SPRING 2020

KEYnote 39

THE WIBU-MAGAZINE

Users and CmCloudContainers

Highlights

- Virtual Systems – Undermining Licensing?
- Lost licenses – What now?
- Licenses for Offline Devices

WIBU SYSTEMS

Content

Dear Clients and Partners!

The current news can make us anxious, and we cannot force ourselves to stop worrying. What we can do now, however, is to think about the things that we can influence: Our future. This goes for our private lives and for our professional and commercial plans.

For us at Wibu-Systems, one of our most motivating plans is our investment in our new head office and the House of IT Security in Karlsruhe, Germany, which will give a new home to established enterprises, aspiring young start-ups, and forward-thinking researchers. Security is becoming more important than ever before, especially in the digital world, whose great potential and practical advantages we are all experiencing now. VPNs and web conferences allow us to work from the safety of our homes; our developer teams to hold virtual meetings; our sales professionals to continue to serve their clients; and even our construction work to proceed with a virtual jour-fixe with developers, architects, planners, and builders. I personally thank everyone whose hard work helps us, and our company stay healthy and active!

Freedom and personal liberty are always on our minds. Some liberties that we took for granted have been restricted. Our protection, licensing, and security solutions can give you more freedom: the freedom to choose any license container – CmActLicense, CmCloud, or CmDongle; to choose any target system from micrcontrollers and embedded systems or PLCs to PCs and the cloud; to choose any platform from x86, ARM, MIPS and PPC with Windows, macOS, Linux, or real-time operating systems; and to integrate all of this in established business processes and ERP, CRM, and e-commerce platforms.

This freedom to choose the right business model for you creates new win-win opportunities: You can provide your clients with additional temporary home office licenses or provide devices with basic features at a lower price without compromising your revenue streams in the future. And, you can help potential clients today with limited test licenses for your products and build up a new and loyal user base for the long term.

I hope this issue of KEYnote magazine will show you many interesting ideas and opportunities and am looking forward to hearing from you and continuing our conversation. Stay healthy!

Best regards from

Oliver Winzenried

CEO

CodeMeter and X.509 Certificates

Any conversation about security or authentication will, sooner or later, come down to the matter of certificates. Still, certificates are a foreign concept for many people, and their actual application and management in practice remains frequently too complicated and laborious.

Let us delve into the topic and explore what certificates do and how CodeMeter can be used to make their management and all other processes dealing with certificates easier and more comfortable for the user.

X.509 Certificates and PKI

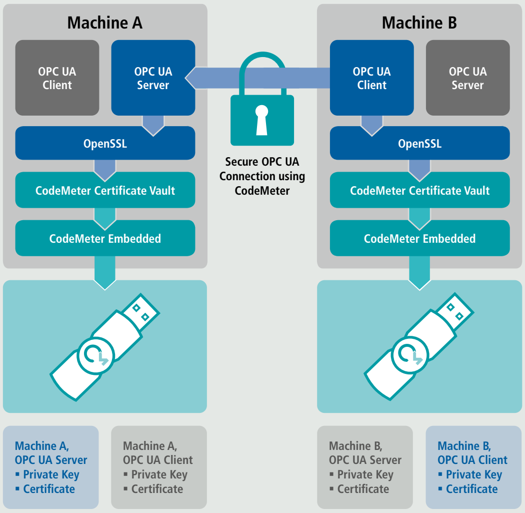
Certificates are used to tie identities to public keys and to the related private keys. Certificates are used exclusively with public key algorithms such as RSA or ECC. In these algorithms, the key consists of a private key and a matching public key; therefore, they are always referred to as a key pair. Identity, in this case, means not just the identity of actual human beings. It can also refer to the identities of machines, devices, or roles. Whatever the case may be, for a certificate to link an identity with a key pair, it has to contain certain information about it, such as the device name or an IP address, and about the public key.

This establishes the link with the public key, but it is no proof that the identity in question indeed belongs to the owner of the key pair. A third entity is required to check and confirm that the identity goes with the key. This is done with a Public Key Infrastructure (PKI), consisting of a hierarchy of one or more anchors of trust, defined as Certificate Authorities (CAs). In order to obtain a certificate, a Certificate Signing Request (CSR) must be sent to a CA, signed with the private key going with the certificate to show the CA that the requesting entity actually holds the private key. The CA also needs to verify that the identity stated on the certificate matches the one of the requesting entity. In the case of individuals, this can be done by checking their ID cards or verifying their identity over the phone. Machines or other devices can have their identity verified either through a "device owner" – again an individual whose identity can be checked – or ideally through a set of unique device markers that can be tested automatically by the CA. Whichever route is employed, if the verification is successful, the CA signs the certificate to confirm the link between the identity and the key pair. With X.509 certificates, the entire edifice depends on the reliability of the CA, since a certificate can only be trusted if the issuing CA is trusted. This makes the CA the single point of failure.

Let us see how certificates can be used for authentication by looking at their use with the OPC UA protocol.

Safer Communication with OPC UA and CodeMeter

OPC UA is becoming an increasingly popular choice for communication between machines and devices in industry. This type of communication deserves particular safeguards, as it often contains sensitive data that needs to be protected from theft and tampering. OPC UA does so with the aid of X.509 certificates, which are used by the client and the server to authenticate themselves in OPC UA communication. If every device has a certificate and if all devices trust each other's certificates,


Machine A
OPC UA Client
OPC UA Server
OpenSSL
CodeMeter Certificate Vault
CodeMeter Embedded
Secure OPC UA Connection using CodeMeter
Machine B
OPC UA Client
OPC UA Server
OpenSSL
CodeMeter Certificate Vault
CodeMeter Embedded
Machine A, OPC UA Server ▪ Private Key ▪ Certificate
Machine A, OPC UA Client ▪ Private Key ▪ Certificate
Machine B, OPC UA Server ▪ Private Key ▪ Certificate
Machine B, OPC UA Client ▪ Private Key ▪ Certificate

the TLS implementation included in the OPC UA server and client can be used to establish reliably secure communication.

The challenges lie in setting up a PKI by equipping each device with an OPC UA server or client with certificates or keys, integrated in the OPC UA processes. The situation is complicated again by the fact that the keys are currently stored without any added protection in each device's file system. This is where CodeMeter comes in: CmDongles include a secure storage element that is the perfect place to keep keys. For these keys, hidden on CmDongles, to be accessible by OPC UA, the CodeMeter technology is integrated in the OPC UA server and client as illustrated on the previous page.

