



KEYnote 44

THE WIBU - MAGAZINE

Consumption-based licensing

Highlights

- License monitoring with CodeMeter
- Staging the software development process
- User hierarchies in the License Portal

WIBU
SYSTEMS

Content

CORPORATE

New IT Infrastructure for Wibu-Systems 4

LICENSING

Consumption-Based Licenses 5

LICENSING

License Monitoring with CodeMeter 7



LICENSING

Staging the Software Deployment Process 9



PROTECTION

Cloud FSB 10

PROTECTION

Racing the Quantum Hare 11

LICENSING

User Hierarchies in the License Portal 13



HIGHLIGHTS

News in Brief 15

CASE STUDY

Daimler Buses 17

INFORMATION

Wibu-Systems Training 18

Dear Clients and Partners!



Regular innovation is a crucial ingredient for our growth and we have a track record to show for it, as we documented by winning the German Innovation Award for CmCloud and AxProtector JavaScript. A different type of innovation can be seen in the cooperative work done in our IT Security Club: www.wibu.com/itsc. This is your chance to get involved by becoming member!

This issue of the KEYnote magazine includes more details about our investments into our own IT and information security in accordance with the ISO27001 standard. You will also read about new products like the License Portal with reseller integration, the choice of hosting packages for CodeMeter License Central, the option of using a CodeMeter FSB in the cloud, license monitoring, usage reporting, and consumption-based licenses. And there's more: You can also discover our roadmap for post-quantum cryptography, read a great success story about the secure 3D printing of automotive parts from our work with Daimler, and lots of other news.

I wish you all a safe and healthy autumn and winter and lots of energy to help you master the challenges ahead. And we may see each other and have a chance to speak at one of the coming expos, such as Electronica, Medica, Formnext, or SPS.

Best regards,

Oliver Winzenried

CEO

Recently, the Karlsruhe IT Security Initiative came to us to ask whether they could lift the veil and show some visitors how we work our magic at a very special behind-the-scenes event here on the Wibu-Systems Campus. As one of the very few producers of security hardware in Germany, we are more than just pioneers for secure IT and software. We are ourselves a model for good practices in this area, and all of that without magic or trickery. We know which challenges exist in the procurement, processing, quality assurance, and certification of security hardware areas, and we can demonstrate how we overcome these challenges in our modern production facilities. In particular, we can answer the especially tough question of how we can put in place and maintain a completely secure lifecycle when manufacturing our products.

Wibu-Systems is a partner you can count on to supply you with products that will be available and will continue to be developed and updated long into the future. This is our promise even in these difficult times of strained chip supplies and price hikes. Our long-term approach to procurement is paying dividends now.

ALERT

One idea at the right time
can change everything.

Subscribe to our blog





New IT Infrastructure for Wibu-Systems

The new Wibu-Systems Campus in Karlsruhe was built to make working easier and more enjoyable – and that also goes for the all-new network infrastructure. The internal IT team has made Wibu-Systems fit for the challenges ahead.

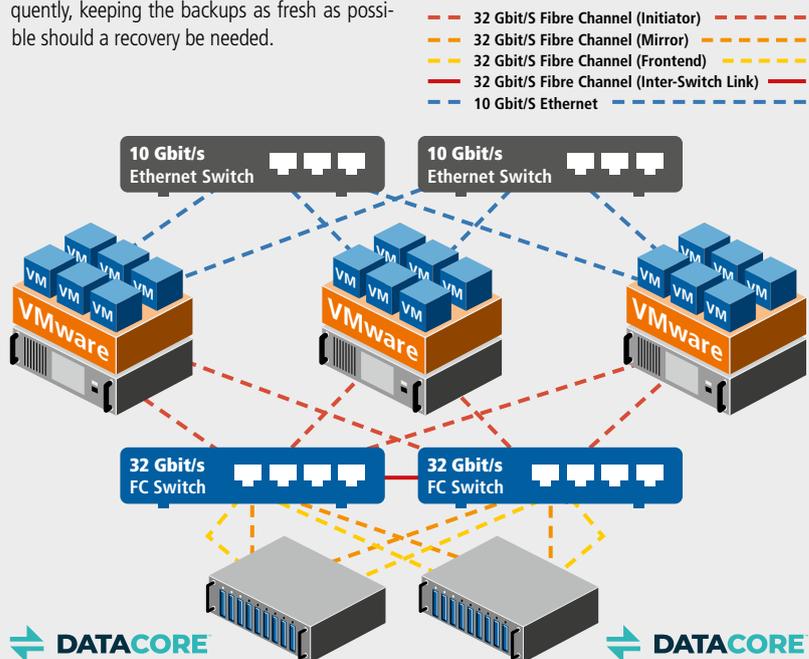
The move into our purpose-built head offices has brought not only a new work environment for the people of Wibu-Systems, but also realized a complete updating of the company's internal network infrastructure. The internal virtualization platform has been redesigned from the ground up, a change driven by the pursuit of greater availability, better load balancing, and the ability to recover faster and more reliably from failures or other incidents.

With the support of the service team of Leitwerk (<https://www.leitwerk.de>), our internal servers have a new, faster cluster with DELL hardware, datacore memory management, and VMware vSphere, which meets current standards and keeps the system scalable and fit for the future. As an added bonus, a Veeam backup solution was built right into the new setup.

The traditional 3-level approach was chosen specifically because of its tried-and-true reliability and the independence from individual hardware brands it offers. While the current hardware comes exclusively from DELL, it is not the only solution: When the system is expanded or updated later on, the technology can come from other makers, with a flexible choice of component providers.

All pieces of the system are linked by fast fiber connections. Virtual machines can be moved around at a moment's notice, and the system rapidly backed up or recovered. This means that critical machines can be backed up more frequently, keeping the backups as fresh as possible should a recovery be needed.

The chosen setup has put Wibu-Systems in a perfect place for smooth and secure operations in the coming years.





Consumption-Based Licenses

It is a story many of us have experienced in some form or another: In my college dorm, we did not have laundry. Instead, there was a laundromat on campus where all students could go to get their laundry done for a sum that even the poorer ones of us could afford. When one of those big washing machines broke down, it would be replaced. Would it have made financial sense for me to buy my own machine in that case? Most likely not. Would it have paid off to pay for a laundry service to do my laundry whenever I needed it, for some form of monthly payment? It might have, but then there were the months that I did not spend on campus. In the end, I was actually quite happy that I did not have to worry about moving a big old washing machine from my dorm room up on five flights of stairs.

It is the same story with software. How much is software worth? Does it make financial sense for us to buy a certain application? There are no blanket answers to these questions. The same software is not worth as much to one user as it is to another. It depends on the particular situation and how well the software on offer fits the actual use case. How often do I need to use it? Are there alternatives? Even the best software in the world is not right for me if I cannot afford it.

All of this makes pricing policy a crucial decision for vendors. Too high a price, and nobody will

buy the product. Too low, and you lose money with every sale. A true win-win outcome can only come about if the needs of the customer and the needs of the vendor are balanced.

Licenses make pricing flexible: Prices can be adjusted to fit the needs of customers, and bespoke solutions can be tailored to attract any type of target group.

