SPRING 2017

KEYnote 33

THE WIBU-MAGAZINE

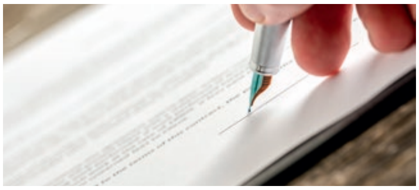
Inside the professional's toolkit: The lesser known side of CodeMeter

Highlights

- Document Protection
- Greater Revenue with Subscriptions
- Highly Available Licenses

WIBU SYSTEMS

Table of Content



Dear Clients and Partners!

Digitalization and Industrie 4.0 are trending, but they are not an empty hype. What they have in common is that they create new value by connecting people. Value for end users and consumers as well as enterprises everywhere. The connected world benefits from all people around the globe working as one. The strengths of the emerging economies can come together with those of the G7 nations. The Internet and the cloud have shown the way. Digitalization will get us to our destination.

The Chinese Year of the Rooster started on January 28th. The rooster is a symbol of honesty and reliability, but he also knows how to fight. Let us all join the fight for freedom and free trade. New tariffs and other barriers to trade should not be part of our world.

The great benefit of CodeMeter for your business is protection and flexible licensing for software-realized functions and data. Used intelligently, it can help you reach new clients, introduce digital business models, and grow your business. Automation and business process integration with licensing offers you limitless opportunities.

Read this KEYnote and learn about new use cases and innovative developments to inspire you, from the new WebDepot with Activation Wizard and Gateways, subscription licenses, licensing with OPC UA, to the all-new CmStick/CM. Don't miss our practical demonstrations in Hall 8 of Hannover Messe, at the *SmartFactory*^{KL} booth, the Plattform Industrie 4.0, and the Industrial Internet Consortium, and the ZSK embroidery machine at our very own booth.

I wish you all a rewarding year 2017. Let's share our insights – the many expos and conferences in Germany and abroad give us a great opportunity to do so.

Kind regards,

Oliver Winzenried

CEO

Flexible License Portal

A license portal can increase customer satisfaction and reduce operating costs by offering self-service functions. Your users are given a ticket, which they can use to activate their licenses, transfer licenses from computer to computer, or recover a lost license themselves. As a developer, you have three basic variants of license portals at your disposal: A ready-to-use WebDepot, a customizable CustomDepot, and powerful web services for seamless integration with any portal that you might already be using.

For a quick start, WebDepot is typically the ideal solution, and it can easily be changed and expanded later on to become a CustomDepot. WebDepot allows you to adjust the color scheme, the fonts, and the logo to match your corporate design. But even if you choose the ready-made WebDepot, the customization options do not have to be limited to such surface aspects.

All in one piece

One of the most common customizations is the ability to activate a ticket as a single, inseparable item. You can use this setting to make sure that your users do not split up different licenses from a single ticket and share them across several CmContainers. Typical use cases would be product bundles or updates for specific licenses.

You can combine this feature with the ability to hide all licenses on a ticket except for the most current one. Under the hood, all previous licenses are also activated or deactivated, as the case might be.

Spring cleaning tickets

Maintenance contracts or subscriptions will often mean that a single ticket slowly gets crowded with many licenses. Most of them might be outdated and have already been replaced by a new license. WebDepot can automatically clean up these licenses and dump them into a garbage ticket.

Check before activating

The newest version of WebDepot comes with an interface with which you, as the developer, can add functionalities. It enables you to include certain checks before every activation, deactivation, or reactivation. You can check the dependencies and settings and either return relevant messages or start defined automatic actions.

Also for gateways

All settings in WebDepot are also available in the new version of ActivationGateway. Both WebDepot and ActivationGateway are based on the same source code, with ActivationGateway representing the scripts that are executed on the server. The user interface appears as ActivationWizard on your users' computer. WebDepot provides the interface and the functions under the hood.

Custom tables

You can tailor the tables in WebDepot to suit your choices, e.g. how the lists are sorted or which columns are displayed. The new version gives you an interface with which you can set up your own tables. You can now include e.g. drop-down or fully sortable tables.

With the many configuration settings and versatile interfaces for your own code, you can build WebDepot to match your unique needs and workflows perfectly.

Document Protection

Intellectual property comes in all shapes and sizes. Software is just one of them. If you want to protect your software, Protection Suite is the ideal choice: You encrypt the executable file, and it can only be run with the right license. The decryption mechanism is integrated into the file itself, and the decryption is started automatically. But what if your intellectual property is not a software application, but a digital document? Unlike with software applications, you cannot simply add the decryption mechanism to the file, because the document file is not executed itself, but opened by another application.

There are four basic scenarios for protecting documents:

1. The documents take the form of PDF files that are displayed with a PDF viewer.
2. The documents are opened and saved with one of your own applications or the application of one of your partners.
3. The documents come in a standard format and are opened and saved with a standard application.
4. The documents come in a different standard format and can only be viewed with a standard document viewer application.

Protecting PDF files

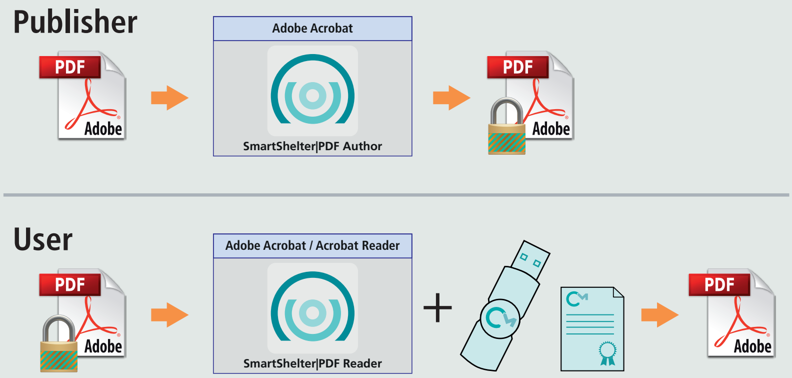
One typical case of PDF files that need to be protected are handbooks, technical manuals, guidelines, or service instructions. Service documents in particular often contain very sensitive technical details. Their authors might not want them to get in the hands of competitors, unauthorized service personnel, or even media outlets. Since the PDF file type as such has become a global standard, passing on the files themselves is extremely easy.

Adobe already offers a password-based solution for encrypting PDF files. It allows special settings to prevent e.g. printing, copying, or changing the files. This standard solution, however, has three major drawbacks:

- Passwords are often too short and weak, allowing a straightforward dictionary attack.
- The user of the file needs to know the password, and might disclose it to others.
- Nothing stops screenshot applications from capturing the data.

This is where SmartShelter|PDF comes in. SmartShelter|PDF is an official Adobe-certified plugin for Adobe Acrobat and Adobe Acrobat Reader. It starts where the standard protections stop: The password for the document is created automatically under the hood, away from the eyes of the user. It will will be strong and no unwitting or dishonest user could share it with others. The password is created with a CodeMeter license entry.