These capabilities are integrated by means of CodeMeter CertificateVault, which provides the necessary interfaces with common TLS implemeta-tions like OpenSSL. CodeMeter Certificate Vault itself uses the CodeMeter API to access keys on the CmDongle. In our illustration, Machine B wants to communicate with Machine A. The OPC UA stack makes this possible through its TLS implementation, OpenSSL in this case. OpenSSL is integrated into the server and client in a way that it does not use its own cryptographic algorithms. Instead, CodeMeter Certificate Vault comes into the equation and uses the hardware implementation of the required cryptographic algorithms, e.g. RSA on the CmDongle. The same happens on Machine A to facilitate authentication with Machine B.

This explains how keys can be used securely with OPC UA; but, how do the keys get onto the devices and where do the certificates come from?

Managing Keys and Certificates with CodeMeter License Central

Software developers and the operators of manufacturing plants need to have a central means to manage and allocate the available keys and certificates, ideally without any changes to their established processes.

Wibu-Systems offers CodeMeter License Central and its CodeMeter Certificate Vault extension as the perfect choice for them to consolidate their key and certificate management systems.

CodeMeter License Central already facilitates license management by integrating seamlessly with existing CRM, ERP, or e-commerce solutions, which guarantees support for established processes. Licenses can be activated either through a browser-based solution or through integrating dedicated interfaces in a given software product.

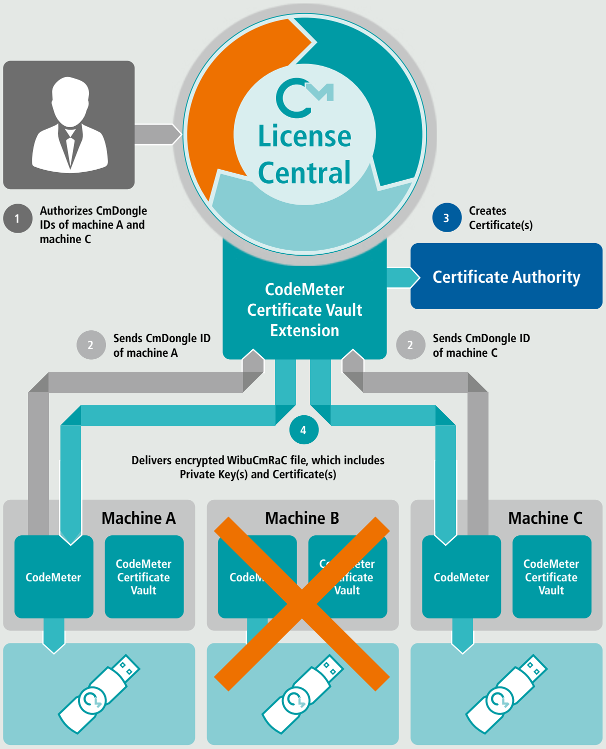
The CodeMeter Certificate Vault module is the CodeMeter License Central extension for creating, managing, and allocating keys and certificates. Certificates can be created either when an order is placed or when licenses are activated. The extension comes with the interfaces that external processes need to access with the data required for the new certificate.

Our illustration reveals how CodeMeter License Central with the Certificate Vault extension manages keys and certificates. The operator first decides in CodeMeter License Central which devices are entitled to a certificate or key and creates an order in CodeMeter License Central to do so.

To get a new certificate, the entitled device would send a WibuCmRaC file and all additional information needed for the certificate to the CodeMeter Certificate Vault extension. If no RSA key already created externally is to be used, CodeMeter Certificate Vault can create a new key pair.

A defined interface with a client-specific implementation is then used for creating the actual certificate. The software developer or machine producer can choose how the certificate is created from a wide variety of options. Step 3 in our illustration shows this choice, ranging from self-signed certificates to external certification authorities.

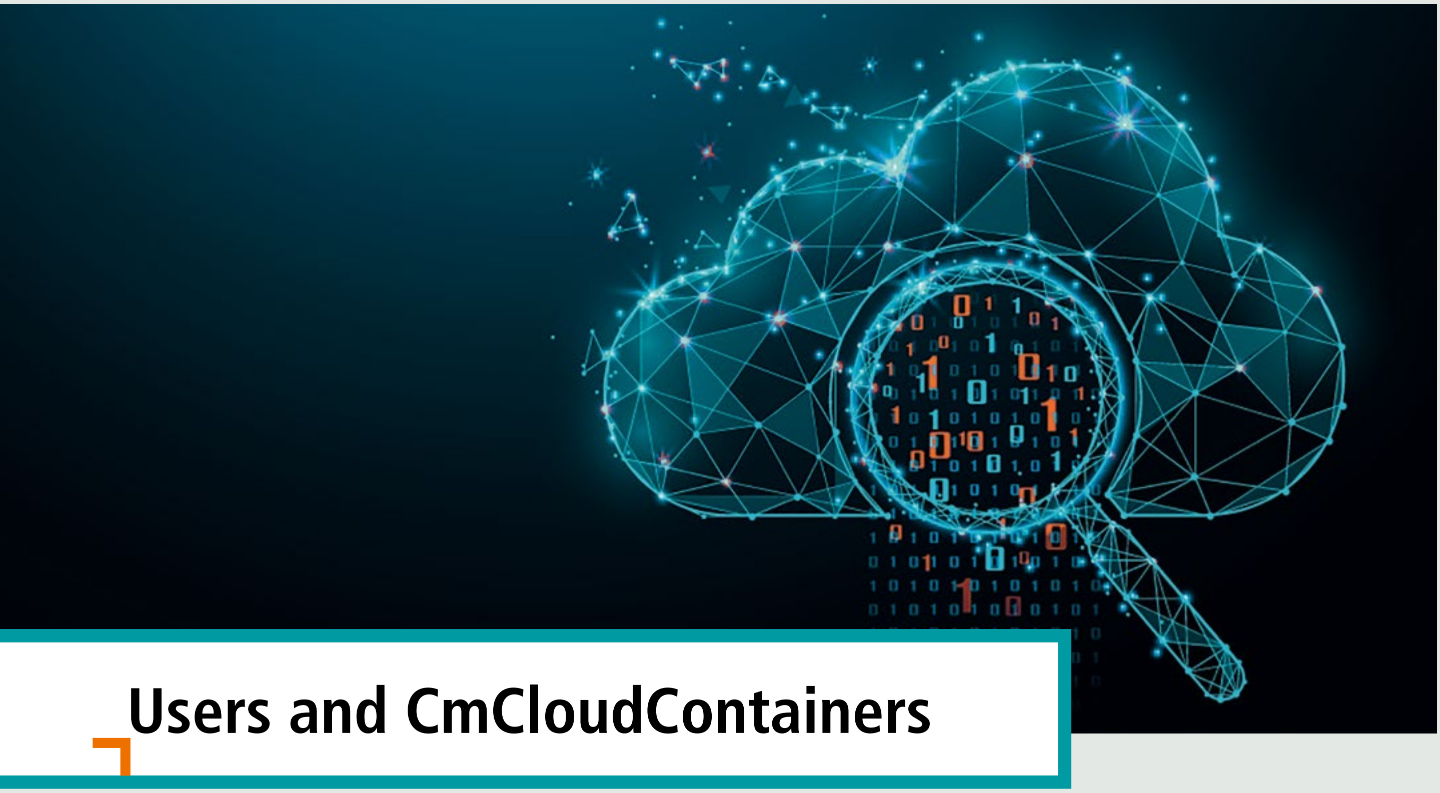
Once the certificate is ready, it is packaged up by CodeMeter License Central in a WibuCmRaU file with the private key and sent back to the requesting machine (step 4). Additionally, the key is backed up in CodeMeter License Central. After the file has arrived, the certificate and key are stored on the CmDongle and can be used by CodeMeter Certificate Vault, e.g. to establish secure communication.