One way of approaching this concept is Consumption-Based Licensing, or CBL for short. This article will look at CBL, how it differs from other

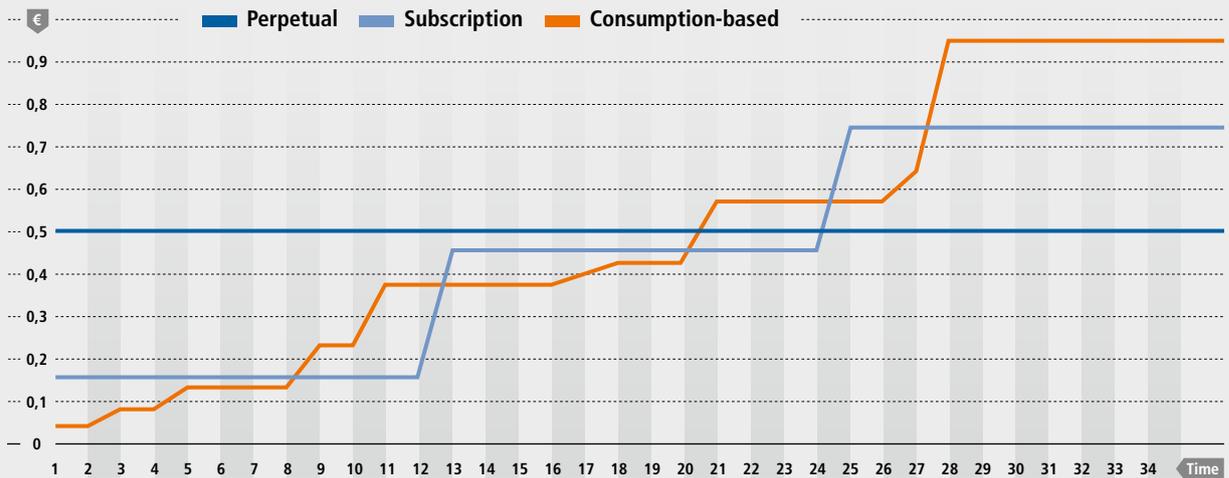
models, and its benefits and risks. It will also explain who CBL is a good choice for and how easy it is to sell software with custom CBL models.

What are Consumption-Based Licenses?

Consumption-Based Licenses are what is called a recurring-revenue model. Colloquially, they are also known as pay-as-you-go licenses. They are based on consumption in the sense that the users only pay for what they actually use.

Everybody knows the concept from e.g., paying for gas: Nobody wants to pay more at the pump than they got. Prepaid cellphone contracts are another type of consumption-based pricing: The customer gets a certain data contingent on usage and can increase it when needed. CBL

Sample Company		130-2598857357	CmActLicense/UFC 3.00		
Licenses		CmContainer Info		User Data	
6000947	Professional Service	Unit Counter	Valid Until	License Quantity	Feature Map
1001	Webinar Pay Per Click	10	n/a	1	0x1



can also be combined with other types of licenses. To stay with the last example, some cell-phone contracts require a monthly payment on top of the data package. For Infrastructure-as-a-Service providers (IaaS), CBL is becoming an increasingly attractive option. Users can e.g., buy additional server capacity when a limit is reached, or there are no limits, but the actual amount of data is tracked and must be paid for.

How do they differ from perpetual and subscription licenses?

CBL are quite unlike other types of licenses, like conventional one-off perpetual licenses or subscriptions.

With conventional licenses, the user pays once for the software and either becomes its outright owner or gets an unlimited, unrestricted license. In many cases, this is combined with a maintenance subscription. The traditional model is still the norm in B2B business, but it is fast falling out of fashion for consumers because of its drawbacks: There is no incentive for the developer to keep improving the product, and the upfront cost can be a too high threshold for some people.

Subscriptions are the more flexible option. With them, the user does not buy the software outright, but instead pays for a temporary right to use it. As long as the subscription is not cancelled, it keeps getting renewed, and the user can go on enjoying the software. For private consumers, this has become quite normal. Spotify, Netflix, or Adobe are just some of the big names in the market offering monthly service subscriptions. The advantage over a perpetual license is the lower entry threshold for new customers. And they receive a product that is always kept up to date. In turn, the providers have an easier time with attracting new customers and a steadier, more predictable cashflow. Subscriptions have proven their power as the fitting solution for balancing customer loyalty

and generating revenue with the needs of the end user in mind. The model is the right choice in particular for products that work with regularly updated content.

Why do I need CBL? What are its pros and cons?

In many cases, CBL can be the ideal choice for customers and vendors alike. This holds true in particular when the key factor is maximum flexibility in terms of volumes, usage periods, or the time of use.

Before going with a CBL model, one should consider whether a different model is a better fit to the specific conditions and requirements on the ground. Power users might benefit from paying for a full, perpetual license. Subscriptions might be better if the product is used steadily and regularly. CBL might be the best choice when flexibility is paramount.

The costs can develop in very different ways depending on the chosen model. The chart shows how perpetual licenses mean high upfront costs that stay the same over the entire period. A subscription comes at an initially low cost, but that cost is incurred repeatedly at regular intervals, whereas the costs of a CBL license would change and develop in response to the actual use. It is easy to see how the choice of licensing model depends on the needs of the user.

To return to our initial example: Neither buying a washing machine nor paying for a laundry service subscription would have made sense for me. The machine (or the service) would have gone unused during vacations or semesters spent abroad. Paying for actual use, i.e., for the laundromat, was the ideal choice for my flexible and changing demand for fresh laundry.

Companies can often benefit from CBL models. If there is no upfront fee at all, there is essentially no risk to it, and the entry threshold is mini-

mal. If the software is not used, you do not actually pay for anything. The software would typically be used when this promises a benefit that outweighs the cost of paying for it. In a sense, the software pays for itself during use. This makes CBL an easily calculated choice, as it links the investment directly with the gains. Flexibility and scalability are the great advantages here.

For companies whose demand and needs change by the season or with every project, CBL are a way to manage their cost situation by avoiding the need to spend money for software that is not used when the business is slow. And when things pick up again, the software is there, waiting to be used.

What do I have to do to offer CBL? What can Wibu-Systems do for me?

Wibu-Systems gives you an extremely easy way to sell your software with a consumption-based business model. Our CodeMeter License Central lets you cover all conceivable scenarios: Do you want to bill your clients for the period of use, or for the times that they use a certain feature? All this is easily done with Wibu-Systems technology.

You can learn more by watching the replay of our masterclass „How and Why to Create and Sell Consumption-based Licenses“ (<https://www.wibu.com/wibu-systems-webinars/consumption-based-licensing.html>) or by contacting our sales team, who will be happy to advise you.

Conclusion

CBL are an exciting way of getting your software into new markets and to new users with modern, flexible, made-to-fit licensing models. 



License Monitoring with CodeMeter

What is happening to your software out in the field? That is a question that many software developers and vendors are asking themselves – and not just out of pure curiosity.

Detailed insights into user behavior and preferences offer valuable information about the frequency of use or the popularity of individual features. Such analyses can help optimize products, focus on the components that are used most often, and adjust license models to the changing needs and expectations of users in the field.

CodeMeter offers a range of ways to track how licenses are treated and to limit how often and for how long they can be used.

License Tracking

License Tracking helps monitor how licenses are used by customers or users.

The CodeMeter License Server provides licenses through the network, with the number of usable licenses and metrics defined by the vendor. Possible metrics include the number of launched applications or the number of workstations (StationShare).

License Tracking is activated by the user. The CodeMeter License Server records every instance when a license is accessed or when it is denied, with detailed information about the user name, device name, or IP address, and the ID

of the license. The data can be accessed via an interface in CodeMeter WebAdmin for simple statistics (see image 1); more complex analytics can be obtained by exporting the license tracking data as a separate logfile (see image 3).

License Tracking for ISVs

In addition to greater transparency about costs, license tracking helps identify unused or missing licenses, giving software vendors new ways to optimize their licensing systems. Combined with overflow licenses (i.e., additional licenses that customers are allowed to use beyond the number they actually paid for), this helps track with precision and confidence which licenses are in use. The data facilitates billing after the agreed usage period.

