FALL 2012

KEYnote 24

THE WIBU MAGAZINE

Software protection: An integral part of the process

Topics

- The signature myth
- Project protection using encryption
- CodeMeter® and virtualization

WIBU SYSTEMS

Content

Dear Customers and Partners,

Make sure you optimize your software licensing and protection when you integrate them into your processes! The main topics in this issue of the KEYnote magazine show how this can be achieved with the minimum of effort.

We have recently increased our investment in R&D to provide you with the high performance support tools you need. We have expanded in the fields of development, innovation management, support and consulting. As part of our service we assess your situation on site, if requested, and accompany you in the development and implementation of your own individual concept. On page 14 we introduce our new staff member, and in the article titled "Quo Vadis CodeMeter?" discuss how we balance innovation with continuity.

In "The signature myth" article you can discover what asymmetric cryptography has to do with software licensing and how you can benefit from it using CodeMeter. A further topic looks at how to protect your application's data and what CodeMeter offers you here. Have your customers already moved into virtualization? If so, you would do well to use CodeMeter with its activation-based CmActLicenses, or CmDongles which can also be used in virtual environments, for example with a dongle server from the German company, SEH. Another topic in the newsletter looks at how to customize the WebDepot for CodeMeter License Central. The WebDepot is the web interface seen by your customers or staff when they fetch licenses via the Internet or Intranet. Our new webinars, listed at the end of the newsletter, let you acquire valuable know-how with minimal effort, for example, while sitting at your desk. Now what could be more convenient than that? The Sirona case study shows how CodeMeter has been integrated into the company's Cerec devices to create an impressive piece of dentistry software which is used to make dental implants.

The articles here are intended as a general introduction to the topics. Please do not hesitate to contact us to discuss your specific needs. I hope 2012 will turn out to be a good business year for you and that this issue of the KEYnote newsletter will inspire you with lots of new ideas. I look forward to meeting you soon at one of our events, trade fairs or webinars.

Best regards from Karlsruhe,

Oliver Winzenried (C.E.O.)

Quo vadis CodeMeter?

Many trends come. Some stay, others find a niche, but most disappear for good. It can be just as fatal for an organization to miss a trend as it can be for it to waste valuable resources following one which goes as quickly as it came. How does Wibu-Systems face this challenge and decide which trends are worthy of a look?

Continuity and innovation

Our principal aim is to establish reliable and long term partnerships with our customers and provide them with high-value, high-quality products and solutions tailored to their needs. Although we are dedicated to long-term collaboration with our customers, we are also quick off the mark to provide them with support for new technologies – a fact we have proved many times in the past. The USB dongle and support for the .NET framework are just two examples of groundbreaking ideas from Wibu-Systems.

Perhaps you wonder how Wibu-Systems tackles the two opposing concepts of continuity and innovation?

Wibu-Systems' first priority is to focus on its core competencies (i.e., the protection and licensing of digital intellectual property).

Our **Innovation Team** carefully examines new trends, sometimes in cooperation with the Karlsruhe Institute for Technology (KIT), the Research Center for Information Technology (FZI) or other institutions. By participating in numerous partner and early adopter programs, we are able to evaluate new trends at an early stage.

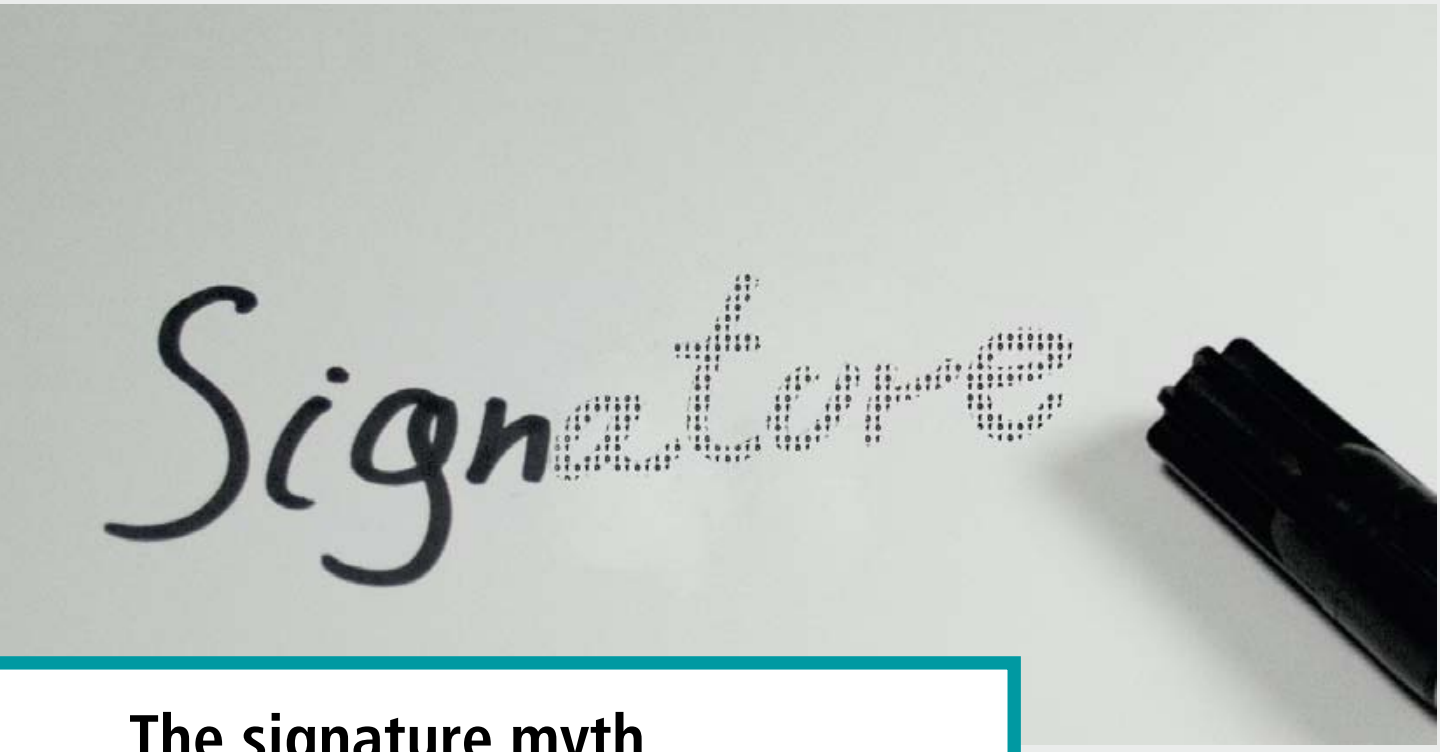
Our **Architecture Team** is responsible for seamlessly integrating our latest innovations into existing products and solutions so as to optimize the effects of synergy.