License Central
1 Authorizes CmDongle IDs of machine A and machine C
3 Creates Certificate(s)
Certificate Authority
CodeMeter Certificate Vault Extension
2 Sends CmDongle ID of machine A
2 Sends CmDongle ID of machine C
4 Delivers encrypted WibuCmRaC file, which includes Private Key(s) and Certificate(s)
Machine A
CodeMeter
CodeMeter Certificate Vault
Machine B
CodeMeter
CodeMeter Certificate Vault
Machine C
CodeMeter
CodeMeter Certificate Vault

Conclusion

CodeMeter Certificate Vault brings the reliable security of CodeMeter Dongles to the world of storing and using keys and certificates.

With the CodeMeter Certificate Vault extension, existing processes can link up with CodeMeter License Central for a smooth and seamless creation and management of certificates.



Users and CmCloudContainers

CodeMeter License Central was Wibu-Systems' first foray into the world of cloud licensing: The system creates and delivers licenses through the cloud, and the users import them to a secure hardware CmDongle or a CmActLicense file, bound to a known device. Since early 2020, licenses can now be kept in a special container in the cloud, the CmCloudContainer, that is bound not to a specific computer, but to a known user. This article shows how CmCloudContainers work and what purpose they serve.

Simple setup with WOPS

The server that is home to the CmCloudContainers is provided by Wibu-Systems through the cloud. The costs for operating that service depend on its usage, especially for cryptographic functions. Wibu-Systems offers three attractive hosting packages with three expansion packs. To make their move into the cloud, software developers simply need to order the package that best meets their needs, and the Wibu Operating Services (WOPS) team takes care of the rest. A few working days later, the CodeMeter Cloud Server is ready for action.

No need to change the software

CmCloudContainers are fully compatible with CmDongles and CmActLicenses. Any software protected with CodeMeter can be used immediately and without any adjustments with a CmCloudContainer, as long as CodeMeter Runtime 7.0 or newer is used. It does not even matter whether the software is protected automatically by CodeMeter Protection Suite or by CodeMeter Core API.

The only restrictions that apply between the different CmContainer types (as of Q1 2020) are:

- Executable code can only be moved into and run in CmDongles. This function is not available in CmActLicenes or CmCloudContainers.

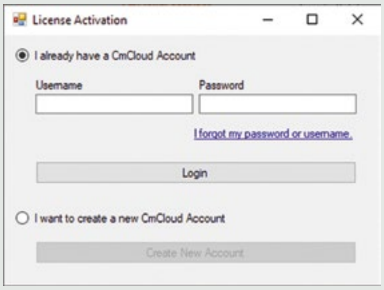
- Licenses can be moved and borrowed offline between CmDongles and CmActLicenses, but not CmCloudContainers. This is no restriction in practice, because anyone using a CmCloudContainer would be online when accessing the license. These licenses can be returned to CodeMeter License Central and moved from there to a CmDongle or CmActLicense. Checkpoint licenses can be used for the same purpose as usual borrowed licenses, even if the local device on which they are used is not always connected to the Internet.

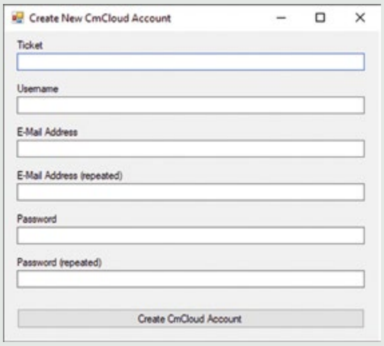
- CmDongles and CmActLicenses can be activated simply and directly with the license portal and WebDepot. The process for CmCloudContainers relies on a file exchange; a direct activation is, however, possible with the Software Activation Wizard. The Software Activation Wizard alone needs to be adjusted, since the processes for creating empty CmCloudContainers or using existing CmCloudContainers from other computers are new or differ slightly from the usual approach with other CmContainer types.

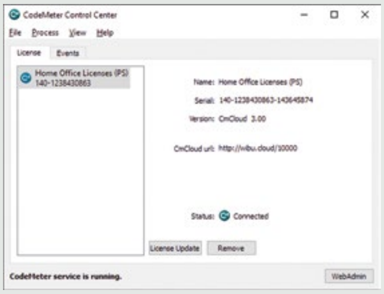
The path to a new CmCloudContainer

CmDongles are delivered either blank or preloaded with licenses. After plugging the CmDongle into the computer, the CmContainer is available for transferring licenses.

With CmActLicenses, the software developer would create a template for all users, which defines how the soft license is bound to the users' machine. This template is imported onto the users' computer, making the CmContainer available in the same manner as a plugged-in CmDongle.


License Activation
I already have a CmCloud Account
Username
Password
I forgot my password or username.
Login
I want to create a new CmCloud Account
Create New Account





Home Office Licenses (PS)
140-1238430863

Name: Home Office Licenses (PS)
Serial: 140-1238430863-143645874
Version: CmCloud 3.00
CmCloud url: http://wibu.cloud/10000
Status: Connected

CodeMeter service is running.

When using a CmCloudContainer, the template contains the access details for each user, requiring one template per user – the so-called credential file. Typically, this file is created automatically for the user when a license is first activated; otherwise, credential files can be created and sent to their intended users manually.