With CodeMeter, you as the publisher decide whether the license is to be stored on secure hardware, the CmDongle, or in a computer-bound license file, a CmActLicense. The document could only be opened by users who possess the license on the CmDongle or in the CmActLicense file. SmartShelter|PDF includes an author plugin and a reader plugin. The Author plugin creates the password with a master dongle, the Firm Security Box, which you also use to create the users' licenses. The reader plugin creates the password with the assigned license on the CmDongle or in the CmActLicense and passes it on to Acrobat Reader without the user's knowledge. As long as the user has a valid license, he or she can open the file and use it to the extent allowed by your chosen settings.



SmartShelter|PDF uses another Protection Suite technology to identify disallowed applications. It immediately closes protected documents when it notices that a screenshot application is running.

With CodeMeter as licensing system, all CodeMeter licensing options can be used, including time-bound licenses or licenses with a usage counter.

Proprietary documents

Your documents might come in a proprietary format, like settings files, construction blueprints, design patterns, or audio and video files. Your reasons for protecting them might be just as diverse. Common use cases include:

- Your software needs custom settings that you adjust specifically for each user. Different users should not be able to share these settings.
- You sell documents as an additional revenue source on top of your software. These should only be used by the people who actually bought them.
- Your software produces certain types of data, like live recordings of concerts. This has to work anytime and anywhere. Artists like Peter Gabriel will not sit and wait backstage, because you have to go and get your license. However, back in the studio, the resulting recording should only be readable and editable with the right license. Or more generally: A license is needed to open the document.
- Your software processes data, e.g. by cutting sheet metal based on a specific design pattern. Your software should only process data coming from somebody with the right entitlements, be it for financial reasons or for reasons of liability. Again put more generally: A license is needed to save the document.

These use cases can be combined as preferred with the legitimate protection needs of your partners. For instance, a partner should also have the right to produce documents that your software can open.

CodeMeter can handle all four use cases and their many combinations. With the CodeMeter Core API, you have a powerful API for encrypting, decrypting, and signing data. The toolkit is versatile enough to cover all of the above scenarios.

Individual settings can be encrypted with a unique key that is created for each client. Protected in this manner, the data cannot simply be shared anymore.

Companies in the business of selling documents can use the same concept that is used to sell software features on demand. Each individual package is given its own product code for encryption, which is accomplished either by AxProtector or by another custom tool. Just like software features, the licenses are activated in CodeMeter License Central. Again, all license options are available.

When it comes to managing the rights for saving or opening files, CodeMeter Core API offers asymmetric methods. Data can be signed with a private key that requires a valid license, and the data can only be read if the signature is present and correct. In this scenario, the author of the file needs to have a license. In asymmetric encryption, the data is encrypted with a public key and can only be opened again with the right license and the right private key. Now, it is the user that needs to have a license to open the document.

Our Professional Services Team is available to help you choose the optimum concept for your specific use case and to assist you, if you wish, with implementing your chosen solution.

Standard documents

When you are working with your own type of document, you can integrate cryptographic capabilities in your software. But what happens if you are using standard files that a user can access with a run-of-the-mill viewer or other standard application? In these cases, SmartShelter|SDL is the solution. SDL stands for Secure Data Layer. SmartShelter|SDL slips a layer of insulation between the operating system and the application handling the protected document.

SmartShelter|SDL can configure which operations are allowed and which are prohibited. This is easily done for viewer applications. Encrypted documents can be decrypted if the right license is available. Unencrypted documents can be loaded into the application, but saving is prohibited. It gets more complex if the application in question should also be able to save data. You can define whether saving is allowed at all and whether saved files have to be encrypted or can be unencrypted. This is where it gets challenging: Let's imagine a user opening a protected document. He then creates a new document in the same application. SmartShelter|SDL cannot recognize whether the new document is a copy of the protected file (which can only be saved in encrypted form) or a completely different file that should stay unencrypted. This is why using SmartShelter|PDF in a write mode is technically possible, but limited to very specific use cases. By contrast, a read-only mode in a viewer application is always and easily enforceable.

Summary

Protecting documents is a far more complex task than protecting software applications, because the question always comes down to the specific application that is using the documents. CodeMeter can shield PDF files from prying eyes in a simple, safe, and fully conformant manner. It is also easy to protect other standard document types with a read-only mode in a viewer application. Whether write modes are possible often depends on the specific procedures and use cases in question. If you are using proprietary formats with proprietary software, CodeMeter gives you a powerful API to cover all use cases imaginable: Licenses for opening files only, licenses for saving files, or licenses for any type of access. The level of flexibility offered by CodeMeter is without rival.

Greater Revenue with Subscriptions

Successful brands like Adobe, Microsoft, and Sony are convinced: Instead of selling licenses, their users can rent their software and services. These subscriptions guarantee a lasting and predictable revenue stream. But is this model suitable for all types of software? What do software developers have to remember when they introduce subscriptions? This article answers both questions.

What are subscriptions?

Subscription can refer to many things in the software industry. The most traditional meaning is a **license subscription**. In this case, the user does not buy a permanent license for a piece of software, but instead rents the software. Technically, it is a license with a defined expiry date. When the license expires, the user loses his right to use the software. The advantages are simple: lower upfront costs, fair billing for the actual rental period, and software that is always up to date.

Subscriptions can also refer to special maintenance arrangements. Such **maintenance subscriptions** have the user buying the actual software and then subscribing maintenance services. The user has the right to use the software indefinitely, even after the subscription expires. However, during the subscription period, the user has guaranteed access to new versions of the software. When it ends, the version is, in a sense, "frozen" at that point in time. Technically, the license is a permanent license with a defined-duration maintenance agreement.

Hire purchases are not technically subscriptions, even if the term is commonly used to describe them. In this case, the user pays for the software in installments. When the last payment has been made, the user gets full and indefinite usage rights. This is a particularly popular model in Latin America. On a technical level, it is a temporary license that is transformed into an unlimited license after the final payment has been received.

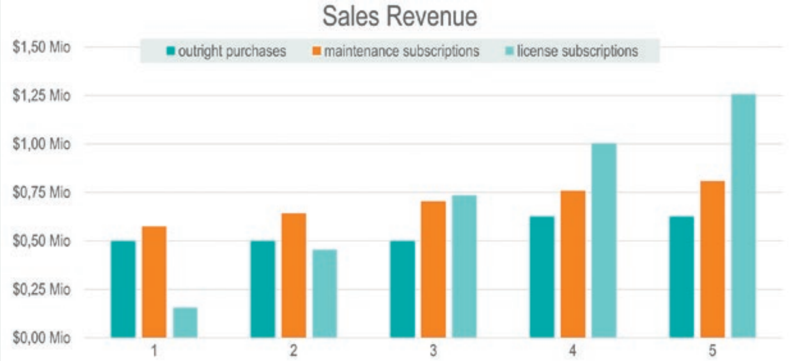
Pricing

A rule of thumb for pricing software subscriptions is that the rental price should equal the full-purchase price after 2 to 3 years of use, i.e. the monthly rental payment should be between 2% and 5% of the full price. Annual maintenance fees should be between 12% and 25% of the purchase price. Hire purchases usually have installments over a period from 1 to 2 years, with interest rates between 5% and 20%.

Is a subscription the right choice for my product?

