



KEYnote 46

THE WIBU - MAGAZINE

Licensing in the Cloud

Highlights

- Developing Secure Software
- CodeMeter Licensing in Kubernetes
- Creating Licenses in CodeMeter License Portal



Content

CORPORATE	
Wibu-Systems International Partner Summit 2023	3
LICENSING	
CodeMeter Cloud Lite Usage Reporting	4
PROTECTION	
CmReady – Three Cheers for Diversity!	6
CORPORATE	
Developing Secure Software	8
SECURITY	
Licensing and Protecting Industrial Edge Devices	10
LICENSING	
TMR: The Solution for Fail-Proof Licensing Setups	12
LICENSING	
Creating Licenses in CodeMeter License Portal	14
LICENSING	
How our clients get their ROI with CodeMeter	16
LICENSING	
Licensing in the Cloud	20
LICENSING	
CodeMeter Licensing in Kubernetes	24
PROTECTION	
Reliable Licensing in a Changing World: CodeMeter and SmartBind	27
HIGHLIGHTS	
News in Brief	28
CASE STUDY	
ETM professional control	29
INFORMATION	
Wibu-Systems Training	30

Dear Clients and Partners!



IT security is an executive issue. We are living through a period of global tension. The threats are getting more severe every day, and the question is not whether a company will be affected by a cyberattack, but when and how severe that attack will be.

With our responsibility for our businesses comes a duty to care, to act, to equip our people with the means they need to enforce compliance with standards like NIS2, ISO 27001 and different EU acts (cyberresilience, cybersecurity, AI, data, ...), and to take the right steps to mitigate the remaining risks. In essence, we must make a make-or-buy decision: Should we buy the expertise we need for all of this, or should we make it by teaming up with external specialists to support, advise, and test us with penetration tests, ISO 27001, external IT security officers and the like?

Our products must be secure. Our users, and we ourselves, must be able to configure and run the products securely, keep everything up to date, and ensure fundamental IT security.

As manufacturers, it is our duty to produce secure products: "Security by default" means that our products can only be used in a secure configuration. We pay attention to and comply

with many standards: there are the Security Assurance Levels in IEC62443, the Common Criteria and Cybersecurity Assurance Levels (CAL), not unlike the ASIL of ISO 26262, and the MDR and IEC13485 in the medical sphere. With the CodeMeter cryptographic tools at your disposal, we are helping you integrate the necessary security precautions into your own products.

In addition to our security focus, we gladly share with you the latest technologies and tricks of the trade for you to reap the most benefits from our licensing and protection solutions. Read this issue of our KEYnote magazine to learn more about how to calculate the ROI of CodeMeter for different types of users and clients, our fail-proof TMR license server, Kubernetes, industrial edge devices, license binding to i.MX boards with SmartBind, and CmReady, our latest innovation for binding licenses to mass storage media instead of end user devices. Included as well are two special reports: A look at the development processes that need to be in place for truly secure software and a tour of the success story of SIMATIC's WinCC open architecture.

I wish all of you a successful end to the year and am looking forward to seeing you in person at one of the upcoming fairs and expos!

Yours,

Oliver Winzenried

CEO



Wibu-Systems International Partner Summit 2023

For most, summer means travelling, discovering new places, meeting new people, and in some cases, simply enjoying life. That is also true for Wibu-Systems: We took the opportunity of the quieter summer days to gather our team in Germany and our colleagues from our subsidiaries worldwide to our new campus in Karlsruhe. For many of our colleagues, this was the first chance to meet up again in person after four years, and they came from the US, Japan, China, South Africa, the Benelux states, France, Italy, Spain, Sweden, and the UK for our meet-up, training, and team building event: WIPS, the Wibu-Systems International Partner Summit.

The success of WIPS came from its full and engaging agenda, including workshops with regional use cases as well as technical training classes about our product innovations. Joining up with colleagues and friends from the entire Wibu community let the participants discover more about our strategy and



vision, learn about the specific situations in their respective countries and markets, and feed their new insights and product ideas into our roadmap for even better solutions for our clients. But WIPS was not just about working hard together: the participants enjoyed the sunset views from rooftop of our head office, fine dining, and a trip to the historic spa town of Baden-Baden.

In sum, the WIPS gathering was more than a series of meetings; it was a fusion of minds aimed at enhancing our collaborative efforts and solutions for clients globally. This confluence of talents, hailing from different parts of the world, resulted in a synergy that promises to elevate not just our individual performances, but also the efficiency and effectiveness of the entire Wibu-Systems ecosystem. By sharing best practices, uncovering new opportunities, and investing in continuous education, we've laid a strong foundation for innovation and excellence that benefits all stakeholders. The Wibu-Systems International Partner Summit was not just a memorable

event; it was a step forward in achieving unparalleled performance in the industry. 





CodeMeter Cloud Lite Usage Reporting

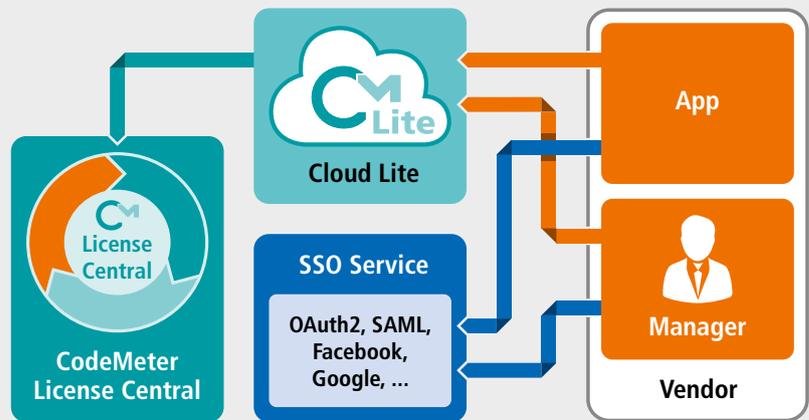
Introduction

Many software vendors have already discovered Wibu-Systems' suite of software products that can help protect intellectual property and control and manage software entitlements. Licenses and other sensitive information can be securely stored on highly sophisticated hardware, specially encrypted files, or remotely in a managed cloud environment.

Key to all these features is CodeMeter, which acts as the interface between the software to be protected and the information entitlement that is crucial to the software vendor business, securely held in CmContainers.

But there are instances where it is not possible or desirable to use CodeMeter. Some externally managed platforms (SaaS, mobile) might restrict the installation of sophisticated security software: after all, CodeMeter itself is an incredibly complex security solution that uses state of the art encryption and security features. There are also occasions where asset protection, a cornerstone of the CodeMeter skillset, is simply not required. CodeMeter Cloud Lite was written with these uses in mind.

CodeMeter Cloud Lite offers user-based licensing in the cloud. Licenses are created and delivered through CodeMeter License Central, but instead of activating or transferring the license in a CmContainer, it is allocated to a user in CodeMeter Cloud Lite.



CodeMeter Cloud Lite allows multiple heterogeneous devices to be used (for example, you could access your license on your computer in the morning and then on your mobile device in the afternoon) and offers a simple route to license management through the provision of a number of easy-to-use REST APIs.

REST Reporting API

Version 3.10 of CodeMeter Cloud Lite introduces a new suite of APIs to supply information on license usage reporting. It provides an interface through which information about the use of licenses can be queried. In addition to the purely technical view, it is also possible to enrich the data with product and license information from CodeMeter License Central. It utilizes a powerful filter mechanism to pro-

vide the key information to be queried and can provide two reporting views. Information flows are via JSON.

Reporting Query Filter

The query filter structure contains all the information about the report to be created. For example, to retrieve all entries within a specific time range, the following filter can be used:

```

    „filter“: {
      „from“: „2023-08-01T00:00:00“,
      „to“: „2023-08-31T23:59:59“
    }
  
```

There is a lot of flexibility contained in the filter. It is possible to also specify various license attributes such as firm code, product code, or

feature code, or CodeMeter License Central attributes such as customer number, ticket id, and item id. When called, the reporting services will identify the specifically required information and return just this to the caller.

Reporting: License Based View

The LicenseUsage structure contains all information about the usage of a license, with the specific data focused through the query filter. As an example, if we consider the following request:

```
{
  „session“: {...},
  „filter“: {
    „from“: „2023-08-01T00:00:00“,
    „to“: „2023-08-31T23:59:59“
  }
}
```

Then the following data might be returned after the call:

```
{
  „errorCode“: 0,
  „licenseUsageList“: [
    {
      „accessTime“: „2023-08-08T09:18:28“,
      „fail“: 0,
      „featureCode“: 0,
      „featureMap“: 0,
      „firmCode“: 6000145,
      „invalid“: 0,
      „productCode“: 201001,
      „releaseTime“: „2023-03-08T09:24:27“,
      „seconds“: 359,
      „success“: 1,
      „ticketLicenseId“: 40,
      „userIdentification“: „474ce7a1-903f421d“
    },
    {
      „accessTime“: „2023-08-14T16:46:14“,
      „fail“: 1,
      „featureCode“: 1,
      „featureMap“: 0,
      „firmCode“: 6000145,
      „invalid“: 0,
      „productCode“: 10000,
      „seconds“: 0,
      „success“: 0,
      „ticketLicenseId“: 0,
      „userIdentification“: „7ae99d49-4a41-4934“
    }
  ]
}
```

Reporting: Product Based View

The ProductUsage structure contains all information about the usage of a product from CodeMeter License Central. The return is essentially a list with a summary of all product-level license accesses for the specified filter options.

For example, the following options show all product uses of a customer:

```
{
  „session“: {...},
  „filter“: {
    „customerIdentification“: „20230306“,
    „from“: „2023-08-01T00:00:00“,
    „to“: „2023-08-31T23:59:59“
  }
}
```

The answer looks as follows:

```
{
  „errorCode“: 0,
  „productUsageList“: [
    {
      „customer“: „20230306“,
      „item“: „F-00002-145“,
      „name“: „Feature #2“,
      „seconds“: 24377,
      „success“: 1,
      „user“: „xyzKLF4711eDxSdfs6y“
    },
    {
      „customer“: „20230306“,
      „item“: „F-00003-145“,
      „name“: „Feature #3“,
      „seconds“: 9939,
      „success“: 1,
      „user“: „xyzKLF4711eDxSdfs6y“
    }
  ]
}
```

To query the usage of a product of all customers the following options can be used:

```
{
  „session“: {...},
  „filter“: {
    „itemIdentification“: „B-00001-145“,
    „from“: „2023-08-01T00:00:00“,
    „to“: „2023-08-31T23:59:59“
  }
}
```

For example, the result looks like this:

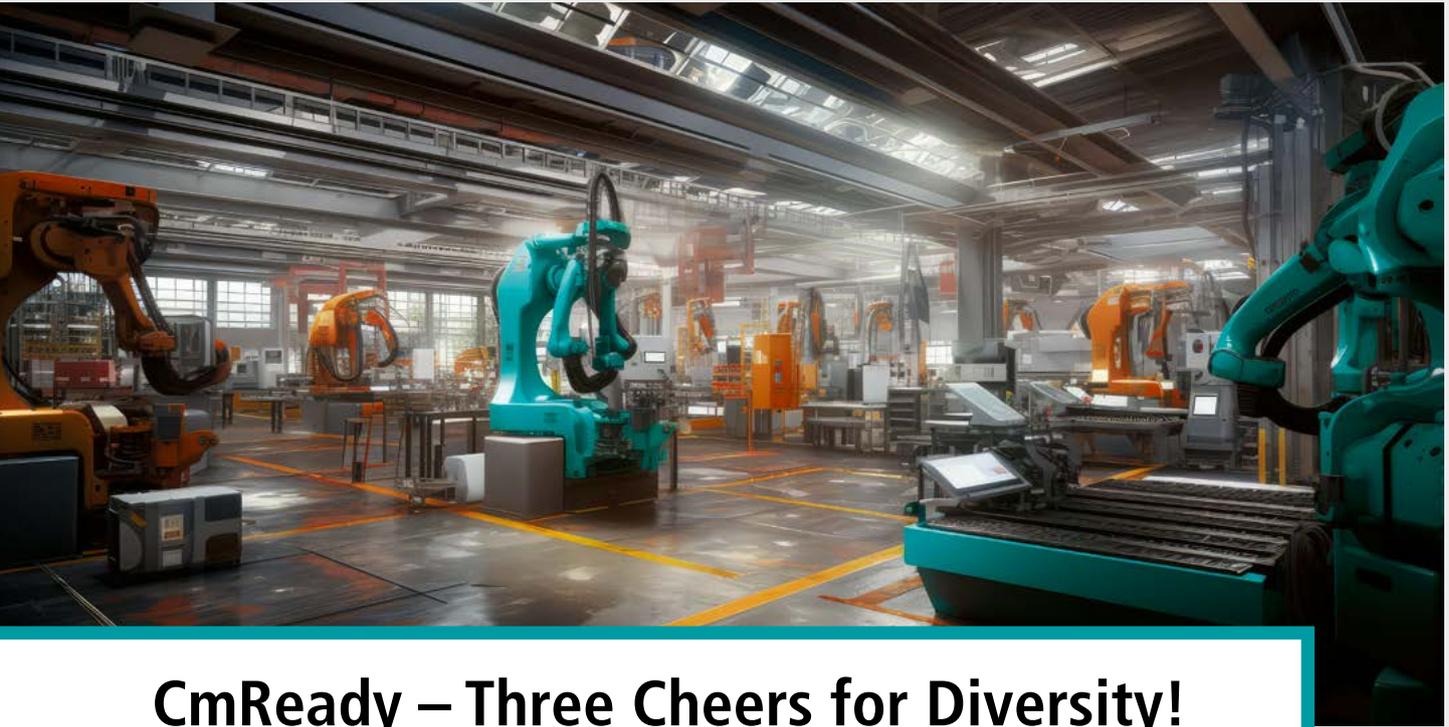
```
{
  „errorCode“: 0,
  „productUsageList“: [
    {
      „customer“: „20230315“,
      „item“: „B-00001-145“,
      „name“: „Bundle #1“,
      „seconds“: 3237,
      „success“: 1,
      „user“: „217521f2-385f-4c52“
    },
    {
      „customer“: „20230315“,
      „item“: „B-00001-145“,
      „name“: „Bundle #1“,
      „seconds“: 1324,
      „success“: 1,
      „user“: „217521f2-385f-4c52“
    }
  ]
}
```

Easy Start

In modern environments, the idea of one size fits all is simply not appropriate. Software and hardware vendors must operate in increasingly complex environments, adhering to increasingly complex rules, and of course they themselves have wildly disparate requirements that need to be met. Where cutting edge asset protection is required, ensuring that key intellectual property is fully safeguarded when it leaves the direct control of the vendor, CodeMeter has for many years been the go-to mechanism for providing this: it has saved numerous companies huge amounts of money in preventing loss of revenue through piracy or reverse engineering. When this is not a requirement, either because IP protection is simply not needed or because specific environments do not allow such solutions, CodeMeter Cloud Lite has you covered.