The standard workflow begins with the user launching their software for the first time on their computer. The software recognizes that no license is yet available on the device and starts the Software Activation Wizard. The wizard allows the user to create an account in the license portal, an extension of CodeMeter WebDepot that is either hosted by Wibu-Systems on behalf of the software developer or run on the developer's own server. In the background, the license portal then connects with the CodeMeter Cloud Server operated by Wibu-Systems, where a credential file is created for the user in question and placed on the license portal. The Software Activation Wizard receives this file in response to the creation of the new account, and the file is automatically imported onto the user's local system. Next, the user enters a ticket; in response, the requested licenses are imported into the CmCloudContainer and immediately made available for the user. From the user's point of view, all that needs to be entered is a user name (typically an email address), a new password, and the ticket. All of the rest happens automatically and transparently, but in the background.

New computer – Same CmCloudContainer

One of the inherent advantages of a CmCloudContainer is its location in the cloud, which enables users to access it on the go. The process is also easy when users install software on a new computer. Upon launch, the software will see that there is no license on the new system, and the Software Activation Wizard springs into action. Alongside the option of creating a new account, the wizard can also use an existing account if the user enters their username and password. The Software Activation Wizard logs onto the license portal with this information and retrieves the credential file to be imported onto the local computer. All activated licenses are now immediately available on that device as well, as the system has accessed the CmCloudContainer again.

There is no need to worry about licenses being used more than they are meant to be: Even a CmCloudContainer does not allow users to use more licenses than they paid for. They can import the CmCloudContainer they own to any number of devices, but the license in the container can only ever be used one at a time. The system resembles network servers using floating licenses. Users that own two licenses can use them either concurrently on one computer or separately on two computers. This works because the licenses are not accessed on the local computer, but in the cloud – which is why users need to be online when using a CmCloudContainer.

Adding more licenses

Adding more licenses to an existing CmCloudContainer is easy and the same as the process used with CmActLicenses and CmDongles: The users enter their tickets and pick their CmCloudContainer.

Since CmCloudContainers are always online by nature, software developers can pre-activate them. Licenses can be bound to the CmContainer already upon creation in CodeMeter License Central, if the target CmContainer is known at that point. When the software is launched, the Software Activation Wizard can check with CodeMeter License Central whether any license updates are waiting for this CmContainer and activate them automatically if there are any. This process works with all types of CmContainers, but CmCloudContainers even allow software developers to activate licenses immediately with an auto-update trigger and without the Software Activation Wizard coming into the picture.

Dealing with lost passwords or credential files

What happens when things go awry? The license portal includes a set of standard options for resetting a lost password, which require the user's email address.

A lost credential file can be replaced by downloading it again from the license portal or Software Activation Wizard. If the lost credential file "turns up again" with another user, that "user" would be able to access the licensed software, instead of the rightful owner. In such a scenario, the original owner would have to request a new credential file from the license portal, which would invalidate the previous file and prevent the "finder" from accessing the licenses, giving exclusive access back to their true owner. If that user works with several devices, they would have to replace the credential file on all affected devices. All of this happens automatically without any manual intervention required from the software vendor.

Lost licenses – What now?

"My dog ate my dongle." What sounds like a poor excuse is actually the start of a true story I like to tell. Or almost true, because the dog did not eat the dongle, but a piece of paper with the dongle password. Whatever the dog ate, the story illustrates how people can lose licenses or license containers, or access to their license containers.

With CodeMeter, license containers are called "CmContainers" and come in the form of separate hardware (CmDongle), encrypted license files bound to a known device (CmActLicense), or user accounts in the cloud (CmCloudContainer). Independent software developers can choose which CmContainer types to provide to their users; they can mix and match CmContainer types to their liking, let their users decide, or set specific rules, such as regional restrictions.

Depending on the CmContainer, licenses might get lost in several ways. In all of these scenarios, developers will want to help their users quickly and ideally automatically, without need for any manual action on their part. At the same time, they want to avoid the potential outcome that the users or "finders" of the lost license have access to more licenses than they legitimately own.

Automatic Replacement

CodeMeter License Central plays a key role for automating this process. As the developer, you decide whether users are allowed to replace licenses in another CmContainer (irrespective of the type in question) and how often the users can do so by themselves. The restriction can be a finite number of licenses or an enforced wait period before trying another recovery. If you know that your user base typically replaces their hardware e.g. every three years, a replacement at the start of the period and again after two years would be a reasonable timeframe that keeps the need for support down. You can, of course, allow additional license replacements manually at any time to show your goodwill where you believe it warranted.

When using CmActLicenses, you can also put in place certain rules for replacing licenses in a new CmActLicense on the same device. Again, you define the initial number and the minimum hold period before another license replacement is allowed. You can also choose the hardware properties that show whether the user is still using the same machine. This reduces the risk of a continued fraudulent use of the old, allegedly lost CmActLicense. Even if a lost license was used alongside its replacement, it would normally be bound to the same computer, which constitutes no real threat for single user licenses. This allows you to be more liberal with the restrictions than you would be with license replacements in any other CmContainer. Again, you have the power to authorize manual replacements at any time.

Automating the manual authorization process via SOAP is an appealing option. In this case, you would not allow any automatic replacement, and instead ask the user to contact a portal that checks the criteria defined by you before deciding whether the user is entitled to an automatic replacement. If this is the case, the replacement can be released transparently via SOAP, using a completely automated workflow.

Blacklist

When using automatic license replacements in a new CmContainer, you can either allow the process for the entire existing CmContainer or only for the specific licenses to be recovered.

You can also put the affected CmContainer on a blacklist, using one of three options for applying the blacklist to the old CmContainer:

1. CodeMeter License Central can generate an automatic update (as a honeypot trap)

that enacts the block. Your software will regularly check via the Internet whether any automatic updates are available. If the honeypot update is imported, it locks all licenses in the old CmContainer.

2. The user activates another license for the old, allegedly lost CmContainer. CodeMeter License Central recognizes that the container has been blacklisted and locks the licenses.

3. You export the blacklist and integrate it in the next version of your software. Should the user try to use the new version with the old "lost" CmContainer, your software locks all of your licenses in that container.

Sample code is available for scenarios (1) and (3). The latter option (3) even allows you to set a time-delayed lock, which hides the link between the version update and the blacklisting and makes it more likely that the dishonest user contacts your support team. After all, it is in your interest to record such cases, so that the user can be contacted and persuaded to buy a new license. The record is kept automatically in cases (1) and (2).

A less radical option would be to withdraw the old replaced license. As in cases (1) and (2), an automatic update would be created and rolled out by your software or imported in response to any action by your user. In this case, you would only remove those licenses that were replaced in a new CmContainer but were obviously not lost and are still available in the old CmContainer.

Checkpoint Licenses

The blacklist mechanism described above requires the information to be transferred back to the user. But what if an unscrupulous user keeps operating the old CmContainer in the privacy of his home computer, cut off from the Internet and possible updates? This is virtually impossible in our age of IoT, IIoT, and cloud applications, but CodeMeter License Central also packs a technical solution for these unlikely cases.