Our solutions for you

Wibu-Systems' main goals for the future are:

- **Software protection and licensing.** As a vendor of classical software you have always been able to depend on continuity with Wibu-Systems. We can reassure you, that you'll be able do so in the future as well.
- **Document protection and licensing.** Hidden champions in diverse sectors such as road milling and woodworking machines already use Wibu-Systems solutions to protect their service documentation. The technology used here is the same as the well-proven technology used to protect software. The license models and the license generation, shipment and management processes are exactly the same. The only difference is an extra module needed to integrate the technology into Adobe Acrobat®.
- **Embedded device protection and licensing.** Our solutions are already in widespread use in the automation industry thanks to our successful partnerships in this area. Solutions include protection of machine construction data, protection of PLC software from piracy and reverse engineering, integrity protection and authorization of PLC software, and licensing of on-demand features. Once again, the solutions are based on our well-proven CodeMeter technology. Our Embedded Team is responsible for making the special adjustments required by PLCs.
- **Protection, licensing and authentication in the cloud.** Our solutions in the cloud are based on our well-proven CodeMeter technology and are available to software vendors who want to license and protect their software. There are occasions where protection as well as authentication is required. CodeMeter is particularly well-suited here as its basic technology covers both aspects: authentication uses asymmetric methods while protection uses symmetric ones. And it goes without saying that our Cloud Team uses synergies from the basic development so as not to put a strain on the core resources of Wibu-Systems.

Wibu-Systems has enjoyed continual expansion over the last few years, a growth completely funded through its own resources. The development of new lines of business will have no detrimental effect on existing solutions and products. As our customer and partner, you can rely on us in the future to provide the products you need. We're committed to being your ideal partner in a longstanding and successful business relationship!



The signature myth

"I use standard certificates so I'm safe." The only safe thing to say about this statement is that one cannot safely say if it's true as it fails to look at threat scenarios such as "safe for whom" and "safe from what." The use of standard signatures and certificates with emails, for example, can be regarded as safe if the verifier is trustworthy. In the case of software protection, however, signatures and certificates often give a false sense of safety. And this is where CodeMeter proves to be invaluable. In addition to the above mechanisms, it also uses concealment and disguise to deal with the unsafe environment in which verification takes place.

A signature verifies that the software hasn't been modified and guarantees the identity of the publisher.

What is a signature?

A signature is a person's name written in a distinctive form to identify that person. Another person uses suitable methods to verify the name. Signatures are implemented using asymmetrical cryptography.

Asymmetric cryptography is based on two keys: a private key and a public key. As the names imply, the private key should be kept secret, while the public key can be accessed by anybody.

Let's look at how to send emails safely. Both the sender and recipient have their own pair of keys. Each knows the other's public key. If I want to be sure nobody other than the intended recipient can read my message, I encrypt it with the recipient's public key. The message can then only be decrypted by the recipient using his private key. If the recipient wants to be sure the message really is from me and that it hasn't been tampered with, I sign it with my private key. Any recipient who has my public key can verify that I sent the message.

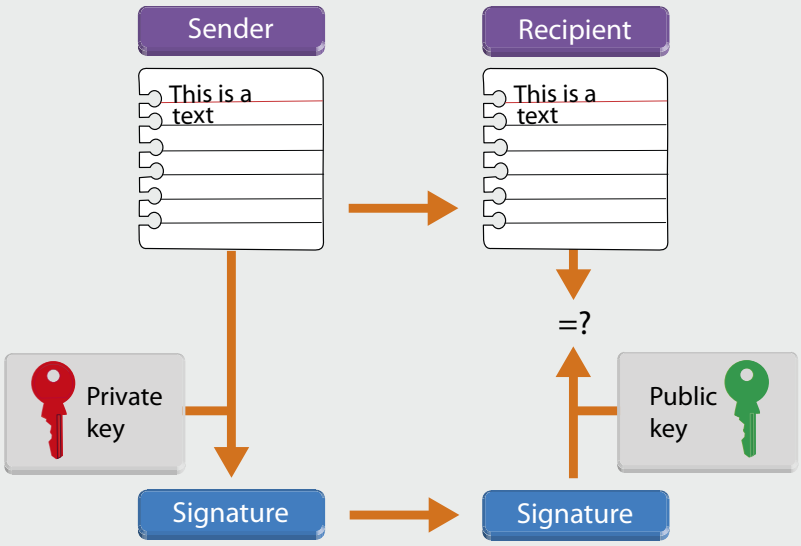
Of course, it is also possible to combine the two methods (i.e., to both sign and encrypt the message). The above description greatly simplifies the process as, in practice, a hash value must be generated prior to signing the email and a hybrid scheme comprising symmetric and asymmetric encryption is used for the encryption. The basic concepts still apply though.

A matter of trust

As explained above, the public key is not secret. It can be passed on to and used by anyone, for example, to secretly send me something or to verify my signature. But how does my email partner know for certain my public key is really mine and not somebody else's?

This is the central issue with asymmetric cryptography. Now we need to look at certificates. Someone who knows me or to whom I can prove my identity issues me a certificate. This certificate contains my name, public key and period of validity. My email partner is now able to verify my public key. But wait, how does he know my certificate is genuine? He can only be sure if he has the public key of the person who issued me the certificate. And so you see, we start going round in circles: for who certifies the certifier?

No matter how long the certificate chain is, at the end of the day I have to trust someone or something, for example, a root certificate. Computer operating systems usually contain one or two root certificates from certification



The signature is generated by the private key. The correctness is checked by the public key.

authorities. For a closed system such as the iPhone or a games console, the root certificate is the equipment manufacturer's certificate.