There is no one correct answer for this question, because the calculation depends on many different factors. Let's imagine a case with the following setting: As developer, I will reach 100 new buyers per year with my software priced at $5,000.00. Typically, half of them will buy an update after three years, for which they would pay half the original price.

I expect that 75% of my customers would buy maintenance services if I offer a maintenance contract. This would cost 20% of the original software's price, and 10% of the subscribers would cancel the contract after a year. I also offer the software on a subscription license, at a fee of $200.00 per year. 5% of these subscribers can be expected to cancel their subscriptions every year. These are fewer cancellations than in the case of the maintenance contract, because the users could not use the software at all anymore in this case. The lower upfront cost suggests that I might reach 25% more new clients in the first place, even though this depends a lot on the



specific market and the specific product. How many more users would I be able to reach that I would not reach otherwise? In this scenario, the success of the model would be visible quite soon – if I cannot reach more clients with a subscription model, it would mean less turnover overall compared to outright sales.

The above chart shows the typical development of sales revenue for outright purchases, maintenance subscriptions, and license subscriptions.

The picture might be completely different for your specific software, but the general rule is that a license subscription is slower out of the blocks, but will then outpace the other options going forward. In many cases, the model should initially be used for specific - ideally new products - or specific markets.

Implementing subscriptions

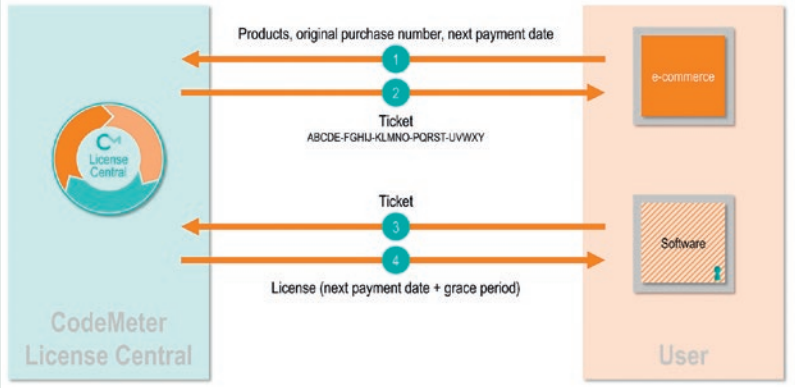
There are two basic ways to set up subscription licenses:

1. You create unlimited licenses and cancel them when the subscription ends.
2. You create limited licenses that are active until the next payment date (plus a grace period) and renew them automatically when payment has been received.

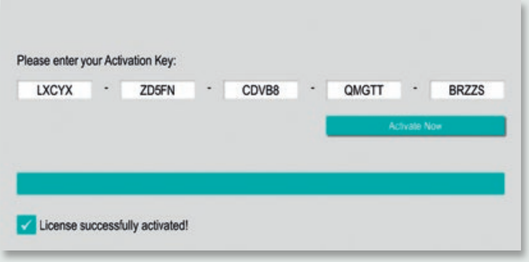
The first approach makes for simpler handling, as it only needs one action in the case of a cancellation. However, it does leave considerable room for fraud: Dishonest users could try to keep their licenses active by either not going through the cancellation process or by interrupting that process by not going online. This is why the second approach is preferable. The common objection that it forces users to get active regularly to renew their licenses is easily explained away: Simply use an automatic renewal process, ideally with a certain grace period. For most users, this will let the renewal just happen automatically and in the background. Another advantage of the second option is how simple it makes it for the subscription to be transferred to a new computer. Since the license on the old machine is time-limited, it will simply run its course, and you can show goodwill and allow the user to activate the new one on the new machine in the meantime.

Technical workflow

In order to introduce a subscription model, you need CodeMeter License Central to create and automatically deliver the licenses, and you need a billing system. This can be a popular ERP system like SAP, an e-commerce solution like CleverBridge or Digital River, or a CRM system like Salesforce.


Products, original purchase number, next payment date
1
2
Ticket
ABCDE-FGHIJ-KLMNO-PQRST-UVWXY
e-commerce
License Central
Ticket
3
4
Software
License (next payment date + grace period)
CodeMeter
License Central
User

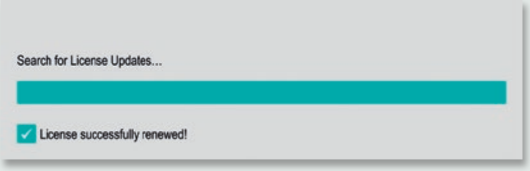
When a subscription is ordered, the billing system sends the necessary information to CodeMeter License Central. The order has to include details about the products covered by the subscription, the original purchase number, and the next payment date. CodeMeter License Central then produces a ticket with the required temporary license, with which the user activates the subscription. The ticket is stored in the license or on the user's computer.


Please enter your Activation Key:

LXCYX - ZD5FN - CDVB8 - QMGTT - BRZZS

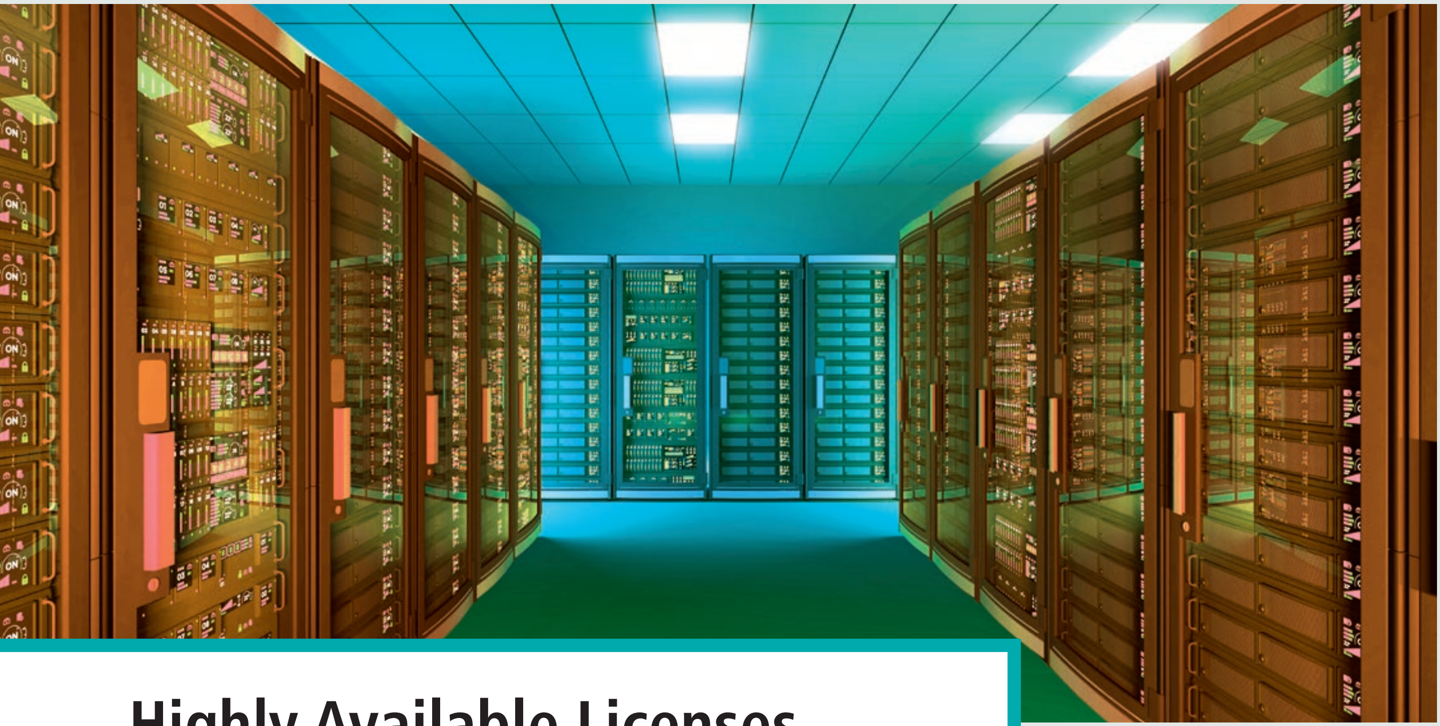
☑ License successfully activated!

