SPRING 2015

KEYnote 29

THE WIBU-MAGAZINE

Revolutionary invention: Blurry Box® Technology

Highlights

- CodeMeter License Central 2.10
- CmDongles with flash memory for unique new possibilities
- CodeMeter in Plant Automation

WIBU SYSTEMS

Content

Dear Clients and Partners!

"Hackers costing the economy €300 billion." The headline of Germany's FAZ on 30 December was stark. Cybercrime has reached a new level: be it straightforward snooping and spying, the manipulation of production management systems, public infrastructure, or the Sony hacks. The 31C3, the annual meeting of the Chaos Computer Club in Hamburg, has again revealed new methods used for illicit ends. This is not the reserve of the criminal underworld alone: secret services everywhere are ramping up their capabilities. Governments, East and West, are preparing for the cyber wars of the future.

Germany's Federal Office for Information Security (BSI) speaks of a veritable flood of attacks in its annual report and laments the 'digital carelessness' of the people making the decisions in business. There is no such thing as absolutely airtight protection, but that is no excuse for not doing anything. We have spent the last year adding more and more talent to our team. Our new Blurry Box® technology has been awarded the coveted German IT Security Prize of the Horst Görtz Institute – an honor and another motivation for us to keep one step ahead of the hackers. It encourages us to continue to provide you with simple-to-use solutions to protect you against the worst threats. Minimum effort for maximum security. Come and speak to us about your protection, licensing, and security needs. By the way: A study conducted by BITKOM Research shows that the IT industry is becoming more attractive than ever before: 32 percent of all high school graduates in Germany expressed interest in a future in IT – coming close on the heels of engineering careers. This is a trend we all have reason to celebrate.

Read this KEYNote and let yourself be stimulated with new ideas about how CodeMeter is used in production automation, about the PKCS#11 and CSP-compliant storage of certificates, about innovative features for our License Central, and about the use of CmDongles with Flash memory.

Finally, I would like to invite you to come and visit us at one of our events this spring – I am always looking forward to meeting likeminded people. I wish all of you a happy and successful 2015!

Yours, Oliver Winzenried

CEO

CodeMeter in Plant Automation

Why does automation need CodeMeter?

Industrial controllers are becoming more and more intelligent every day. The highly specialized, often custom components of the past are being replaced by generic industry PCs or smaller ARM-based embedded devices whose functions are not just dependent on what their hardware allows, but also on how they have been programmed. The same hardware can operate an industrial loom, regulate the turbines of a power plant, or move data from barcode scanners to fieldbusses. All of this is integrated and connected for remote maintenance. It is just a matter of the right programming. Such versatility is a great cost-saver and a guarantee of maximum flexibility, but it also creates new challenges for the security of these IT systems.

These small computers have come to be known as embedded devices. Two decades ago, the concept of Programmable Logic Controllers (PLC) replaced the old fixed relay systems. As the devices are spread around the facilities they control, they are often interconnected for easier maintenance and supervision. More and more sensors are also included in these networks. One typical example is a smart meter that reports consumption levels to higher controllers in real time.

Using IT components made this a workable and inexpensive option for the manufacturing industry, marrying the disciplines of mechanical engineering and IT. Manufacturing 4.0, the Internet of Things, and the much-vaunted cloud are just a few of the many buzzwords in the industry. PLCs in production plants are linked with servers in the order processing department. Developers send their designs directly to the toolmaking machines. Managers can watch their production reports in real-time dashboards, even if they are continents away from the actual factory. This new type of system has been called a "cyber-physical system".

Much of this has become an everyday standard. What is new is that components are not operated in isolation, but vertically integrated from the field to the SCADA systems up to MES at the top.

Manufacturing facilities are designed to operate over long periods of time. All of the mentioned functions have grown over time. Old parts are linked with cutting-edge systems. Many of them used to operate in closed networks or rely on proprietary interfaces. Whenever the system is expanded, people care about three criteria: functionality, security, and cost effectiveness. But new functions often outpace the necessary protections trying to keep up. Too often, virus scanners and firewalls are all that people think of – two minor building blocks of a total security concept and two building blocks that are often out of place in plant automation.

Secure Networks

The security of manufacturing facilities and industrial systems is defined primarily by the security of their perimeters. That means protecting the factory on the outside with such simple means as high fences and thick doors. Production networks are similarly fenced in and protected by firewalls against the virtual world around them. There are also internal access restrictions with doors and login-protected systems.

But experience tells us: This is not enough. Trust in secure perimeters alone is trust misplaced.

Modern IT networks have more loopholes and backdoors than ever before. From WLAN to remote maintenance or site integration and internet access to the reliance on cloud services, firewalls have many openings to allow the functionality expected and required today. Many large and medium-sized businesses have done their homework and establish strong safeguards in their networks. The attackers have followed suit and often do not come in through the front door, but rather via third parties. Germany's Federal Office for Information Security warns of the dangers of the network connections of smaller business partners. Lacking security expertise and resources make these more prone to exploitation than the actual target of the attacker – a preferred bypass for cyber criminals.

The problem is made worse by the many unintentional holes in the fence: bugs, surplus LAN ports, unmonitored remote access and so on.

If an attacker has overcome the first hurdle, he is already in the network and can start his malicious work. There will never be a foolproof yet commercially viable network.

The Inside Man

Attacks over the net might sound impressive - a common sight in movies and everyday news, and a very real danger. However, the most straightforward and most immediate danger is too often ignored: the attack from the inside. Attackers from within do not have to overcome the outer fences in the first place. They can walk right through the door and enjoy the trust of their peers.

A recent study by VDMA, the German Engineering Federation, considers malpractice and sabotage as well as the intentional injection of malicious code the greatest current threats, with online attacks trailing behind. A majority of current security incidents are caused by insiders whose motivations reach from the archetypal disgruntled employee sabotaging production facilities to the selling of internal secrets as outright industrial espionage. The results of the study show that the concept of ring-fencing businesses with sophisticated access controls is powerless to stop this.