The license-based view combined with the product based view of the new reporting API gives a compelling addition to the ever growing suite of REST APIs, flexible enough to allow the vendor to gather precisely the data they need.

To make this feature set as easy as possible to use, some sample applications are available in Java, C++, and C# to help you get up and running as quickly and painlessly as possible. Of course, Wibu-Systems' Professional Services are always at hand to provide advice, implementation tips and tricks, and anything else the vendor needs to do what they do best. 



CmReady – Three Cheers for Diversity!

A favorite of developers with decades of success in the software industry has truly arrived in the hardware world of modern industry: CodeMeter for software protection and license management. A new partnership with Swissbit and the CmReady label by Wibu-Systems is creating a world of opportunities for engineers in the field.

In Focus: Product security and monetization

Wibu-Systems has been innovating the software and know-how protection landscape and offering flexible monetization solutions for a range of target platforms since the company was founded more than 30 years ago, and it has never ceased to follow its pursuit. What started for software makers only has now become a popular choice for industrial enterprises around the world. Industrial devices like Programmable Logic Controllers (PLCs) are run by the software and firmware on board, and the makers of CodeMeter soon realized that they could transport their protection and licensing know-how to a whole new market by tweaking it for the needs of industrial automation and engineering clients.

On top of pure product security considerations, driven not least by legal requirements (e.g. IEC 62443, Cyber Resilience Act) or the wish to protect one's know-how in the form of software or data, more and more businesses are interested in how they can monetize product features and create new business models through licenses. Most hardware devices are,

in essence, built with the entire feature set on board, but it is left to the end users to decide which of these features is worth paying for and should be activated. They can buy the licenses for individual features when they need them for a specific purpose, creating an attractive aftermarket sales channel.

The advantages of CmDongles

Device makers have a choice of ways to get their licenses rolled out to their users, depending on the use case. Alongside pure software license containers (CmActLicense) that are bound to a specific hardware fingerprint of the target device, or cloud-based licenses (CmCloudLicense), fully hardware-based dongles (CmDongle) remain a popular evergreen choice for industrial device makers in particular. Their key unique selling point (USP), the ability to store cryptographic keys in a secure element physically built into the dongle, goes hand in hand with the great mobility afforded by the licenses, especially when devices need to be serviced. If needed, the device makers can even choose CmDongles with added flash storage for the hat trick: IP protection, monetization, and storage space, all on one medium.

All shapes and sizes

Wibu-Systems was quick to realize these requirements and has long offered a range of CmDongle formats and form factors. Many makers of embedded and IoT devices prefer run-of-the-mill mass storage media like SD or microSD cards, which avoid the need for adding a USB interface or integrating a CmASIC to add CodeMeter functionality right into their devices' inner workings. The CmCard line was made for them. Whatever the form factor, all options support the complete feature set and all flexible licensing models allowed by CodeMeter.

Bane or boon?

Every upside comes with a downside: Which type (SLC, pSLC, MLC) and which size of flash storage a device maker picks has a major impact on costs, translating directly to higher costs in the device maker's bill of materials. This can become a dealbreaker for low-end or discount devices in particular. At the same time, the vast range of memory types and sizes means that there is a CmDongle for virtually any requirements in the field, even if this means higher costs for development and qualification. Would it not be better to have a new

	CmActLicense	CmReady card	CmDongle
Time / Feature / Usage-based Licensing	✓/✓/✓	✓/✓/✓	✓/✓/✓
IP Protection	✓	✓	✓
Virtual Clock	✓	✓	✓
Mass Storage		✓	✓
Mobile Usage		✓	✓
Easy Offline Replacement of a broken Device/Computer		✓	✓
Hardware Clock			✓
Strong Authentication			✓
Key and Counter Storage in the Smart Card Chip			✓
Form Factors		Memory card	USB stick, memory card or ASIC

concept that combines the many advantages of CodeMeter with standard storage cards? It would, and that is why CmReady was born.

The solution: CmReady

The technological wizardry that makes all of this possible is not as complex as one might think: Wibu-Systems' purely software-based container type, a CmActLicense, is normally bound to a fingerprint of the target device's hardware properties. Instead, it is now bound to a CmReady-compatible card and stored directly on it. This makes the licenses much more portable, while keeping them as easy to use as ever, since they can be managed with the popular and familiar CodeMeter license management system – no additional implementation required to bind the licenses. Technically, the binding is done by a combination of the hardware's Unique ID (UID) with a specially protected incremental counter that prevents replay attacks against the license container. This keeps the binding secure and the licenses mobile, a great advantage when the system requires service. Even in a catastrophic scenario, the card could simply be taken out of the broken device and inserted in its replacement. There is no easier way to move licenses around. Cards that use the CmReady standard are supported by both CodeMeter Runtime and CodeMeter Embedded, making them perfect for any type of use case.

Swissbit supports CmReady

Swissbit, a long-standing partner of Wibu-Systems and specialist for industry-grade storage and security solutions based in Switzerland

with operating manufacturing facilities in Berlin, is the first maker using the CmReady standard for its Data Protection Edition (DP) cards. This makes the DP range of industry-grade microSD and SD cards equipped with CodeMeter technology ideal for know-how protection and monetization.

Which containers for which purposes?

The different properties and capabilities of each license container type are visualized in the table. All types support the tried-and-tested CodeMeter protection and licensing functions, which make it easy to introduce versatile licensing schemes like feature-on-demand, pay-per-use, or subscription licenses. The latter is protected against tampering by means of a virtual clock built into the container or, optionally, an actual battery-supported real-time clock fitted on the CmDongle.

For the perfect combination of product security, licensing, and flash storage, CmDongles and CmReady-compatible cards are the way to go. Both options offer great portability for the licenses, with an attractive choice of hardware variants in the case of CmReady cards in particular.

In addition to pure software protection, CodeMeter can be used for working with signatures, for encrypting files, or for authentication purposes. CodeMoving alone, the sophisticated ability to run protected code in the safe confines of the container, is exclusive to CmDongles and CmCloud containers.

Three cheers for diversity!

With CmReady, Wibu-Systems has created nothing short of a new global standard for the combination of storage media with software and IP protection as well as CodeMeter-enabled monetization. It allows device makers to pick the optimal storage options from a choice of CmReady-compatible options and lets them benefit from the great diversity of hardware choices and the versatility of CodeMeter's protection and licensing mechanisms. 





Developing Secure Software

No software is perfect. This is one of the hard truths of software development. But it does not mean that we cannot try to prevent mistakes, bugs, and flaws, mitigate their impact, and improve how we respond to such problems.

In this article, we take a look at the situation we are facing. It is impossible to say how many undiscovered flaws and vulnerabilities there may be, but we have estimates that offer us a good starting point. In the second half of this article, we look at some of the measures we are taking to prevent these problems and at our response for managing vulnerabilities.

The Situation

In order to understand how we can avoid and prevent bugs and flaws and how we should ideally respond to the remaining problems, we need to know which types of problems can occur, how often, and where.

For a general estimate about how many bugs and flaws there will be in thousand lines of code, people often go to Steve McConnell's book "Code Complete". Ignoring some exceptional cases, the statistics say that we should expect between 10 and 50 flaws in every thousand lines of code. Statistically speaking, there is an error in every twentieth or one-hundredth line of code that the compiler misses. This is surprisingly frequent. In truth, it should surprise us that our IT systems are working as well as they are.

But it is not a question of numbers. The type of flaw can be the critical factor. As we are concerned with the development of secure software, we need to consider two types: bugs and flaws. Bugs are run-of-the-mill programming errors. Flaws, on the other hand, are issues within the design itself. To find bugs, we can rely on a large toolkit that helps us scour the code for many types of possible errors, as we will explain below under "Prevention". Flaws, on the other hand, are harder to spot, since they often come from certain assumptions in the software's design or development that might be wrong or invalid and that can create vulnerabilities for hackers to exploit.

That is the key for prevention: We need to make sure that flaws will not become exploitable vulnerabilities. Not every error in the code can be exploited. If we understand the structures we can use to prevent attackers from exploiting bugs and flaws, we can make sure that potential mistakes in development do not turn into real vulnerabilities and we get a better sense for whether a bug or flaw we noticed can indeed be exploited. This means that we need a sense for the possible effects and repercussions of potential flaws when analyzing our work, and particularly when planning a new product.

Prevention Software Architecture

The base of every software is a comprehensive

requirement analysis. The results of our requirements analysis are used to design the software architecture in functional and technical terms. That design is the collaborative work of experienced software developers and architects certified by the International Software Architecture Qualification Board (ISAQB®), with input from a product-independent team of security experts that put the concept through its paces from its architecture to its use of the cryptographic basics.

Coding & Testing

When we produce the actual software to fit our designs, we use a range of technologies to catch and remedy any errors in the code at the earliest possible point. A proper versioning system should be standard for any software development (Wibu-Systems uses Git) that enforces a peer review principle. No single developer should be able to weave their code through to the final release without any checks and balances.

SonarLint is used for a static code analysis in the development environment; for the continual static analysis of the source code and for testing technical software quality, we employ the commercial versions of SonarQube on our build server. SonarQube includes more than 5000 static analysis processes (MISRA-C, CERT C/C++) and helps us produce genuinely clean code. We get compiler warnings and the results of the static analysis after every build.

Dynamic code analysis is used to check the application during runtime. Fuzzing can simulate a range of inputs and usually reveals many vulnerabilities. For this purpose, we use Radamsa, LibFuzzer, AFL, WinAFL sowie GCC, ASAN, UBSAN, and Valgrind.

For new implementations, we put unit tests in place to keep on top of regression. These unit tests and our automated integration tests are regularly tweaked in response to flaws. Configuration management and orchestration is entrusted to Ansible and Terraform. All in all, we have a large infrastructure in place for development and testing, which we treat like our code.

Our build and test processes are automated with Jenkins and GitLab Runner, because no developer could produce nightly builds for tests on all the operating systems we support and be ready for working with the results the next morning. Should the automated tests reveal any problems, they are prioritized and entered into the backlog, the causes explored, and the problems, ideally, remedied. Critical problems are flagged when they are discovered, irrespective of how they were noticed or who noticed them. This makes sure that tickets for such critical problems are always given our full attention.

Secure products can only be made by developers that know how to write secure code. Regular training on security aspects like the OWASP Top 10, best practices for specific languages, operating systems, or containers, fuzzing and much more are offered to teach developers how to avoid typical flaws in their code. With our mandatory training during onboarding of new staff, we make sure that IT security – and the right awareness of the issue – will never be forgotten. We use internal and external options for regular training on different security aspects, which should give our people a better sense for the various threats out there and the ways to mitigate the risks. In the long run, this will create an ingrained sense for security in all of our people.

Third Party Software

Any software developer knows that not all features are developed from scratch but brought in by libraries made by other developers. A poor choice of libraries can be a serious issue for software security, one that attackers can exploit to gain access to businesses or even their suppliers. Attacks like this, called supply chain attacks, are on the radar of Wibu-Systems, which has taken measures to reduce its dependencies and introduced a careful selection and close monitoring of the components it does

bring in from elsewhere. Wibu-Systems considers build processes particularly risky if they load the current code version on the fly from the supplier's repository. Although this should mean that all recent secure patches are in place, it also entails a risk of as yet unidentified harmful code slipping through the net. For this reason, our build systems are designed so that they do not require, and consequently do not have, online access.

Operation

Wibu-Systems offers not just software products, but also services. Several of our products are hosted on behalf of our clients, e.g. our Cm-Cloud solution. The services hosted by us are permanently watched, monitored, and serviced, as are our operating systems. We believe that products should be continuously updated and our clients always provided with new versions bringing new features and improvements.

For older versions of our products that might be running on operating systems we no longer fully support, we can offer extended support. CodeMeter Software Version 7.21 includes all security updates for our most recent version and even runs on Windows 7.

The Response

With all of these precautions in place, it should be possible to claim security. But we know and admit that this ideal state has not yet been reached, and the authors of these pages would never suggest that all flaws can be eradicated. Remember that a simple flaw can become an unexpected vulnerability. We all remember Log4Shell, and there is no need to bring that litany of mistakes up again.

If we cannot prevent all problems, we need to consider how to cope with flaws and problems. The first and most important aspect is accepting the existence of flaws, both in the software we create and in the software made by third-party developers. The issue is not whether we made or found an error, but how we deal with it. If we go with the assumption that the vulnerabilities were not created intentionally or by gross negligence, there is no reason to get exasperated.