For an automatic renewal of the subscription, the billing system transmits again details about the products, the new purchase number, the next payment date, and the original purchase number. CodeMeter License Central uses the latter number to allocate the renewal to the right subscription and produces a license with a new expiry date, which is set to the existing ticket.


Search for License Updates...

☑ License successfully renewed!

The user's software uses the ticket it has stored and checks regularly whether a license renewal is available. If it is, the license is automatically updated. Within a certain grace period, in which the license stays active beyond the next payment date, the whole procedure can run transparently in the background, without ever interrupting the user in his daily life with the software.



Highly Available Licenses

When software on a regular consumer computer stops working, it is a nuisance. If it stops working in a commercial environment, it can threaten the mission (mission critical incident) or the entire business (business critical incident). As a software developer, it is essential for you to understand your users' availability requirements and to respond to them with the right strategies and capabilities. You should never forget to include the question of licensing in your availability concepts.

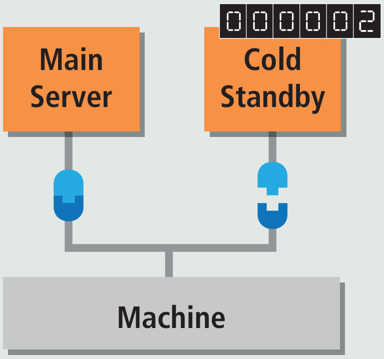
One obvious and simple solution is to forego any licenses at all. In such cases, the software could simply be copied to a replacement computer, and the user can keep on working. However, this option has one often ignored condition and one potentially disastrous effect on your business. For the software to be installed on a replacement computer, that computer would have to be available or be bought on the spur of the moment if something happens. It would have to be fully compatible as well. Buying or organizing a replacement license would be just as easy as buying or organizing such a replacement computer. The great disadvantage of foregoing licensing in general is obvious: Unscrupulous or unwitting users could simply copy and use your software without paying for it at all. In any case, the lost revenue, especially in the form of unintended overuse, can be life-threatening for small and medium-sized enterprises.

The cotton sorter

One of our clients produces specialized sorting machines for cotton processing. The unique intellectual property of that client lies in the software that controls the sorting process – the rest of the machine is simply nuts and bolts and a few cameras, which any skilled engineer could copy without too much effort. As the machine sorts cotton during active production, any outage or disruption means an immediate loss, because production comes to a standstill. High availability is key. The sorting usually happens literally in the field, i.e. on the cotton plantation, so that an Internet connection is not always available when problems occur.

A solution would be to install two devices for controlling the machine. One of them has a dongle with an unlimited license for the control software. The second one has as a similar license, but it is limited to 30 days of use after first activation. If anything goes wrong, the first controller can be replaced or repaired without production having to be interrupted, whatever the problem might be. Service technicians would have 30 days to repair the system on site and set up a new emergency license.

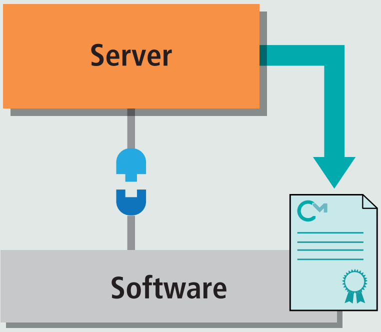
This is called a **cold standby** solution. An additional license is available and ready for use as needed. Because it is for temporary use only, the user would not be able to trick the system and use it as a second full-scale license. Technically, this can be achieved by defining a usage period or integrating a unit counter. In the former case, you define for how many days the license should work after it is first activated. In the latter case, the unit counter tracks the number of individual actions or the actual time in use, down to the last minute.



The architect

Another scenario would be an architectural studio that owns a number of floating network licenses, stored on a license server. The studio's architects have to work in the studio, from home, and on building sites, but they need full access to their software. VPN connections might not always be possible when they are in their home office or out and about in the field.

The solution is to borrow licenses from the license server and transfer them into a local CmContainer on the architect's computer. The license is flagged as active on the server, and over-use is prevented. Architects can then work offline on their computers even with an unstable or without any VPN connection at all.

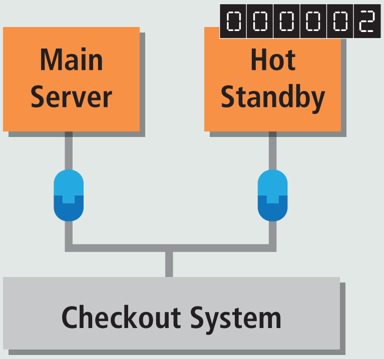


This approach represents a type of **local caching** of licenses. As developer, you decide whether this feature is allowed and for how long the user can borrow the licenses. You can integrate the borrow feature intelligently in your software to keep it as transparent as possible as a background process. Your users can also return licenses early when they do not need them anymore.

The checkout system

Everybody has been there: You wait in queue at the supermarket, and then there is a problem with the checkout system. The queue gets longer and longer, and people are getting more and more impatient. A high availability strategy is the ace in the hole for such situations.

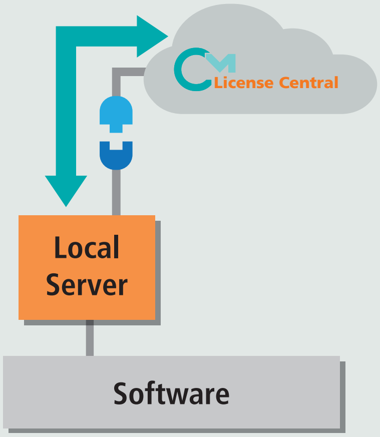
The solution uses two license servers. The first contains all licenses as floating network licenses. The second contains the same licenses, but with a unit counter. The software checks whether the first server is available and uses the licenses from there. If all licenses are in use, an error is returned, because all licensed checkout systems are already active. The backup server comes into play only if the first server is not available. The software counts down the unit counter with minute-by-minute precision, allowing you to check the usage of your backup server and identify any potential misuse. This solution is called **hot standby**. The first server can also be combined with local caching.



The holiday season

In the run-up to the holidays, many supermarkets would love to have more checkouts open that they might have licenses for. It is the busiest period of the year by far. The supermarket would be ready to pay for these additional licenses, as long as it means fewer people having to queue at the checkout.