Countermeasures

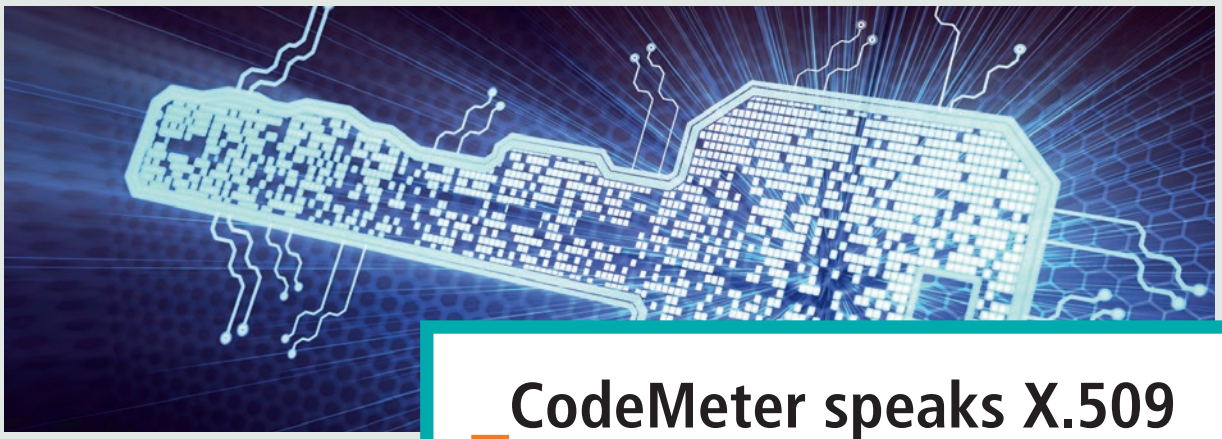
Rolling out additional security down to the level of individual controllers (with the respective licenses this needs) is often regarded as too complicated and cost-intensive. Such security is not essential for actual operations. However, current news about the activities of domestic and international secret services, not least in the field of industrial espionage, has given this topic a new relevance. The many individual attacks on single controlling systems or entire plants and institutions often go unnoticed in this flood of headline-grabbing news. The damage caused by lacking or flawed protections far exceed the upfront investments. The established precautions need to be expanded to protect the individual components. The security concept should begin as soon as any device is turned on, using a secure boot process to make sure that the software from the operating system to the individual application and its configurations has not been tampered with. Software developers are also interested in protecting their products against piracy. Just like their peers in mechanical engineering, they want to make sure that their expertise cannot be stolen or emulated. All of these protection needs for embedded devices are covered by CodeMeter technology. Working with License Central, this makes the allocation of licenses and keys user-friendly and stops the end user from having to worry about complex CAs or cryptographically secure key exchange processes.

In the IT world, CodeMeter's dongle solutions and hardware-based license files are a long-established and trusted option, used frequently with specialist software like CAD applications. The principle has been adjusted for the world of embedded systems, as its implementation differs considerably from the old PC-based scenario: There are more operating systems and hardware platforms, all with their own tool chains. The available system resources also matter. Add to this the constraints of real-time operations and lifecycles of 10 years or more.

Ready-made CodeMeter Embedded Libraries are available for common combinations of operating systems and processor models. These can be integrated immediately in the protected applications. In the end, the CodeMeter Embedded Drivers are ready for virtually every device that has a libc. Keys and licenses can be stored on USB dongles, SD cards, ASIC chips, or in CmActLicense files.

The market already has solutions with integrated CodeMeter technology as a simple-to-use feature for the end user, e.g. CODESYS for PLC programming or Wind River VxWorks 7.0. Both come with CodeMeter built into the core of their development environments, making the solution available for use without any specialized know-how. There are many other custom implementations for controllers, embedded systems, medical devices, or entire production systems, protected by CodeMeter Embedded.

Any given manufacturing plant has many different parties involved, all with their own protection needs: the makers of controllers, mechanical engineers, the producers of the components, and the actual operators. Every party has a legitimate interest to protect. Plant engineers want to protect their intellectual property from being copied or stolen. Component suppliers want their set operating parameters to be maintained for warranty reasons, and they might have a licensing system integrated with their components. The plant's operators care about the reliability and integrity of their facilities, and they want their process data and operating parameters to stay protected. Technicians commissioning and servicing the facilities need a licensing process that does not stop them in their work. What all of these people care about is a fully secure system whose protections simply work as they should and safely hidden from view - which answers the original question of why automation needs CodeMeter.

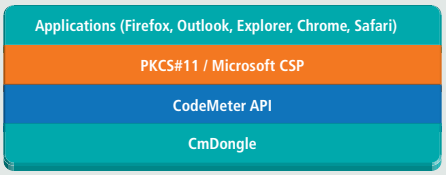


CodeMeter speaks X.509

Server certificates are a ubiquitous sight. They offer users the certainty that they are indeed on the right website and have not fallen prey to a phishing attack. By contrast, client certificates continue to be held in low regard. They are virtually ignored by the wider public, even though they are a simple, safe, and fully compliant means of authenticating users. This is particularly true when they are stored on secure hardware like CmDongles.

Authentication with certificates

The user possesses a private key and a matching certificate. As part of the handshake and key exchange, the user uses the private key to sign the hash of the message. The signature and the client certificate are then transmitted to the server, where their validity is checked and ascertained. If both are valid, the identity of the user can be retrieved from the certificate and used.



Layer model

Standard interfaces

- There are many versatile uses for certificates, including:
- Email certificates to sign and encrypt emails
- Client certificates to authenticate end user devices in IT networks
- OPC UA certificates
- User certificates for authentication on computers and in networks

There are many different software products that rely on certificates, such as mail clients or web browsers. At the same time, several providers offer secure hardware that can be used to store certificates or, in many cases, purely software-based storage solutions. The following interface standards have been established to ensure a reasonable degree of interoperability between all of these systems:

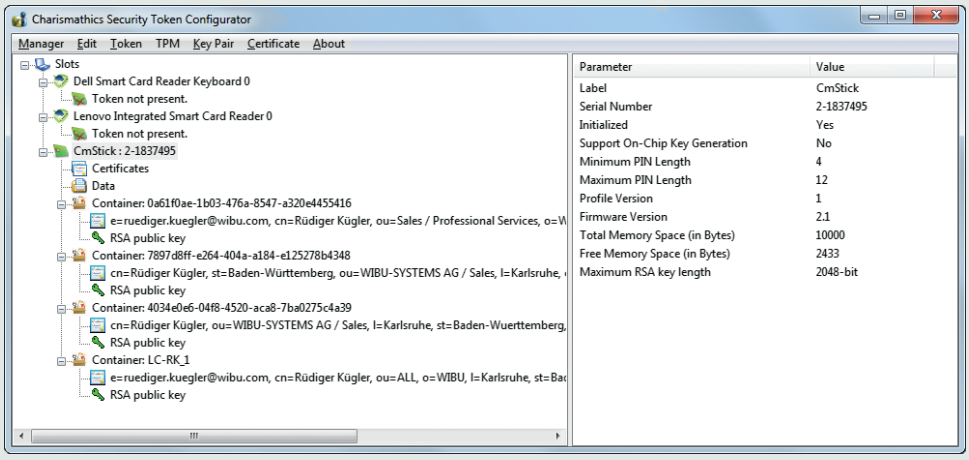
- PKCS#11 for all computer platforms
- Microsoft Crypto Service Provider (CSP) for Windows
- Token Daemon (tokenD) for Apple OS X.