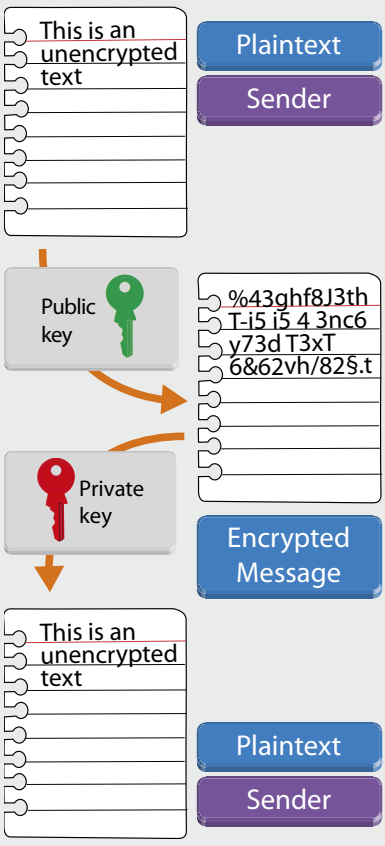
Who verifies the signature?

Just because signatures and certificates exist, it doesn't mean they protect you. If you think you can leave protection to the operating system (Windows, Mac OS), you're mistaken. Signature and certificate verification in operating systems has only been designed to keep you safe from malware such as viruses and worms. It doesn't stop you running software with an invalid signature or a missing signature, if you decide to ignore the warnings. Although a signature exists, it won't protect your software from being tampered with or illegally copied.

Windows provides you with an API to verify the signature of an application (exe or dll). You verify the existence of a signature, its validity and whether you issued it yourself. At first, this sounds good but it has two drawbacks. First, signature verification is implemented as a yes/no decision in your software which can be manipulated by a hacker. Second, you are asking the operating system to verify the signature and it is precisely this operating system which is controlled by the hacker, who can decide how to respond to your request. This is a generic hack of the signature API. Verification of a standard signature and certificate using operating system tools might be relatively simple for beginners to implement but it doesn't effectively protect your software from tampering and piracy.

CodeMeter is the solution

CodeMeter also uses signatures according to the book (i.e., as a software vendor), you safely store your private key in your FSB (Firm Security Box or master dongle). When you protect your software using AxProtector, it automatically signs your software with your key. The verification methods and your public key are hidden at various locations in your software.



Public key encryption: The recipient's secret private key is used to decrypt the text.

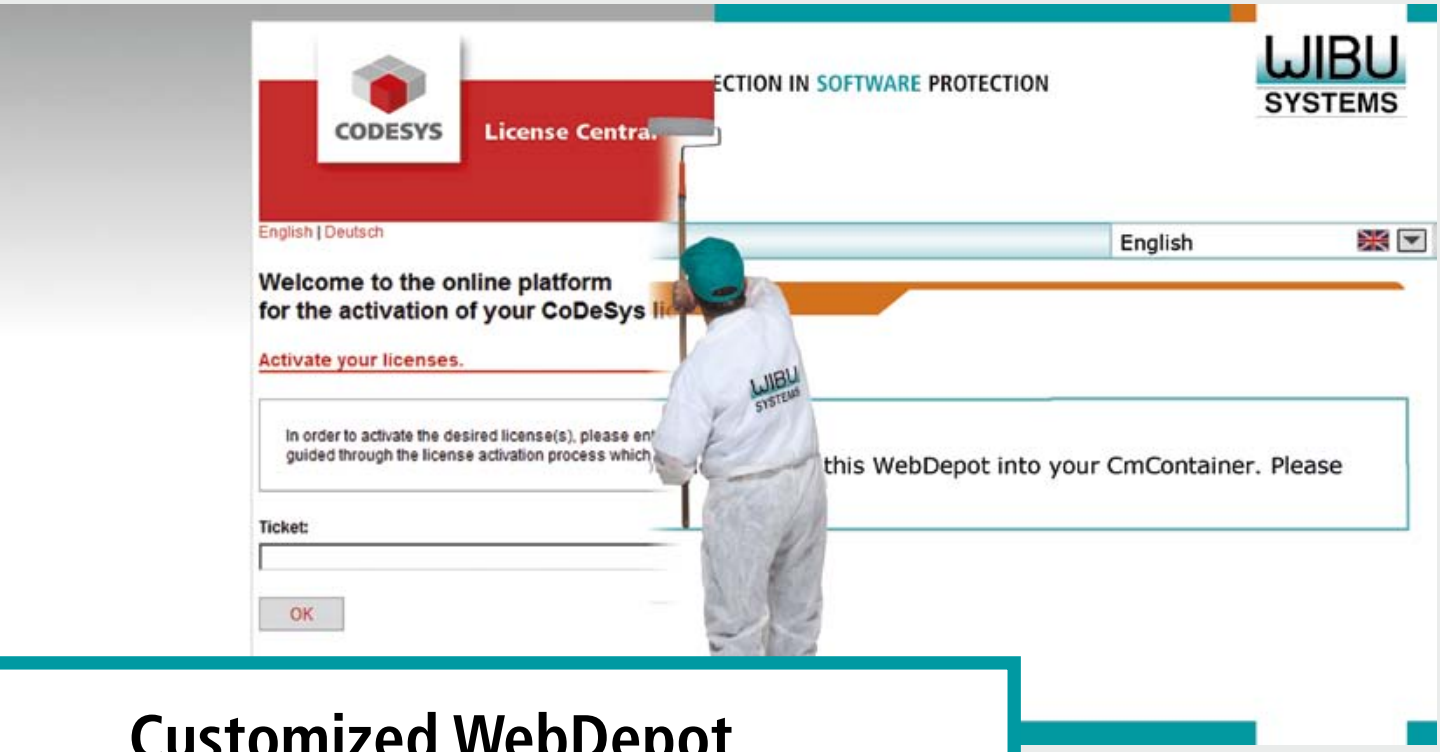
The signature is verified every time your application starts. Verification takes place at several locations in your software. This renders it impossible to externally simulate the software and tamper with even a single byte of it. CodeMeter provides full protection of your software by integrating signature verification into its general anti-piracy mechanism.

Summary

From a safety point of view, an approved standard method is always better than an individual proprietary one. The validity of this statement remains unquestionable as long as the standard method is deployed within the scope of its defined configuration. And this is precisely the problem with using signatures to protect software: one of the fundamental parameters cannot be fulfilled (i.e. a desktop PC is unable to verify whether the certifier can be trusted). As a consequence, CodeMeter relies on a healthy mix of standard methods and proprietary technologies to safely protect your software from every threat scenario, not only in the areas of integrity protection and anti-piracy protection but also in the PC world of your customer.