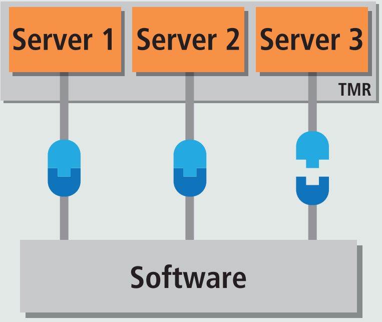
The solution is not unlike a hot-standby option, and it is called **overflow licensing**. Again, a second license with a unit counter is used. By contrast to the standby approach, this license is also used when all other licenses are in use. This gives the operator additional licenses to buffer any peaks in demand. Their use is recorded to the minute to ensure precise and accurate billing. Combined with a hot-standby solution, the entire setup needs four categories: Normal licenses, overflow licenses, backup licenses, and overflow backup licenses.



The carmaker

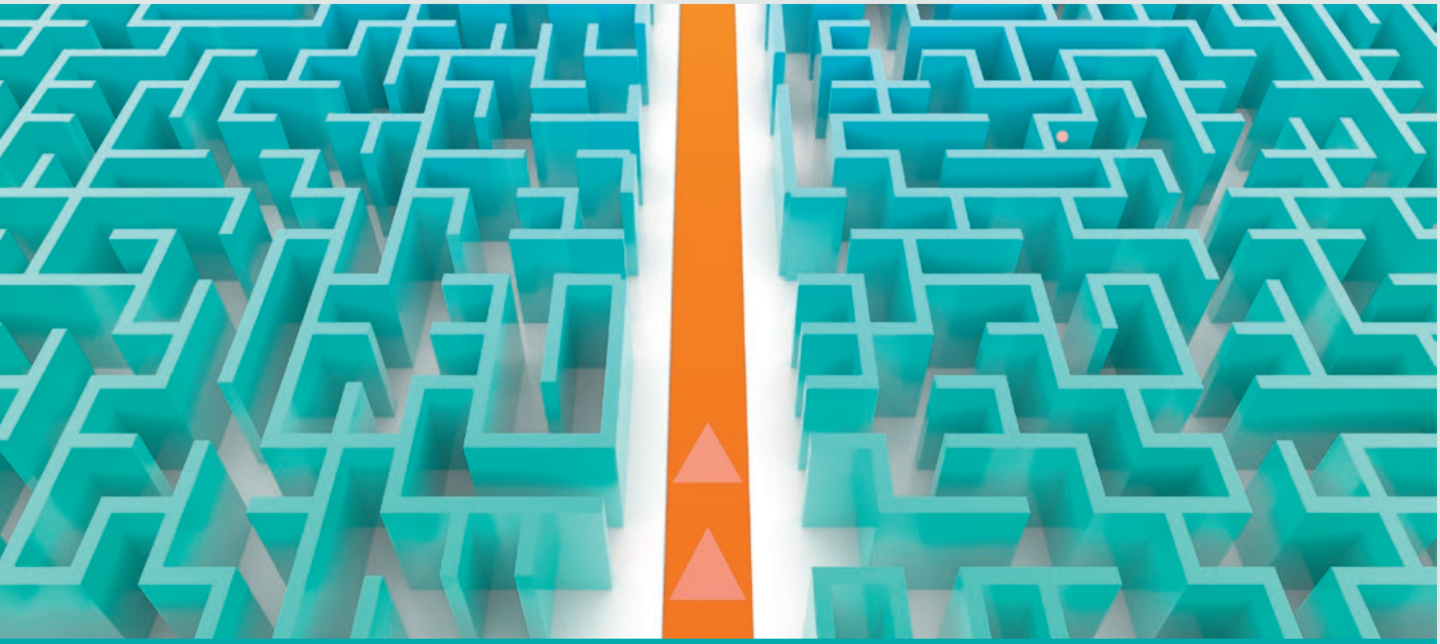
With factories spreading around the globe, licenses should be available 24/7. There are several ways of doing so: One strategy would be to distribute the licenses across **local license servers**, which keep the licenses directly available at each site. With CodeMeter License Central, you can allow the user to move licenses dynamically from one server to the next. Any licenses that are not currently needed can be shifted back into the cloud and activated at some other factory that needs them – and all of this without any manual support efforts.

An alternative strategy would be to install a centralized license server, which can be coupled with local caching and a hot-standby solution. A third option would use three license servers and a manual mechanism in the software that only starts up if two of the three servers are available and the required licenses are not used elsewhere. This **Triple Mode Redundancy (TMR)** solution lets you choose which rules you want to enforce. As a minimum, two servers have to be available and the active licenses have to be consistent. As a solution, it is ideally suited to permanent licenses.



Software about to retire

All software has its unique lifecycle, and every software will get to a point after which you would not sell or support it anymore. However, legal requirements might force you to provide your clients with licenses even after that point. This will not only mean the added effort of a highly manual process. Keeping an outdated licensing system running might also incur extra maintenance and licensing fees. Faced with these costs, many companies prefer to switch their older software to an unprotected version. But even this can mean high costs for implementation and testing. Not so with CodeMeter: A Protection Only License can be created at any point with an unbound general license. This creates a freely installable version of the software without any additional work. And even better: You get to keep your protections against reverse engineering.



Software Protection – Safe and Simple

Protecting software should be safe and simple – but isn't that a contradiction in terms? Wibu-Systems shows that it does not have to be with CodeMeter Protection Suite. Its tools protect against fraud, are easy to build into software applications, and make software protection work seamlessly with existing processes.

CodeMeter Protection Suite

Protecting intellectual property and making sure that only licensed software can be used is just one of the many challenges that software developers have to contend with. Software can be delivered in different forms: as executable applications or as libraries. Whether you are making software for Windows, macOS, or Linux – the solution for this challenge can be found in the sophisticated tools included in CodeMeter Protection Suite.

AxProtector

AxProtector (Automatic Executable Protection) gives you a perfect tool for the automatic protection of compiled software. The software can come in many shapes and sizes: from "regular" binaries, written in C/C++ or Delphi, to precompiled code produced in .NET for Windows or cross-platform Java. All of these types can be protected with AxProtector, AxProtector .NET, or AxProtector Java, with each tool using a unique technique to protect your work.

Uniform interface

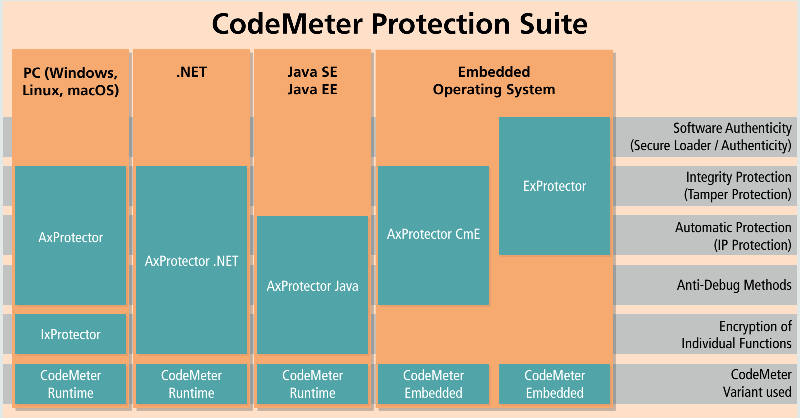
Upon launching AxProtector, you first need to select the application type. The assistant then opens and helps you protect your unprotected application in a few simple steps. The intuitive process needs no manual or special instructions. AxProtector supports several licensing systems, so that you could encrypt one and the same software with different licenses. When using a Universal Firm Code, you can also simply encrypt your file and decide later whether you want to use a device-bound license file (CmActLicense), secure hardware (CmDongle), or a user-specific license from the cloud. If you have a Firm Code for a CmDongle, CmActLicense, or WibuKey, you have the option of encrypting the application with it. Wibu-Systems is committed to full backward compatibility: The current protection mechanisms will also be available for older licensing systems.