License Tracking for Users

License tracking allows corporate users to assign and bill their licenses with granular precision to different cost centers within their organizations. With the data for the active licenses, the usage per license and cost center can be tracked with ease.

License Tracking Technique

License tracking uses a parser-friendly format to monitor all successful or failed license allo-

cations through the CodeMeter License Server. It creates a logfile from this data for later automatic analysis; the data itself can be transferred into formats that work well with third-party analytics tools or ERP systems.

License tracking monitors which licenses are available or in use down to the second, and it keeps track of which licenses are still out in the field or already returned to the CodeMeter License Server. Any changes in the form of updates are recorded, creating a virtual history of the license lifecycle.

License Tracking Security

License tracking captures data with cryptographic security to prevent any tampering by the user or other parties. This is done by signing the logfiles with the key stored securely on a CmDongle, in a CmActLicense, or in the CmCloud.

The captured data is transmitted back to the developer at regular intervals, making it available for analytical and statistical purposes. It is possible to validate the real-time data (see image 2).

Use Case: Product Management

Consider a software vendor who offers a selec-

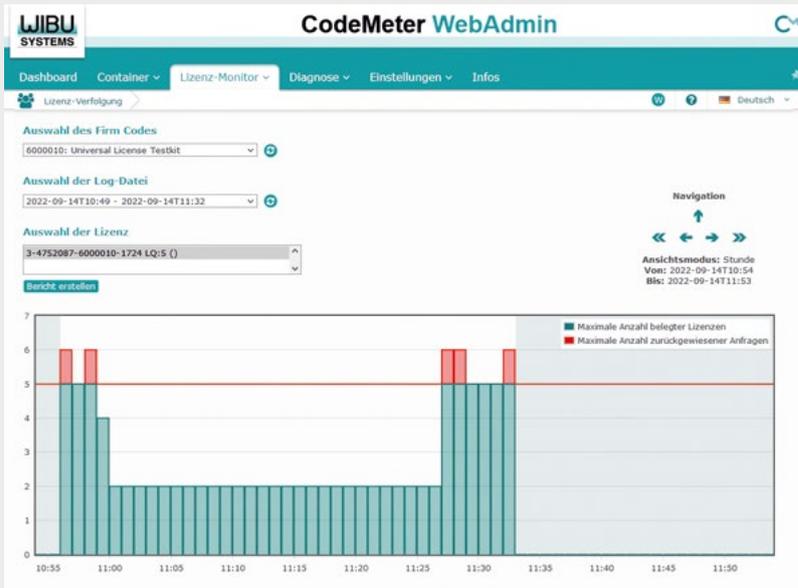


Image 1: Active and denied license allocations as viewed through CodeMeter WebAdmin

tion of products or modular licenses for the individual parts of a bigger software package. That vendor would want to know which product or which feature is used and how often. The License tracking data enables the vendor to precisely analyze this in detail, by users, by use periods, by feature, or even by the time of day. This allows invaluable insights for decisions about where to focus future development efforts.

The tracked data also reveals long-term trends in the use of licenses.

Use Case: Consumption-Based Licenses

Pay-per-use is a common way of billing for e.g., Internet or cellphone service providers, but it also has its uses for software licenses. The use of CmCloud licenses can be monitored directly through the cloud. But even without this direct thru-line, e.g., when the software is used in a cordoned-off, offline production environment, it can be analyzed with confidence afterwards. With the right contract terms in place, software vendors can get license tracking logs back from their users at regular intervals.

The analysis allows precise billing, down to the second. It can also track when licenses are moved around at a client. Even interim license upgrades or changes in the pricing structure are no problem for billing, as the actual activation times are recorded at the user.

Possible Applications

There are many situations in which License Usage Monitoring can be used to good effect. Retailers could, for instance, activate additional checkouts to cope with busy shopping periods in the run-up to Christmas. Or highly specialized software like that used in some construc-

tion and engineering jobs could be used and paid for by actual usage.

Simple Time Limits

Not all users will accept that the usage of their licenses is tracked in detail, and sometimes technical or operational reasons might make it impossible. In these cases, the software maker could simply limit the usage period for their licenses.

The Product Item Option "Unit Counter" lets license creators program licenses that are limited to a certain number of uses. When the protected software is launched, the counter de-

creases accordingly. Alternatively, this can be done through the CodeMeterAPI with an action chosen by the developer.

Software developers can also use the license to set time limits by letting the unit counter decrease at specific intervals during use. This is an easy way to implement different time-based license models. For instance, the limit could be set to a specific number of minutes or hours, and the counter would decrease by one unit for every minute or hour.

But the unit counter is not only good for enforcing limits. It also helps with consumption-based billing, e.g., by returning the license to the vendor after an agreed (and paid-for) period of use or by swapping out the license with a new incarnation after the usage period expires. The real in-use time can be calculated by the unit counter and billed accordingly with the chosen pricing model.

If modular license models are used, the usage time can even be limited or tracked for billing purposes for every single licensed function or feature.

You can find more information on our website or in our webinar on Consumption-Based Licenses, which took place in September 2022 and can still be accessed via our website.

```

C:\Users\jcydrive\c:\Users\jcydrive\Desktop\license_tracking_log_files
$ CmBoxPgm -vs17:pubkey.csv,licenseTrackingFC6000010_2022-09-14-104929.log
Started at 2022-09-15 14:00:37
CmBoxpgm has Version 7.51.5429.500
*** Validation of File "C:\Users\dabu\Desktop\license_tracking_log_files\licenseTrackingFC6000010_2022-09-14-104929.log"
*** Validation successful!
CmBoxpgm finished at 2022-09-15 14:00:37