If the problem originated with another company's software, we usually want three things: First, that we get a new version without the vulnerability as quickly as possible to be able to protect ourselves and our customers from attacks. Second, that we are given as much information as possible about potential consequences, so that we can decide for ourselves

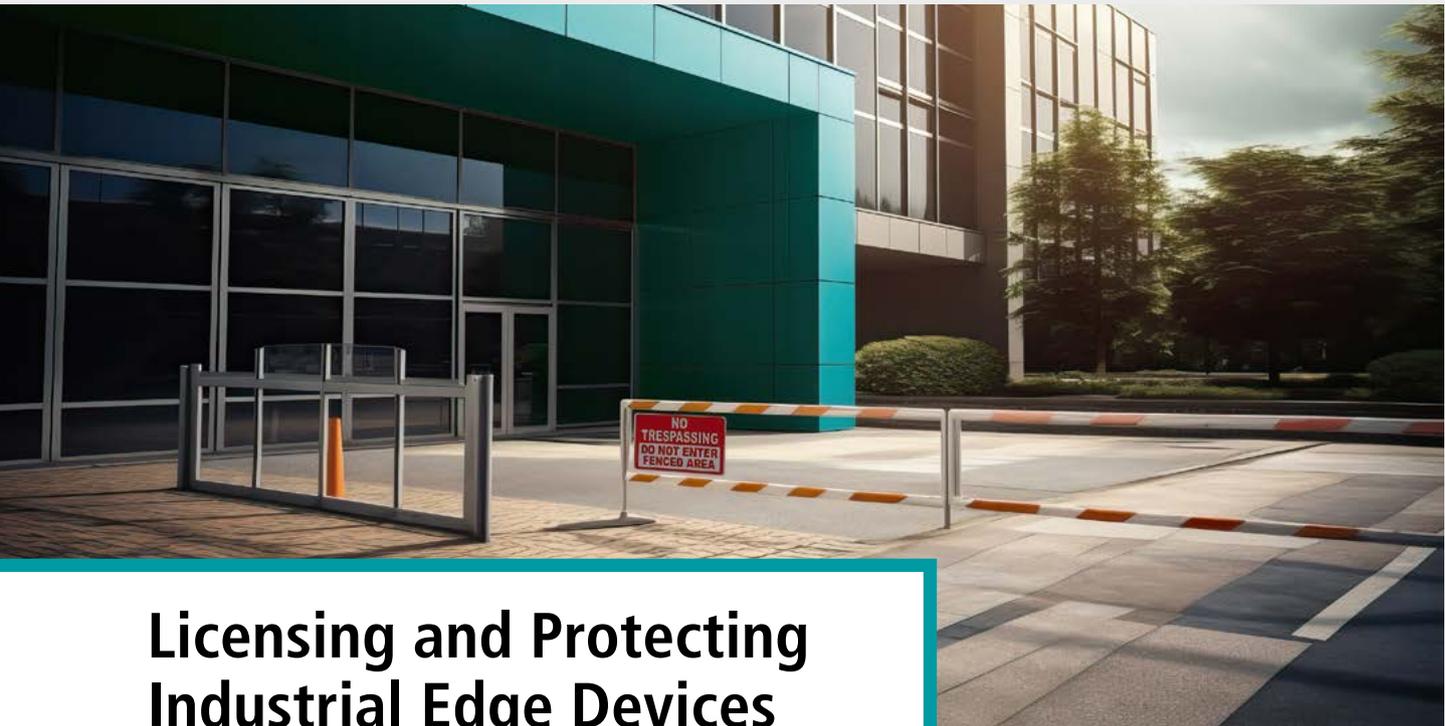
how we should respond. And third, that we are always kept up to date.

But what does the other side look like? To get the best possible support for our clients, we need some structures in place at the company whose software was found to have a vulnerability. This starts with a proper point to report such vulnerabilities and goes all the way to a team to coordinate the response to major vulnerabilities (CERT) and defined lines of communication with representatives for every product and with the client out in the field.

Every single aspect deserves full attention (entire books could be written about the details of every single aspect). Let us consider the coordination systems in place and the necessary structures. If a single vulnerability affecting a single product is already a headache, a vulnerability that affects multiple products can become a serious issue for any business. The limited central resources now have to take care of issues on multiple fronts, and the information about the issue has to be communicated, ideally in a coordinated and standardized fashion. A company of Wibu-Systems' size could not keep an emergency team on hold to take care of all relevant aspects. This makes it even more important to train the necessary procedures and to learn from every incident in the form of improvements to those procedures. One of the improvements that Wibu-Systems introduced is the Product Security Board. It brings together a member of every product team and the CERT, supported if need be by staff from other departments. This allows us to collect and share our know-how quickly. Every Product Security Board Member speaks for the entire developer team, which keeps the lines of communication short and our response fast. CERT supports the analysis of the vulnerabilities by adding expert cryptography know-how and consolidating the resulting information for communication to the client. We included a more detailed report about our responses in KEYnote 43. 

<https://www.wibu.com/magazine/keynote-articles/article/detail/professional-response-to-security-incidents.html>





Licensing and Protecting Industrial Edge Devices

Does the advent of Software as a Service (SaaS) mean the end of software licensing as we know it? Not all solutions are suitable for SaaS, which has only served to make containerization in edge computing even more complex.

What is Edge Computing?

The era of data being processed and software run exclusively on local hardware is over. The rise of SaaS has changed how companies work. Predictive maintenance and CRM systems that used to be hosted on local servers are now typically kept in the cloud and accessed by users over the Internet.

Cloud landscapes do not come without their own challenges, starting with questions of bandwidth or availability and going to issues of latency or data security. The exponential growth of IoT devices has exacerbated the data deluge, which means that a balance needs to be found between cloud and on-premise solutions. This is where edge computing comes in.

Edge computing happens at the threshold between both worlds. Instead of the cloud, applications run on the end users' devices, and only a minimal amount of data is sent to the cloud. By keeping a part of data processing on the ground, edge computing reduces latency and allows data to be processed virtually in real time. Sensitive data or algorithms can also stay on the user's hopefully secure premises, which improves data security and helps with data protection regulations.

In essence, edge computing is the software provisioning option that enables companies to benefit from the advantages of the cloud without accepting all of its drawbacks.

Challenges for software licensing

For software developers, keeping control over how their products are distributed is paramount, because illicit use can threaten entire business models. Technical evolution and the constant and growing threat of software piracy means that software publishers need to adjust how they protect and license their software all the time.

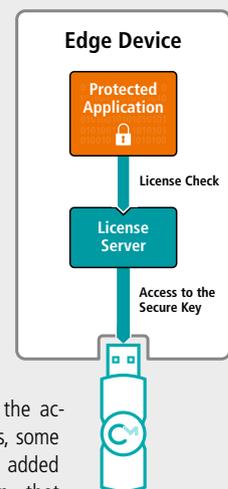
The same is true in edge computing. The term does not really say anything about which hardware or system architecture is being used, even if the systems in question run in a set of containers in the large majority of cases. So-called Containerization has made it much easier to keep tabs on the applications running in the containers.

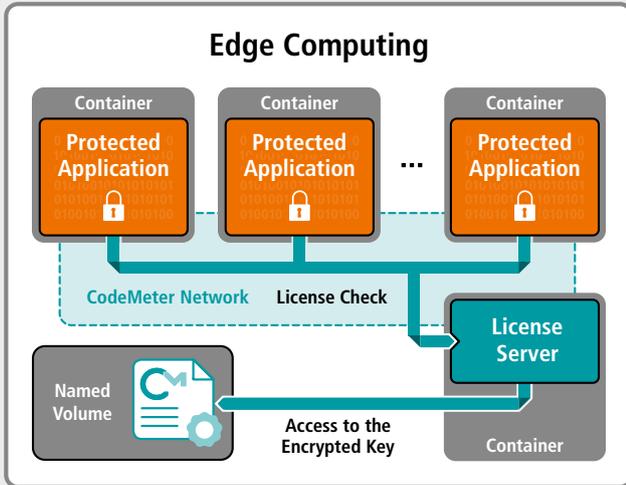
But there are challenges: Edge computing is used in a diverse range of contexts. Not all of the systems in question can be kept online at all times. There needs to be a way to make sure that they can run without jeopardizing the

license terms even if the system is disconnected from the Internet.

Product managers, software architects, and developers for all types of applications running on edge devices need to get together and consider how they can protect their intellectual property and their license terms in actual practice.

There is another option: Separate protection and licensing. An application could be protected in the IP Protection mode of AxProtector from CodeMeter Protection Suite. For the actual license checks, some tolerance can be added in the application, that is the application can be allowed to run for a while even if the right license cannot be found. Naturally, these deci-





sions need to be taken at an early point in planning and development.

Solutions

The great advantage of CodeMeter by Wibu-Systems is that the access and cryptographic operations with the licenses are identical for any type of CmContainer. This means that the way of rolling out licenses can be adjusted perfectly to match each individual situation. When initially encrypting and protecting an application, it does not matter at all how or where the license is provided to the end user.

CmDongles

If technically feasible, a CmDongle can be used to benefit from its dedicated hardware with a built-in crypto chip. Since a CmDongle can be connected with only a single CodeMeter component, a setup with multiple containers usually runs a container with a CodeMeter license server that links up with the CmDongle. From there, the licenses are made available to all the other containers.

CmActLicense

The purely software-based CmActLicenses are another choice that binds the licenses to a fingerprint of the system's properties. For meaningful security, the license needs to be bound to a secure anchor. This is usually done by selecting a whole set of system traits that are then combined by the patented SmartBind technology to create a unique,

but also sufficiently tolerant fingerprint.

Enforcing system-specific licensing can be harder in a container environment, because containers were designed to make everything as abstract as possible and limit data flows to the host or other containers to the desired minimum. Aside

effect is that the usual set of system properties can normally not be read out, and the license data cannot be kept persistent over time.

For Docker environments in particular, Wibu-Systems has already tweaked its binding technology for CmActLicenses. The necessary data is stored in a so-called named volume and bound to that volume at the same time. This makes it impossible to simply copy or move licenses around. However, this also needs more rights for the container accessing the license. For CmActLicenses to be installed in a container, the license provider needs to specifically activate this option.

CmCloudContainers

Another highly secure variant is provided by CmCloudContainer, a cloud-based licensing system. The keys on the license never leave the private cloud operated by Wibu-Systems and all cryptographic operations are also executed

there. Of course, a CmCloudContainer needs an Internet connection, which has to be permanent and stable for the licensing system to work as it is supposed to. If that is not guaranteed, it helps to separate IP protection from licensing and add some tolerance for the latter.

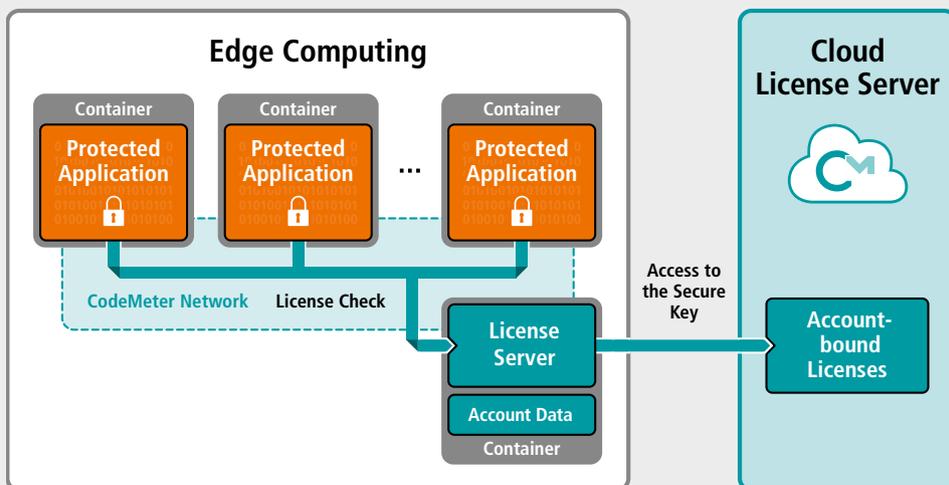
Taking a detour

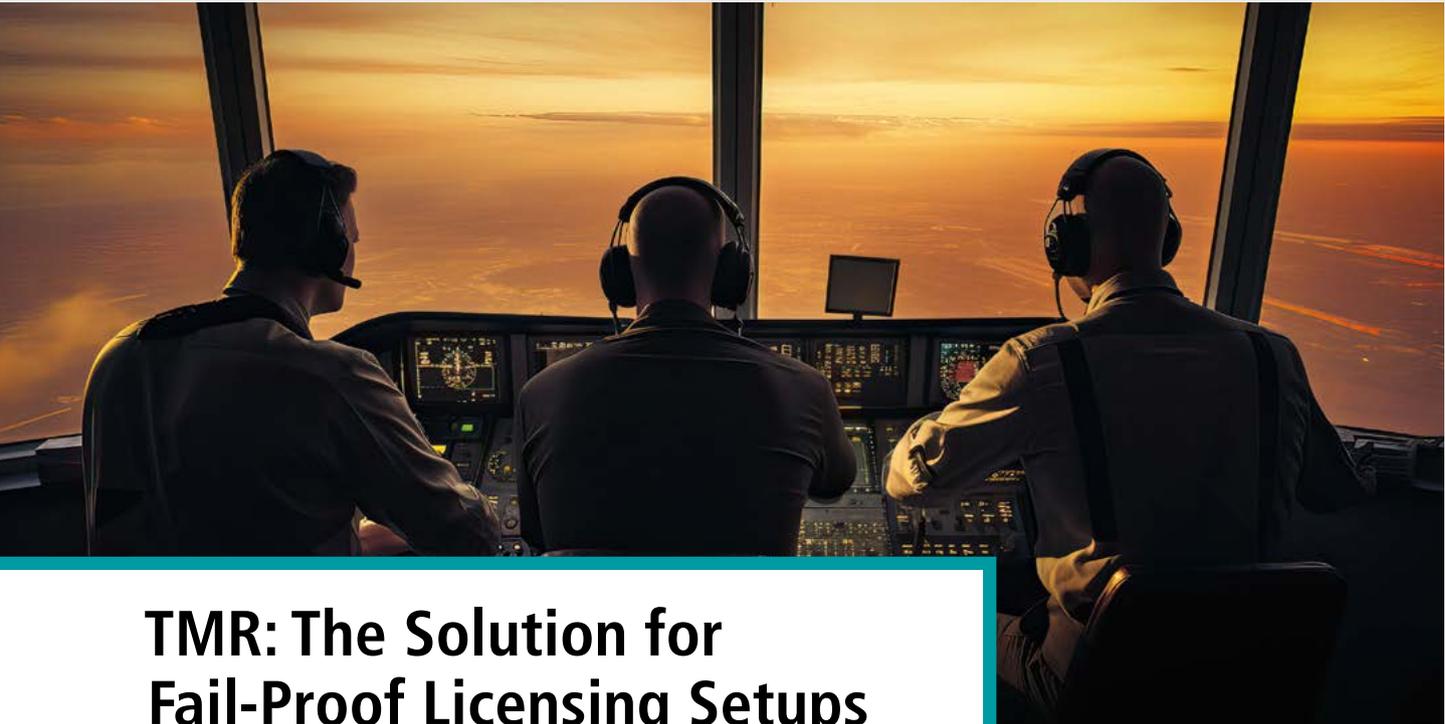
On top of the options explained here, there is another way: using CodeMeter licenses indirectly. The edge device or the container with the CodeMeter license server can connect to any CodeMeter license server on the network. It is there that licenses could be provided (using any type: CmDongle, CmActLicense, or CmCloudContainer).

A final option is providing a CmDongle indirectly via an USB-over-Ethernet setup. This is favored by many administrators for its easy management and ability to keep CmDongles and the dongles of other makers in a single physical place.

The right stuff

It is simple: Different use cases need different solutions. When picking the right option, it helps to ask an expert and carefully weigh up one's choices. There is no one final answer to everything that could determine which solution is best for any scenario. But the versatility of CodeMeter ensures real compatibility with a vast range of use cases, making it the ideal solution for software makers who want to master the complexity of licensing in edge computing environments. 