When a protected application is launched, it will look for the right license in one of the allowed licensing systems.

It is easy to determine how the license for the protected software is counted, e.g. once per launch or only once per computer. Whether

AxProtector protects the following file types:

- Windows applications (32-bit, 64-bit)
- Windows libraries (32-bit, 64-bit)
- macOS applications (32-bit, 64-bit)
- macOS libraries (32-bit, 64-bit)
- Linux applications (32-bit, 64-bit)
- Linux libraries (32-bit, 64-bit)
- .NET Assembly
- Java applications
- Java web applications


CodeMeter Protection Suite
PC (Windows, Linux, macOS)
.NET
Java SE Java EE
Embedded Operating System
Software Authenticity (Secure Loader / Authenticity)
Integrity Protection (Tamper Protection)
Automatic Protection (IP Protection)
Anti-Debug Methods
Encryption of Individual Functions
CodeMeter Variant used
AxProtector
AxProtector .NET
AxProtector Java
AxProtector CmE
ExProtector
IxProtector
CodeMeter Runtime
CodeMeter Runtime
CodeMeter Runtime
CodeMeter Embedded
CodeMeter Embedded

and how frequently the license should be checked is just one of the many settings at your disposal, pre-set to the most meaningful option.

Beating attackers

The protected application will notice when hackers tamper with it or attack it otherwise and automatically lock the license in such incidents. This keeps your know-how protected and prevents any additional attack. AxProtector uses the full power of CodeMeter in the encryption: On top of the keys stored in the license, there is a variable key to make the encryption unpredictable. AxProtector also checks whether the protected software has been tampered with since its original encryption and prevents manipulated applications from running.

More security – IxProtector

The strong protection provided by the automatic encryption can be made even tougher by using function-level encryption. A selection of functions is encrypted additionally and only decrypted into working code when the functions are specifically required. This individual form of protection is called IxProtector and is easily integrated in software. Just mark the target functions, including an API call for decrypting them as needed, and include the functions in the settings – it is as simple as that.

In the case of .NET and Java applications, the different format means that the encryption is automatically applied on the level of individual methods. AxProtector .NET and AxProtector Java come with IxProtector integrated without requiring any special configuration. The methods are automatically decrypted during execution.

It is just as easy to include modular protection and the checking of special license details. The user interface lets you define additional licenses, e.g. for modules licensed separately. These additional licenses can be checked with the Wibu Universal Protection Interface (WUPI). Combined with function-level encryption, this creates a strong shield for these additional modules.

User-friendly notifications

When no licenses are available – be it the basic license or additional licenses – a flexible error management process springs into action: Its response to an identified incident and the notifications given to your users can be adjusted with the settings of AxProtector and the so-called UserMessage library. An application could return a customized error message, or the incident could be recorded in a special log file in the case of a protected function.

Simple process integration

The protection process should be fully integrated into your standard workflows, so that your software is already protected during its initial testing. You can integrate the encryption of applications and libraries already in the build process. The settings defined with the AxProtector UI can be exported into a settings file at the push of a button, and the encryption process can be executed automatically with a simple command line call.

Safe investments

Wibu-Systems regularly publishes new versions of CodeMeter Protection Suite with new and improved security capabilities on board. The free updates strengthen the protection of your applications without any effort on your part and keep your work safe from attackers. Protecting software with the tools in CodeMeter Protection Suite is not just simple – it also gets better over time. The evolution of new technologies will easily integrate into your software without any complexities.

Safe and simple!

CodeMeter Protection Suite gives your application or library a double layer of protection in a few simple steps: It stops would-be attackers from copying your software or analyzing its code and safeguards your revenue streams while shielding the invaluable know-how you have developed!

On embedded systems, AxProtectorCmE can protect applications running on:

- Linux ARM (32-bit, 64-bit)
- Windows Embedded
- Android

ExProtector – a version of AxProtector made with the special needs of embedded systems in mind – can protect know-how and prevent manipulation on the following platforms:

- Linux
- VxWorks
- Other OS on request

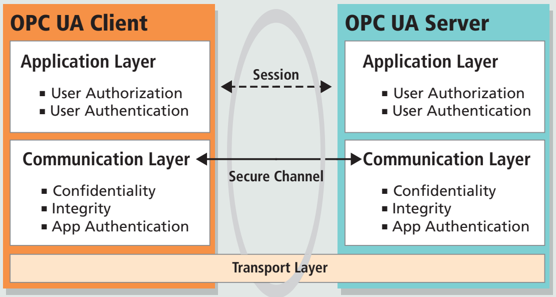
OPC UA and CodeMeter

OPC Unified Architecture (UA) is increasingly establishing itself as the accepted standard in the automation industry. The open IEC 62541 standard guarantees platform independence, object orientation, and type safety, and now adds IT security as another technological cornerstone. It is completely interoperable from the smallest device to enterprise-level IT, and even cloud solutions. As a world-leading protection and licensing technology, CodeMeter is an ideal partner for OPC UA, storing keys and certificates in secure hardware and adding not just greater security, but also new business opportunities with licensing for OPC UA devices.

OPC UA offers exceptional security on the protocol level

OPC UA is more than a communication protocol. The open standard covers:

- Confidentiality: Encrypting data
- Integrity: Signing data
- Application authentication
- User authentication
- User authorization
- Auditing
- Availability



Source: OPC Foundation

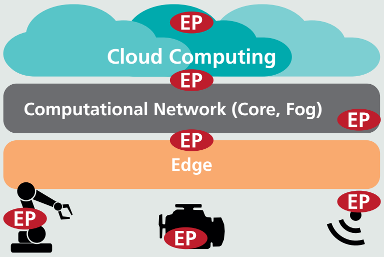
It offers authentication on the transport layer, with X.509 certificates and trust managed with a public key infrastructure. OPC UA also guarantees top security during data transmission.

Broad support

OPC UA has won extensive support e.g. from the Industrial Internet Consortium (IIC) the Chinese Alliance Industrial Internet (AII), and Plattform Industrie 4.0. Germany's Federal Office of Information Security has evaluated its security. It will not be the only standard accepted around the world, as e.g. DDS by Object Management Group (OMG) is also available and as its use depends on the specific application.

Endpoint security

In a connected world, all endpoints need to be secure, whether they are sensors or actuators, controllers, or historians in the cloud.