Certificates on CmDongles

CodeMeter includes a PKI client application as an add-on module (Charismatics Smart Security Interface - CSSI). The CSSI middleware comes with a Microsoft CSP and a PKCS#11 interface, which makes the private keys and certificates stored on CmDongles available for almost all applications, including Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari, and Microsoft Outlook.

A CmDongle can store up to 8 private keys and the matching certificates, using an RSA algorithm with a key length of up to 2048 bit. The private key can either be imported from an external source (using the pfx or p12 format) or created immediately within the CSSI middleware. It is stored in dedicated secret data fields and protected from prying eyes.

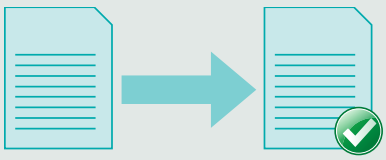
The CSSI middleware can request a certificate (Certificate Signing Request – CSR) from a source issuing the certificates and import the resulting certificate itself. Alternatively, it can create a self-signed certificate from within the CSSI middleware itself.



CodeMeter License Central 2.10

Creating, delivering, and managing licenses has never been easier with the latest edition of CodeMeter License Central. Many changes, new capabilities, and improvements under the hood automate many tasks to streamline the routine work of software developers everywhere. Read more about the new features in Version 2.10:

Revised Activation Confirmations



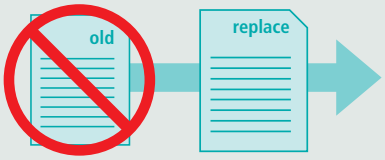
When a license is activated or deactivated, a receipt is created and sent to CodeMeter License Central which makes sure that the license was updated successfully. To do so, CodeMeter License Central uses a dedicated value in the license, the Firm Update Counter. Every change to the license, including its deactivation, is added to the counter. CodeMeter License Central knows the past count and can decide immediately which updates were implemented successfully and which might still be missing.

If the state of the CmContainer does not match the known record in CodeMeter License Central, the CmContainer is flagged as "Manipulation detected" and requires a manual decision by the owner.

Automating Missing License Updates

It can happen that no receipts are created for an update, especially when licenses are updated offline. Before any new update, all previous instances are recorded as far as the received remote activation context file allows. If there are any missing updates remaining, these are included automatically with the next, multi-step update. When the user begins the update, the CodeMeter Runtime uses the Firm Update Counter to determine the right place to begin. This process means it is irrelevant whether or not the user has completed the previous updates – the license will be brought up to the correct and current state in every case. This automatic feature is included in current CmDongles.

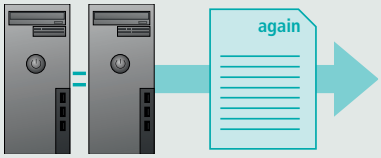
Automating Reactivations



Should any license be lost, e.g. by the complete loss of a computer with a CmActLicense, it is up to you as software developer to allow your users to reactivate their licenses, either in every case, after a defined hold period, or for a manual choice of cases (any combination allowed).

You can decide whether the old CmContainer should be automatically blacklisted after the reactivation. The blacklist check can be integrated in your software to lock down any lost CmContainers automatically. The blacklist can also be distributed offline with your next update.

Reactivating Licenses on Previous Computers



One particular scenario is the reactivation of a license or a complete CmContainer on what should be the same machine. The typical case would be a clean install of the complete system. You can define your own rules for this scenario that operate independently from the reactivation of individual licenses. These rules also apply either generally, for defined periods, or for manual instances only.

All licenses in the CmContainer created by CodeMeter License Central are recovered. The old CmContainer is automatically blacklisted.

When a license is created, a unique identifier, the TicketLicenseId, and a generation counter are stored in the license. This information shows you if a single license is kept in multiple copies on the same machine or in the same network. How you respond to this is for you to decide.

Push-Updating Licenses

Licenses are usually delivered in a three-step process: The client sends a request to CodeMeter License Central. An update is prepared for the user, and the procedure ends with an optional receipt, which is only required in the case of returns. Online activations manage all of these steps in the background without any actions required on the part of the user.

For push updates, you select a CmDongle that was programmed by CodeMeter License Central and is now used by the client. You produce the update and push it to the user – a simple, one-step process.

As a software developer, you can always switch between simple push updates, the standard process with receipts, and current data.

Updating Dedicated CmContainers

In normal operations, you send your user a ticket with which to activate the license in a CmContainer of the user's choice. You can decide whether this should be a CmDongle or a CmActLicense and whether the user is free to make this choice.

There are certain scenarios in which you would create licenses for a specific CmContainer. In this case, you would set the serial number of the CmContainer when creating the license. The user now needs no ticket and authenticates himself or herself with the CmContainer.

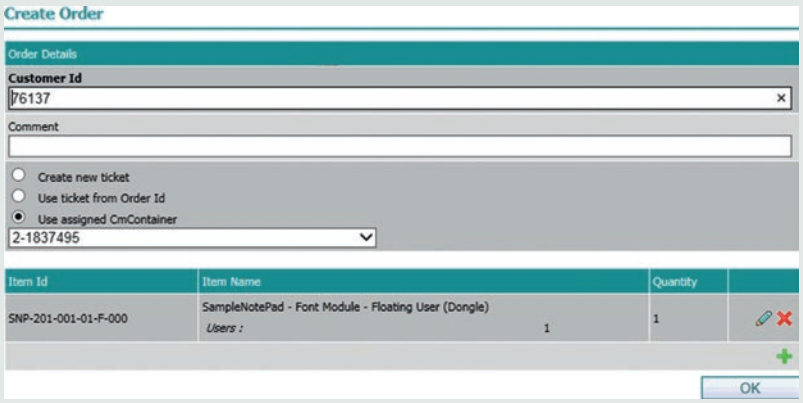
The system also allows a hybrid approach with tickets and licenses allocated to named CmContainers. In that case, the allocated licenses are retrieved automatically and in the background when the ticket is checked in.