```

Image 2: License Tracking Validation

```

LicenseTrackingFC6000010_2022-09-10-132035 - Editor
Datei Bearbeiten Ansicht
2022-09-20T13:20:35 SignedLogfile FirmCode:6000947, PublicKey: f17e92d3e20c30da53e98ba06155b27130b5532c4e8db640820a2a0000000061922d1682524b964010d4
*** New LicenseList: begin release all. ***
2022-09-20T13:20:35 ListOfLicenses
2022-09-20T13:20:35 License Server: "lap-rk-115.wibu.local", LicenseID:140-2568909601-6000947-16, SN:140-2348547282, FC:6000947, PC:1002, PH:1, ET:neve
2022-09-20T13:20:35 License Server: "lap-rk-115.wibu.local", LicenseID:140-2568909601-6000947-16, SN:140-2568909601, FC:6000947, PC:1001, PH:2, ET:2022
2022-09-20T13:20:35 License Server: "lap-rk-115.wibu.local", LicenseID:140-2568909601-6000947-19, SN:140-2568909601, FC:6000947, PC:1001, PH:2, ET:neve
2022-09-20T13:20:35 License Server: "lap-rk-115.wibu.local", LicenseID:140-2568909601-6000947-20, SN:140-2568909601, FC:6000947, PC:1001, PH:2, ET:neve
2022-09-20T13:20:35 License Server: "lap-rk-115.wibu.local", LicenseID:140-2568909601-6000947-17, SN:140-2568909601, FC:6000947, PC:1111, PH:0, ET:neve
2022-09-20T13:20:35 License Server: "lap-rk-115.wibu.local", LicenseID:140-2568909601-6000947-18, SN:140-2568909601, FC:6000947, PC:1309, PH:0, ET:neve
*** New LicenseList: end of previous Accesses. ***
2022-09-20T13:21:49 Access Server: "lap-rk-115.wibu.local", LicenseID:140-2568909601-6000947-20, AccessID:140-2568909601-6000947-20-1, Client:"127.0.0.1"
2022-09-20T13:21:49 Signature: Signature:cf495c309240ba3735afce51a204596a14d22c0aba15115a000000005ae7d9c041a8f5d56c72193a16165697b21833180E
2022-09-20T13:21:50 Denial Server: "lap-rk-115.wibu.local", LicenseID:140-2568909601-6000947-20, Client:"127.0.0.1", User:"XIBU/vrk", AppID:0, AppText:
2022-09-20T13:21:50 Release Server: "lap-rk-115.wibu.local", AccessID:140-2568909601-6000947-20-1
2022-09-20T13:22:50 Access Server: "lap-rk-115.wibu.local", LicenseID:140-2568909601-6000947-20, AccessID:140-2568909601-6000947-20-2, Client:"127.0.0.1"
2022-09-20T13:22:50 Signature: Signature:08a5c8281c05f639f41d747a9c954021895400016781137000000000011ebac549844a95f87c0b48cc0f50a273b3a1
2022-09-20T13:22:51 Denial Server: "lap-rk-115.wibu.local", LicenseID:140-2568909601-6000947-20, Client:"127.0.0.1", User:"XIBU/vrk", AppID:0, AppText:
2022-09-20T13:13:17 Release Server: "lap-rk-115.wibu.local", AccessID:140-2568909601-6000947-20-2
2022-09-20T13:13:17 Signature: Signature:2255c5848b070f43650806e1244a5015096216c7077478a2a36772500000000595efebef572aa762855c2d307f4cc936680b609ff
*** New LicenseList: begin release all. ***
2022-09-21T07:08:15 ListOfLicenses
2022-09-21T07:08:15 License Server: "lap-rk-115.wibu.local", LicenseID:140-2568909601-6000947-16, SN:140-2568909601, FC:6000947, PC:1002, PH:2, ET:2022
2022-09-21T07:08:15 License Server: "lap-rk-115.wibu.local", LicenseID:140-2568909601-6000947-20, SN:140-2568909601, FC:6000947, PC:1001, PH:2, ET:neve
2022-09-21T07:08:15 License Server: "lap-rk-115.wibu.local", LicenseID:140-2568909601-6000947-17, SN:140-2568909601, FC:6000947, PC:1111, PH:0, ET:neve
2022-09-21T07:08:15 License Server: "lap-rk-115.wibu.local", LicenseID:140-2568909601-6000947-18, SN:140-2568909601, FC:6000947, PC:1309, PH:0, ET:neve
*** New LicenseList: end of previous Accesses. ***
*** New LicenseList: begin release all. ***
2022-09-21T07:08:18 ListOfLicenses
*** New LicenseList: end of previous Accesses. ***
*** New LicenseList: begin release all. ***
2022-09-21T08:40:09 Signature: Signature:f02948e68236311fcb7a9c95402189540001678113700000000096154889b3a3e7814709f24ab810bc0e665e4f
2022-09-21T08:40:09 ListOfLicenses
2022-09-21T08:40:09 License Server: "lap-rk-115.wibu.local", LicenseID:130-3313947415-6000947-16, SN:130-3313947415, FC:6000947, PC:1001, PH:1, ET:neve
*** New LicenseList: end of previous Accesses. ***
2022-09-21T08:40:10 Access Server: "lap-rk-115.wibu.local", LicenseID:130-3313947415-6000947-17, AccessID:130-3313947415-6000947-17-1, Client:"127.0.0.1"
2022-09-21T08:40:10 Signature: Signature:083ecb13999e0e64c5079e2f881a9995386962494c5a080143765000000001f0b5f801fe474800e08c20c56489446c0ae1313
2022-09-21T08:40:10 Release Server: "lap-rk-115.wibu.local", AccessID:130-3313947415-6000947-17-1
2022-09-21T08:50:39 Access Server: "lap-rk-115.wibu.local", LicenseID:130-3313947415-6000947-17-2, AccessID:130-3313947415-6000947-17-2, Client:"127.0.0.1"
2022-09-21T08:52:59 Signature: Signature:f8a2fb20e99726495a83cbfcc18c3d375668c83dad28cf5e02b00000000005bc3a38a9f9262981c677b644c8e58a1bdcb111
2022-09-21T08:52:59 Release Server: "lap-rk-115.wibu.local", AccessID:130-3313947415-6000947-17-2

```

Image 3: Excerpt from a logfile



Staging the Software Deployment Process

Setting up a new system in an untouched greenfield environment is like playing in god mode. All components are perfectly matched up with each other. Everything has the right version. All tests can be conducted at leisure and everything is checked and cleared with real peace of mind. “Going live” is almost a formality, as the system used for development and testing is simply elevated to be the production system. But what happens in the messy reality of multiple product cycles bringing in new extensions and updates over the course of a product’s life? Interfering with the working system is not really an option and the entire experience feels like open-heart surgery . The better choice is a dedicated staging process.

When new products or systems are developed, they go through a long series of specific steps until they are finally finished and ready to be released. From the development of each component and the complex and lengthy tests involved to the final clearance checks and release, a product’s lifecycle is essentially a long sequence of individual process cycles. Ideally, each phase has its own, separate server environment to avoid unwanted effects slipping through and cross-infecting later phases in the cycle.

Developers do their work on a separate development system – D – under specific, known conditions, such as a specific version of the operating system, a specific compiler, or a certain set of libraries and frameworks. On the D system, the developers create the individual states of the software up to the final release.

Quality assurance again happens on another,

completely separate system – Q – which has the same conditions and parameters as the D system. The Q system conducts the tests and clears each state in the process up to the final version. Once that clearance has been received, the new version can be deployed on the actual production system – P – and delivered to users in the field.

A staging approach is perfect for a rolling development and update process that should not disrupt or, in the worst case, take off line the testing or production systems. This is particularly true when updates for third-party components (tools, libraries, databases, or even the entire operating system) are concerned, which can have serious repercussions for the stability of the system, but are rarely designed to play nice with the other components of other makers. The D system allows a risk-free assessment of the effects of updates on the existing system. Only when all components are taught to play in har-

mony with each other can the testing and clearance process start on the Q system and then everything eventually being deployed on the P system.

Wibu-Systems also recommends a staging process for CodeMeter License Central. Upgrades to new versions should be tested for their fundamental compatibility with the system as a whole and cleared beforehand, especially if custom CodeMeter License Central extensions come into the equation. This is easy with an established D to Q to P staging process. And if setting up and maintaining such a chain is too much of a hassle, the entire effort can be outsourced to the certified data center of Wibu-Systems.

With the right people and the right preparation, even open-heart surgery is an option! 



Cloud FSB

Automatic build systems and continuous integration have become the standard for modern software development processes. Typically, the environments in which these processes happen are virtual to enable the developers to scale the resources involved up or down to meet their needs. Moving all of these build environments into the cloud, e.g., in Azure DevOps, seems the logical next step.

But one key component in the development process is protecting the software by encrypting the executable files of the application. This means that it has to happen after the software has been compiled, but before the actual installation package is put together.

One of the USPs of CodeMeter is its strong link between this encryption and the software license. A secret key, called the Product Item Secret Key (PISK), is stored in the license itself and is needed to decrypt your software. This means that the same PISK also has to be known during encryption. CodeMeter does so by calculating the PISK from your Firm Code, your chosen Product Code, and your secret master keys. These secret keys are hidden in your Firm Security Box or FSB, which is a CmDongle that Wibu-Systems has prepared for you with your very own Firm Code.

When you enter a Product Code, such as 201000, for the encryption process, the PISK is calculated from the combination of that code and your Firm Code, and the software can be encrypted. The same PISK is calculated and stored in

licenses when you create a license with the same Product Code. The end result is simple:

- License is present and correct: The software can be decrypted.
- License is missing: The software cannot be decrypted.