Licenses can also be configured as checkpoint licenses. These are perpetual licenses from the user's point of view, but technically fitted with an expiry date, which is a period of time, defined by the developer, from the licenses' first activation. As long as the licenses remain valid, the period is renewed regularly. This is done by returning and reactivating the license as the checkpoint draws closer. The expiry timer is then reset, and the license works as if nothing has happened.

Should a user keep using the old CmContainer offline, the licenses within will expire and become worthless. The secure virtual clock built into the CmContainer makes it impossible to set back the clock for the licenses. These checkpoint licenses do not need a permanent Internet connection, but simple checks back at regular intervals. Sample code is again available.

CmDongles

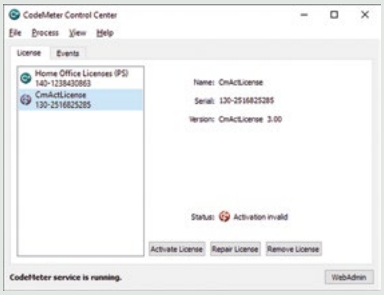
CmDongles can break. This is unlikely with an MTBF (Mean Time Between Failures) of several million operating hours. CmDongles can also be destroyed by force, even if their robust design, especially of the CmStick/B and CmStick/C Basic, makes this a rare event. In either case, there is little to worry about when replacing the CmDongle if the user returns the damaged piece.

It is a different story if the CmDongle has physically disappeared, possibly thrown out by mistake with an old computer or stolen, in all likelihood by a common thief who mistook it for a memory stick. This used to be quite rare and is even rarer now that flash memory and storage have become cheaper than ever before. It is very unusual for a CmDongle to be deliberately stolen. In such cases, it often pays to put the lost CmDongle on a blacklist. There have been stories about CmDongles suddenly turning up again at the first mention of a potential blacklisting.

CmActLicenses

Licenses can be moved between computers by returning them to CodeMeter License Central. Valid licenses can also be parked in the cloud, specifically again in CodeMeter License Central, if a computer needs to be reinstalled. CmActLicenses could only be lost if the entire computer has disappeared or if the hard drive they are stored on is reformatted. This rarely happens by accident, because migrating to a new computer is a complicated process that is usually planned well ahead of time. If it does happen, automatic replacements and blacklisting can take care of the process, either by replacing the lost license in a new CmContainer if the old computer has indeed been discarded or by replacing the CmContainer on the same computer if the system has 'only' been reinstalled.

It can happen that licenses break. This might be the case if the user changes too much of the computer's hardware. There are almost no false positives – the license seeing a change where none has occurred – because of the robustness and tolerance for errors built into CmActLicenses. In normal office settings, it has become unusual for users to open up and tinker with their computers. Modern computers pack a lot of power at low prices, which has turned customization into a hobby for IT enthusiasts and gamers. Broken licenses are therefore a very unlikely occurrence.



Home Office Licenses (PS)
140-1238430863

CmActLicense
130-2516825285

Name: CmActLicense
Serial: 130-2516825285
Version: CmActLicense 3.00

Status: Activation invalid

CodeMeter service is running.

The same goes for invalid licenses. These can occur if the license file and the values hidden in the computer do not match up, e.g. because the user has manually changed a file or if another software has written over these values. The hidden values are, however, kept in several redundant copies, again making this event very unlikely to happen.

Both for broken and for invalid licenses, the best solution is to replace them in a new CmContainer, combined with a blacklist mention.

CmCloudContainer

CmCloudContainers live in the Wibu-Systems cloud and cannot be lost by definition. CmCloud Containers are bound to known users who can access them with a credential file. It can happen that these credential files are lost or stolen. In both cases, the users could download a new credential file from their license portal, which invalidates the old access details. You can find more about CmCloudContainer in this issue of the KEYnote magazine.

Licenses for Offline Devices

Industry 4.0, IoT, IIoT, SaaS, Azure, and AWS: We are living in a world of devices that are always online and communicating with each other in the cloud. This is definitely true for office and home electronics, but it is only slowly picking up in the industrial realm. The makers of revolutionary smart controllers and devices who want to find ways to monetize their software face an uphill challenge: How to roll out licenses and license updates to offline devices. CodeMeter offers not one, but several ways to do so.

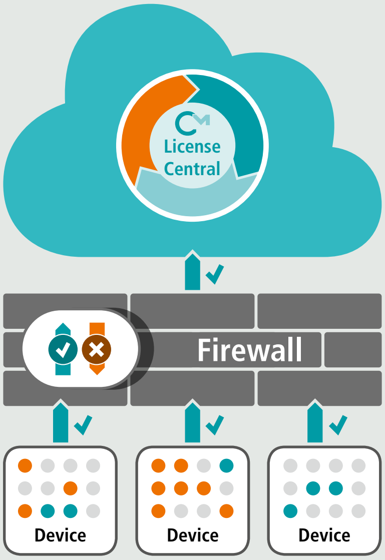
Not entirely offline

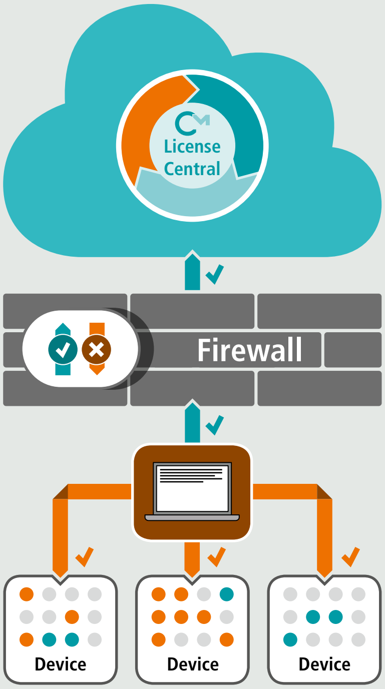
The 1996 blockbuster "Independence Day" included the iconic line: "Mr. President, that is not entirely accurate." Another thing that is not entirely accurate is the belief that certain devices are completely offline and cut off from the outside world. With this in mind, let us consider how CodeMeter licenses are allocated.

Whenever any message is shared, the transfer can occur in either of two ways: Push or pull. Push messages are sent from a central server to a local device; the server decides when to initiate the transfer and calls a service that is running permanently on the target device, not unlike the webservers that run on such devices for configuration purposes. However, many companies keep their devices seemingly offline by blocking this access route – and that is why CodeMeter does not include a standard push implementation.