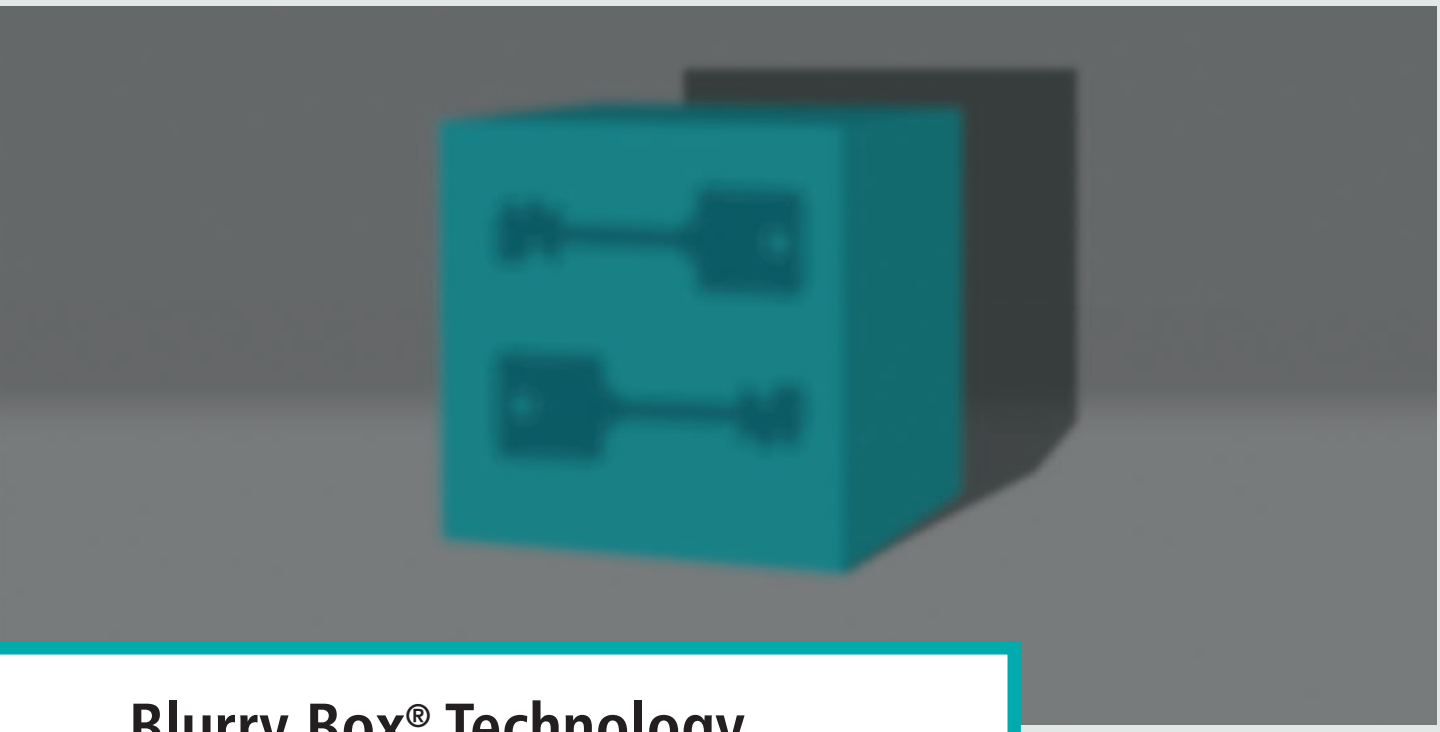
Recycling CmDongles

Users might return their CmDongles to the software vendor, e.g. when trials end. CodeMeter License Central now allows you to recycle such CmDongles, deleting the dongles and removing any activated licenses from current records.

Summary

CodeMeter License Central 2.10 equips you as the software developer with lots of new automated features. You can decide whether and which actions should take place in the background when a license is reactivated. The rules for such reactivations now also include activations on the same computer. You can distribute updates for CmDongles via the push service or link licenses with a specific CmContainer. The recycle function allows you to reuse any dongles returned from the field.





Blurry Box® Technology

Software is contributing an ever greater share to the value created in our economy. This makes software protection an increasingly important part of IT security: Software protection stops the illicit copying and reverse engineering of products containing software and is therefore an important safeguard against industrial espionage.

Kerckhoffs' Principle

Kerckhoffs' principle states: "The key is the secret and not the method."

All software protection solutions currently in use violate Kerckhoffs' principle, since they rely essentially on guarding the secrecy of the protection method itself. An attacker who knows these methods is already half-way through the fence. In theory, the methods that can protect software in compliance with Kerckhoffs' principle are already known. However, these are not used in practice for resource and performance reasons. CodeMoving, essentially the execution of the protected program in a secure special hardware key (dongle), is equally too slow for regular operations in complex applications.

The Blurry Box Approach

Blurry Box makes Kerckhoffs-compliant software protection a reality. Blurry Box® technology was developed in partnership with the FZI research center, the Karlsruhe Institute for Technology and Wibu-Systems. It is scheduled for release to software developers in mid-2015.

Blurry Box technology assumes would-be attackers know the Blurry Box method, and the protected software product is not a black box for them. They can use the software and access the executed code in cleartext form. But Blurry Box technology makes static code analysis impossible and adds more solid layers of protection against dynamic code analysis.

Blurry Box technology and its proof of concept come in response to empirical observations and experiences from software development and the world of hackers and IT criminals over the last 20 years.

- Typical software is so complex that nobody could run the entire code simply by operating the application. A typical user uses around 10 to 20%, a power user 30 to 50%, and internal quality inspectors 80 to 90% of the code.
- A hacker will usually have considerable knowledge about the act of hacking itself. He or she might find hidden code, change return values, combine code fragments, or read and reenter code in the computer's memory banks.
- A hacker does not know the actual purpose of the software or its internal workings.

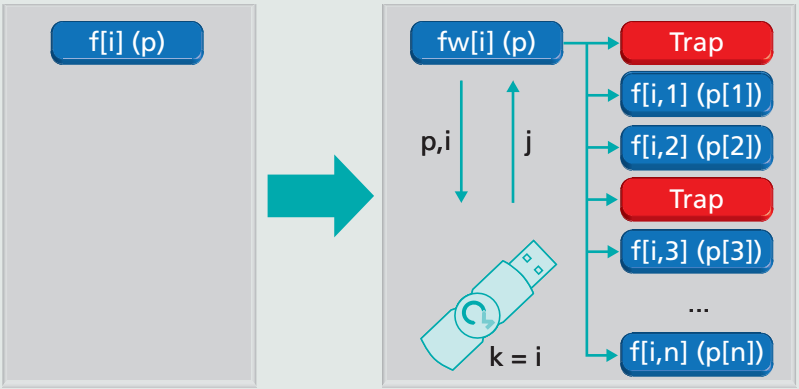
These insights, specifically the lack of specialized subject-matter expertise, help establish software protection that works without having to outsource substantial amounts of the executed code to a dongle.

How the Blurry Box Works

Blurry Box technology combines multiple methods which will be showcased here.

Multiplying function blocks as variants

Any application can be broken down into a group of function blocks. A function block f[i] can have the entry parameter pIn[i] and output parameter pOut[i]. Depending on the pIn[i], the function block will return pOut[i]. In the Blurry Box process, the individual function blocks are multiplied into several variants: A function block f[i] is turned into blocks f[i,1] to f[i,m]. The function blocks f[i,j] are accessed with a wrapper function fw[i] depending on the access parameter pIn[i]. The output of variant f[i,j] is returned as value pOut[i], which means that the code executed



Calculation of variant selection in the dongle

during each cycle is minimized, governed by the chosen wrapper parameters.