This shows why the FSB is essential for encrypting your software. But how can you plug a CmDongle into a virtual machine or Docker container in the cloud? Wibu-Systems introduced a solution to this conundrum in mid-2022 in the form of the Cloud FSB. It is hosted by Wibu-Systems and acts like a virtual dongle. The build system connects to it on port 80 or 443.

As with a regular CmDongle, nobody can retrieve the master key in a CmCloudContainer. A system that has the right to access the FSB can use the key, but cannot steal it.

For your build system to connect with the Cloud FSB, you need a credential file, which includes a strong password and takes over the job of establishing a secure and encrypted connection.

In CodeMeter Runtime, a Cloud FSB would then appear as a regular local CmDongle. You can access the Cloud FSB through the CodeMeter Developer Portal and connect it directly to your local device or download the credential file. The latter option makes sense for your build system, although the file should definitely be kept safe and secure. You can find more about how to do this in the Azure DevOps topic "Use secure files".

FSBs come in two types. The first is a standard FSB, which can create licenses and encrypt software with a licensed version of AxProtector. The second is an Encryption-Only FSB. As its name implies, it can encrypt software, but it cannot create licenses. It is recommended for automatic build systems, since the damage in the case of loss or theft would be less dramatic than with a full FSB. Should it be lost and somebody else starts to use the credential file illegally, it can simply be voided through the CodeMeter Developer Portal. The credential file would be recreated and be ready for roll-out across your systems with little disruption. 



Racing the Quantum Hare

What can a German fairy tale tell us about the threat of quantum computing and the fate of post-quantum cryptography? Surprisingly much! The story of an unequal race between a hare and a hedgehog reminds us of the situation that the cryptographic world has found itself in: With the advent of commercially viable quantum computers that can break established cryptographic algorithms, any outside observer would say that the race has already been lost. But that is far from the truth.

Most modern cryptography relies on a simple premise: For encryption algorithms, you use a mathematical problem that is so complex that conventional computers would require decades or centuries to crack. It may not be impossible in theory, but it certainly is in any real-world scenario. When Peter Shor demonstrated how a working quantum computer could factorize large numbers with ease and speed, all of this confidence went out of the window. Though quantum computers were still the stuff of science fiction at the time, the cryptographic community started looking for new hard mathematical problems to build new cryptographic algorithms on, some for the love of math and theory, and some because they saw the actual thread – in the far future.

Nearing the Tipping Point

But quantum computers have now become a real factor to contend with, as working devices, however immature and limited the technology might still be, are already being operated by state and private actors and even available via cloud access. So, is now the right time to panic?

How Serious has the Threat Become?

Indeed, conventional cryptographic algorithms have lost their USP as practically unassailable fortresses. Well-known schemes like RSA are no longer absolute guarantees for security. The technical underpinnings of digital signatures and certificates, like the DSA and ECDSA algorithms or the Diffie-Hellman key agreement, have become vulnerable. Sooner or later, a powerful-enough quantum computer could crack essentially any protocol, or even work back from any public key to compute the matching private key and break through any protection layer.

No Need to Panic

However, all of these threats apply primarily to asymmetric encryption. Symmetric schemes like the popular AES encryption or hash functions like the SHA family are not as easily broken. Quantum computing pioneer Lov Grover did propose an algorithm that would allow quantum computers to work out the secret key for AES encryptions or calculate back from a hash value, but not with the dramatic leaps in

performance that are proving so worrying for other cryptographic approaches. It is not years or decades of computing turned into a leisurely afternoon's work for a would-be hacker, but just a noticeable, but minor acceleration in the calculation process.

For symmetric encryption schemes, the response to the quantum threat is therefore simple: Just up the key length! Switching from AES-128 to AES-256, an easy change even for standard consumer devices, would level the playing field again and return the cryptographic arms race back to its old balance.

Taking Stock

How fares the cryptographic world? Even though symmetric encryption schemes still offer real security, the threat to asymmetric encryption is real, and that has serious implications for our ability to securely exchange encryption keys and maintain integrity and authenticity.

And the arms race is heating up: Modern quantum computers have passed into what is called

the NISQ (noisy intermediate-scale quantum computers) stage, as they are large enough to conduct fundamental computation and error correction operations, but still far from sophisticated enough to pose a real threat for actual cryptography. In practical terms, quantum computers are currently working with several dozens to hundreds quantum bits or qubits, but they would need around 2000 logical qubits to break RSA 1024 or EDSA/ECIES 256. And with their inherently error-prone nature, this would translate into more than a million actual qubits to get to the necessary 2000 error-corrected qubits.

The quantum computers of today are also still unwieldy in more than the logical sense: They require massive investments and extremely sophisticated technology, e.g. for cooling the superconducting qubits down to near absolute zero. At the time of writing, any attempt to crack current encryption algorithms would be prohibitively costly and very far from worth the effort, if even technically possible.

Still, Pandora's box has officially been opened, and quantum computers are constantly evolving and getting better, cheaper, and more easily available. With this prospect, the National Institute of Standards and Technology NIST and Germany's Federal Office of Information Security BSI are officially recommending that the cryptographic world starts thinking about alternative options. The magic term is: Post-quantum cryptography.

Entering the PQC Arms Race

NIST officially began the new game of cat and mouse in 2016 by standardizing quantum-secure algorithms. The sense of urgency in the industry meant that the complex and usually slow standardization process was accelerated beyond expectations. Candidates were screened in several rounds, a shortlist prepared, and

the algorithms selected for standardization announced in 2022.

The thinking was to prepare a set of algorithms that use different mathematical means under the hood. Should any one of them be broken by quantum computers, this would leave other options open and keep the arms race active by the simple and brute principle that underlies much of cryptography: Making it harder, costlier, and simply not worthwhile for attackers. A quantum computer might, at considerable cost in terms of money, manpower, and time, break one algorithm, but that victory would be short-lived, as others are already being put in place by the defenders.

The NIST approach offers some reassurance for the cryptographic community, although one candidate, SIKE, has indeed already been broken, not even requiring a quantum computer at all. This should remind everybody that the threat is serious, acute, and not to be ignored, and that nothing can be taken for granted.

The Hare and the Hedgehog: Speed beats Agility?

In the fairytale of the hare and the hedgehog, the apparent loser hedgehog challenges the obvious winner hare to a race that seems a foregone conclusion. But on race day, the hare darts off, leaves the hedgehog trailing in the dust, nears the finish line – and finds himself face to face with the hedgehog waiting for him. Little did he know that it was the hedgehog's wife, waiting there all along. Frustrated and hurt in his honor, the hare races back to the starting line and back again, back and forth until he dies from exhaustion.