TMR: The Solution for Fail-Proof Licensing Setups

Wibu-Systems has been pioneering software protection, licensing, and security technology for more than three decades. The company has made a mark with its user-centric philosophy and its dedication to always listening to its clients' specific needs, and it has been a trailblazer especially in the ability to license individual software functions.

Why license software? Licenses are used to protect the intellectual property of the developers and to make sure that the protected software runs exactly as it should. This would make it a worst-case scenario if a license server broke down, which can bring entire production lines to a standstill. It is in response to the call for fail-proof, high-availability licensing environments that Wibu-Systems has designed CodeMeter TMR.

TMR stands for "Triple Mode Redundancy" and combines the concept of fail-proof license availability (2-out-of-3) with field-tested data-center technology. A cluster of five servers, two of which working as load balancers and three as license servers, forms a combined system. As long as two of the three license servers are available, the entire licensing setup will work – reliably.

CodeMeter TMR was made for the following use cases:

1. **Manufacturing:** In automated production lines where a lost license server would mean

downtime and considerable lost revenue.

2. **Mission-critical applications:** For software in e.g., healthcare, finance, or infrastructure management that depends on the high availability of the license servers.
3. **Global distribution:** For companies that operate across geographies and need consistent licensing, even if a local failure happens.

The cleverly tiered and coordinated interaction between CodeMeter and CodeMeter License Central in a TMR Setup means effective license availability, complete license monitoring and efficient load balancing.

1. **License availability:** When a server breaks down or needs to be serviced, the system will keep working (redundant infrastructure). If one license fails, the ISV can reissue it with a workflow integrated into CodeMeter License Central and get everything synchronized properly.
2. **License monitoring:** All paid licenses are always available (as licenses linked across the shared servers). License protection is ensured throughout without any additional licenses, rights, or entitlements having to be issued to users in the field. This gives the vendor complete control over the type and limits of their licenses.

The 2-out-of-3 principle

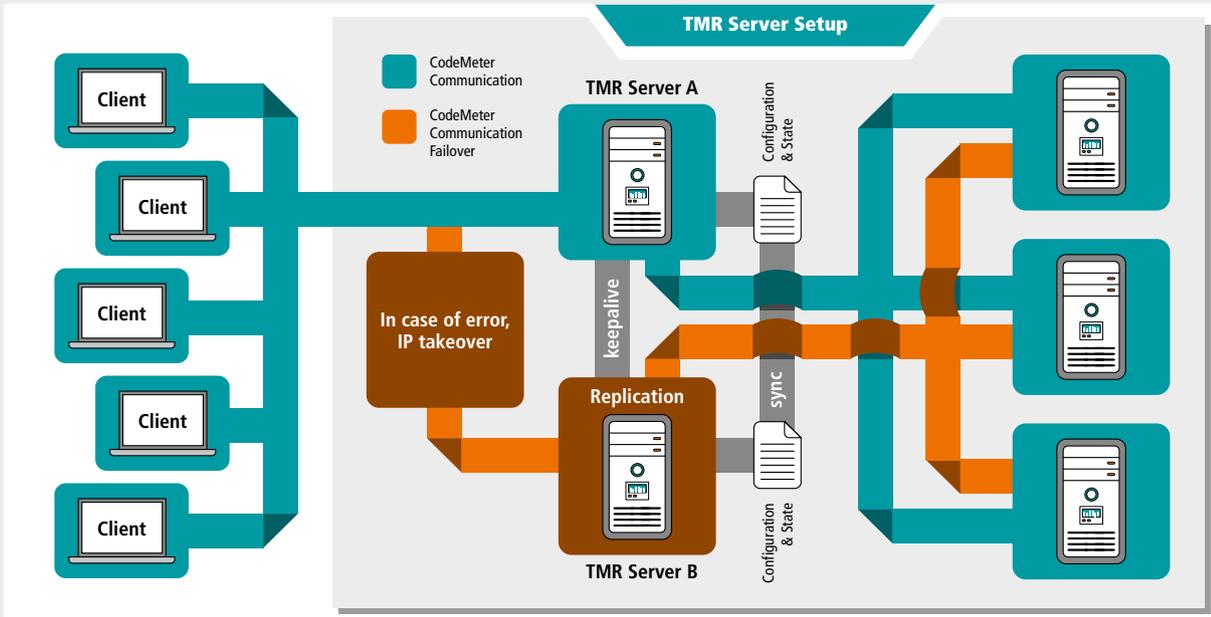
A TMR Setup is needed to make all this possible. The TMR Setup includes five servers that

are usually run as virtual machines. Two of them act as the interface to the user clients (here called TMR Servers). The other three work as Backend Servers that receive the license queries from the user clients.

The TMR Setup has a single virtual IP address in the network. Over that address, all queries are routed to the TMR Server that is active at the time. If that one cannot be reached, the other TMR Server steps into the breach, switching from standby to active. The switchover works according to the standard criteria: If the active TMR Server cannot be reached, the standby server notifies the infrastructure that it wants to receive all packages sent to the virtual IP address and seamlessly slots into the role of the active server. The formerly active server can return to being the standby server as soon as it is reachable again.

This is done by a Keepalived daemon installed and working on both TMR Servers. Switching the status is always possible since the current state of the active server is always synchronized. All active data is replicated.

Working behind the TMR Servers, three CodeMeter Backend Servers are organized as CodeMeter network servers on either Linux or Windows. They act as the recipients of the instructions passed through to them by the TMR servers.



Licenses in a TMR Setup

For CodeMeter licenses in a TMR Setup, a different set of conditions applies than for normal licenses not working in a high-availability arrangement. This is why the parameter TMR-Id was introduced. The TMR-Id is an additional property in the license quantity that is used to clearly identify the three licenses belonging together in the 2-out-of-3 context. Firm Code, Product Code, and TMR-Id all must be identical for the licenses to form one TMR license. Similarly, all other properties for the Product Item are identical for all three licenses. The three licenses are placed in three separate CmContainers with the same CmActId.

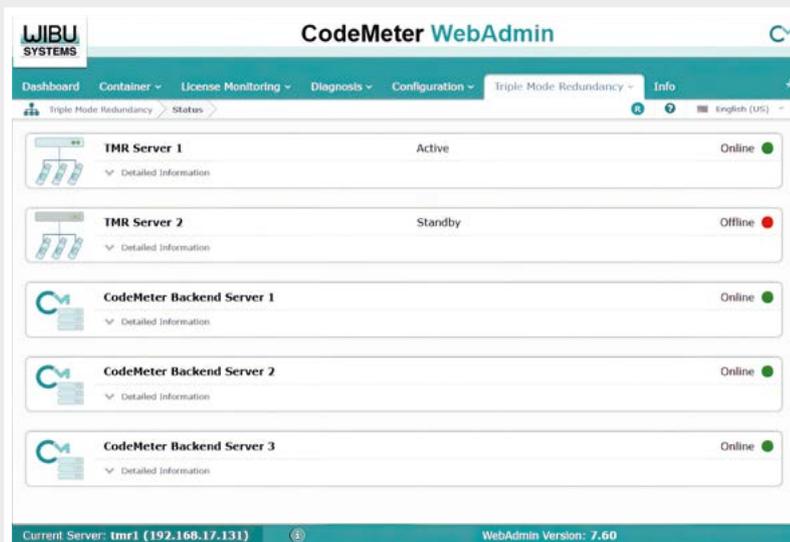
When adding a TMR license to a TMR Setup, the TMR Server combines all CmContainers with the same CmActId into a single virtual CmContainer, which is given a standard serial number starting with 131. The user will only see that container. For the TMR licenses to be valid and available, at least two out of three of the constituent licenses need to be available. If only one of the three is there, the TMR license will not show up in the virtual CmContainer. A potential attacker that only has one of the containers with one TMR license could not use the TMR license. The CodeMeter server prevents misuse of licenses with a TMR-Id. These licenses can only be used in a TMR cluster.

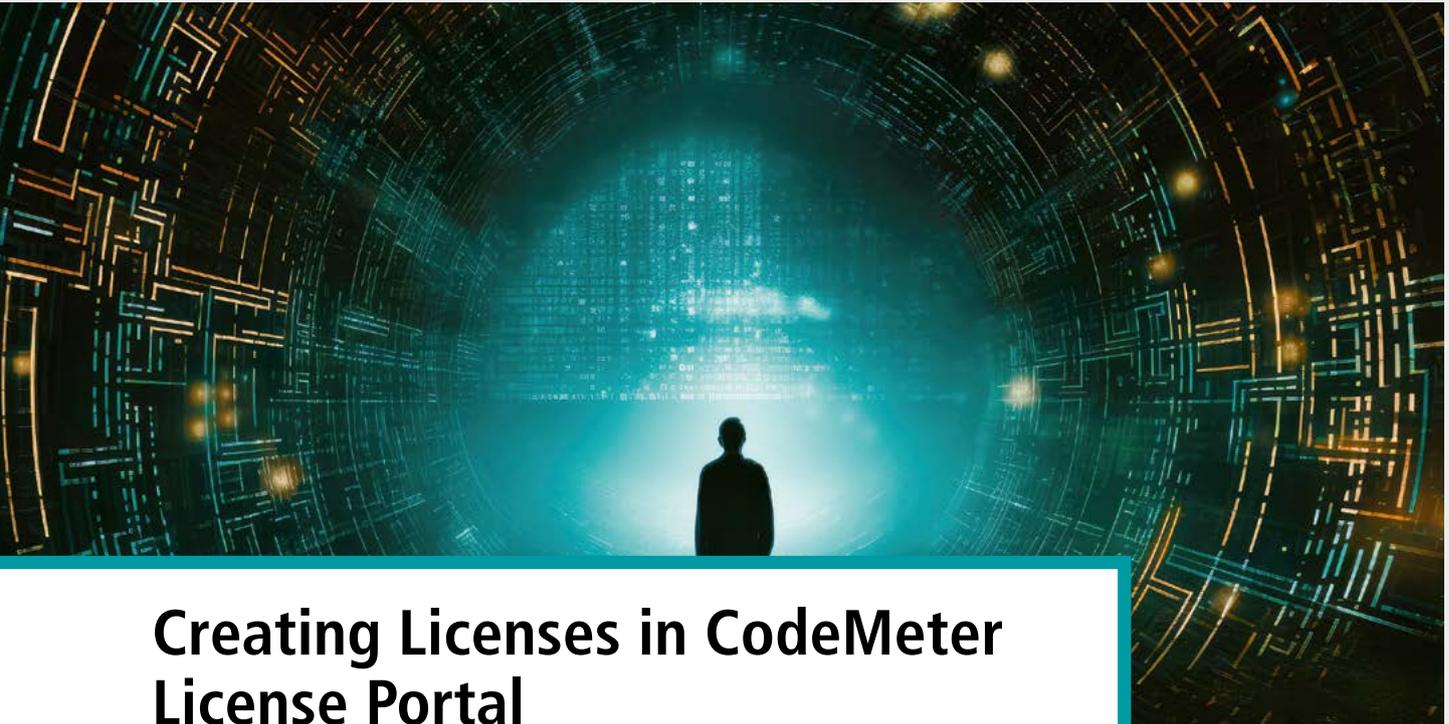
The configuration settings in CodeMeter Web-Admin allow the TMR licenses to be passed through to the Backend Servers via the IP address.

In the case of a failure or a planned maintenance event, this means that license operations can go on as planned. If one of the backend servers fails, the other two can handle license queries until the issue is solved or the maintenance finished.

Fail-Proof

If you are looking for fail-proof licensing software that gives you full control over your licenses, CodeMeter TMR is the right choice for you. If you are already using one or more CodeMeter components, TMR can be activated with a simple click in the global settings of CodeMeter License Central if you have the necessary infrastructure in place. Wibu-Systems' team is happy to help you with installing and configuring your TMR Setup.





Creating Licenses in CodeMeter License Portal

CodeMeter License Portal is the customizable, adaptable, and expandable frontend for CodeMeter License Central, and the corresponding backend in charge of technically creating licenses, handling all automatic processes in the background, and providing the interfaces needed to integrate third party systems. On the front end, CodeMeter License Portal handles interactions with the user, can accommodate additional data fields, and offers a range of customizable workflows.

Overview

CodeMeter License Portal includes a set of functions:

- Managing client data
- Creating and managing licenses and subscriptions
- Supporting users with license activations
- Managing CmCloudContainers
- Providing a substantial automation API
- Providing customizable workflows

Read more to learn about the ways to create and manage licenses and subscriptions in CodeMeter License Portal.

Lean and mean

You might wonder why you should create subscriptions or licenses in CodeMeter License Portal, instead of going right to CodeMeter License Central. Naturally, you can do so as well, but the real strength of CodeMeter License Central lies in its powerful API that you can use to hook up with third-party systems like CRM, ERP, or e-commerce solutions. When integrating with such systems, subscriptions

are usually managed within those systems and not in CodeMeter License Central, which lets CodeMeter License Central hold only the fundamental functions you need for managing subscriptions from the outside. This clear line of demarcation keeps CodeMeter License Central lean and mean. For management purposes, you rely either on the third-party system or on CodeMeter License Portal.

Configuring articles

Products are by default configured in CodeMeter License Central. You only use CodeMeter License Portal to manage additional information like article groups or data needed for visual elements in the sales process. You can configure it as you need, e.g., with multilingual descriptors or standard values or allowed values to adjust the license creation interface to match your needs and preferences or to provide the necessary technical terms. For instance, you could use it to define whether a trial version is allowed for 5, 30, 60, or 90 days and enter a preset of 30 days.

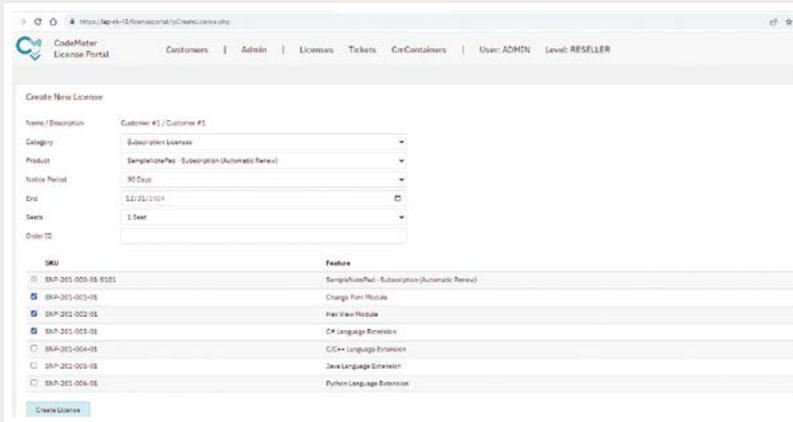
Managing rights

Product groups fulfill two purposes: They let you organize the products for selection and they let you assign the necessary rights for each group. Users can only create licenses for products in groups they are entitled to and revoke licenses or cancel subscriptions for these products.