Modifying the Variants

One trivial means of bypassing the variants would be to tamper with the wrapper function fw[i], so that only a single variant is executed in every case. To close this door against attacks, Blurry Box technology modifies the variants for a function block to only work with the correct range of parameters. An attacker without inside knowledge will not be able to recover other unknown variants or the original function block simply from single (or even several) variants.

By modifying the code, the variants would deliver incorrect output for parameters not within their range. Without a specialist's insights, the attacker would have no means for correcting this intentional mistake. The unknown variant could therefore not be replaced with a known substitute.

Encrypting all Variants

Every single variant is fully encrypted, with the encryption key stored securely on the dongle, which also holds an API function to load the encrypted data and decrypt it inside the dongle. The decrypted code is returned by the dongle API and executed as a code variant. Without the dongle with the correct key, no variant can be decrypted. The encryption uses the Advanced Encryption Standard (AES) and includes a random value in the computation to represent blocks with similar contents in different cipher texts.

Built-in Traps

To prevent attackers from decrypting all variants by the dongle without the application being executed concurrently, several trapdoors are built into the system. These trapdoors are encrypted variants that would flag the license in question as invalid when they are encrypted by the dongle. For the trapdoors to work not only for statistical attacks, but also for attackers who try to analyze the source code in question, the source code includes links leading directly to the booby-trapped blocks. These would never be accessed during regular operations, since they would only be accessed in variants that are not expected to be executed when the application is run normally.

Computing the Choice of Variants on the Dongle

Code moving (executing the program code on the dongle) is usually not a feasible option, as it slows down the protected application too much. Selecting only a sensible portion of code to be executed on the dongle is, in turn, too complex to be implemented meaningfully. The code for computing the selection of variants, however, is a very good choice for code moving. It is a short, but essential piece of the puzzle. The selection and implementation works without involvement of the software's original developer and is fully automated. For this purpose, the index of the wrapper function (i) and the relevant parameter pIn[i] are moved to the dongle, where the index of the variants to be accessed is computed and returned (j). This makes it impossible for attackers to predict which variants (or trapdoors) are chosen or not chosen, even if they know the valid parameter range, unless the code is run with the right parameters.

Using the Dongle as State Engine

The sequence in which blocks are decrypted during regular operations is not random. A block can only be followed by a very specific selection of other blocks. The memory of the dongle allows the Blurry Box to distinguish between valid and incorrect sequences and to lock down the operations in the latter case.

Security of the Blurry Box Technology

Hackers are experts for different attack methods, but they often lack insight into the inner workings of the applications they are trying to crack. This lack of knowledge can be formalized, which is the backbone of the formal proof of security of the novel process developed by the FZI research center and the Karlsruhe Institute for Technology. It has been shown that all successful attacks are equivalent to attacks that are by their nature not preventable. The proof covers all attacks, including those by attackers who know the method. It complies with Kerckhoffs' principle, which means that the method can be tested and validated independently. This is not possible for protection methods kept secret, making it a great advantage in the fight against industrial espionage and sabotage.

Availability

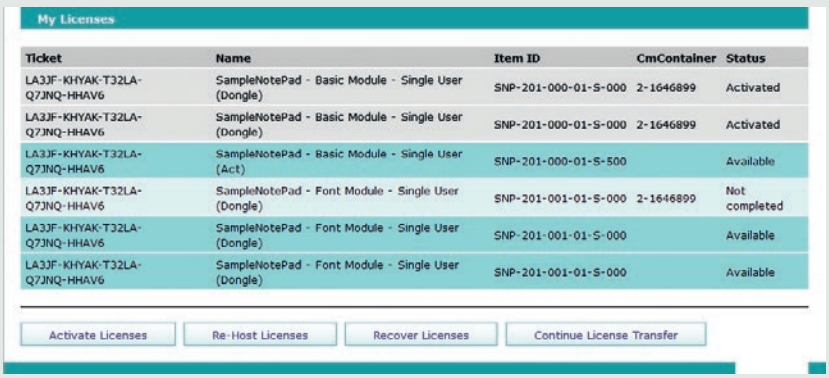
Blurry Box technology is being integrated in CodeMeter and AxProtector. As software developers, you will have access to a framework that enables you to integrate the Blurry Box concept in your software starting mid-2015.

WebDepot 14.12.

There are many ways to activate licenses. One option is to integrate an activation wizard in your software. Another elegant option is to use browser-based activation with the CodeMeter License Central WebDepot. The WebDepot is a PHP application that can be tailored to your specific needs with minimal effort.

Find the Right Look and Feel

The design of the WebDepot can be matched with your corporate design by means of a CSS file. The multilingual WebDepot is currently available in the following languages: Chinese, Dutch, English, French, German, Italian, Japanese, Portuguese, Russian, and Spanish. You can add further languages as required by creating additional language files, hide any languages you do not need, or adjust the copy in the existing language packages to your liking. Adjusting the WebDepot to your corporate language is easy.



All Licenses at a Glance

All Licenses at a Glance

After the end users have entered their tickets, they are taken immediately to the license overview, where all licenses for their ticket are listed. If the users enter multiple tickets (separated by ";"), they will receive a summary overview of the licenses for their tickets.

As vendors, you can define which columns are included in the list, choosing between: Ticket, Article Number, Article Name, Status, Order Date, Serial Number of the CmContainer, and Comment. You can also freely define the order of the columns and licenses, group similar licenses, or hide older licenses on the same ticket.

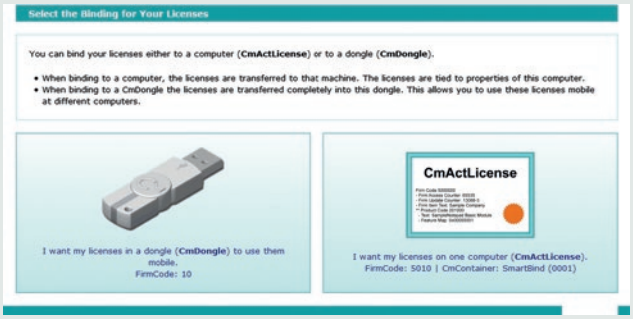
The overview shows the user all available options: "Activate licenses," "Transfer licenses," "Recover licenses," and "Continue transfer."