CodeMeter and VxWorks

CodeMeter protection methods are already safely integrated into the VxWorks operating system. CodeMeter fully protects the whole operating system so that software can only be downloaded from approved partners of the equipment manufacturer.



Customized WebDepot

Activation-based solutions such as CmActLicenses are very much state-of-the-art. Hardware-based solutions like the CmDongle, on the other hand, have often been declared a thing of the past, but every now and then they too enjoy a renaissance. In the meantime they have certainly become an indispensable component of solutions across many fields and industries.

Dongle vs. activation

Generally speaking the advantage of a dongle for the customer lies in license portability. That is, the customer knows exactly where the license is: in the dongle. When he works on another computer he simply takes the dongle with him and plugs it in there. If, for whatever reason, he urgently needs a license, there's nothing quicker than an activation-based solution which enables the license over the network. CodeMeter combines the important characteristics of CmDongle and CmActLicense to provide a unique, best-of-both-worlds solution (i.e., transparent and transportable software licenses and quick online programmable dongles). The License Central WebDepot, which is adaptable to individual needs, plays a key role here.

What is the WebDepot?

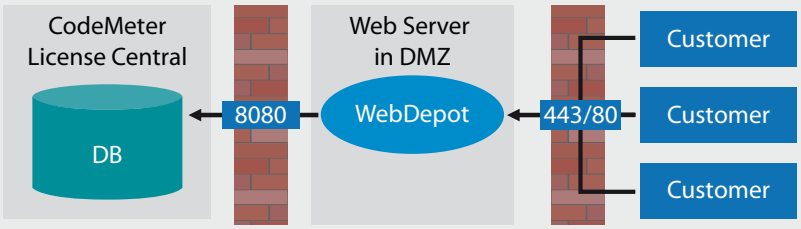
The WebDepot is a web-based application accessible via the Internet. It provides an interface for your users to the CodeMeter License Central. A PHP version of the WebDepot exists for the Apache web server. The end of 2012 will see the launch of a .NET version for IIS (Internet Information Server).

The user can access the WebDepot via any browser in order to single-handedly transfer licenses to both a CmActLicense and a CmDongle. The license is transferred directly to either a local computer or a CmDongle plugged into the local computer. An optional functionality allows the customer to download a license file and subsequently transfer the license offline to another computer or CmDongle. Other options which can be integrated into the WebDepot include functions to handle returned licenses and to compute an activation code for code-based (telephone) activation. These two options are not included in the standard scope of delivery. The user can choose between Microsoft Internet Explorer, Mozilla Firefox, and Google Chrome as the browser. For OS X he can use Safari. Whatever browser he chooses, he must make sure it's the latest version. Direct license transfer requires JavaScript and Java or ActiveX. Even if JavaScript, Java and ActiveX have been disabled, the WebDepot implementation still allows file-based activation. This means the user can still single-handedly activate licenses even if security has been configured to the highest level.

Why use a WebDepot?

Why do you need a WebDepot at all? Wouldn't it be easier to make CodeMeter License Central fully accessible via the internet? There are two arguments in favor of the additional WebDepot:

1) Security
2) Customization



Why does the WebDepot increase security?

For security reasons, CodeMeter License Central implementation is based on diversity. In other words it deploys a broad spectrum of technologies. The same concept is used, for example, in control systems for ships and nuclear power stations: If a systematic error (i.e., one which also occurs in a second identical component) causes one technology to fail, a second technology takes over to maintain safe operation. In the case of CodeMeter License Central this concept protects you from intrusion, data theft and unauthorized license generation.

The Apache web server or IIS is located in the DMZ and hosts the WebDepot. A tomcat behind the internal firewall processes requests from the WebDepot. If a hacker detects a systematic error, he might well gain access to (exploit) the web server including the WebDepot, but he can't get any further than that. Your database or Firm Security Box are safe, thanks to the internal firewall which makes sure the computer running the WebDepot only communicates with the tomcat via the web service. The hacker would need a second exploit for the tomcat to further penetrate the system.

The following basic rules therefore automatically apply when hosting a License Central Internet:

- Direct access to the CodeMeter License Central via the Internet is prohibited
- The web server in the DMZ must be regularly updated with security patches
- The WebDepot and CodeMeter License Central are installed on two separate computers
- A tomcat for the WebDepot is not allowed

Our hosting package has been carefully prepared for you by Wibu Operating Services and includes the CodeMeter License Central Internet which runs in the Wibu cloud. Our experienced team takes over responsibility for making sure the rules listed above are complied with.

How can I customize the WebDepot?

The user interface of the CodeMeter License Central has been designed for you, the software vendor, and no provisions have been made to allow you to adapt it to your corporate design. On the other hand, a web-based application designed for your customers should be given the look and feel of your company's brand or image. This is exactly what WebDepot lets you do, albeit in a rather primitive way.

You define your own styles in a CSS file and exchange the existing neutral images for the ones you want to use. The WebDepot now uses your colors and fonts instead. You can further customize the WebDepot to reflect your corporate image by swapping over the page header and footer.

The core functionality is the only thing which cannot be changed:

- A table of available licenses
- An area for help topics and error messages
- An action area with online and offline activation

It is also possible to individually customize the text. All the text is stored in a separate language file making it as easy as possible for you to adapt them to your design.

In principle, the WebDepot provides support for any language. The standard version is shipped with an English and German language file. To add another language, all you need to do is make the corresponding changes to the configuration file and translate the language file into the language you require. The WebDepot supports UTF8 encoding which means you can integrate any language you want.

How can I integrate the WebDepot and develop it further?

A software vendor very often has his own portal for customers. In this case there's no reason why he shouldn't integrate the WebDepot into his existing portal. The software vendor can use the WebDepot as an example of how to call the tomcat web services directly from within his portal, or he can even copy large chunks of the WebDepot code and paste them into his development project code.

Another alternative is to use the WebDepot and manage customer tickets in the customer portal. Instead of entering a ticket code, the customer logs into the customer portal. On selecting a ticket here, he is forwarded to the WebDepot where he can pick up the corresponding licenses.

The possibilities for further developing the WebDepot are numerous. Functions such as login, license return and license overview can be easily added to the WebDepot.