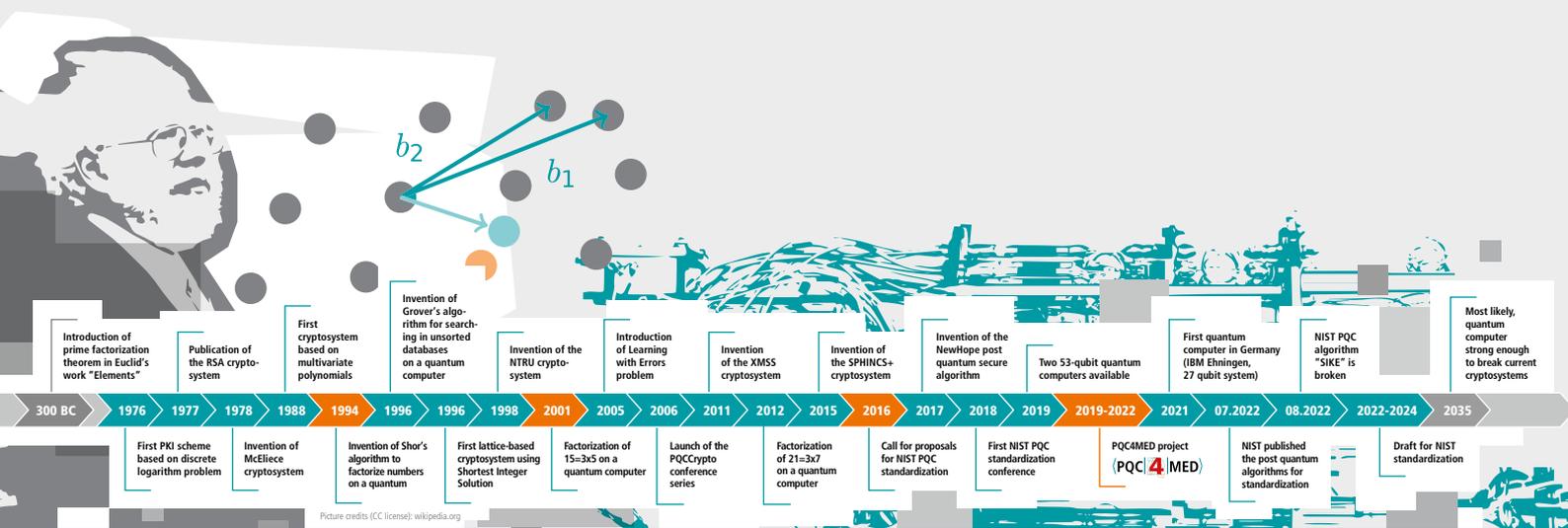
The hedgehog can be a model for what is needed now in cryptography: Not speed – where the quantum-computer-empowered attacker has the natural advantage – but cleverness and crypto-agility.

If single cryptographic algorithms are likely to fall in the future, the crypto-agile answer would be to have in place other algorithms to take their place. Software architectures need to be designed to allow cryptographic algorithms to be replaced immediately in the case of a breach. When one quantum-safe system is revealed to be not as safe as we had hoped, migrating to another system should be an obvious and immediate option.

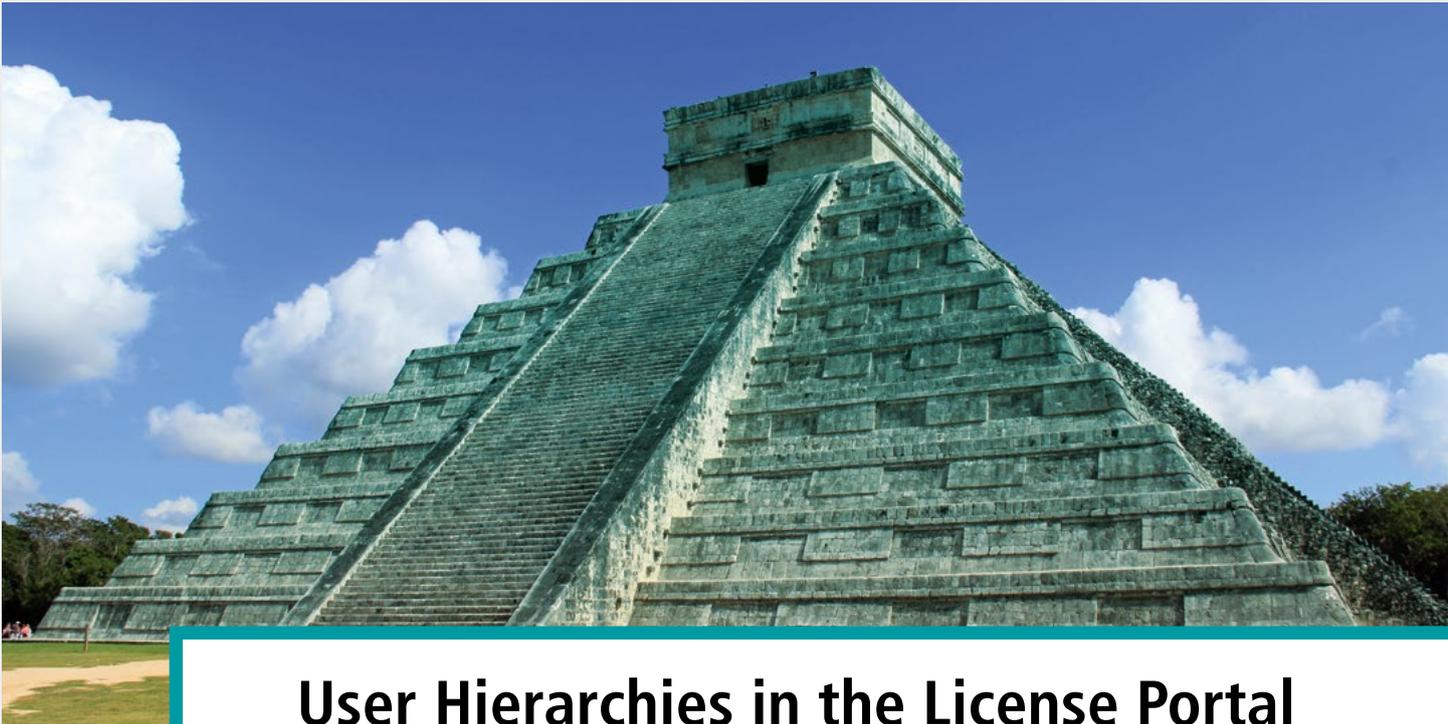
Crypto-agility calls for more than flexibility. It needs a new way of developing software, as new performance tradeoffs need to be made, new algorithms or entire protection systems need to be introduced that require more work in terms of protecting against side-channel attacks or all the other factors that one could consider the soft underbelly of cryptography. And as the threat still seems so far-off and unreal, developers might be wary of switching outright to real quantum-safe algorithms. Ideally, they should allow for a combination of conventional and quantum-safe cryptography to cover all possibilities.

I'm Already There

"I'm already there", the hedgehog's wife taunted the hare. Post-quantum cryptography needs to be able to say the same: When the quantum tipping point is reached, it has to already have its house in order. Now is the right time to start preparing your organizations, your cryptographic choices, and your software architectures for the post-quantum moment.



Picture credits (CC license): wikipedia.org



User Hierarchies in the License Portal

The last issue of our KEYnote magazine explained how the License Portal can integrate the automatic creation of CmCloud-Containers. We are now following this up with a look at different user levels. The License Portal could distinguish between lecturers and students at a university, between admins and regular users in a corporate setting, or between resellers and customers. These License Portal capabilities include the allocation of custom rights.

Hierarchical Structure

The users are arranged in a hierarchy, not limited to the two levels of the above example. This can go up to a wide chain of levels, such as resellers, client admins, and client users.

Groups

The individual levels are defined as groups. De-

pending on the user interface of the Portal, the displayed terminology can vary: One Portal might call them clients, another employees, and a third could call them students. The top-level groups in the hierarchy can only be created by a special user with "isvadmin" rights. Each group can have additional subgroups, which can be formed by any user with the "admin" rights

in that group. There is no limit to the number of subgroups in a group, but every group has exactly one higher-up (parent) group or, in the case of top-level groups, none at all.