Activation

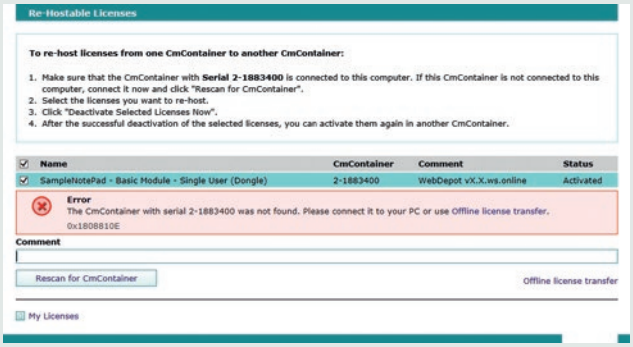
Depending on how your licenses are configured, the users have the option to transfer them to a CmDongle or computer-bound CmActLicense. You can also let the user decide, in which case a selection is offered before the actual activation.

The users select the appropriate licenses and click on "Activate selected licenses."

On this page, you can determine which licenses are pre-selected (either all, no, or every individual license once). All activated licenses are automatically hidden on this page.



Select your License Container



Re-Hostable Licenses

Transferring Licenses

Activated licenses can generally be deactivated or returned. Your settings decide whether this can be done for your licenses. There are two typical cases for returning a license: A planned transfer to another computer or the rescission of the actual sales contract. Since you, the vendor, can be expected to support the planned and legitimate transfer of licenses, the button is named "Transfer licenses."

The "Transfer licenses" page also handles the returning of licenses. If the licenses are distributed on multiple CmContainers, the users first choose a CmContainer, then select the licenses to be returned, and finally click on "Return selected licenses".

After confirming the successful return of the license, it can be re-activated again as if it had never been activated before.

Recovering Licenses

In individual cases, it is impossible for licenses to be returned after the machine they had been activated on has changed. In such cases, license recovery is the right option. As the license vendor, there are two basic cases in which you can allow a recovery: the recovery of single licenses, or the recovery of entire CmContainers. CodeMeter License Central 2.10 or newer is required for the latter case.

Licenses can only be recovered with your express permission. You can allow it either automatically with a defined waiting period or by manual request.

The users are also notified that the original license is voided and placed on a blocked list.

Continuing the Transfer

All of these cases are common for online activation, where the user has the right CmContainer connected to an internet-enabled computer with a browser that supports Websockets, ActiveX, or Java. In all other cases, licenses can be transferred by offline means in three simple steps: upload a request, download the license, and upload the receipt.

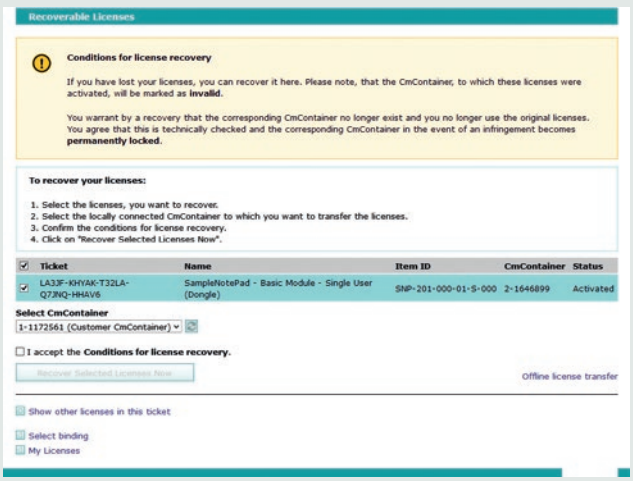
The "Continue Transfer" page lists all processes that have not yet been completed with a receipt and can be continued.

Additional Options

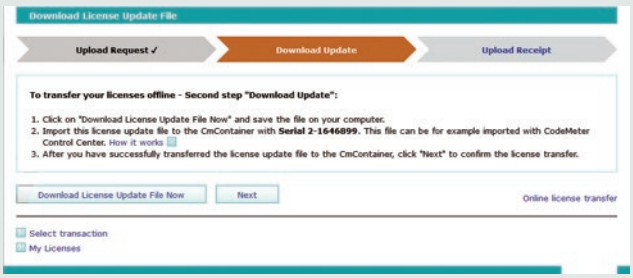
You can also define certain rules for retrieving licenses. For instance, you can determine that all older licenses on a ticket are also retrieved when a new license is downloaded. This would be a perfect means for ensuring that no user can skip an update in sequential updates. This also applies in the other direction – the return or recovery of licenses. With the right settings, all newer licenses are also returned. Other settings include "always all licenses" and "only the most recent license."

Conclusions

CodeMeter License Central WebDepot gives you a simple-to-use and elegant way of distributing licenses to the users of your software. Activate, transfer, or recover: everything is possible without any manual effort on your part. The WebDepot is flexible and versatile enough to match your needs in look and feel.



Recoverable Licenses



Download License Update File

CmDongles with flash memory for unique new possibilities

The CmStick/M, a CodeMeter dongle with a USB interface and integrated flash memory, was first introduced in 2004. Since its inception, the cryptographic capabilities of all CodeMeter dongles have expanded considerably, including all CmDongles with flash storage. Mobile applications that store data and program files on the CmDongle are now a simple option, such as refitting existing embedded and control systems with a slot for storage devices.

Cryptographic features in all CodeMeter dongles

In contrast to most other dongles, CodeMeter comes with substantial storage space on a smart card chip to allow the storage of multiple licenses (even for separate rights holders) with flexible options. At the same time, CodeMeter is a cryptographic genius in your pocket: CodeMeter masters symmetric encryption, asymmetric encryption, hashes, and signatures and can store X.509 certificates. There are also other stateful functions, enabling many applications from copy protection and flexible licensing to secure booting and code integrity protection of software, controls and devices for the Internet of Things.

CmStick/M, CmCard/µSD, /SD, /CF, and CmCard/CFast

CodeMeter dongles with flash memory are available for most common interfaces: µSD cards, SD cards, CF cards, CFast cards, USB sticks. What they all have in common are the trusted CodeMeter functions and a partition accessible as a regular storage device. All CmCards use SLC flash memory; the CmStick/MC (Commercial grade) employs premium Samsung eMMC 2-Bit-MLC memory, offering large storage capacity at an unbeatable price point. There are special models of SLC products for greater temperature range, conformal coating for use in damp environments and many other options. All of this makes the dongles ready for use under tough industrial conditions, such as GSM relays or trains.

Storage Partitions: CmPublic, CmPrivate, CmCdRom, and CmSecure

The CmCards offer a CmPublic partition and a CmSecureDisk partition accessible via CodeMeter API. The USB-CmStick/M also offers another protected CmPrivate partition and a read-only CmCdRom partition that the host would recognize and treat as a CD-ROM. In detail, these partitions allow the following uses:

CmPublic: This partition comes as standard on all CmCards and the CmStick/M. As default, this is the standard full-size partition with read/write access for the host (PC). CmCards and the CmStick/M also use it to store the Codemtr.io file, which communicates with the smart card chip. The new CmStick/MI and /MC models also allow this disc to be configured and removed, as CodeMeter communicates via USB HID on these devices.