Software protection: An integral part of the process

Software development is a time consuming and costly business for a software vendor. The end product often contains extensive specialist knowledge which must be protected. Each year piracy, reverse engineering and manipulation cost the worldwide software industry billions of dollars in lost revenue. Integrating software protection early on into the existing software development process has a two-fold benefit.

Software protection is essential

These days professional software development is a well-defined process which, on the one hand, requires all functions to be defined with their input/output parameters before development begins, and, on the other hand, allows transparent tracking of schedule and budget. It is irrelevant whether development is based on the classical waterfall model or agile development methods such as SCRUM: early integration of software protection measures always pays off.

Whether the application under development is a custom software, a niche product for a particular sector, a software for the mass market, a solution for the cloud or an industrial controller application, besides the time and money spent on its development, the software also contains a large amount of the organization's intellectual property. If, as a result of piracy or reverse engineering, this knowledge falls into the wrong hands, the organization's future may be put at risk. Illegal copies are one of the largest causes of revenue loss in the software industry. A recent study carried out by the Business Software Alliance (BSA) in 2012 revealed that 42 per cent of software currently in use is unlicensed.

Integration into the development process

Integration of software protection and license management into the existing software development process inevitably affects every stage of the process. It is therefore advisable to decide your strategy early on or, better still, before starting the project. At this stage the project is at its most flexible and the members are more likely to accept the concepts of software protection.

Wibu-Systems also offers simple and quick solutions for later phases of the project, including following completion. A few mouse clicks with AxProtector add high level protection to software without making any changes to the source code. The result is a fully encrypted application with protection mechanisms such as anti-debugging, changing keys, intrusion detection and secret locking codes which invalidate the license as soon as an attack is detected. Besides protecting your application, you can also implement a license model to meet your requirements. Here Wibu-Systems' IxProtector can be used to develop a modular license model which allocates separate licenses to each application module.

A broad diversity of license models is available for your application, ranging from single-user through network licenses, time-limited models, feature on demand to pay per use models. You can combine the models according to your needs, and choose between a hardware dongle (CmStick or CmCard) or 100% software license (CmActLicense) for the license container. The software can be shipped with either or both types of license container which means you can adapt the license model to local market needs. Wibu-Systems is fully committed to the principle of "one solution fits all."

A major benefit of Wibu-Systems solutions is that no decision needs to be made during development regarding the type of license

container (dongle or software license). Following release, product management, for example, can decide the type and scope of the license and revise their decision at a later date without having to modify the software. The result is a simpler development process with more flexibility, lower development costs, and a strict separation of development, software protection and licensing.

The overall process of software encryption and license model specification comprises four simple steps which are illustrated in the diagram below. By using Wibu-Systems solutions, unprotected and unlicensed software is transformed into an application with anti-piracy and reverse engineering protection and a license model.

Process support

Wibu-Systems provides high performance tools for all four steps. The tools have a corresponding user interface, plus extensive programming interfaces for full integration into the development process environments. For example, a tool may integrated into a build server which automatically compiles and subsequently encrypts newly developed models as part of a specified development process. Pre-defined automatic test scenarios can be subsequently used to test the models.

Summary

Cost-optimized and transparent software development requires consistent use of software development processes. It doesn't make any difference these days if classical or agile methods are used. In both cases, software protection and license management are extremely important aspects which should be addressed at the start of process planning or in the initial backlog for agile methods.
The result of a well organized and executed process incorporating scalable and versatile solutions from Wibu-Systems is a fully protected software with flexible license models, increased net income and lower development costs.

The following will then apply to you as well in the future: "Planning is the replacement of chance by knowledge."

Software protection in four simple steps

1) **Define the application features:** Decide which software modules you want to license individually.

2) **Protect your software:** Fully encrypt your software with easy-to-use AxProtector from Wibu-Systems without modifying the source code. Protect individual modules with IxProtector to add an extra layer of protection. Set the basis for customized licensing.

3) **Generate your licenses:** Map your own license models in a straightforward and flexible manner using CodeMeter License Central. Sale and distribution of licenses can be mapped online directly or offline, and integrated into the organization's existing back office processes.

4) **Ship your application:** With CodeMeter you have a wide range of shipment options. Choose between a hardware-based dongle (CmDongle) or a computer-specific software license (CmActLicense), pre-programmed or shipped as license code.

Project protection using encryption

Practically every piece of software processes data in some way or antoher. Depending on the actual application, the data may contain a large amount of the software vendor's or user's know-how and intellectual property. This article shows how you, the software vendor, can protect the data. Not only do you benefit from this, but it also provides your customer with added value.

Automation with AxProtector

AxProtector's file encryption tool provides a quick and effective way to map simple requirements. To protect your application, first of all you need to enable file encryption. You can think of AxProtector as a guard between your protected application and the file to be read. If the data file to be protected has also been encrypted using AxProtector, your protected application automatically checks whether a valid license exists for this data file. If it does, the file is automatically decrypted.

If the license is missing, the protected application will refuse to read the data file. And here you face the first restriction associated with automatic file encryption: error handling. Your original application processes this error and might therefore need to be modified slightly. Writing to the data file is the second challenge the protected application faces. You can use a set of rules to very precisely define how to write to the file, including even the file extension.

Manual encryption

If the simple automation does not meet all your requirements or you prefer to control the system yourself, you can use the powerful functions of the CodeMeter Core API to manually integrate encryption and decryption into your application.

Each combination of firm code and product code provides a unique key which is available for you to use. CmAccess2 opens a handle to the license entry. CmCrypt2 encrypts your data and CmRelease releases the handle. CmGetLastErrorCode can be called to fetch detailed information about the last error.

Besides the firm code and product code, an encryption code is also needed to decide which key to use. You can choose any value for the encryption code but it must be a constant value stored in the source code of your software. The secret is now spread across several locations. The actual key is located in the CodeMeter license, together with all the other keys and the secret encryption code is stored in your software. The latter determines which key in the CodeMeter license is the valid one. Consequently only your software can decrypt the data. A fake or replica of your software doesn't know the code and which key to use.

The "Create CRC" option should be enabled during encryption. Store the generated checksum together with the firm code and product code in your data file. Enable the "Check CRC" option during decryption to verify the data file has been correctly decrypted. We recommend using AES in CBC mode for the encryption. This allows data of any length to be encrypted into a single block (minimum length 16 bytes). With CodeMeter, only the first 16 bytes are transferred to the CmDongle. The remaining bytes are stored in encrypted format in the computer's main memory so as not to compromise security. This method also guarantees high performance with large amounts of data.