The alternative option for push messages is that the target device has a special client software installed that establishes the connection with the server in the cloud and logs on in order to receive the push messages. The server can then use the opened channel, and the target device receives the messages. This method again requires a permanent Internet connection and a permanently active client. This is the method used e.g. by iPhones: The operating system provides the client and push message server as ready-made infrastructure, which means that only a connection needs to be kept open – which, however, is again a problem for many industrial users.

Pull messages are received by the client on the device regularly checking in with the server whether there are any new messages. The connection is outbound, with dedicated and known data packages sent to a dedicated server. The answer is verified by the client before it is used, which keeps the security risk down. In some projects, this option is available, which is why Wibu-Systems supports it with the Software Activation Wizard (as the client) and CodeMeter License Central. The client does not even have to run permanently. In most cases, it is run automatically at regular intervals, e.g. once per day (Cron-Job); a manual launch can also be required for special cases.

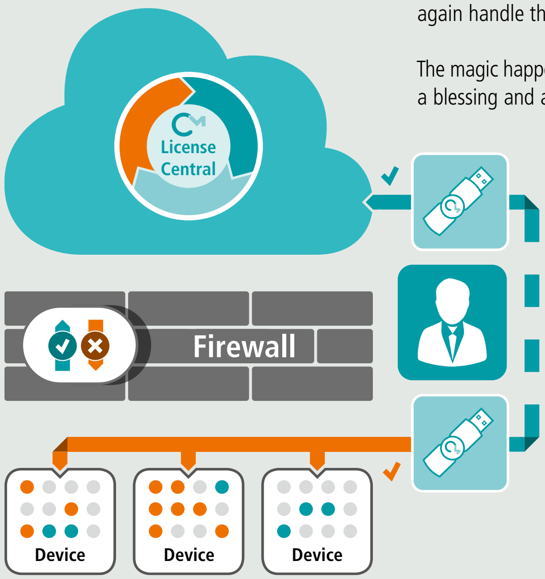




Bridges and Ferries

Whenever a device cannot or must not create an outbound connection with the Internet, a separate computer can often be used as a bridge. That computer is located on the internal network and can therefore access the target device. At the same time, the computer can make the connection with CodeMeter License Central on the Internet. A service technician would initiate the update, which would then be transferred automatically without any further manual intervention by the technician.

This can be implemented in two ways: The first option is to include the entire technology in a webserver that is usually already available on the device. The technician would then only have to use a browser to call that webserver.



The second option is a customized Software Activation Wizard on the technician's computer. The wizard uses the gateway API to communicate with CodeMeter License Central and a proprietary protocol to speak with the target device, which is usually already made available by the device's maker. Typically, only three new types of transactions need to be added: Listing CmContainers, receiving the context file of CmContainers, and using update files for CmContainers.

Using a software activation wizard offers another great advantage: If it is not possible to create a simultaneous connection with the device and with the Internet, the context and update files can be 'parked' and the process broken down into three separate steps. The third and final step is optional, as it only handles the receipts. This approach could be visualized as a ferry service that moves from riverbank to riverbank.

License Transfer (Move)

In this scenario, any number of licenses can be transferred onto a CmDongle (the transfer dongle). The target device that these licenses are intended for does not have to be known at this point. A service technician would use the transfer dongle and connect his laptop with the target device, resembling the bridge with CodeMeter License Central. The license is again transferred as in the case of the bridge: A special lean Software Activation Wizard uses the proprietary protocol to transfer the licenses, and the mentioned three transactions again handle the process.

The magic happens offline in this case, which is a blessing and a curse. No Internet connection is required, but that also means that CodeMeter License Central has no up-to-date information about the licenses' current state, which limits the ability to update licenses. The approach is particularly good for rolling out individual additional licenses (as separate Product Items), but not for updating licenses.

Push It

Let us return to the push approach: Once a device is known to CodeMeter License Central, a context file of the CmContainer on the user's device will be available in CodeMeter License Central, and the update file can be created for the target device. No data from the device, except the serial number of the used CmContainer, is needed to create the license update. The assignment between license and CmContainer can already be made when creating the license in CodeMeter License Central or later by the technician on site, when they download the license update.

The update file can be imported onto the device via a memory stick, requiring only one new transaction "Using update files". All of this can happen locally on the target device without any additional computer or proprietary protocol, or the bridge approach can be replicated by importing the file via a webserver and browser on the technician's computer.

It is not a problem if an update is missed in this case. If CodeMeter License Central did not receive a confirmation that the license has arrived at the target device, it will include all older updates in the next update. This is transparent for the user, as the updates are all packaged up in one combo-file.

This resembles the ferry scenario, with the only difference that the selection of a CmContainer in CodeMeter License Central or WebDepot is replaced by the creation of the context file. This can be done beforehand without technicians needing physical access to the target device

Our Service at Your Service

Let us take a quick personality test. You are trying to solve a particularly hard puzzle while you are home. Would you A) keep working until you have solved it by yourself, or B) let your friends and family help you? Whichever type you are, one thing is certain: You usually cannot play out your personal habits at work. In a professional environment, efficiency is key. It is about finding the best solution with the minimum input of costs and resources. Long gone are the times when you could give yourself days and weeks to solve a problem. Wibu-Systems is here for you when you need to find the perfect software protection, licensing, and security solution as soon as possible, and we will stay at your side before, during, and after you launch it. If you want, we can even operate it for you.

CodeMeter gives you so many ways to introduce protection and licensing for your software. This can make it hard to find the perfect choice for your specific needs. We want to ensure that your design decisions and protection concepts are perfect from the word 'go', which is why our Professional Services team offers foundation courses on many CodeMeter topics. You can invite us for in-house training at your business location. Our in-house seminars can be tailored specifically to match your needs and interests, e.g. covering only the relevant aspects of our foundation course on the first day and then moving on to a workshop to help you pick the right licensing concepts. At the end, you will have everything you need to kick-start your licensing and protection solution.

And should you still have questions when integrating CodeMeter into your software, Wibu-Systems' support team is again ready for you with competent advice. Our service portal is open for your questions around the clock, or you can send us an email or contact us by telephone. Our support team has the in-depth technical know-how to answer all of your questions and boost your confidence. Our technical support will sort your queries and answer all of them quickly according to their priority and your chosen support package. The choice is again yours: You can build on the free basic support with two premium levels – silver and gold – that give you guaranteed access to a named partner, comprehensive support, and a contractually agreed response time.

If any of your users have a question about installing or using the system or encounter any disruptions, they can contact our support team directly by email or phone. Many questions are answered faster and better in a direct conversation with your users than if your support team had to pass the issue through to us. Our specialists have seen almost every possible issue and can save the day with competent advice. This additional service is free of charge for your users, and for your business.