This rights management capability lets you use the portal as an exclusive internal solution that your employees can use to create licenses; alternatively, you can open it up to your sales partners for similar purposes. You even can assign that right to your users, that is, delegate license creation to that level of your hierarchy. This can be done for clients with volume contracts that cover an unlimited number of licenses. By allocating products to separate categories, you can even assign these rights differently for different products.

Creating licenses

The most basic use case of CodeMeter License Portal is license creation. To do so, the regis-



tered user – it could be a client, your company, or a subgroup at a client – would select the relevant group that they have the admin rights for.

The user then selects the product category from the choice they are entitled to. The products from that group will be displayed and the user can make their choice. The last step asks for the relevant entries for that product and any optional features. Such features are normally handled as Module Items in CodeMeter License Central.

A click on “Create License” is enough to start a new order in CodeMeter License Central and create a new license. The resulting ticket is automatically allocated to the selected group and immediately available for the group’s members.

Allocating licenses

One license = one ticket. That is our best practice for CodeMeter License Portal. It can be allocated to a single person or a group of users. If a ticket is assigned to a named person, only that person will be able to see it on the activation page, other than the group admins who can see and change the ticket’s allocation on their group page. When a ticket is assigned to a group, you can determine whether the license that goes with the ticket is visible for all members of the group. If not, only the admins can see the newly created license and either allocate it to a specific person before activation or make it visible for all. You can change the default workflow to your liking.

Creating subscriptions

Subscriptions are created in much the same way as licenses, although there are different ways to do so in practice.

Let us consider subscriptions that are automatically renewed in CodeMeter License Portal. They have two additional fields: The (initial) expiry date and the cancellation period. The ex-

piry date defines the subscription’s first period. The subscription runs for that period, both commercially speaking and technically.

If the subscription is not cancelled within the defined period, it will automatically be renewed for another year for commercial purposes. On the technical side, the user gets the ability to renew the license, which synchronizes the subscription’s technical expiry date again with the commercially defined subscription period. Usually, this activation option is handled automatically by the activation assistant of the subscribed software, so that the end user does not have to do anything manually.

Expiry dates for subscriptions are normally defined in one of two ways: Either exactly one year from the date of purchase or activation or for the end of the calendar or fiscal year. The latter option is often chosen when the company has no means in place to account for ‘moving’ expiry periods that fall into two fiscal years and therefore create revenue in both years.

Cancelling subscriptions

People cannot only buy subscriptions, they can also cancel them. The cancellation will switch off the automatic renewal process, and the user loses the right and ability to use the software on the expiry date.

Revoking licenses and subscriptions

Cancellations are a normal part of any subscription’s lifecycle. No subscription runs indefinitely. Alongside such cancellations, however, CodeMeter License Portal also includes the means to terminate a subscription immediately and revoke the license. This should normally be a rarely used process. Technically, the license is set to “revoked” in CodeMeter License Central, and it is removed immediately at the next opportunity, e.g., when the software activation assistant is launched again.

Billing reports

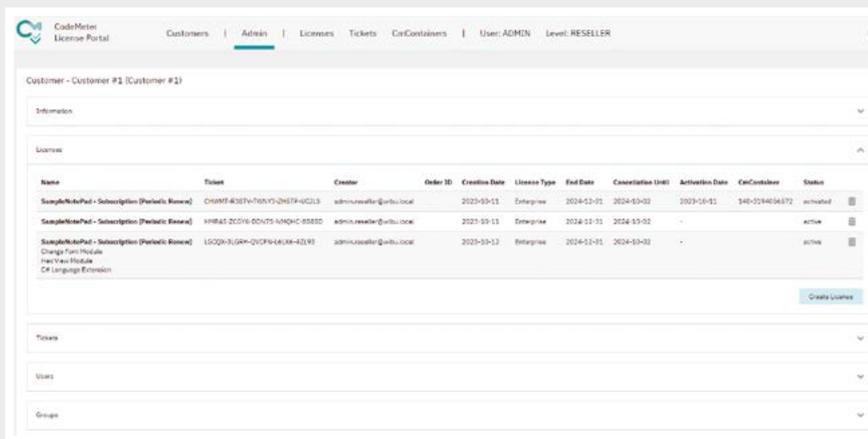
CodeMeter License Portal lets you create billing reports. By default, two report formats are included:

Renewal report for users: This report lists all subscriptions that are not cancelled and that have been renewed in the report period. You can add prices to these and automate the entire billing process in your ERP system via the import function.

Active subscriptions for resellers: This report lists all active subscriptions for a defined day of the month. It can be used to create batch invoices for one of your sales partners. Again, invoicing can be automated by ERP import.

Conclusion

CodeMeter License Portal is designed to be flexible and modular. You can adjust and configure it to your liking. Our Professional Services Team is also available for you to implement custom expansions like additional report formats or custom workflows.





How our Clients get their ROI with CodeMeter

We wanted to know how our CodeMeter protection and licensing solution impacts the business of our clients. To answer that question, we met four selected clients for detailed interviews to compare the costs and advantages and get a meaningfully complete analysis of their ROI.

Software piracy, inefficient licensing models, the need to protect one's intellectual property, and the wish for more flexible and innovative usage and pricing models were named as key challenges for software businesses.

With powerful encryption, special protection

Initial Start-Up costs

Software License fee	[TEUR]
CodeMeter Protection Suite	[TEUR]
Wibu-Systems Professional Services	[TEUR]
Wibu-Systems Academy / Training	[TEUR]

Initial costs CodeMeter technology

ISV development costs for integration into software products	[TEUR]
ISV development costs for integration into backoffice systems	[TEUR]

Initial development cost ISV

Total Initial Start-up costs [TEUR]

Illustration 1: The initial investment

Revenue Increase

Revenue	Average Sales price per unit [EUR]	Annual quantity [pcs.]	-----	Annual revenue [TEUR]
✓ Revenue increase by reducing illegal copies	Piracy rate in market: 15%	Annual quantity increase [pcs.]	-----	Revenue increase [TEUR]
✓ Revenue increase by IP protecting (software + data)	Market share increase: 10%	Annual quantity increase [pcs.]	-----	Revenue increase [TEUR]
✓ Revenue increase by offering flexible pricing models	Revenue growth by flexible pricing models [%]	Revenue growth by new pricing models [%]	-----	Revenue increase [TEUR]
by offering new pricing models			-----	Total Revenue increase [TEUR]
			-----	Total Quantity increase [pcs.]

Illustration 2: The different categories of revenue increases

hardware, and anti-cracking techniques, CodeMeter offers reliable protection for intellectual property and ensures the security of software licenses. Included on board: Granular and smart controls over licensing, integrity protection during runtime, and secure update mechanisms.

The protection technology can be built into software at virtually any level to achieve the right degree of security. Back office integration allows

our clients to automate their processes, and everything is flexible and scalable to perfectly blend in with their circumstances and requirements.

Our method for calculating ROI

A precise calculation of the Return on Investment (ROI) is essential when one wants to understand the real added value of modern licensing for software developers and vendors.

Cost savings				
✓			Number of licensing order-taking [FTE]	
			Reduction of licensing order-taking [FTE]	
FTE cost per Order-taker	65,0	[TEUR]	Cost savings licensing order-taking	[TEUR]
✓			Number of legacy licensing developers [FTE]	
			Reduction of licensing developers [FTE]	
FTE cost per developer	100,0	[TEUR]	Cost savings development	[TEUR]
✓			Number of legacy support experts [FTE]	
			Reduction of support experts [FTE]	
FTE cost per supporter	70,0	[TEUR]	Cost savings support	[TEUR]
Total Cost savings				[TEUR]

Illustration 3: Potential savings

The fundamental figures and insights gleaned from our interviews with our clients form the basis for these calculations.

We started by first adding up the initial investment needed to put in place the specific licensing system. That includes the cost of the protection software and the effort to program and integrate it into an existing process landscape.

During routine operations, there are additional costs for providing the CodeMeter license containers for each unit of software sold.

On the plus side, we find revenue increased by the reduction of illegal copies and by the effective protection of intellectual property, which helps sell more legitimate licenses. There is also the option of offering flexible pricing models, matched more to the end user's needs. Novel pricing models can generate entire new revenue streams.

After the introductory phase, the ability to automatically roll out licenses can help save running costs. The integration of the licensing technology can also reduce development costs, because CodeMeter offers a streamlined, uniform solution, which keeps admin efforts consistent and efficient and will eventually bring down service and support costs.

A look at real-life use cases

We analyzed every one of the four clients individually. One of the two smaller customers sells a specialized simulation software while the other wants to protect their intellectual property in the form of 3D printing data. In the former case, licensing was approached by way of computer-bound licenses (CmActLicenses), while the second company's 3D data was protected with hardware secure elements (CmDongles). The third use case is a medium-sized mechanical engineering business who wanted to monetize their machine operating software, formerly simply part of the on-board package of their

machine sales, in a modular business model. They chose a combination of software, hard-

ware, and cloud licenses. The largest client we interviewed sells a popular ERP software.

Costs and gains

The companies we looked at reported the start-up costs shown in table 1 to get their systems up and running.

Table 2 covers all operation costs of the licensing system. Every sold and licensed piece of software needs a license container. Depending on the chosen model, these fees could either be calculated as a flat sum, chosen to mirror the client's revenue with the software, or calculated precisely as unit costs per license

Start-up Costs – until Date of Sale [EUR]	Large	Medium	Small SW	Small HW
License fees for CodeMeter Protection Suite	-1,200	-1,100	-800	-800
Wibu-Systems Professional Services	-39,000	-13,000	0	0
Wibu-Systems Academy / Training	-5,000	0	0	0
ISV development costs for integrating CodeMeter in the client's software	-150,000	-50,000	-12,000	-12,000
ISV development costs for integration into the back office system (ERP)	-350,000	-150,000	0	0
Total	-545,200	-214,100	-12,800	-12,800

Table 1

Wibu-Systems Licenses – until Date of Sale [EUR]	Large	Medium	Small SW	Small HW
Total operation costs	-1,071,000	-258,000	-13,900	-29,500

Table 2

Revenue Increase – until Date of Sale [EUR]	Large	Medium	Small SW	Small HW
Revenue increased by preventing illegal copies	1,755,000	315,000	10,800	10,800
Revenue increased by expanding the market (IP protection)	585,000	157,000	7,200	7,200
Revenue increased through novel, flexible licensing models	1,213,000	269,000	10,800	10,800
Total	3,553,000	741,000	28,800	28,800

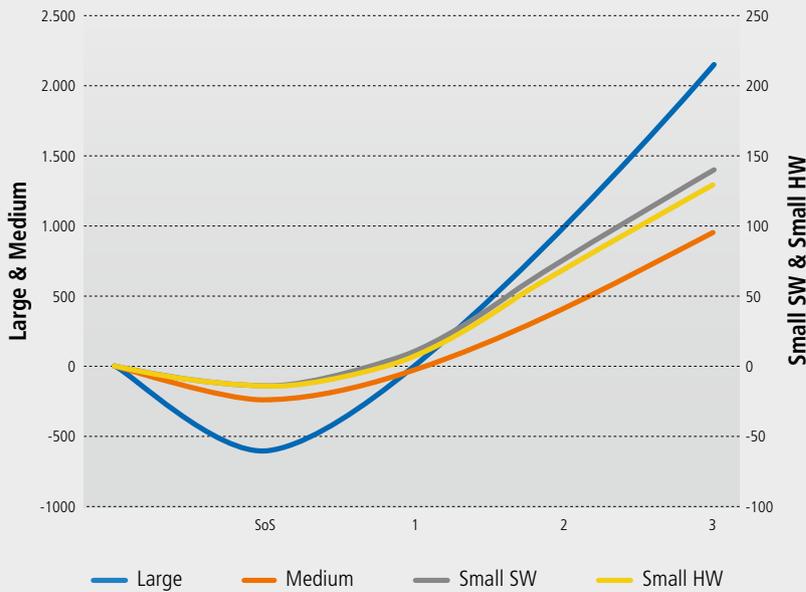
Table 3

Costs saved – until Date of Sale [EUR]	Large	Medium	Small SW	Small HW
Savings in order processing	300,000	112,000	39,000	39,000
Savings in development	875,000	188,000	85,000	85,000
Saving in support	200,000	160,000	0	0
Total	1,375,000	460,000	124,000	124,000

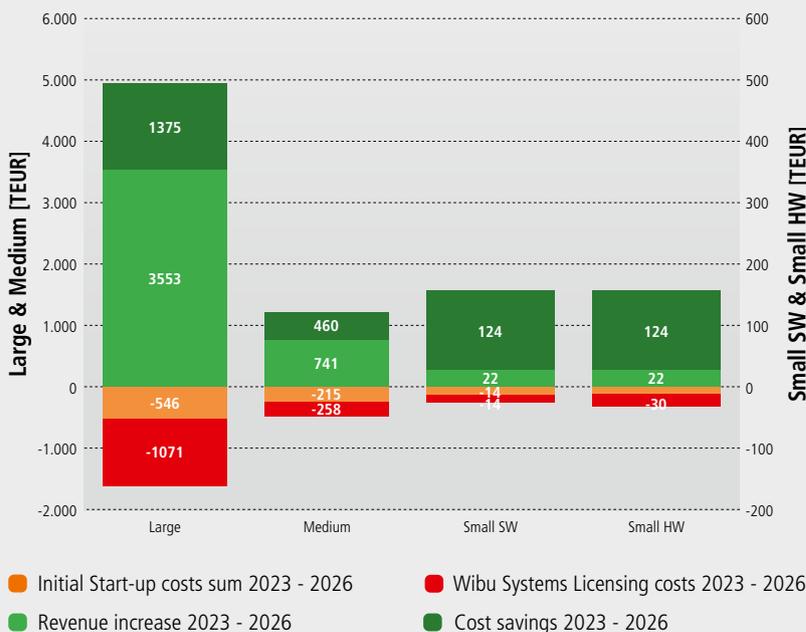
Table 4

Costs saved – until Date of Sale [EUR]	Large	Medium	Small SW	Small HW
Present Value of Net Margin Increase and Initial Costs [EUR]	2,142,900	952,900	104,600	92,900
Start-up Costs [EUR]	-599,700	-235,500	-14,000	-14,000
ROI	357%	405%	745%	661%

Discounted and Risk Adjusted Free Cash Flow Over Time [TEUR]



Costs and gains



container bought. Customers who want to automate license creation and deployment also order CodeMeter License Central and License Portal and sometimes need support assistance.