Permissions management

If you want to sell data file encryption as added value to your customers, you'll need a management strategy to access the data. There are two main methods in use:

- License-based permissions management (firm code and product code)
- Identity-based permissions management

License-based encryption

Each combination of firm code and product code produces a unique key which can be used as an individual privilege. The technical implementation is described in the "Manual encryption" section of this article. In the software you also offer the possibility of using the firm code and product code for the encryption.

If your customer, the user, wants to allocate the privileges himself, he will need his own firm code and an infrastructure to generate the licenses (CodeMeter License Central). This solution involves a lot of work to implement but the result is a truly flexible system for allocating access privileges, including time-limited access privileges, and for transferring licenses online.

Identity-based encryption

In many situations, the allocation of permissions is based on identity. Each person is assigned a unique identity. A data file is encrypted specifically for the specified identities which ensures that only recipients with these identities can access the data. The system is similar to the encrypted communication used for emails. Here also emails are encrypted for specific recipients. The person who encrypts the data file can also sign the data to guarantee its authenticity and integrity.

In comparison to license-based encryption, this method brings the benefits of integrity and authenticity, plus straightforward implementation. A CmDongle already has a unique identity and can easily acquire another one. The user does not need a special infrastructure to generate and manage the licenses and privileges.

Implementation is based on asymmetric cryptography. Each identity has its own private and public key pair. The private key is used to create a signature and decrypt data. The public is used to verify a signature and encrypt data. The implementation presents two challenges. First, the data must be readable by more than one recipient. Using the recipient's public key to encrypt the data means, however, each recipient is sent different data. Second, asymmetric cryptography is unsuitable for encrypting large amounts of data.

Hybrid encryption solves both challenges. You begin by selecting a random AES and encrypting the relevant data with this key. Next you encrypt the random AES key with the public key of each recipient and append the results, together with the recipients' IDs, to the data. You can also decide whether to sign the data with the sender's private key before the data is encrypted, or to sign the whole message after the message has been encrypted. The data is usually signed before it is encrypted to guarantee its authenticity. If you sign the data after it has been encrypted, the authenticity of the whole message is guaranteed but you have no legally binding verification of actual data.

You can optionally combine this hybrid scheme with your own password blueprint for downward compatibility with your existing solution.

The protected data now contains the following information: the encrypted data, the individually encrypted key for each recipient plus the recipient's ID, and the signature verifying the authenticity and integrity of the data.

You use the recipient's private key to decrypt the data and the sender's public key to verify its authenticity and integrity.

The entire process is based on the assumption that each participant knows the correct (authentic) public key of the other participant. If, for example, you have defined your public key as a constant in the source code of your software, you can verify whether the data files belong to you and reject them if they don't. If the sender has a database with the public keys of all recipients, he can generate a data file for each recipient without having the corresponding CmDongles.

Best of both worlds

Group keys can be used to extend identity-based encryption to include the features of license-based encryption. As well as an identity, a person can be allocated a group or data-specific key which is stored as a license entry in a CmDongle. All possible license options are now available, but the private key stored as hidden or secret data is used for encryption.

CodeMeter License Central can then generate and distribute both permanent and temporary privileges. Only CodeMeter offers you this flexibility, as only CodeMeter combines asymmetric and symmetric methods in a CmDongle.
CmActLicenses, which are tied to a specific computer, offer exactly the same functionality as CmDongles. In this case encrypted versions of the keys are stored in the license file on the computer.

CodeMeter, the key monster

You may have heard the term RSA in connection with asymmetric cryptography. This is an outdated encryption method which requires a long sequence of bits to generate a key considered sufficiently secure. Calculation of the public and private key is also complicated. Successful attacks in the past which managed to crack RSA were often focused on this calculation.

For this reason CodeMeter deliberately uses the new ECC standard. A 224 bits ECC key provides the same level of protection as a 2048 bits RSA key. This means more than 2,000 different keys/identities can be stored in a CmDongle.

Compared to RSA, ECC provides an additional benefit. The private key is a pure random number which can be used to calculate the public key. This makes the process of generating key pairs easier and more robust. CodeMeter offers you support here too. Each CmDongle contains an FIPS 140 conform random number generator which you can use to generate private keys.

Summary

Whether you want to protect your data using license-based methods, identity-based methods or a mixture of both, you can be sure that CodeMeter provides an easy-to-use and secure solution for your application.

Glossary	
AES	Advanced Encryption Standard (a symmetric encryption method)
CBC	Cipher Block Chaining Mode (concatenation of blocks to encrypt large amounts of data)
RSA	Rivest, Shamir and Adleman (an asymmetric cryptographic method)
ECC	Elliptic Curve Cryptography (an asymmetric cryptographic method)
FIPS	Federal Information Processing Standard
CRC	Cyclic Redundancy Check (checksum)
Hash	Cryptographic checksum

CodeMeter and virtualization

Virtualization was already making headway in the 90s, it's impossible to imagine the IT world of today without it. The key benefits include better use of resources, lower investment costs and platform independency. This article shows how Wibu-Systems solutions successfully handle these topics in virtual space as well.

Areas of use

Virtuality is defined as the property of an object not to physically exist in the form it appears to. The virtual object however has the same nature and effect as the object which really exists. In the IT sector, virtuality refers to an additional environment (virtual machine) on a real computer in which another computer virtually exists and runs its own operating system. The virtual computer shares the available resources with the real computer and other virtual environments installed on the computer. Within the scope of virtualization, a computer physically connected to the network can be configured to allow multiple persons to log on to it and share its applications and resources (terminal server). The aim is to use the available resources as efficiently as possible. And this is the decisive point: Multiple use of resources in a virtual environment inevitably means multiple use of licensed software which is a violation of its terms of use. The software vendor must therefore endeavor to find a simple yet long-term solution to this problem.

The challenges

CodeMeter software protection and licensing solutions from Wibu-Systems provide software vendors with the tools they need to protect their intended license models from violation in a virtual environment.