CmPrivate: This partition can be set up on all CmStick/M and only becomes visible after a password has been entered or when the API "Enabling" feature is used. The partition can also be set as read-only. New CmStick/MI and /MC also offer AES encryption for the data in the flash memory.

CmCdRom: This partition can be configured on all CmStick/M. The host sees the partition as a CD-ROM with autostart capabilities. The user can neither delete nor change the data. Only the "Enabling" feature, managed via the API, allows data to be saved to and updated on this CmCdRom partition.

CmSecureDisk: This partition can be set up on all CmStick/M and CmCards. It enables

block-by-block read or write access via the CodeMeter API and is not accessible by the host (PC) as a disc. This makes it particularly suitable for logging, black-box functionality, or the storing of confidential data. The read/write access is managed by the CodeMeter feature "Enabling". The CmStick/MC and / MI can also be configured as pure USB-HID devices, making the stick not appear as a disc and protecting the system from any potential viruses or malware. The CmSecureDisk can only be accessed via the CodeMeter API and the CodeMeter Runtime working on the host system. CmSticks are generally protected from attacks like BadUSB that rely on manipulating the storage devices firmware, because the firmware of CodeMeter is signed for added security.

CodeMeter "Enabling"

The CodeMeter feature "Enabling" allows the use of a special access code to activate or deactivate the entire CmContainer or individual entries, not unlike a traditional latch. The various disc partitions are managed via product items in the IFI. By linking these product items with enabling blocks, the API controls which functions are available. Specifically, access to the disc configuration (PI 6), read access to the CmPrivate disc (PI 4), write access to the CmPrivate disk (PI 1), write access to the CmCdRom disc (PI 5), access to the CmSecureDisc (PI 7), and write access to the CmSecureDisk (PI 9) can be controlled. This makes for top flexibility and security, since the "Enabling Access Codes" are used with a challenge-response process.

Why are CmDongles with flash memory more expensive than consumer products?

Storage products are produced in immense numbers for the IT market. Be it storage for digital cameras and camcorders or USB drives for computers, millions and millions of devices are produced every day, equipped with extremely cheap MLC and TLC flash memory that saves multiple bits of data in each cell. Sophisticated controllers allow quality sufficient for private usage at unbeatably low prices. Every few weeks, a new, cheaper product enters the market.

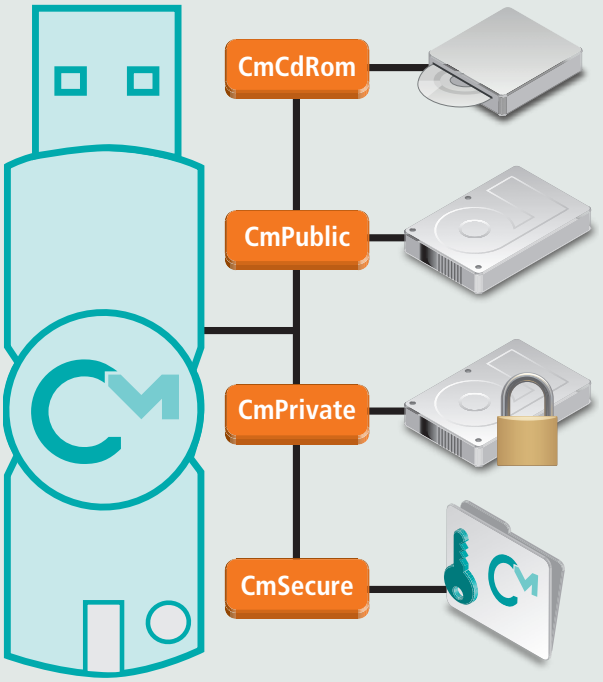
CodeMeter and other storage devices used for industrial applications in control devices, medical technology, telecommunications devices, or routers are designed for long life and reliable performance over many years, coping with constant write access and complying with exacting quality standards. Unchanging electronic components and firmware guarantee that CmDongles continue to operate reliably, whatever the client's application. Extensive qualification checks and EMC / environmental conformity tests promise top quality. All of this requires substantial and costly efforts, but pays off in the long run for the customer.

Use Cases

Wincor-Nixdorf uses the "CrypTA" stick to give its service technicians secure access to confidential documents and applications on the go. The system also relies on two-factor authentication with the CmStick/M's password protection and records all log-in data. The forensic software made by Access Data and Guidance also relies on CmStick/M's secure access to protected application and storage. With CODESYS, the source code can be protected in the development environment and transferred to the CmStick/M. Expansion APPs can be licensed online and used with a CmDongle connected to a PC. A VxWorks Embedded Development Kit published by Wind River uses a CmStick/M to boot the Eclipse-based development environment under Linux and provide CodeMeter functions for creating encrypted and signed applications. A CmCard/µSD is included in this kit to boot an embedded target system from a secure image.

Summary

CmDongles with integrated flash disc offer unique advantages with their versatile interfaces and flexible storage capacity, combined with the CodeMeter's characteristic security. Contact our experts to learn how they can benefit your application.



Configurable partitions of a CmDongle with Flash Memory

Latest news summary

CodeMeter SDK 5.21

The CodeMeter Runtime 5.21 includes small, but powerful improvements for SmartBind®, the patented activation process of Wibu-Systems, as well as new functions for higher-grade protection. Similar security improvements have been included in AxProtector 9.11 for Windows, working with runtime versions 5.21 and higher. Wibu-Systems recommends to always use the newest version.

License Central 2.10

CodeMeter License Central 2.10 comes with a whole range of improvements (more details in this magazine). The installation and update process has been optimized on top of general performance enhancements and a special high availability solution that have been developed. The demo version of License Central now includes the WebDepot, an ideal starting point for a trial and new users.

SmartShelter PDF 11.12

Adobe MEMBER Solutions Network

The newest version of SmartShelter PDF has been updated for current Adobe applications and operating systems. The update includes several minor improvements, including the ability to prevent screenshot-prohibited documents from being opened in the sandbox mode of Adobe Reader, available for Windows 8 and higher.

First place in the German IT Security Prize 2014

It is the most prestigious private award in Germany: the German IT Security Prize, awarded by the Horst Goertz Foundation every two years since 2006. With its total endowment of €200,000 in prize money, the award celebrates the best German innovations in the field of IT security.

The first prize for 2014 and the €100,000 prize money went to the FZI research center, the KIT (Karlsruhe Institute for Technology) and Professor Jörn Müller-Quade, and Wibu-Systems for the "Blurry Box®" technology, a groundbreaking software protection solution that does not rely on keeping the protection methods secret. You can read more about Blurry Box® in this magazine.

