYSTEMS AG, supplier of software protection, and 3S-Smart Software Solutions GmbH, manufacturer of CoDeSys automation software, will be presenting the results of their successful collaboration for the first time at the CoDeSys shared stand in hall 7-530 of SPS/IPC/DRIVES 2011. The CodeMeter® encryption tools have been fully integrated into the CoDeSys development environment and will be available in future under the name of CoDeSys Security.

Current software versions:

- CodeMeter SDK4.30d, 2011-10-14
- CodeMeter SDK 4.40 Beta on request
- CodeMeter License Central 1.40, 2011-11-07
- CmIdentity 4.30d, 2011-10-14
- WibuKey SDK 6.0c ,2011-06-14
- AxProtector 7.20, 2010-10-14
- 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.

New: CmStick/C with keyring and cover

CmStick/C Basic has been on the market since Spring 2011 and is the world's smallest CodeMeter dongle. Its design has been kept simple: it has minimum dimensions and its housing only lengthens the metal USB connector by a few millimeters. It is intended to be left plugged into the laptop or built into an embedded device.

The new CmStick/C with keyring can be attached to a bunch of keys and easily removed from the USB socket. CmStick/C has the same functionality as other CodeMeter® variants based on the Smart Card Chip .

The CmStick/C also convinced the jury of the Most Successful Design Awards 2011 (www.designsuccess.cn) who awarded it a design prize.

Nerd-Zone project in Karlsruhe

Wibu-Systems has joined the Nerd-Zone project (www.nerd-zone.com) in Karlsruhe to help attract talented undergraduates to the company. Graduates will get to work on exciting projects in a location which is home to many high-tech companies.

CodeMeter® ready for Windows 8

CodeMeter® already works with Windows 8. Wibu-Systems's direct contact with the experts at Microsoft made this possible. Awards such as Gold Partner status and successful completion of the Windows 7 and WQHL tests convince our customers that by using our licensing solutions their products will be future-proof and function reliably for the user.

New AxProtector is CodeMeter®-protected

We are continually improving the protection offered by our software licensing solutions. One of our most important products is AxProtector which protects software without modifying the source code. The improved protection in version 7.20 of AxProtector makes it even more resilient to attack as it now requires a CodeMeter® license. The license is available free of charge to customers when they update their existing CodeMeter Firm Security Boxes (FSBs). Users of WibuKey will need to contact the sales department to get a CodeMeter® FSB.

New wibu.com website

In September 2011 we launched our new global wibu.com website. A centralized Typo3 Content Management System and distribution of static content via the Amazon Cloud Front guarantee up-to-date content and high speed downloads all over the world.
Extra personalized logins means we can offer customers and partners special information on top of the normal information and downloads, for example previews and beta versions of our software.

Register today. It's worth it!

WIBU SYSTEMS
Flexible CodeMeter Solution
PERFECTION IN SOFTWARE PROTECTION
CodeMeter SDK
Demo Version

Wincor Nixdorf customer story

CrypTA success story at Wincor Nixdorf

Wincor Nixdorf is a leading global supplier of IT solutions and services for retail banks and commercial enterprises. The CrypTA authentication tool has been in use since 2009 and guarantees maximum security. It not only protects applications and sensitive data, it also protects access to equipment during maintenance work. The tool has been realized using CodeMeter® protection and licensing technology from Wibu-Systems.

Wincor Nixdorf's catalogue of requirements for effective software protection and identity and access control comprised several components. Access control via a strong two-factor authentication e.g. knowledge of a password and PIN was extended to include ownership of a uniquely identifiable object (dongle). A single password should start all protected applications, with each user having their own password. The solution should be flexible to cope with the heterogeneous system landscape of the service applications (Java, C), and mobile to allow maintenance work to be carried out on the applications.

CodeMeter® protection and licensing technology from Wibu-Systems fulfils all these requirements,

For authenticated access to CrypTA, users not only need a CmDongle, they also need a second factor such as a personal password. The password must be reentered each time the CrypTA stick is plugged in. As with a mobile telephone, the same password activates all protected software applications. Because the stick is automatically deactivated when it is removed, there is no risk of a security breach if the stick is lost: a person can only access the device and applications if he knows the password. CodeMeter®'s "Enabling" feature is deployed here i.e. the correct password must be entered to activate the complete CrypTA Stick. The stick remains activated as long as it's plugged in and supplied with power.

CrypTA applications are written in Java and C. They are protected by CodeMeter® AxProtector and IxProtector and the software protection API which supports a variety of operating systems and languages.

As the CrypTA Stick is really just a CmStick/M with additional flash memory, it not only functions as an authentication dongle, it can also be used as a storage device.

The complete CrypTA software can be distributed on the stick. The software starts directly from the CrypTA stick and doesn't need to be installed first.

Not only does Wincor Nixdorf protect its software applications, it also protects its documents using SmartShelter | PDF and uses the same CmStick for authorization.

An expiry date means licenses which are used to access protected applications and documents are only valid for a certain period of time. They can be reactivated though after they have expired via remote programming.

For example, an employee's password becomes invalid when he leaves the company.

Guido Walther
Director Technical Support at Wincor Nixdorf

"Thanks to Wibu-Systems technology, we have been able to guarantee high level security for the protection of our Intellectual Property, while at the same time implementing the required flexibility into our processes."

Oliver Winzenried
Chief Executive of Wibu-Systems:

"The implementation at Wincor Nixdorf shows how versatile CodeMeter® is: secure protection of both software and documents, two-factor authentication with personal password, and mobile use without installation: it's all in the CmStick/M."

Roadshows, trade fairs and events

Join us at the following trade fairs and conferences:

ESWC 2011
19.11 – 20.11.2011
London, UK

Microsoft TechDays
16.2 – 17.2.2012
The Hague, Netherlands

CeBIT
6.3 – 10.3.2012
Hannover, Germany

SPS / IPC / Drives
22.11 - 24.11.2011
Nuremberg, Germany

Embedded World
28.2 – 1.3.2012
Nuremberg, Germany

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

15 November 2011	SCS Darmstadt, Germany
22 November 2011	SCS Bletchley Park, Milton Keynes, UK
22 November 2011	Security in Automation, Nuremberg
29 November 2011	SCS Breda, The Netherlands
08 December 2011	SCS Karlsruhe, Germany
01 February 2012	SCS Madrid, Spain
27 February 2012	VDMA User Forum, Frankfurt
14 March 2012	SCS Bletchley Park, Milton Keynes, UK

The current dates of our Secure Code Seminars can be found on our website.

Germany:	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

Order your free CodeMeter® Software Development Kit with dongle and activation today from: www.wibu.com

Imprint
KEYnote
22nd edition, Fall 2011

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
Terry Gaul
Ruediger Kuegler
Wolfram Mueller
Frank Semrau
Oliver Winzenried

Design and Production
Wolfram Mueller, Markus Quintus

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

WIBU, CodeMeter® and SmartBind® are Wibu-Systems trademarks. All other companies and product names are registered trademarks of their respective owners.
Copyright © 2011 by Wibu-Systems.

Cover picture "Airplaine window"
©iStockphoto.com/Kyoungil Jeon

MEDIA
ACCESS
PERFECTION IN SOFTWARE PROTECTION
DOCUMENT

WIBU
SYSTEMS