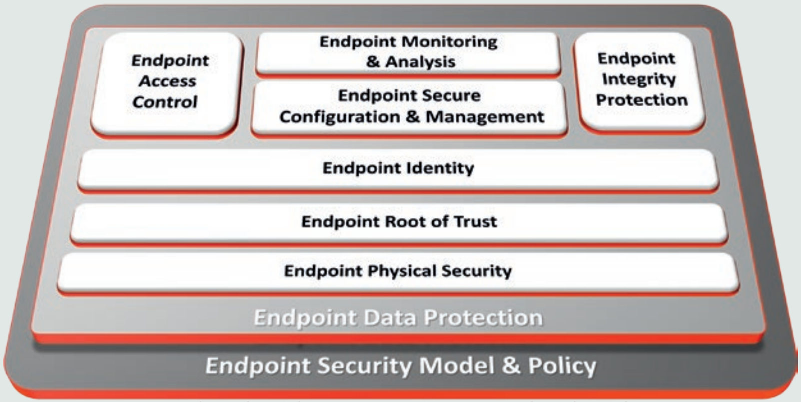


The Industrial Internet Security Framework (IISF) published in September 2016 describes the many elements of endpoint protection.

Holistic security does not stop at the protocol layer

In addition to communication, the security of endpoints is just as important.

Endpoints are where operating systems, libraries, drivers, and applications are exposed


Endpoint Access Control
Endpoint Monitoring & Analysis
Endpoint Secure Configuration & Management
Endpoint Integrity Protection
Endpoint Identity
Endpoint Root of Trust
Endpoint Physical Security
Endpoint Data Protection
Endpoint Security Model & Policy

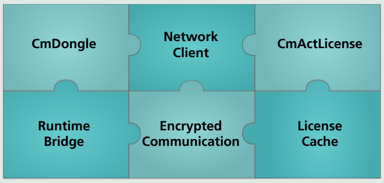
Source: The Industrial Internet Securitv Framework- Industrial Internet Consortium

to attacks. The consequences of compromised endpoints can be disastrous: Cryptographic keys can be stolen, the identity of the device affected, settings data like trust lists and certificates tampered with, applications manipulated, and invaluable know-how lost.

This calls for extensive protections. Many devices using OPC UA are still not protected enough, with private keys and trust lists stored in the regular file system and applications left unguarded against tampering. Attacks against endpoints might succeed and compromise entire infrastructures. Functionality, reliability, and know-how are all at risk.

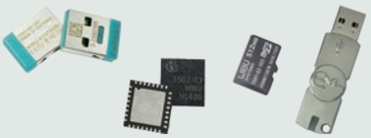
OPC UA SDK, CmEmbedded, and CmDongles - A match made in heaven

CmEmbedded is a small-footprint modular runtime used to access the CodeMeter license container and the secure CmDongles. It supports many common operating systems out-of-the-box and can be extensively customized, as it is delivered as ANSI C source code.



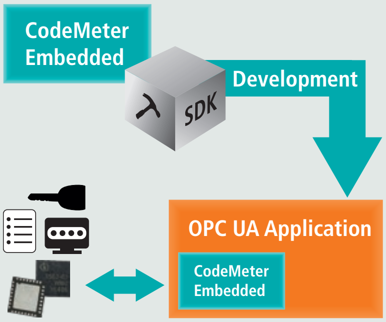
CmDongle	Network Client	CmActLicense
Runtime Bridge	Encrypted Communication	License Cache

The CmDongle hardware uses smart card chips made by Infineon that are Common Criteria (CC) EAL5+ certified, including the cryptographic libraries. All keys are securely stored and all cryptographic operations happen on this hardware.



The integration of CmEmbedded into the OPC UA SDKs offers additional security without additional effort and adds new licensing capabilities on top.

Making OPC UA more secure in the field



The private keys are stored securely in the CmDongle hardware, using RSA keys with up to 2048-bit and ECC with 224-bit. The encryption of the OPC UA software on the device prevents tampering and reverse engineering and makes sure that critical processes occur only on fully protected hardware.

Advantages of license management with OPC UA

More and more devices with OPC UA depend on software to realize their capabilities, be it PLCs, intelligent sensors, RFID readers, or engines and actuators. With CodeMeter, individual functions can be licensed and novel pay-per-use or subscription business models be introduced to develop new after-sales business. No physical changes are needed to set up the licenses in the devices, which is done simply via the OPC UA protocol.

Available today

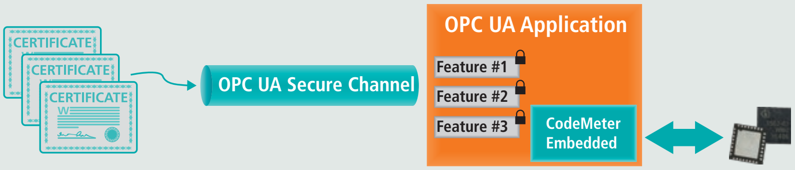
CodeMeter's solutions, with CmEmbedded and CmASICs with USB/SPI communication, CmSticks for USB, or CmCards, are available as a module for the Unified Automation ANSI C OPC UA SDK and for the High Performance OPC UA SDK.

They have been tested and proven their worth in many projects, such as *SmartFactory*KL, secure plug&work with the Fraunhofer Institute IOSB, OpSIT in the healthcare sector, and IUNO, the national reference project for IT security in Industrie 4.0 introduced by the German Ministry for Education and Research.

Summary

The IoT, IIoT, and Industrie 4.0 depend on fully interoperable and secure endpoint communication and semantics. OPC UA is supported by many organizations and players in the industry and can deliver what is required.

With its security and licensing capabilities, CodeMeter is a powerful enabler for new projects. Invaluable know-how is invested into flexible production processes, software, or technical and production data. Protecting these assets against theft and manipulation and seizing the opportunities of the digital age in new business models is CodeMeter's mission.



Short News

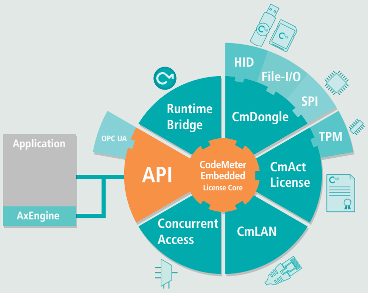
CmEmbedded 2.0

CmEmbedded is the modular CodeMeter Runtime for all types of embedded system platforms. The modular design allows the perfect integration of the features required for the chosen application. Modules include CmDongle communication with USB HID, File-I/O, or SPI, CmActLicenses, software-based activation, CmLAN, network access to licenses, and a runtime bridge for use on systems with standard runtimes. New features include:

License Core: Consolidating and caching license details for all CmContainers increase performance and enable simultaneous and concurrent access by different applications.

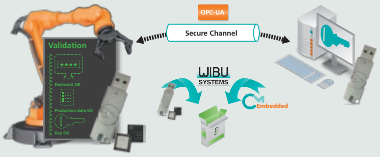
Universal Firm Code support for CmDongles

The TPM module allows highly secure binding of software CmActLicenses with TPM modules (1.2 or 2.0) on the target system.