By introducing the CodeMeter licensing technology, the companies had a chance to markedly increase their revenue, especially by significantly reducing the number of illegal copies – approximately 15% in several markets. This is shown in table 3.

Table 4 shows how the CodeMeter licensing solution also reduced costs by a considerable margin by integrating everything perfectly with existing internal processes. The complete automation of the license creation and provisioning part led to a massive reduction in operating costs.

ROI calculation and analysis

For our next step in trying to understand the ROI, we looked at the results from the first three years after CodeMeter was introduced and compared them to the running costs. This produced the so-called net margin increase that comes from operating a CodeMeter licensing solution.

Since no one can really predict the future, we added a blanket risk adjustment factor of 20% to the net margin increase. To calculate the present value, we used an internal rate of return of 10%.

When we compare the gains against the costs, we can find a clearly positive ROI in all four cases.

Finally, our calculated ROI has revealed that CodeMeter was an extremely good investment in all four instances. The initial costs paid off within a year and significantly increased revenue in the long run, making CodeMeter the convincing choice for companies that want to optimize their software licensing and security performance.

Costs and gains over time

These ROI calculations for Wibu-Systems' software licensing solution are impressive proof of the financial advantage that comes with choosing a professional licensing and protection system. And the added value of such a system lies not just in its ability to monetize software effectively: Companies gain far more, in the form of a stronger competitive advantage and in the form of long-term commercial health and viability.

WIBU BLOG

One idea at the right time
can change everything.

Subscribe to our blog





Licensing in the Cloud

Cloud licensing comes in many shapes and sizes. What they all have in common is that the licenses are created and managed through the cloud. What happens next can differ: The scenarios can range from full and permanent online use to a choice of offline options.

Offline vs. Online

“Offline” means that the licenses are managed via the cloud, but kept offline on the end user’s device. Depending on the specific implementation, updates can be rolled out by synchronizing the end user’s device and the license creation server whenever an online connection is established. Time limits can be set to the license to force users to connect to the Internet regularly and enforce license synchronization.

In purely online scenarios, the licenses are managed, stored, and used in the cloud. The end user or end device needs a permanent Internet connection for this to work, but this setup has two great advantages: The licenses are always up to date, and it is no problem at all to move from device to device, e.g. office in the morning and home office in the afternoon.

CodeMeter working Offline

For offline use, CodeMeter License Central can offer license management through the cloud in the form of a backend for creating and managing licenses and, optionally, CodeMeter License Portal as its frontend. This is usually used when no ERP or CRM system is involved and

a simple-to-use option is needed to manage licenses and client data.

CmActLicenses represent the simple solution for handling offline licenses. These containers are bound to a fingerprint of the end user’s device and can be used completely offline once the licenses have been activated.

That activation can be done either through CodeMeter License Portal, WebDepot, or a Software Activation Wizard (SAW), which can also be used to keep CodeMeter License Central and the local licenses in sync by communicating with CodeMeter License Central through dedicated gateways and updating the licenses as needed.

CodeMeter working Online

In online scenarios, CodeMeter License Central again works as the backend for creating and managing licenses. The great advantage in this case is that offline and online licenses can be used together with CodeMeter License Central. ERP and CRM systems can be integrated with no changes to the processes: Everything is integrated once, and the licenses can be created

as needed for each use case in play. CodeMeter License Portal can, naturally, be included in the mix as well.

With CmCloudContainers hosted on the servers run by Wibu-Systems, one has a secure environment for licenses in the cloud. CmCloudContainers are again compatible with local CmActLicenses, which keeps everything true to the motto: Integrate once and then configure the licenses to your liking or to match the needs in the field.

Licenses in CmCloudContainers can similarly be activated through CodeMeter License Portal, WebDepot, or a SAW. The only difference to offline licenses is that they can be activated by an admin of your client or even by you as the vendor.

Licenses can be updated either through the SAW or, for a transparent and even sleeker option, through an auto update trigger in the background.

Personal vs. Concurrent

Licenses can be given to a single user or single

device, or shared by multiple users and devices. The former is called a single user license or personal license, the latter a floating network server or concurrent license. Whichever option you need, CodeMeter can handle both in online and offline scenarios.

Personal CmCloudContainer

A Personal CmCloudContainer is a container assigned to a single person. Users need to connect the device they are using the licensed software on directly to the Internet. Distributed applications or software suites that have parts running on a local PC and parts on a mobile device are also possible, as the Personal CmCloudContainer can be active on up to three devices at the same time. As the software developer or vendor, you can decide on how many of these active devices your software can be run concurrently by configuring the license quantity setting accordingly.

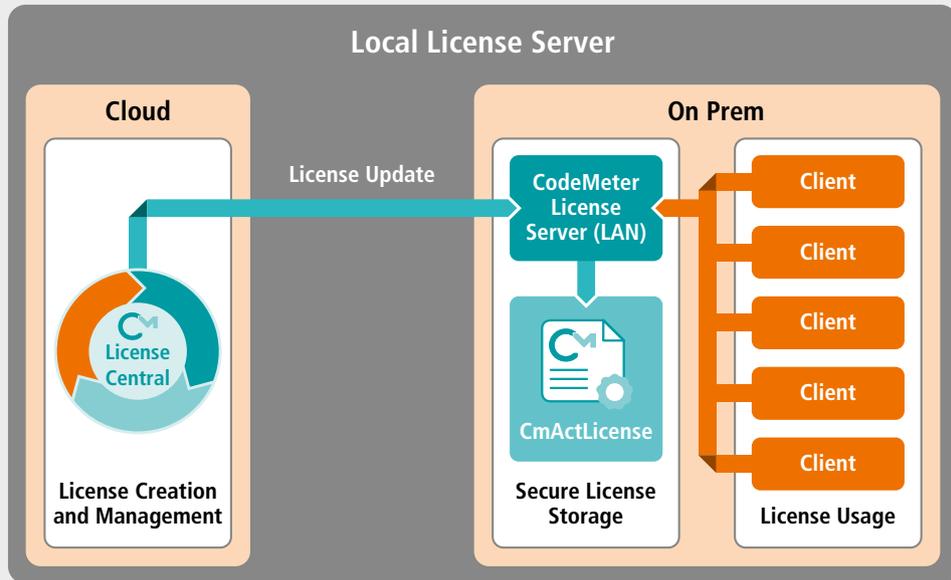
On CodeMeter License Portal, each Personal CmCloudContainer is assigned to a specific user who can access it and activate licenses from up to three active devices. If the user belongs to a group, e.g. a company, the group's admins can manage the CmCloudContainer and its licenses.

On CodeMeter License Portal, each Personal CmCloudContainer is assigned to a specific user who can access it and activate licenses from up to three active devices. If the user belongs to a group, e.g. a company, the group's admins can manage the CmCloudContainer and its licenses.

Enterprise CmCloudContainer

Enterprise CmCloudContainers are meant for use by multiple users, making them the containers built for concurrent licenses.

On CodeMeter License Portal, Enterprise CmCloudContainers are assigned to groups whose members can access them from their devices. The groups' admins have the right to manage the CmCloudContainers, including the rights to activate or deactivate licenses, add or remove users, or reset the access data needed to connect to a CmCloudContainer.



A SAW can be used to automatically restore the link between a device and the CmCloudContainer when the access credentials have been reset. This usually becomes relevant when a user is removed from a group and has to be restricted from continuing to use the licenses.

Options for a Floating Network Server

CodeMeter offers three ways for clients to run a floating network server:

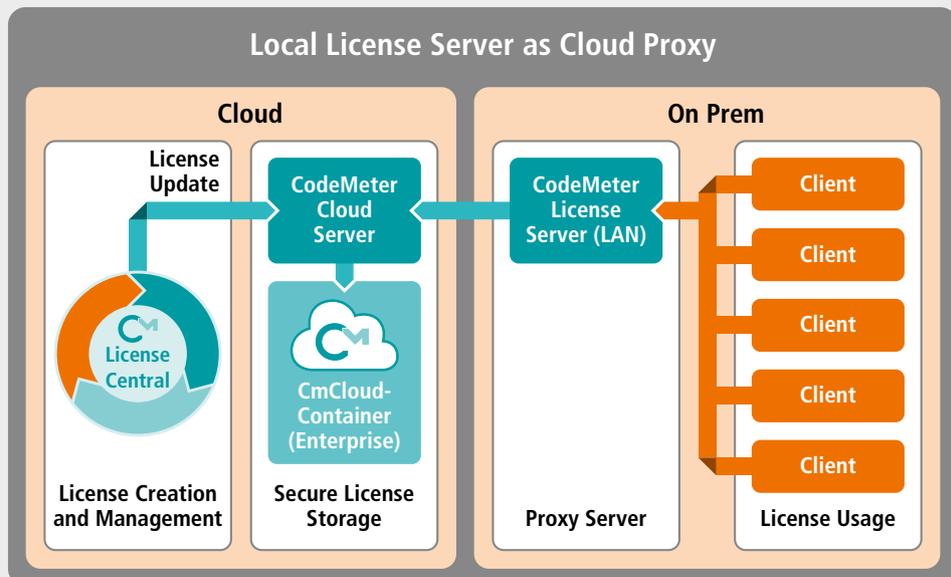
- A local license server with a CmActLicense
- A local license server as proxy for a CmCloudContainer

- Direct access to a CmCloudServer

All three options have specific advantages and drawbacks that will help you decide which fits your scenario best. As licenses are all managed in a similar fashion in CodeMeter License Central, the choice does not have to be final: You can decide on a case-by-case basis and change your choice at any time. You can even allow your clients to do so themselves.

Local License Servers

In this case, CmActLicenses are activated on a license server and bound to that server. This



removes the need to capture a fingerprint of every end user's system.

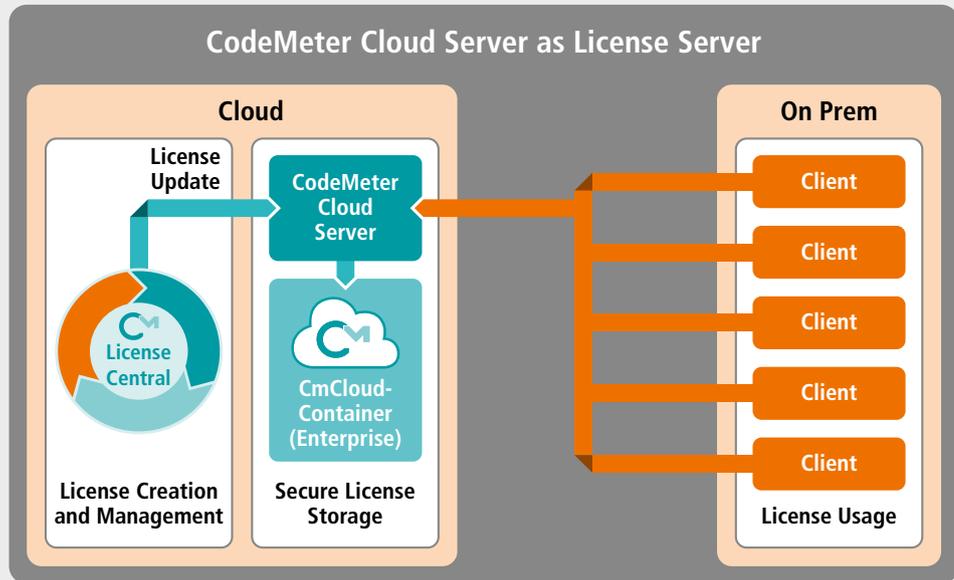
CodeMeter Runtime is configured as a license server on the local server. Clients on the same subnetwork can access the licenses immediately, whereas clients on other subnetworks need the name or IP address of the license server to use the licenses. The necessary settings can be configured via CodeMeter.

Access to the licenses on the license server can be managed by an admin, e.g., by allocating licenses to specific systems, IP addresses, Active Directory (AD) users, or AD groups. Local license usage tracking is also available to keep track of how licenses are used.

Local License Server as Proxy

This option resembles the CmActLicense configured as a local license. In this case, an Enterprise CmCloudContainer is imported onto the license server. License configuration, access, and usage tracking are managed in exactly the same manner as in the purely offline scenario. The only difference is that the proxy license server needs a connection with the CmCloudServer.

When users are removed, they will lose access to the internal proxy. Nothing else has to be re-configured in that case. Conversely, when new users are added, they can access the licenses for their AD groups immediately.



Alongside offline usage tracking, you can also capture usage data through the cloud.

Direct Access

The third and final option needs the users to have direct access to the Enterprise CmCloudContainer. This removes all the features provided by the local license server, including AD integration, offline use, and offline usage tracking. However, as in the case of a proxy server, you can use online usage tracking and enforce license updates with an auto update trigger. The advantage of this option is that no VPN connection is needed, as it was in the other two cases, should mobile access to licenses be needed.

Highest Security

CodeMeter offers a variety of ways to achieve top security against reverse engineering and piracy. These include the ability to take particularly sensitive code and have it executed inside a CmDongle (CodeMoving). Everything critical happens inside the dongle and only the output is returned into the wild, so that no attacker could analyze the code in that brief moment it is executed. The use cases outlined for CmActLicenses can also be realized with CmDongles. For performance reasons, CodeMoving is only available for single user licenses with CmDongles; with CmCloudContainers, it is an option if Personal CmCloudContainers are used or, in the case of Enterprise CmCloudContainers, if direct access to the CmCloudContainer is available as in the third case above.

The Three Options at a Glance			
Feature	Local	Proxy	Cloud
License Creation via Cloud	Yes	Yes	Yes
License Update via Cloud	SAW	Automatically	Automatically
Offline Usage	Yes	Partially	N/A
Access Control with AD Integration	Yes	Yes	N/A
Mobile Office Support	Via VPN or Borrowing	Via VPN	Yes
Highest Security (CodeMoving)	N/A	N/A	Yes
Offline License Tracking	Yes	Yes	N/A
Online License Tracking	N/A	Yes	Yes

WIBU NEWSLETTER

Do you want to receive more frequent updates from our WIBU world?