Users – ISV Admin

"In the beginning, there was ISV admin." The initial user of the License Portal is created during

The screenshot shows the CodeMeter License Portal interface. The browser address bar displays the URL: `https://ap-ik-115/extensions.head/src/p/Tickets.php`. The page title is "CodeMeter License Portal" and the navigation menu includes "Licenses", "Tickets", and "CmContainers". The main content area is titled "Tickets" and contains a table with the following data:

Ticket	Type	Owner	
FGMK2-LAT07-VR3L6-XJUSD-L7VAP	personal ticket	ruedi.gueckler@wilbude	Remove
M7PWP-APBX3-CZTAA-VA594-H4PWG	group ticket	Sample Company	
F7USB-WZDUJ-DV9NH-ZDMNK-DQPYF	group ticket	Sample Company	

Below the table, there is a section titled "Add Additional Ticket" with a text input field for "Ticket" and an "Add Ticket" button.

installation and endowed with “isvadmin” rights. They can create new users, share their “isvadmin” rights, and create new top-level groups or new admins. They can see all users in all subgroups and they have the power to delete any user, except for themselves. Another ISV admin would be needed to do so and ensure that there is always at least one user with “isvadmin” rights.

Users – Group Admin

“isvadmin” rights are global rights given to a user. All other active rights are assigned to a user in the context of a group. As standard, the License Portal uses the “admin” rights for a group; users with these rights can create or delete subgroups or additional users for their groups and subgroups.

Users – Group User

Group users are distinct from group admins. They are created by group admins and can only access themselves and the groups they are assigned to.

Users – User

Alongside group users, there are users not assigned to any group context. They are created either by an ISV admin, or they registered themselves via the License Portal. They only have access to their own account.

Upward Blindness – Downward Transparency

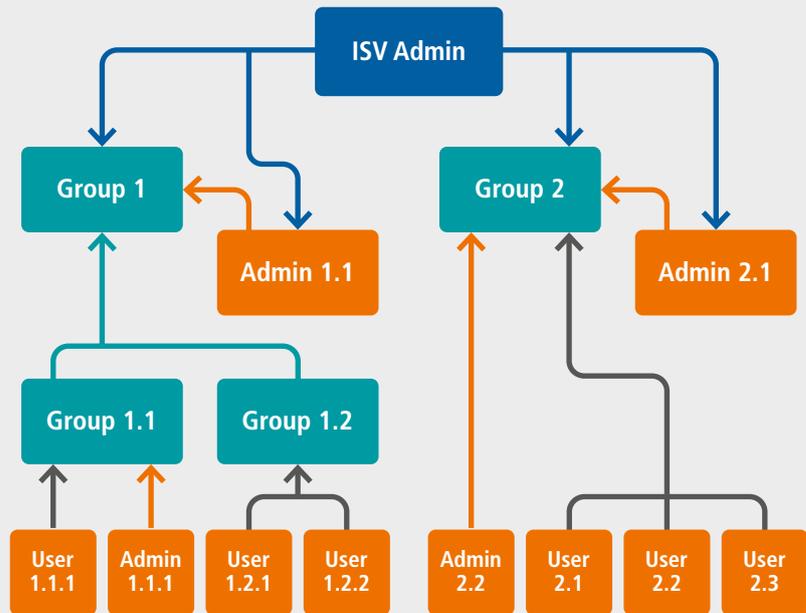
The core purpose of the License Portal is its ability to assign tickets and the licenses they embody to groups or individual users. The principal rule is that users cannot access any ticket higher up in the hierarchy. A user with “admin” rights has access to all tickets on their level and on the lower branches of the hierarchy. A user without “admin” rights can only access their specific level.

An ISV admin is always listed at the top and has access to all tickets through the hierarchy.

Assigning Tickets

Tickets can be assigned as personal tickets for a user or as group tickets for a group. Any ticket can only ever be assigned to a single user; if it is assigned to a new user, care is taken to check whether the user making that transaction has the right to access both the current and the intended holder of the user. If that is the case, the ticket is moved, i.e. removed from the older holder and assigned to the new user. If the user has no such rights, the transaction is stopped immediately and an error message returned.

Tickets that are not yet assigned can be allocat-



ed to any new user. Again, the necessary rights are checked before the transaction is completed.

Visibility and Rights

The following visibility rules and rights apply:

	User	Group Member	Group Admin / Parent Group Admin	ISV Admin
Group Ticket (Protected Mode)	–	–	×	×
Group Ticket	–	×	×	×
Personal Ticket with Group Context	×	–	×	×
Personal Ticket without Group Context	×	–	–	×

Basic Functionality

All fundamental functions of the License Portal are available when it is configured for different levels, including all transactions like license activations or deactivations. The same goes for all user-related functions: Registering and removing users, displaying or editing user info, or changing or replacing passwords.

CodeMeter Cloud Support

One special aspect needs to be considered for CodeMeter Cloud Support. Since group admins can access the users in their groups or subgroups, they also have access to the users’ CmCloudContainers. They could reset the access data for these CmCloudContainers and, for instance, prevent users who have left the group from using the licenses in the Container. Group admins can also activate or deactivate licenses in the CmCloudContainers of the users assigned to them. This makes it easy and comfortable to

move licenses from one user to the next.

A user can download the credential file for a CmCloudContainer to distribute it offline to a headless system. This is particularly interesting if the

software is run in virtual machines or container environments like Docker and if the license is to be preconfigured in the relevant template.

Expansion by Wibu-Systems Professional Services

The License Portal can be expanded by our Professional Service team, e.g. to allow resellers to create licenses or, more specifically, tickets. This is done by assigning additional custom rights, e.g. “create_ticket”. Users that have this right get access to the features they need to create licenses.

One project that our team completed for a partner organization added a filter for the products to allow the partner to create licenses for selected products. The resulting tickets are automatically assigned to clients of our partner; our partner only needs to create a new user for the client and the client can start activating licenses right away. 

News in Brief

CodeMeter License Central Internet Extensions 21.04c

Starting with Version 21.04c, subscriptions can be managed with time contingents. The vendor creates licenses (tickets) with these contingents, e.g. 30 days or one year, for sale through any retail channel. When tickets are activated by the user, the contingents are intelligently combined for the ticket activated first. 

CodeMeter License Central Internet Extensions 22.05

Version 22.05 introduces the CodeMeter License Portal, a WebDepot levelled up with user management and CodeMeter Cloud Support features.

With the License Portal, users can be given the ability to register themselves. Alternatively, they can be automatically registered via REST-API. Once registered, they can create their own CmCloudContainer, activate or deactivate licenses in it, or reset their log-in data. 

CodeMeter Cloud 2.30

Version 2.30 includes a new REST-API for the creation and management of CmCloudContainers through the CodeMeter License Portal. It can create or delete CmCloudContainers, create credential files, change the CmContainer's name, export context file, or import update files. These functions can be used or be provided to users as a self-service feature through the CodeMeter License Portal.

The version also includes UX/UI improvements for the CodeMeter Cloud Dashboard. 

CodeMeter License Central 4.02

Version 4.02 adds new configuration options for the CmActLicense containers via the web interface, allowing use in recovered snapshots of virtual machines, in container environments like Docker, or in EWF / FBWF mode. 

CodeMeter 7.50/7.51

Version 7.51 improves performance for updates to CmActLicenses with Universal Firm Codes on the users' side. Typically, less than 10 ms are needed to create a context file or add an update for each Product Item.

Version 7.50 introduced log rotation for the Code-Meter event log. Expanded license access rights are now also available on Linux and macOS systems for more granular rights management.

Software developers can now have their FSB for Universal Firm Codes equipped with a so-called Soft LPK to allow the programming API (HIP) to conduct complex cryptographic operations in the working memory. 

CodeMeter Protection Suite 11.10

AxProtector .NET NC 11.10 introduces a new technology for protecting .NET software as a console application for Windows, Linux, and macOS.

This offers better performance during encryption and, crucially, when executing protected software. A new protection architecture allows dynamic performance improvements, accelerating frequently used features and functions automatically. More anti-reverse-engineering measures were introduced for greater security. 