CodeMeter supports the use of both hardware (CmDongle/CmCard) and software based protection solutions (CmActLicense) in the virtual environment. The general aim is to make sure licenses are only visible where they are allowed to be used. Unfortunately there is a serious discrepancy here between the hardware and software solution: Whereas a CmDongle contains and protects an actual license, the software equivalent is directly stored on a system and is copied whenever a virtual system is created or cloned. The only way to prevent this is to devise some way to tie a software license to a virtual machine.

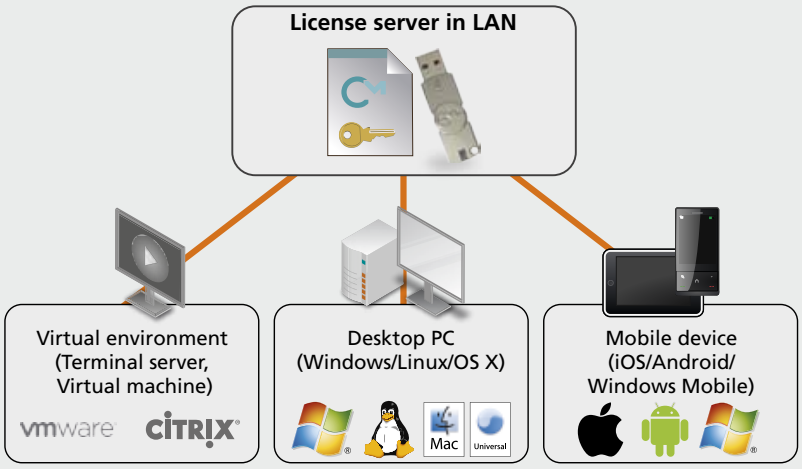
And this is exactly what Wibu-Systems has done with SmartBind®. This system, which benefits from many years of experience and for which a patent has been filed, ties a software license to hardware. It not only binds the software license to various hardware features of a computer but also to features particularly relevant to virtual environments. The probability now of successfully recognizing a clone increases to 98 per cent. A license which has been copied or moved as a result of cloning can now be safely invalidated.

Efficient use

A virtual machine implemented as a network license server offers major benefits in terms of efficiency and utilization by allocating and monitoring the available licenses in the network. A license server can also be used in heterogeneous networks containing real machines with diverse operating systems, and virtual environments and terminal servers.

Generally speaking, it doesn't matter whether the available licenses are stored in a CmDongle plugged into the hardware or in a CmActLicense tied to the license server, although a CmDongle offers the benefit of greater mobility. It can be moved from one server to another, making the licenses available there instead.

Licenses can be made available in a virtual environment using various kinds of techniques.



For example, if a CmDongle with local licenses is allocated to a specific guest of a host system, the licenses are only visible to this guest. On the other hand, network licenses stored on a host system can be accessed by the host and all the guests installed on that host.

A prerequisite for using licenses on either system is the installation of the CodeMeter service on both the host and guest system. This ensures secure communication between the individual components and correct calculation of the number of licenses in use.

Flexible technology means different virtual systems can be connected together. Network licenses allocated to the host system via a dongle can be made available to other host and guest systems located in the same network. Allocation of local licenses on the other hand is restricted to the respective local system.

A terminal server allows a large number of users to share a host computer including its resources and programs. Efficient resource utilization is very important as the host system's hardware is simultaneously accessed by many users. When subsequentely logging on to the terminal server, the user's computer only functions as an output/input terminal. Users are assigned their own working environment (session) which protects them from other terminal server users. The CodeMeter service from Wibu-Systems ensures the available licenses on the terminal server are correctly allocated and verified for each session.

Using a dongle server

Dongle servers are another way of allocating licenses in a network. Hardware dongles cannot be used in certain situations such as cloud solutions because they cannot be physically plugged into a computer. The question then arises, why not use a dongle over the network? Security can be guaranteed by encrypting the communication and exclusively assigning the dongle to a single user.

The myUTN-80 USB dongle server and myUTN-120 SD card server from SEH-Computertechnik GmbH in Bielefeld, Germany, allow you to use your software normally without having to plug the copy protection hardware dongle into your local PC. Up to eight dongles or one SD card with full functionality are securely and centrally available. As with a locally connected device, the dongle can only be used by one user at a time via a point-to-point connection. It is guaranteed that the software vendor's license terms are not violated at any time.

Here are some of the most frequently occurring situations which dongle servers help to resolve:

- Do you always know where your dongle is? Is it lying around unused or is a colleague using it? Storing dongles in a single central location puts an end to these questions once and for all!
- Do you want to allocate network licenses to specific users or grant them exclusive access privileges? This is quick and easy to set up with a dongle server! The server exclusively assigns dongles to specific users with the corresponding encryption of the interfaces.
- Have you ever you lost or mislaid your dongle, or was it even stolen? The dongle server's lockable box securely protects the dongles inside.
- No USB port on your computer? All USB ports used? Or are you using a virtual computer? If the answer to any of these questions is yes, a dongle server is the alternative solution for your applications.

Latest news summary

CodeMeter firmware 2.0

An update for CmStick, 1001-02 and CmStick/M, 1011-02 is now available but it can only be installed on systems where CodeMeter Runtime 4.50 or later is running. This version contains the following new features and revisions:

- Offline Field Update: With this feature, you no longer need an Internet connection to update the CmDongle firmware from within your software.
- 2048 bit RSA key
- Improved hardware reliability and longer lifetime using new error correction techniques.

Current software versions:

- CodeMeter SDK 4.50a/b, 2012-09-19
- CodeMeter License Central 1.51a, 2012-10-04
- CmIdentity 4.40, 2011-12-20
- WibuKey SDK 6.10, 2012-10-25
- AxProtector 8.20a, 2012-09-12
- SmartShelter PDF 6.01, 2012-06-19

Current firmware::

- CmStick, CmStick/M with Item number 1001-02 and 1011-02: 2.0
- CmCard/µSD, /SD, /CF: 2.0

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

Please update regularly.

Boost to the Wibu team

Sales, Support & Consulting and R&D have expanded. Here are just three of the new team members who are worth getting to know:

L. to R. Dr. Ralf Trunko, Head of Innovation Management, R&D Partner Projects and Patents, Jens Schneider and Wolfgang Greiner, both members of our Consulting Team who will support you in preparing your software licensing strategy.