Subscribe to our newsletter





CodeMeter Licensing in Kubernetes

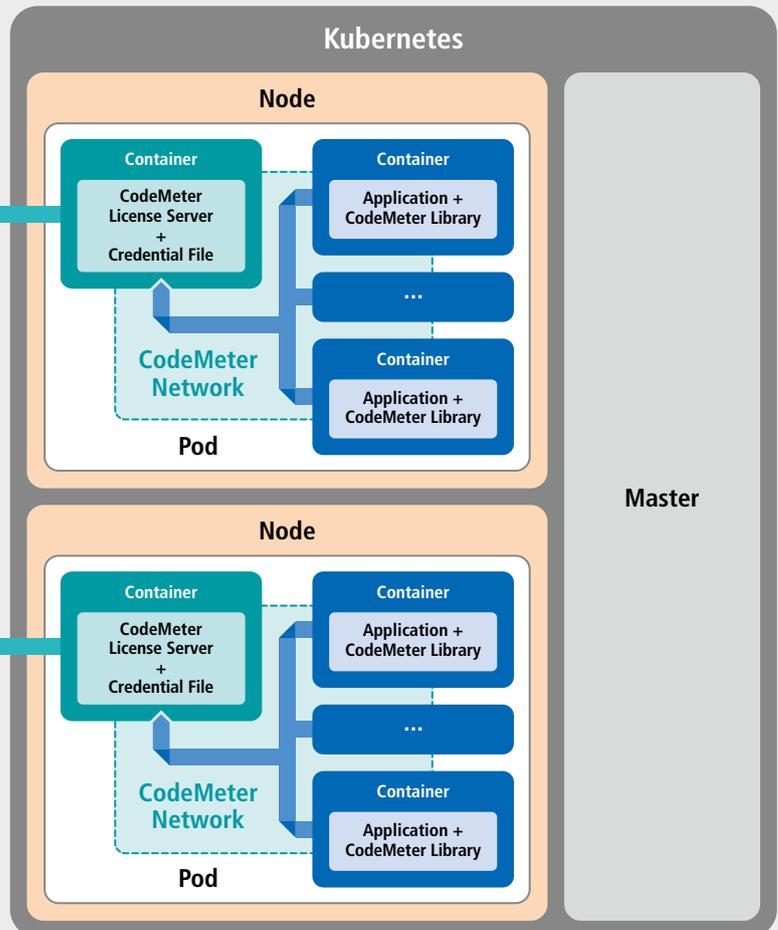
Kubernetes?

Kubernetes is a powerful open-source platform for orchestrating containers, developed to make it easier to roll out and manage applications in distributed environments.

Originally created by Google and handed over to the open-source community in 2014, Kubernetes has caused a stir in the world of DevOps and containerization.

The basic thinking behind Kubernetes is that container applications can be organized in groups, called pods. These pods can be used on an infrastructure, be it in the cloud or in a local data center. Kubernetes takes care of automated scaling, load balancing, rolling updates and rollbacks, which makes for flexibility, tolerance, and high availability.

Self-recovery functions keep applications stable and responsive. Kubernetes offers a versatile and sustainable choice for modern application architectures and has become an important tool for managing complex applications around the globe efficiently.



Protection and Licensing

In distributed environments, the ability to protect one's intellectual property and enforce license restrictions is even more critical than elsewhere. We can rely on the tried-and-true AxProtectors of CodeMeter Protection Suite to run protected applications safely in Kubernetes environments.

The challenge is: How to provide the necessary CodeMeter licenses in a Kubernetes environment? In Kubernetes, there are lots of containers, each providing a specific function or micro service. To use CodeMeter, one needs a working CodeMeter license server. That license server is usually run in its own container, while the other protected and licensed services or applications are placed in other containers.

For the application containers to be able to access the CodeMeter license server in a different container, the variable CODEMETER_HOST needs to be set properly and a dedicated network set up. KEYnote 42 has more information about how this is done.

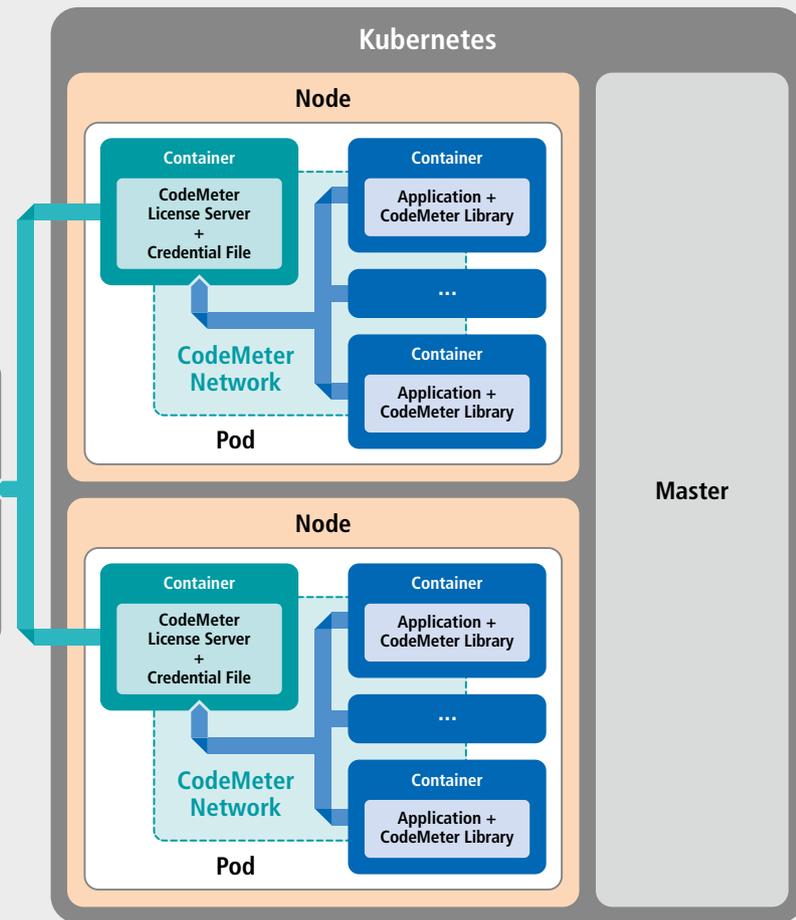
CodeMeter License Server

When designing your own Kubernetes cluster, it is essential to pay attention to the right licensing process. In larger projects, there will likely be a need to run several CodeMeter license servers at the same time, possibly one per pod. Which design fits depends on your needs in terms of redundancy, performance, and the available resources.

Alongside the CodeMeter license server, the licenses themselves also need to be available. These are kept in CmContainers, either in hardware form in a CmDongle, in activation-based CmActLicenses, or in a CmCloudContainer accessed over the Internet. All of these CmContainer types are cryptographically identical for the Universal Firm Code, which means that the licenses in question can be provided in the right CmContainer for each case in hand. The right choice of CmContainer for Kubernetes depends on how and where Kubernetes is used.

Kubernetes in the Cloud

Leading cloud providers AWS, Microsoft Azure, and Google Cloud offer a range of comfortable ways to manage services via Kubernetes, including the means to prepare the system as



easily in the cloud as one would on a local system. For containers running in the cloud, which would mean constant Internet access, CmCloudContainers are the perfect choice. Wibu-Systems operates CmCloudContainers in a private cloud with exceptional availability guarantees. All cryptographic operations and the necessary keys remain safe in that private cloud, and licenses can be activated easily through the CodeMeter License Portal. The individual CodeMeter license servers only need the access details to the CmCloudContainers, which can be provided in image form. The service is billed by the number of simultaneous license accesses, captured in the form of "seats".

Kubernetes On-Site

For an in-house installation of Kubernetes, CmCloudContainers can also be used to gain all of the advantages mentioned above. This does, however, depend on constant Internet access. If that is a risk you are not willing to take or if you want to be independent of the global infrastructure, there are two options at your disposal: CmDongles or CmActLicenses.

Many software developers want to provide their software and licenses in a Kubernetes-ready form without having to account for external dependencies. Why they do so is evident:

They want full control over everything in the container environment and use Kubernetes without any other requirements complicating their chosen method.

A CmActLicense requires a unique and copy-proof anchor to be encrypted and properly bound to avoid simple duplication. Container environments, by their very nature, are designed to make everything as abstract as possible and to switch to and from between systems. The end result is that the necessary anchors are hard to find. For Docker installations, Wibu-Systems has already delivered an innovative solution (reviewed in KEYnote issue 42). That Docker-specific mechanism does not, however, work with Kubernetes. Older binding options, like binding licenses to hard drive serial numbers or the like, are also too easy to simulate. Kubernetes and, in particular, its fundamental containerization technology are also open-source, which means that it is easy to analyze, imitate, and circumvent any mechanisms of this type. In essence, CmActLicenses cannot be used with any meaningful security in Kubernetes and are therefore not offered in this specific scenario.

The remaining option is to handle licensing outside of Kubernetes. As explained, one or more

CodeMeter license servers can be provided as containers. These can connect with CodeMeter license servers kept on physical systems (not containers and ideally not virtual machines). This makes it possible to bind the licenses to a fingerprint of the actual, physical system properties with the patented CodeMeter SmartBind technology.

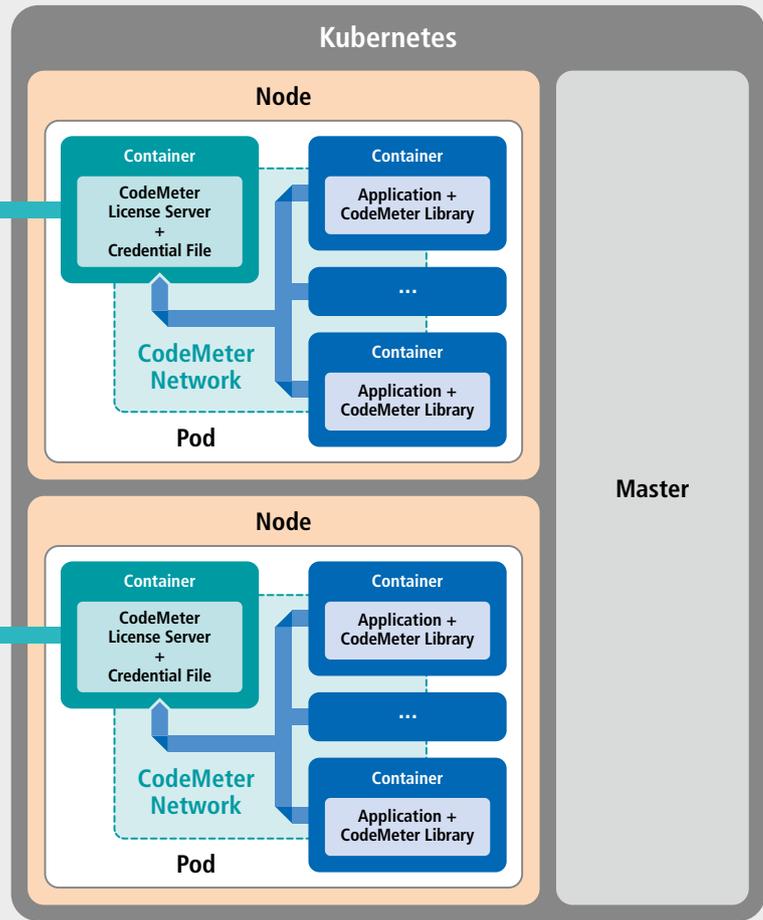
A CodeMeter license server included in the network can also be used for CmDongles in order to access the licenses stored on them within Kubernetes. A popular method for this is connecting the CmDongle via USB-over-Ethernet. A device like the SEH DongleServer can be used to access the CmDongle via TCP/IP from a container in Kubernetes. This solution works even when a container is at rest, as it only needs the connection to be set again.



For high availability of local licenses even during OS maintenance, a TMR server can be integrated in all of this. Read the article on TMR servers in this issue of KEYnote to learn more about this.

Different options

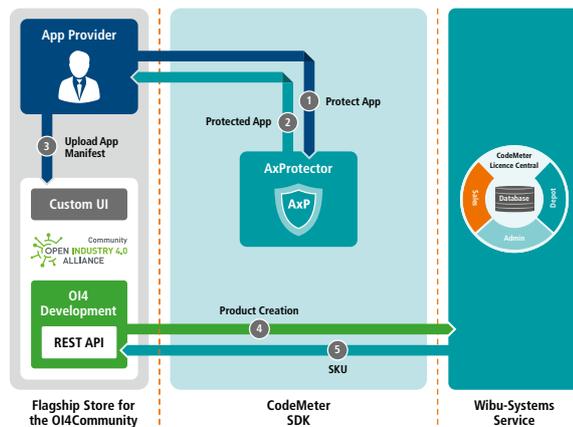
CodeMeter licenses can be integrated outside of Kubernetes by providing licenses through the cloud or through CodeMeter license servers kept on physical systems. This makes licensing secure and reliable. The careful planning and selection of the right channel for licensing purposes is critical for high-availability applications in Kubernetes systems and for intellectual property to be secure and license terms enforced.