OPC UA SDK support

CmEmbedded 2.0 supports the Unified Automation OPC UA SDK perfectly with the secure storage of private keys on CmDongles and full CodeMeter licensing functionality for OPC-UA-enabled devices.



CmStick/CM 8GB

The world's smallest CodeMeter stick with high-speed 8GB flash storage, USB 3.1 interface, and a sleek, chic, and robust ultracompact, full-metal USB body. Equipped with an Infineon SLM97 smart card chip with full CodeMeter functionality, it supports the new Universal Firm Codes and includes an optional encrypted CmSecureDisk flash storage partition. The Hyperstone U9 flash controller and its patented hyMap® firmware meets the toughest industrial requirements in terms of life expectancy, reliability, and the prevention of data loss caused by power outages during writing. The high-tech construction as SIP (System in Package) module in the connector body was designed with extreme environmental conditions, including vibration, humidity, and temperature fluctuations in mind.

Universal Firm Code on all CmDongles

All CmDongles, CmCards, CmSticks flash memory, regular CmSticks, or the CmASIC: all 10xx-03-xxx devices now support the new Universal Firm Code for standard use with CmDongles and CmActLicenses.

CodeMeter Runtime Extension

The extension of the CodeMeter standard runtime enables OEMs to bind CmActLicenses to their own hardware device instead of a PC and to store the license securely on it. The license is then mobile and the software only runs when this device with the associated and valid license is connected to the computer.

CodeMeter License Central

CodeMeter License Central 3.10 now supports Module Items, can configure the behavior when borrowed licenses are returned, supports license pushing with a calculated "modified context" and the revoking of licenses. Our data center offers high-availability hosting, with load balancing and redundant License Centrals. A module for out-of-the-box SAP integration is available through our cooperation with our SAP partner Informatics.

IIC Journal of Innovation

The third issue of the Journal of Innovation published by the Industrial Internet Consortium (IIC) is dedicated to the rise of smart factories. One article explores the Blurry Box® technology's use of Kerckhoffs' Principle for software protection. A great read! Available for download: http://www.iiconsortium.org/journal-of-innovation.htm.

Chinese Alliance Industrial Internet (AII)

工业互联网产业联盟
Alliance of Industrial Internet

In late November 2016, Wibu-Systems sealed its new membership in the alliance with Dr. Xiaohui Xu, CTO of CAICT, in Berlin.

Hannover Messe 2017

Do not miss our live Industrie 4.0 demonstration of the *SmartFactory*^{KL} with B&R and SAP and at the IIC/Plattform Industrie 4.0, using data from the ZSK embroidery machine at our booth in Hall 8, D05.

Success Story Fritz Stephan

The Challenge

Fritz Stephan was looking for a way to offer a cost-effective respiratory device that could be used both in emergency response situations and intensive care units, whose functionalities could be enabled on demand via a secure, internet-connected software licensing system. As an innovative world leader of ventilation solutions, Fritz Stephan also wanted to preserve the integrity of its technology.

The solution

CodeMeter proves to be the perfect match for EVE, Fritz Stephan's emergency ventilator unit. With CodeMeter, the company protects its own Intellectual Property against counterfeiting and reverse engineering; with a CmCard integrated directly in the unit, they protect their secrets from tampering; with CodeMeter License Central, they process license-based customer orders; and with WebDepot, they can upgrade units in the field.

The result

By implementing cutting-edge security and licensing systems, Fritz Stephan is safeguarding its many years of investments into its technology, is able to easily upsell new licenses over the Internet to its global customer base, and can conveniently modify the set of features of its devices.

The Customer

Fritz Stephan GmbH is regarded as one of the world leaders in the development of specialized technical solutions in ventilation, anesthesiology and oxygen supply, with a special focus on neonatology and pediatrics. Clinical experience coupled with a high level of technical competence is achieved by close cooperation and an active dialogue with customers on a global scale. The development and supply of cutting-edge technology solutions for the benefit of the patient is the ultimate goal and vision of both the Fritz Stephan GmbH and its second generation majority owner Ms. Tanja Stephan.

Bernd Hoehne
Marketing Manager, Fritz Stephan

We are excited about the success that our EVE family product is experiencing. The software and hardware-based integration of CodeMeter with EVE has allowed our business expansion to reach new global markets. Our customers appreciate the modular pricing structure we have created, the regular updates of our device software they receive online, and the possibility to upgrade anytime to new functionality.

Wibu-Systems Workshops

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

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

Access the latest training schedule by scanning the QR Code or visit:
www.wibu.com/tr

Training location	Date	Time
Swindon (UK)	29 March	10.00 - 15.00
Paris (FR)	4 April	10.00 - 15.00
Porto (PT)	28 April	10.00 - 15.00
Brussels (BE)	23 May	10.00 - 15.00
Amersfoort (NL)	30 May	10.00 - 15.00

Contact your local sales representative for details about the workshops and/or upgrading your test kit or current solution to Universal Firm Code with secure offline license transfer and borrowing.

United Kingdom / Ireland	+44 (0)2031474727	sales@wibu.co.uk
Netherlands	+31 (0)747501495	sales@wibu-systems.nl
Spain / Portugal	+34 (0)911230762	sales@wibu.es
Belgium / Luxembourg	+32 (0)38080381	sales@wibu.be
France	+33 (0)186266129	sales@wibu.fr

Visit us:

embeddedworld2017
Exhibition&Conference
... it's a smarter world

Embedded World
H4 - 540
14.03 – 16.03.2017

EUROPEAN SOFTWARE & SOLUTIONS SUMMIT

European Software & Solutions Summit
30.03.2017

enova STRASBOURG

enova
15.03 – 16.03.2017

HANNOVER MESSE

Hannover Messe
H5 - D05
24.04 – 28.04.2017

Industrial Ethernet

Industrial Ethernet
16.03.2017

ITEC
16-18 May 2017
Ahoy, Rotterdam

ITEC
16.05 – 18.05.2017

Imprint
KEYnote 33
Edition, Spring 2017

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
Wolfgang Voelker
Oliver Winzenried

Design
Markus Quintus

Print
Kraft Premium GmbH, Ettlingen, Germany, ISO 14001 certified

Letters are always welcome. We will protect the confidentiality of sources. Third party articles do not necessarily reflect the opinion of the editorial office. Write us at team@wibu.com. Wibu-Systems expressly reserves the right to change its programs or this documentation without prior notice. Wibu-Systems®, CodeMeter®, SmartShelter®, SmartBind®, and Blurry Box® are registered trademarks of WIBU-SYSTEMS AG. All other brand names and product names used in this documentation are trade names, service marks, trademarks, or registered trademarks of their respective owners.

Picture credits:
Cover:
©iStockphoto.com/ Greyfebruary
Title page 3:
©iStockphoto.com/milanvirijevic
Title page 4:
©iStockphoto.com/olm26250
Title page 6:
©iStockphoto.com/Gajus
Title page 8:
©iStockphoto.com/Maxiphoto
Title page 10:
©iStockphoto.com/3dts
Title page 12:
©iStockphoto.com/baranozdemir
Page 15:
©Fritz Stephan
All remaining images are copyrighted by their owner.

SECURITY
LICENSING
PERFECTION IN PROTECTION

WIBU SYSTEMS