These services are complemented by our operating services team specialists: Wibu Operating Services (WOPS). As part of our Support unit, WOPS can operate the online licensing solution CodeMeter License Central and the CodeMeter Cloud for you from our data center in Frankfurt, Germany. Our experienced professionals will take charge of the infrastructure and the smooth provision and seamless operation of the systems, naturally including maintenance for the operating systems and the Wibu-Systems applications on the hosted systems. With 24/7 supervision, we ensure online licensing with top reliability for your clients and users. You have a choice of packages to match the number of licenses per month and level of availability you need.

We are here for you – choose one of our many services and save yourself invaluable time and money.

Virtual Systems – Undermining Licensing?

Virtual systems are popular. These days, wherever possible, services and solutions are virtualized. The advantages are plain to see: The services can easily be migrated from hardware to hardware or scaled up as required. Replacing a server used to be a major undertaking; now, services or entire virtual machines can be moved in an instant. Gone is that nail-biting moment upon reboot: Will the old server start up again? Life today is good for administrators – at least in this respect.

Administrators trust their data centers, and they trust the security mechanisms in place. In most cases, that trust is well-placed and well-founded. Software is installed and just works as intended. But consider the same situation from the software vendor's point of view. When the software is installed on a virtual machine, who is in control? Does virtualization mean a loss of control? Who can stop users from cloning entire virtual machines if they want more copies of their software running?

Wibu-Systems offers several answers to these questions in the form of its licensing solutions. The first choice that deserves to be mentioned is represented by CmDongles, powerful pieces of hardware that are not particularly well-liked in data center environments. There are options, however, such as the use of dongle servers that can accommodate multiple USB dongles for access by the other hardware in the data center. CmDongles might also be the right option for single physical servers that need to be operated e.g. because certain hardware components are required in the system. Whatever the case may be, the CodeMeter license server is so resource-efficient that it can operate unnoticed alongside virtually any system.

The current most popular choice is a software-based license, or CmActLicense, which uses special cryptographic operations to bind itself to certain properties of the target system. CodeMeter naturally knows whenever it is running on a virtual system and uses a special combination of binding parameters in such cases. Some configurations allow CmActLicense to be bound to a set of properties of the virtualization system guaranteed by its provider, such as systems hosted in Azure environments. A similar option is in the works for other virtualization environments.

Container environments like Docker represent a special challenge for licensing purposes. While these environments are especially well-insulated and optimized for scaling up, there are ways to license the software running inside such containers. In these cases, licensing needs to be considered long before ever thinking about the eventual release. Licensing should be in the picture when deciding about how services are allocated to individual containers. The last issue of our KEYnote (38) explored several scenarios for this approach.

The most recent option is the use of a CmCloudLicense. Wibu-Systems operates the CodeMeter Cloud exclusively in a data center based in Frankfurt, Germany, where the Wibu Operating Services specialists work to ensure the permanent availability of the licenses. Any CodeMeter installation on a user's system can be linked with the CodeMeter Cloud, giving software vendors and their users the full freedom to use all of the power of virtualization – safe in the knowledge that the licensing system works as it should.

There are many solutions to the challenges presented by virtualization – all you need to do is pick the one that is right for you.

Co-Working and Offices in the House of IT Security

The health and future prospects of our economy depend on IT security as a fundamental "enabler" technology. Artificial intelligence, digitalization, and connected infrastructures all need security. One way to stimulate innovation in this and other fields is co-working: Knowledge workers come together in spaces shared with their peers and professionals from other enterprises and organizations. A study on co-working by the Fraunhofer IAO has revealed that co-working spaces have a measurable impact on innovation. Many companies have already realized the potential of the concept for gaining a strategic advantage in their market.

In addition to providing much-needed ad-hoc space for teams and project work and important all-inclusive services, co-working spaces create an inspiring environment that is proven to boost the innovative output of project teams and inspire a more independent, responsible, and self-driven style of working. The other advantages of co-working spaces include:

- Professional office spaces fully equipped with the required infrastructure
- Meeting venues for shared use
- Completely furnished communal spaces, including kitchens, a lounge, and bar
- Extremely flexible leases in terms of space and lease duration

Breaking with the usual open-to-all formula of regular shared office spaces, the House of IT Security is dedicated to a single area of work: the eponymous IT security. It will only lease space to companies, researchers, and official institutions working for a safer and more secure IT world. The new building enables the installation of top-flight building automation and security technology, including redundant fiber-optic connections and modern access controls. The elegant architecture will house premium workplaces, IT security labs, and communal spaces with lots of amenities. Compared to other co-working spaces, the House of IT Security enables calm and concentrated work in a relaxed atmosphere; separate offices and open-plan spaces ranging from 200 to 500 sqm are available.

By combining a range of actors in one focused "physical beacon" for IT security, the new location will form a completely novel pool of expertise and competencies. Tenants can foster invaluable networks with other IT experts, especially from Karlsruhe's vibrant IT security community, and seize opportunities for new inter-company co-operation. Wibu-Systems is committed to pushing IT security research and progress by bringing together and actively supporting leading research institutes and enterprises working in the field.

The place to be: Wibu-Systems in Karlsruhe

Karlsruhe has established itself as one of Europe's top-four IT hubs, bringing together an exceptional pool of IT competence with approx. 4,200 IT companies in the city. The region's unique advantage is maintained by three centers of competence working on IT security and computer science departments regularly topping the academic rankings and educating the IT professionals of the future. The House of IT Security is already seen and supported as a great addition to the state's business ecosystem by all its local Karlsruhe partners (KIT, KA-IT-SI, FZI, CyberForum, Cyberwehr Baden-Wuerttemberg) and industry associations like bitkom and the VDMA.

Wibu-Systems has deliberately located its new facilities in the heart of Karlsruhe, near the high-speed rail station and with excellent local transport connections. The Citypark located only 100 m away is a perfect place to relax, and local restaurateurs offer a range of cuisines for every taste.

Stay up to date and tell us what you think!

You can request more information or share your feedback with us by taking five minutes of your time and completing our feedback form at wibu.com/hoits. We are interested in what you have to say even if you are not looking to join the House of IT Security. Thank you!

News in Brief

Meeting in the digital space

Connectivity is key and even more relevant and urgent than ever, as the temporary lockdown enforced by several countries has shown. Our live and interactive masterclasses offer unique content that will help migrate your business from a static paradigm to a dynamic concept ready to be easily scaled up or down, meet customer' demands, and withstand emergencies.