CodeMeter Embedded 2.61

This version adds the ability to change LAN settings during runtime to access different license servers. The Runtime Bridge function used to communicate with a local CodeMeter Runtime can now also be turned on and off during active operation. The creation of programming contexts for remote programming has been accelerated, especially when dealing with larger numbers of entries. 

Grand Prix of the Mittelstand

Awarded by the Oskar Patzelt Foundation, the "Grand Prix of the Mittelstand" celebrates enterprising businesses in southwest Germany, with over a thousand SMEs vying for the coveted award. Wibu-Systems is proud to have been among the chosen nominees for the top honor. 

LEA Award

Not all of Wibu-Systems' business is about technology, but it is all about making lives safer. As such, the company has been committed to supporting the nph Kinderhilfe, a charity working with disenfranchised young people in Honduras and Haiti. For this commitment, Wibu-Systems

has been awarded a Certificate of Appreciation, by the LEA corporate social responsibility prize. 

German Innovation Award 2022

Presented annually by the German Design Council, the German Innovation Award honors forward-thinking enterprises who contribute to society with innovative products and technologies. Wibu-Systems was a winner in 2021, and has now repeated that achievement with an award for our protection solution AxProtector JavaScript. 

GIT Security Award 2023

The GIT Security Award is given to the makers of products that add safety and security to people's lives – a perfect fit for our vision for Wibu-Systems. For this year's award, we were included among the nominees for CodeMeter ASIC, our popular choice for modern digital infrastructures. The winners will be announced in the coming weeks. 

Industry 4.0 Innovation Award

Wibu-Systems is a top contender for this popular award. With CodeMeter's potential to help bring to life a safer and more secure digital industry, we have made it onto the exclusive shortlist of candidates hoping to win the award at the gala ceremony in December. 

NEO2022

With our strong roots in our hometown of Karlsruhe, we are proud to be included among the final candidates for the NEO innovation prize, awarded by the TechnologieRegion Karlsruhe for cybersecurity innovations. Our hopefully winning bid: AxProtector Python, our new technology that brings CodeMeter power to the Python world. 

Best of Industry Award 2022

Awarded by MM MaschinenMarkt, the leading German source for news and info in the manufacturing world, the Best of Industry Award has 180 contenders vying for prizes in 23 categories. This year, we are bringing CodeMeter to the additive manufacturing category, as an innovative solution for more IP security in a completely new section of the manufacturing world. 

ALERT

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

Subscribe to our newsletter





Case Study | Daimler Buses

The Challenge

Printing objects at an acceptable level of quality and adequate cost used to be the domain of science fiction, but many technical issues have since been overcome, and 3D-printing urgently needed parts have become a viable option, just at the moment when the global supply chains are buckling under the many stresses of our times and consumers are expecting more sustainability. However, when parts are printed out of the reach of the original rights holder, solutions are required to protect the intellectual property and make the billing process secure and transparent along the entire chain.

The Solution

Many parts for Daimler and Setra Buses are now made available in digital, 3D-printable format on the OMNIplus service portal. Bus operators and service partners can buy these for printing on site. This is made possible with Wibu-Systems' CodeMeter encryption and licensing solution and specially certified printers made by Farsoon Technologies. The files

are sold as encrypted downloads, and the buyer receives a license to use for pre-printing and an actual printing license that allows as many copies to be printed as the buyer has paid for.

The Success

In cooperation with Wibu-Systems and Farsoon Technologies, Daimler Buses has revolutionized the spare parts business from the ground up and raised a flag for additive manufacturing in its industry. The success proves: The ability to protect and monetize intellectual property with the tried-and-tested CodeMeter technology is opening the doors for new business models based on 3D printing.

The Company

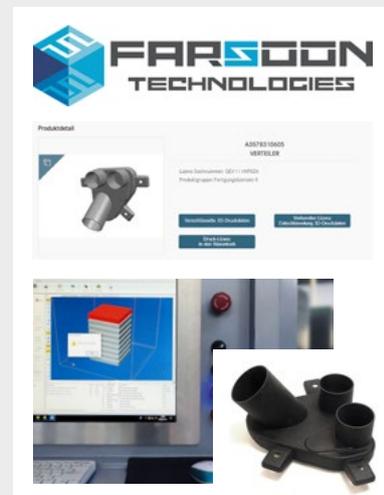
Daimler Buses is a pioneer in the entire automotive industry for industrial 3D printing. The company has been focusing on the potential

of digital production technology since 2016. In the meantime, the OMNIplus service brand has designated around 40,000 bus/touring coach spare parts from the Mercedes-Benz and Setra brands as suitable for 3D printing. Initially, OMNIplus is concentrating on more than 7,000 parts that are to be digitized gradually. A kind of digital warehouse will be created in this way which is being expanded continuously. It includes both regularly required spare parts as well as rarely required parts for special customer requests. The virtual warehouse forms the basis for 3D printing license management, which shall further optimize the rapid availability of spare parts. 

DAIMLER TRUCK Daimler Buses

Ralf Anderhofstadt, Head of Center of Competence Additive Manufacturing Daimler Trucks and Buses

"The successful implementation of the revolutionary AM digital rights management system means that our partners and we have made a real mark in the digital 3D printing business. This opens up completely new vistas for our service operations and for the availability of products where they are needed at the point of sale, both commercially speaking and thinking about the good of our environment."



Wibu-Systems Training

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.



www.wibu.com/tr

Available Courses

CodeMeter Core Features

- CodeMeter at a glance
- Configuring licenses
- The components of CodeMeter Runtime
- Use as a network server

Software Integration for .NET Assemblies with AxProtector .NET and API

- Encrypting .NET assemblies
- Encrypting individual classes and methods
- Integrating Wibu Universal Protection Interface (WUPI)
- Using CodeMeter Core API

Back Office Integration with CodeMeter License Central

- Configuring products
- Creating licenses
- Integrating license activation in applications
- Setting up and configuring license portals

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

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 and its subsidiaries at the following events:



SPS – Smart Production Solutions
8-10 November 2022
Nuremberg, Germany
Hall 6, Booth 428



Formnext
15-18 November 2022
Frankfurt, Germany
Hall 11.1, Booth D69J



Medica
14-17 November 2022
Dusseldorf, Germany



Hannover Messe
17-21 April 2023
Hanover, Germany

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

Also, our monthly fully immersive masterclasses focus on unique content and are designed for beginner, intermediate, or advanced users of our CodeMeter technology. The 2022/2023 season will cover areas such as Machine Learning, Features-on-Demand, Salesforce integration, authentication, cloud licensing, and license monitoring. 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
44 Edition, Fall/Winter 2022

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
Alexander Grill
Matthias Honka
Carmen Kempka
Ruediger Kuegler
Daniela Previtali
Florian Schneider
Oliver Winzenried

Design

Eugen Olchin

Print

Stober Medien GmbH, Eggenstein, 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.

Wibu-Systems®, CodeMeter®, SmartShelter®, SmartBind®, and Blurry Box® are registered trademarks of WIBU-SYSTEMS AG. All other brand names and product names used in this documentation are trade names, service marks, trademarks, or registered trademarks of their respective owners.

Copyright ©2022 Wibu-Systems. All rights reserved.

Picture credits:

Cover: istockphoto.com/deepblue4you
Page 4: istockphoto.com/monsitj
Page 5: istockphoto.com/deepblue4you
Page 7: istockphoto.com/MartinBarraud
Page 9: istockphoto.com/felino
Page 10: istockphoto.com/Olemedia
Page 11: istockphoto.com/Andyworks+BartlomiejWroblewski
Page 13: istockphoto.com/StephaneMoes
Page 17: Daimler Truck AG

All remaining images are copyrighted by their owner

SECURITY
LICENSING
PERFECTION IN PROTECTION