Online tutorials – learning by doing with the CodeMeter SDK

The video tutorials on our website or YouTube show how easy it is to take the first steps with the CodeMeter SDK.

http://www.youtube.wibu.com

Always up to date

Our KEYflash newsletter informs you of the latest developments and trends. If you would like a free copy of our ezine, please sign up now at:

http://www.wibu.com/en/newsletter.html

You can also subscribe to our social media channels: Follow us on Facebook and Google+ and keep up to date with the latest news, software, press releases, trade fairs, events and interviews. Visit our Twitter channel for targeted information on new software releases and programming tips.

www.facebook.wibu.com
www.twitter.wibu.com
www.google.wibu.com

Business whitepaper from Frost & Sullivan

FROST & SULLIVAN

"Secure License Management for effective Software Monetization" is the topic of a brand new paper which reveals important reasons for implementing a licensing system. We highly recommend reading this extremely interesting paper!

Microsoft Gold Partner OEM Hardware Recertification 2012

Microsoft Partner
Gold OEM

Wibu-Systems has achieved Microsoft Gold Partner status for the fifth time since 2008. This award has benefits for our customers. Our direct contact with Microsoft means we are one of the first to receive its new operating systems which in turn implies we are one of the first to offer support for them. We also test our products for compliance with Microsoft's "Windows Logo Tests" and "Windows Hardware Quality Labs" (WHQL).

We still use independent certified testing laboratories such as the VDE and Underwriter Laboratories (UL), to test our products for compliance with the relevant safety and EMC standards. This guarantees you'll have no problems using our device anywhere in the world.

Newsflash

+++ Firefox 16 Password Manager plugin now available +++ License Central 2.0 with sophisticated reporting to be launched shortly +++ New extensions to CodeMeter Compact Runtime +++ WindRiver VxWorks reference systems with CodeMeter coming in November 2012 +++ White paper on integrity protection using CodeMeter +++ Support of Windows 8 and Mac OS X Mountain Lion +++

Sirona success story

sirona
The Dental Company

My name is CEREC and I give you something to chew on.

In the past, you needed two separate appointments for a dental crown. First the dentist had to take an imprint and put in a temporary filling; a week later, after the prosthodontist had created the inlay, you would return for its implantation. With the CEREC procedure developed by Sirona, treatment can be completed during a single visit. The tooth is measured digitally with a camera, the inlay is optimized by the dentist with the CEREC software and milled from a tiny ceramic block matching the color of the tooth. The inlay is then immediately implanted in the mouth: a cost-saving and convenient procedure for the patient.

Sirona 4.0 runs from the highly compact-sized CodeMeter CmStick/C, which was embedded into dental equipments in 2011. In 2012 the dongle was extended to support the specialist inLab software for prosthodontist and lab technicians allowing them to configure their own favorably priced solutions from a range of software modules and license models.

Use of the efficient CodeMeter tools, AxProtector and IxProtector, facilitated integration into the .NET-based CEREC software. By inserting attributes in the source code it is possible to specify how to apply the protection. Even if the entire software is protected, performance remains excellent.

License transfers to the device, including retroactive transfers, use a process fully integrated into Sirona's sales system. The end user purchases a license; the order is activated by Sirona and automatically transferred to the CodeMeter central licensing system. The latter generates a ticket with an unlocking code which is emailed to the end user who then enters the code in the CEREC software to activate the license via the Internet.

The CEREC equipment is accredited in compliance with MPG, the regulatory body for medical products. CodeMeter uses code signatures to prevent manipulation of the tested and released software. Moreover CmStick/C is greatly reduced in size, its OEM version matches the corporate identity color of Sirona and is compliant with all important international security and EMC certifications such as VDE, UL, CE, FCC, VCCI and KCC.

Conclusion: A range of benefits for the end user including IP protection and anti-counterfeiting solutions.

Ulrich Orth
CAD/CAM Software Research and Development Manager at Sirona:
"Our well-established knowledge of IP protection and anti-counterfeiting, and our MPG-compliant medical appliances enable us to provide enterprises with excellent levels of security. With CodeMeter we meet all requirements in an exemplary manner, while our customers enjoy flexibility and competitive prices."

Topics in KEYnote 25:

- Increments to License Central Reporting
- Deploying traps to improve security
- Protecting technical product and service documentation
- Hosting and support

Roadshows, fairs and events

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

You can register for open trainings or a special in-house sessions with an unlimited amount of participants from your company. The open trainings start at 09.00 a.m.; the maximum amount of participants is 12. The sessions can be held in English, Dutch, or Spanish. If a training session for more than three participants, booking an in-house training pays off. The number of participants then is unlimited. In-house training can be adapted to meet your specifi c requirements.

Training location	Protection & Licensing of Software, 1 day, £ 373 / € 399 per participant	CodeMeter License Central Desktop, 1 morning, £ 186 / € 199 per participant	CodeMeter License Central Internet & Back-Office Int., 1 day, £ 373 / € 399 per participant
Edegem (B)	06 November 2012	07 November 2012	07 November 2012
Driebergen (NL)	27 November 2012	28 November 2012	28 November 2012
Hengelo (NL)	22 January 2013	23 January 2013	23 January 2013
Milton Keynes (UK)	06 March 2013	07 March 2013	07 March 2013
Madrid (ES)	24 April 2013	25 April 2013	25 April 2013

Masterclasses
Smart & secure software licensing

Wibu-Systems offers you the opportunity to participate in one of the special seminars about:
- Code protection against illegal use & reverse engineering
- Licensing of software, with hardware or software-based keys (SmartBind)
- Solutions for embedded software in systems or cloud applications
- Back office integration

Training location	Date	Time
De Karpendonkse Hoeve in Eindhoven (NL)	13 November 2012	11.00-15.00
Landgoed Te Werve in Rijswijk (NL)	11 December 2012	11.00-15.00
Faculty Club in Leuven (B)	31 January 2013	11.00-15.00
't Wapen van Haarzuylen in Utrecht (NL)	26 February 2013	11.00-15.00

Bits & Chips 2012 Embedded Systems,
November 08, 2012
Stand 13
Brabanthallen 's-Hertogenbosch, NL

SPS/IPC/DRIVES
November 27-29, 2012
Hall 7, Stand 640
Nuremberg, Germany

Imprint
KEYnote
24th edition, Fall 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:
Ruediger Kuegler
Oliver Winzenried
Stefan Bamberg

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

MEDIA ACCESS
PERFECTION IN SOFTWARE PROTECTION DOCUMENT

WIBU SYSTEMS

5060-002-02/20121115