CodeMeter Embedded 2.40

Beginning with release 2.40, CodeMeter Embedded offers two alternative options for transferring licenses offline: You can either make use of an update file and assign licenses via CodeMeter License Central to the embedded devices already recorded during production, or place the licenses in a CmDongle and transfer them to the embedded device of your choice via a local connection to the laptop the USB device is plugged into.

Embedded

CodeMeter License Central 3.3x

Last December's release of CodeMeter License Central 3.31 supports the new TMR server (Triple Mode Redundancy), our concept for installing a high-availability server at your user's site that complies with the two-out-of-three principle. You need ver. 3.31 only if you use the TMR server. A ver. 3.30 update is planned for April. This is the release for general use without a TMR server.

License Central

CmStick – A dongle for every need

The complete range of CmDongles now consists of no fewer than 18 form factors. Choices include different sizes of the device, casing materials, connecting interface types (USB, SD, microSD, CFast, SPI), USB connector mounting types (SiP or standard), USB protocols (2.0 or 3.1), nand flash memory classes (MLC or pSLC), and temperature ranges in the operating environment, as well as the choice to make the units removable or permanently fixed. All CmSticks with flash memory also come with disk encryption, a private partition, and key storage in the CC EAL5+ certified security controller, which also allows the secure deletion of flash disk contents.

Silver Linings: Licensing in the Cloud

"Cloud computing" has become ubiquitous, but what are the issues when it is applied to cloud-based licensing? Security is always a question mark when it comes to cloud services. This white paper describes secure cloud-based license management with CodeMeter Cloud and License Central and the use of certificate chains to establish trust in the cloud licensing and storage environment and to protect the integrity of the service.

DigiFab4KMU – Paving the way for smart factories

DigiFab4KMU intends to enable a meaningful integration of all construction phases and the underlying data in a single system by developing an innovative Integrated Virtualization System that will consolidate and make available all relevant data and information for the entire project's lifecycle, for all functions and trades, and for all relevant systems already in place.

DigiFab
4KMU

Resilience at the time of COVID-19

Even though the situation triggered by the Corona virus pandemic is evolving rapidly and making it difficult to plan for the long term, Wibu-Systems is taking the necessary measures to protect its staff, customers, partners, and suppliers, while continuing to deliver CodeMeter and WibuKey dongles as scheduled, operate its cloud and hosting services, provide professional consulting, sales, and marketing services, and focus on the next generation of technological innovations.

Secure and easy home office setups

Coming to the aid of software publishers during the Coronavirus crisis, Wibu-Systems is making available its brand-new cloud-based license containers for free throughout Q2/2020, so you can offer software licenses to home office workers from the comfort of a secure cloud environment. This new technology combines the typical robustness of hardware-based protection with greater ease of use and scalability.

Case Study | Desoutter

Desoutter is going for digital gold

With CodeMeter from Wibu-Systems, the company can offer its customers an answer to the expectations generated by Industry 4.0 and protect its intellectual property at the same time.

The Challenge

In the Industry 4.0 world, Desoutter's customers call for a higher degree of flexibility in the way they can use their products. The company looked for a solution that could bring that level of versatility within reach for every customer and help establish Desoutter's position as an Industrial Internet frontrunner in the market.

The Solution

With its hardware products, Desoutter no longer sells software with fixed licenses. Instead, the company implemented an innovative concept that lets its customers dynamically assign a certain budget (in the form of Unit Values – UVs) to access only the features and functions they need. In order to protect the Desoutter UVs against the threat of cybercrime, the company has turned to the expertise of Wibu-Systems.

The Result

While Desoutter's tools remain the focal point, it is with its software that Desoutter makes a real difference. The combined power of Desoutter UVs and the tough Wibu-Systems protection mechanisms ensures that customers can invest only in the features they specifically require. And by providing such a high level of flexibility, Desoutter is strengthening the relationship with its customers.

The Company

Desoutter Industrial Tools designs and produces electric and pneumatic assembly tools, such as high-tech tightening and drilling solutions for the aerospace and automotive industries. Desoutter is headquartered in the French city of Nantes, where more than 200 of its 1300 employees worldwide are engaged in R&D, including 60 dedicated software and electronics developers.

Laurent Macquet,
Line Manager Software & Embedded Systems at Desoutter

"For us, it's important that we can offer our customers the adaptability they need in Industry 4.0. It's not so much about selling as many licenses as possible, but rather providing a solution that meets the peak versatility our customers demand. How do we do that? We have taken a new look at each tool's features and made them more flexible for our users. Together with Wibu-Systems, we have built a solution to free us from the constraints of traditional software licensing."

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.		
German Headquarters	+49 721 931720	info@wibu.com
Belgium / Luxembourg	+32 2 8086739	sales@wibu.be
Canada & USA	+1 425 7756900	info@wibu.us
China	+86 21 55661790	info@wibu.com.cn
France	+33 1 86266129	sales@wibu.fr
Italy	+39 035 0667070	team@wibu.com
Japan	+81 3 43608205	info-jp@wibu.com
Netherlands	+31 74 7501495	sales@wibu-systems.nl
Spain / Portugal	+34 91 1230762	sales@wibu.es
United Kingdom / Ireland	+44 20 31474727	sales@wibu.co.uk

Join Wibu-Systems and its subsidiaries at the following events:

Forum Safety & Security
23-24 June 2020
Stuttgart, Germany

DevSec
28-29 October 2020
Ludwigshafen, Germany

Compamed / Medica
16-19 November 2020
Dusseldorf, Germany

Connected Things
14 September 2020
Cambridge, USA

Electronica
10-13 November 2020
Munich, Germany

SPS
24-26 November 2020
Nuremberg, Germany

Imprint
KEYnote 39
Edition, Spring 2020

Publisher
WIBU-SYSTEMS AG
Rueppurrer Strasse 52–54
76137 Karlsruhe, Germany
Tel. +49 721 93172-0
Fax +49 721 93172-22
info@wibu.com
www.wibu.com

Responsible for the content
Oliver Winzenried

Editors
Joerg Jans
Ruediger Kuegler
Philipp Luedtke
Daniela Previtali
Wolfgang Voelker
Oliver Winzenried

Design
Eugen Olchin

Print
Stober 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.

Picture credits:
Cover: istockphoto.com/alphaspirit
Page 4: istockphoto.com/BrianAJackson
Page 6: istockphoto.com/Who_I_am
Page 8: istockphoto.com/tzahiV
Page 10: istockphoto.com/Petrovich9
Page 12: istockphoto.com/Stas_V
Page 13: istockphoto.com/loops7

All remaining images are
copyrighted by their owner

SECURITY
LICENSING
PERFECTION IN PROTECTION

5060-002-02/20200424 © 2020 WIBU-SYSTEMS AG