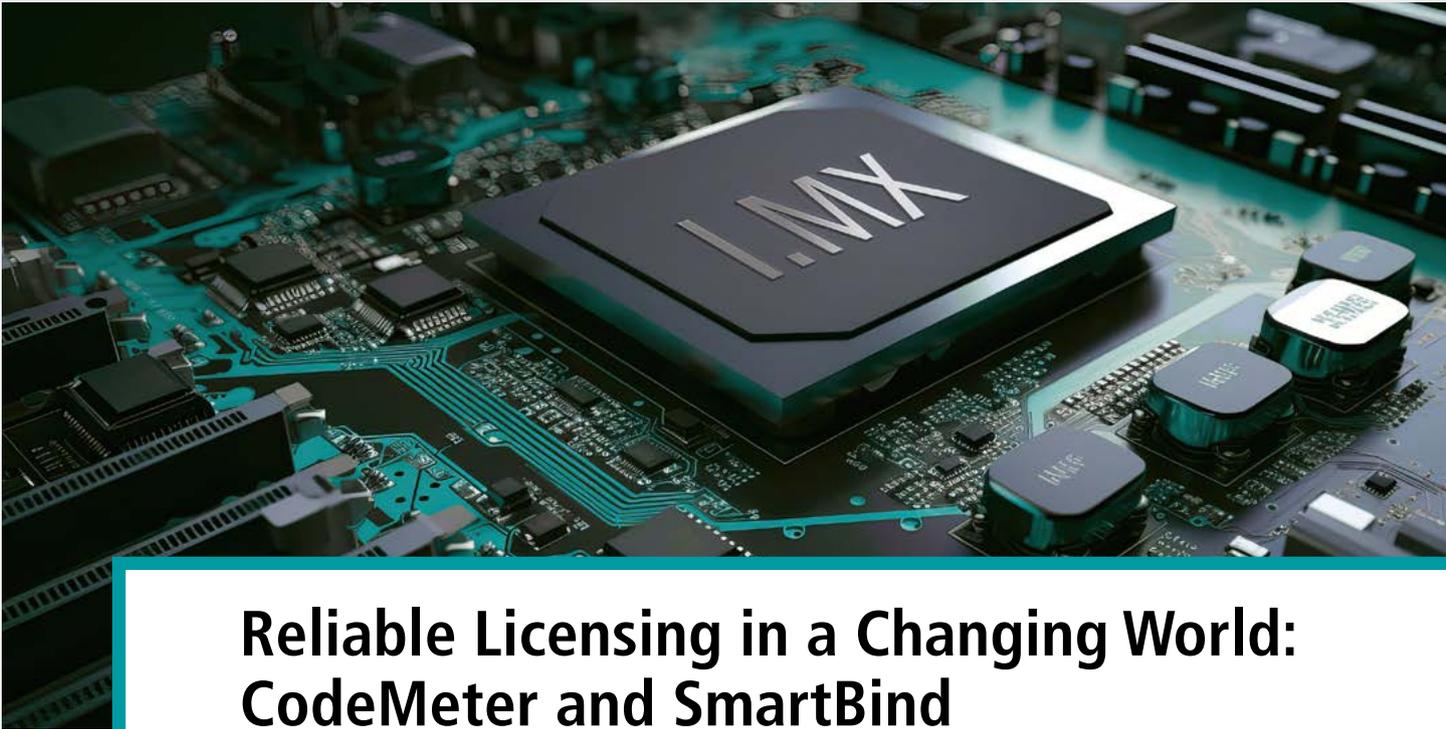


Flagship Store for the OI4 community

In alliance with other key members of the Open Industry 4.0 community, Hilscher and Wibu-Systems are developing an open platform, designated as the Flagship Store for the OI4 community. This initiative promises to accelerate the journey for all stakeholders toward a fully integrated, digital, interconnected, and secure production landscape.

Their collaborative approach aims to benefit everyone, from the on-the-floor app users grappling with productivity challenges and skill shortages to app providers eager for secure yet uncomplicated entry into the digital manufacturing sector. Critically, their partnership ensures robust safeguards for the intellectual property encoded within the software solutions.





Reliable Licensing in a Changing World: CodeMeter and SmartBind

Wibu-Systems' patented SmartBind technology allows CodeMeter to automatically recognize and bind licenses to the target system. The technology reads out the system environment and creates a digital fingerprint with a range of traits and properties given different weighting in the formula. These properties can be the ID of the CPU or the motherboards, the serial numbers of memory chips, the MAC addresses of network adapters, or other values. The resulting fingerprint also leaves some leeway for swapping out or servicing individual components. Software developers can choose between "loose", "medium", and "tight" binding to match the strength of the binding to the expected number of hardware changes on the target devices.

Made to match the environment

Wibu-Systems is constantly improving support for supported system environments. In addition to the popular operating systems like Windows, macOS, or Linux, CmActLicenses can be used in virtual environments like Azure, AWS, and Google Cloud. IoT devices are also still gaining traction and need protection and licensing for the sophisticated software that usually runs on them.

Up and coming: i.MX processors

Wibu-Systems is always improving its SmartBind mechanism to cover the entire range of use cases from cloud services to personal computers or IoT devices. One recent example of

added enhancements is the adjustment made for i.MX processors. After hearing back from clients who use i.MX in a range of scenarios, Wibu-Systems integrated the systems in its test environments, identified necessary changes to the binding scheme, and introduced the new capabilities within only a handful of days.

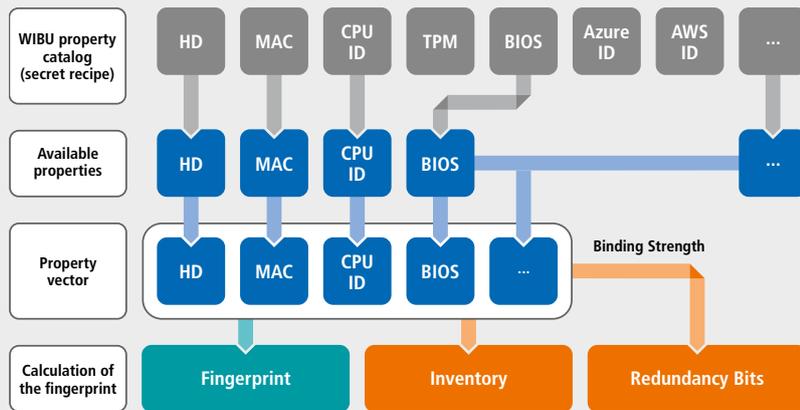
CodeMeter 7.60c introduced automatic extended binding for boards with i.MX processors, which uses the components' processor ID as one of the identifying properties.

The ongoing evolution of CodeMeter SmartBind mechanism continues at a rapid pace: The new version CodeMeter 8.00 will include unique identification for boards with i.MX processors or related models.

Wibu-Systems is always working on evaluating several secure elements that are used on some boards equipped with i.MX processors, which could be a means for a particularly strong binding for digital licenses.

Flexible and secure

Combining CmActLicenses and SmartBind is the robust choice for a range of environments. The continuous improvement and evolution of the technology by Wibu-Systems ensure that the licensing capabilities will always keep pace with the requirements of today's tech landscape. The recent changes for i.MX processors and coming developments like the integration of unique markers keep CodeMeter the gold standard for secure and flexible software licensing. 



News in Brief

New White Paper – CodeMeter Certificate Vault

Certificates are used to authenticate and identify users or devices on the Internet, in emails, machine-to-machine communication, and elsewhere. CodeMeter Certificate Vault provides a secure means to store X.509 certificates on CodeMeter hardware and make them available via standard interfaces. This white paper delves into the guiding principles and challenges of secure certificate storage and the technology and use cases for CodeMeter Certificate Vault.



New Brochure – Cybersecurity in Medical Care and Life Science

We provide cutting-edge security solutions for several industries, including medical technology, healthcare, and life sciences. Leveraging CodeMeter technology, we protect IP, commercial viability, and more importantly, patient health and safety. This field involves years of research, considerable resources, and vast investments; our solutions guard against theft, piracy, and tampering, which are crucial for both business success and societal wellbeing. As AI and Machine Learning advance, our protections extend to data models, ensuring comprehensive security.



Our First Time at WeAreDevelopers

With over 12,000 attendees and 500 speakers, the event delivered on its promise to energize a passionate developer community. Rather than focusing solely on tech gadgets or coding skills, WAD emphasized the value of human connections within the industry. Attendees seized the

chance to network, share ideas, and collaborate. We showcased our Kerckhoffs' compliant Blurry Box demonstrator and joined two panel discussions, exploring new work paradigms and the impact of AI on modern businesses.



Sponsoring the German Federal Computer Science Competition

Investing in education is the cornerstone for ensuring a future filled with prosperity and opportunity. We were immensely honored to host an elite gathering of remarkable students, highly respected jury members, and eminent IT scholars at our headquarters on September 12th on the eve of the final round for the 41st German National Computer Science Competition. Out of the 25 standout students hailing from various parts of Germany and all united by their shared zeal for IT, one gifted young man or woman would advance to the IT Olympics after a decisive final examination at the Karlsruhe Institute of Technology.



Our Support for Code.org

Wibu-Systems USA supports Code.org, an NGO aiming to make computer science a core part of K-12 education for all students. Based in Seattle, the publicly funded organization is especially focused on promoting participation among young women and other underrepresented groups. Code.org offers an array of activities, workshops, and projects globally for students and teachers to advance their educational objectives. The organization makes a substantial impact, with over 80 million students and 2 million teachers participating in its community.



Germany's Supply Chain Due Diligence Act

Enacted on January 1, 2023, Germany's Supply Chain Due Diligence Act (LkSG) seeks to elevate human rights and environmental safeguards in the global economy. Wibu-Systems not only meets RoHS, REACH and Conflict Minerals Environmental standards but also demonstrates a deeper commitment to broader ethical and corporate responsibilities. This includes stringent anti-bribery and anti-corruption measures, environmental stewardship, respect for human rights, occupational health and safety, supply chain accountability, conflict of interest management, robust cybersecurity, data privacy, and business continuity planning, thus exceeding the requirements of the Responsible Business Alliance in its most recent version (see www.responsiblebusiness.org/code-of-conduct).



Anne-Lise Buchheit 90th Birthday

Founded in 1989 by university colleagues with expertise in electronics and information technology, Wibu-Systems takes its name from the surnames of its co-founders, Winzenried and Buchheit. The company's enduring vitality isn't solely a result of their leadership; it's also fueled by the active involvement of their families. Marcellus Buchheit's mother, Anne-Lise, serves as an invaluable Board member to this day, and her spirit along with her business administration education greatly enrich the enterprise. A heartfelt thanks to Anne-Lise for her enduring commitment and influence!





Case Study | ETM professional control

The Challenge

The WinCC Open Architecture stands behind some of the most complex, distributed, and remotely operated SCADA systems running critical infrastructures everywhere in the world. The software technology landscape is rapidly evolving towards the utilization of cloud systems, providing shorter time-to-market and update cycles. Modern operating environments like Docker containers or container clusters, require open and flexible software that is robust enough to protect against fraud while supporting a wide range of platforms, from ARM to x86 on the hardware side and Windows and Linux from an operating system standpoint. The modular structure of WinCC OA facilitates installation growth, easy maintenance, and deployment. The licensing system should be flexible



Dr. Bernhard Reichl, CEO, ETM professional control

"Our SCADA product SIMATIC WinCC OA uses CodeMeter for license generation and protection, enabling us to expand our global business together with our partners. With CodeMeter, not only are we protected against unauthorized usage, but the technology of Wibu-Systems also secures the valuable know-how of our integration partners' solutions."

so that new functions can be added effortlessly. This results in a wide range of items that can be combined in a specific WinCC OA product license.

The Solution

ETM professional control has chosen CodeMeter as a powerful replacement of their home-grown solution to meet the new requirements, providing uniform and fully aligned protection and licensing capabilities across all relevant systems and platforms, ranging from ARM to x86, running on Windows and Linux, and from the smallest IoT device to the cloud. CodeMeter's ability to ensure secure licensing even in distributed and decentralized setups, range of license containers, and its effective integration with ERP systems give users in the field a flexible choice of ways to manage their licenses and tailor their systems perfectly to their projects' needs.

The Success

Robustness and adaptability: Two characteristics that Wibu-Systems and ETM professional control have in common. The integration of CodeMeter as a protection and licensing solution provides a new level of flexibility and convenience with the ability to tailor licenses to specific requirements with true granularity. Always keeping its finger on the pulse, WinCC Open Architecture, protected by CodeMeter, enables them to respond to the rapidly evolving demands of the software technology landscape. As technology and regulatory requirements constantly adapt, so do business models. Thanks to the agile CodeMeter system, ETM professional control can provide a seamless and easy-to-use customer journey. 



CodeMeter Trainings

Wibu-Systems offers custom training to get you off to a running start with CodeMeter software protection and licensing. The training is offered in the form of company courses, typically hosted as in-house classes on your premises. The standard training program includes three days of courses, which can be adjusted to your needs and level of expertise. You can pick and choose the contents you need and shorten the program to 1 or 2 days. Alternatively, you can add a hands-on workshop to allow your participants to try out their own practice cases.

For an up-to-date overview of our workshops, visit mycodemeter.com/workshop/.

Contact our local representatives for training courses on site

WIBU-SYSTEMS AG
Germany
+49 721 931720
info@wibu.com

WIBU-SYSTEMS (Shanghai) Co., Ltd.
Shanghai: +86 21 5566 1790
Beijing: +86 10 8296 1560/61
info@wibu.com.cn

WIBU-SYSTEMS LTD
United Kingdom | Ireland
+44 20 314 747 27
sales@wibu.systems

WIBU-SYSTEMS USA, Inc.
USA: +1 800 6 Go Wibu
+1 425 775 6900
sales@wibu.us

WIBU-SYSTEMS BV/NV
The Netherlands: +31 74 750 14 95
Belgium: +32 2 808 6739
sales@wibu.systems

WIBU-SYSTEMS
Spain | Portugal
+34 91 123 0762
sales@wibu.systems



www.wibu.com/tr

WIBU-SYSTEMS K.K.
Japan
+81 45 565 9710
info-jp@wibu.jp

WIBU-SYSTEMS sarl
France
+33 1 86 26 61 29
sales@wibu.systems

WIBU-SYSTEMS
Scandinavia | Baltics
+46 8 5250 7048
sales@wibu.systems

Join Wibu-Systems at the following events:

sps
14-16 November 2023
Nuremberg, Germany

Hannover Messe
22-26 April 2024
Hanover, Germany

Embedded World
9-11 April 2024
Nuremberg, Germany

MedtechLIVE
18-20 June 2024
Stuttgart, Germany

Wibu Academy

The Wibu Academy is a platform for courses and training delivered by Wibu-Systems top experts on hot topics that are in line with the goals of the House of IT Security: boosting IT security in research and practice. The range of sessions is split into two separate paths:

- Cybersecurity in life applications – from the basics of cryptography and secure software development to AI security and Post Quantum Cryptography
- Publicly funded research projects – best practices for application and management



www.wibu.com/wibu-academy.html

Wibu-Systems' Masterclasses

Also, our monthly fully immersive masterclasses focus on unique content and are designed for beginner, intermediate, or advanced users of our CodeMeter technology. The 2023/2024 season will cover areas such as cloud licensing, triple mode redundancy, post-quantum cryptography, CodeMeter certified third-party containers, and a lot more. Watch out for our forthcoming announcements either on our website or via newsletter and get ready to register for the sessions that are most helpful to you.

Imprint
KEYnote 46 Issue
Fall/Winter 2023

Publisher
WIBU-SYSTEMS AG
Zimmerstrasse 5
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
Stefan Bamberg
Matthias Honka
Ruediger Kuegler
Andrej Krasnik
Bernhard Loewe
David Paine
Karl-Friedrich Press
Daniela Previtali
Florian Schneider
Wolfgang Voelker
Oliver Winzenried

Design
Eugen Olchin

Print
PASSAVIA Druckservice GmbH & Co. KG,
Passau, Germany

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.

BlurryBox®, CmReady®, CodeMeter®, Smart-Bind®, SmartShelter®, and Wibu-Systems® 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.

Copyright © 2023 Wibu-Systems. All rights reserved.

Picture credits:
Midjourney

All remaining images are copyrighted by their owner

SECURITY
LICENSING
PERFECTION IN PROTECTION

WIBU
SYSTEMS