1st Prize - IT-Security Award - © Daniel Sadrowski

New talent

We have added a lot of new talent to our team in 2014. In Germany alone, we have eleven new colleagues in research and development, consulting, support, and marketing. In total, we have over 100 people dedicated to developing our products further and giving our customers only the best advice and support.

CodeMeter SDK for Raspberry Pi

Raspberry Pi has many avid fans in research and development as a cost-efficient platform. For a quick start, the starter kit comes with CodeMeter preinstalled. A CmStick, a Linux OS image with a secure ELF loader, and the ExProtector help protect software against piracy and reverse engineering. The ELF loader only allows correctly signed applications, protecting against code that has been tampered with and malware.

EMC and Environment Conformity Checks up to date

The current generations of the CmStick, CmCards, and WibuBoxes have passed the tests of the VDE testing and certification institute with flying colors. Detailed reports about the electrical tests for electromagnetic conformity and chemical analyses in line with the newest standards and substance lists for RoHS, PFOS, and REACH are available. Conformity and CB certificates were awarded for CISPR 22 (ED.6) and 24 (ED.2). This means even more safety and reassurance – technical and legal – for the users of our hardware.

Successful ISO 9001:2008 re-certification

In January 2015, the quality management system of Wibu-Systems AG was again subjected to an external audit by Lloyd's Register Quality Assurance and has been certified as compliant with the ISO 9001 standards: a guarantee for our users that not only our products, but also our processes fulfill even the highest expectations.

Case Study Faceware Technologies, Inc.

FACEWARE
TECHNOLOGIES INC

The Challenge

When you've developed innovative, groundbreaking software that brings emotion to the gargantuan Godzilla on the big screen or adds life to leading video game characters to the delight of serious gamers, protecting your intellectual property from counterfeiting and reverse engineering is paramount. When evaluating licensing and IP protection vendors, Faceware Technologies, Inc. turned to Wibu-Systems' CodeMeter to protect their valuable intellectual property that was years and over $40 million USD in the making.

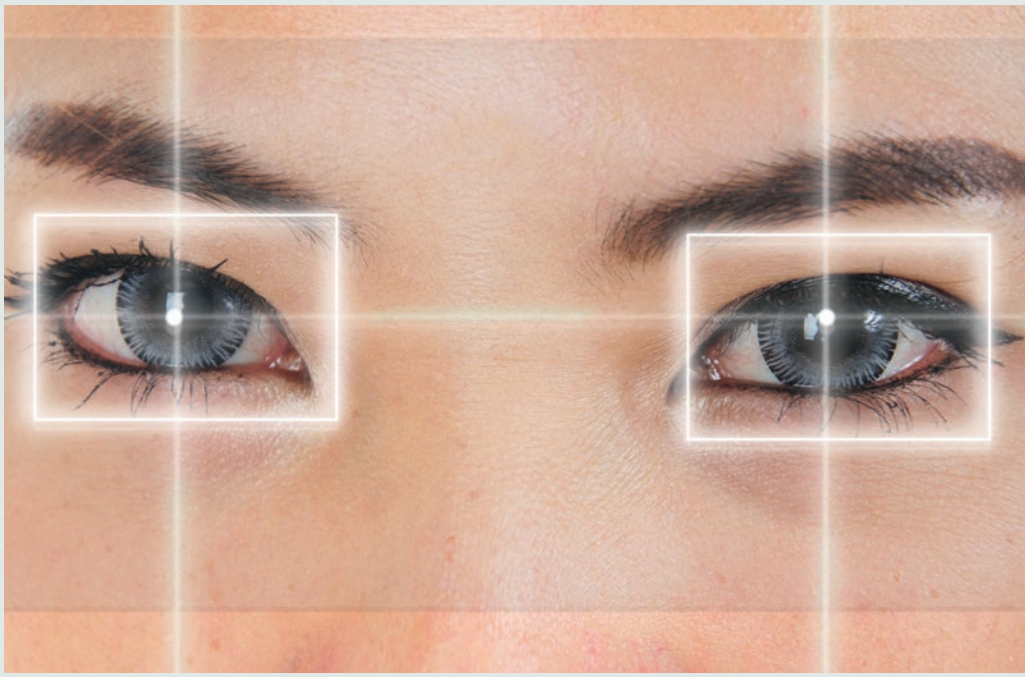
ActLicense SmartBind

The Solution

Faceware chose Wibu-Systems' CodeMeter protection platform because of its proven security features, ease of use, ability for trial licenses, and secure license management system. CodeMeter protected software has never been compromised in global hackers contests. And, with the inherent flexibility of the CodeMeter License Central management system, Faceware Technologies is able to incorporate trial licenses and pay per feature into their business models to reach new markets.

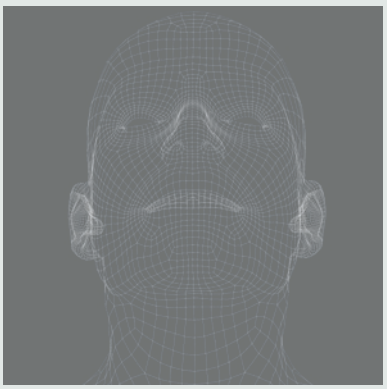
The Success

Since implementing CodeMeter protection, Faceware Technologies has not detected any counterfeit copies of the current software release on the open market, thus protecting and maximizing their license revenues. Utilizing features in CodeMeter, they also have been able to expand their market opportunities by offering "lite" versions of their high end software to make it cost effective for Independent filmmakers and mobile studios.



The Customer

Faceware Technologies is the most innovative and most experienced facial motion capture technology provider in the world. They believe the best facial animation comes from the combination of cutting-edge technology and an intuitive artist-friendly workflow. By empowering artists with easy-to-use products, Faceware Technologies has become the gold-standard for facial motion capture and animation tools. They provide complete solutions for the interactive entertainment, film, video game, television, and commercial markets.



Jay Grenier, Director, Technical Operations
Faceware Technologies, Inc
"With CodeMeter, I rest easy knowing that our technology is completely secure from hackers and reverse-engineering. With this weight lifted off my team, it allows us to focus on what's most important in software development: creating great products."

Software Licensing & Secure Code Seminars

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

- Software Monetization, Back office integration
- Licensing of software, with hardware or software-based keys (SmartBind)
- Code protection against illegal use & reverse engineering

Solutions for embedded software in systems or cloud applications
Access the latest training schedule by scanning the QR Code or visit:

www.wibu.com/trep

Training location	Date	Time
Penthouse Haagse Toren, The Hague (NL)	12 March 2015	11.00-15.00
Office Antwerp, Rooseveltplaats Antwerp (B)	31 March 2015	11.00-15.00
Stadion FC-Twente, Enschede (NL)	19 May 2015	11.00-15.00
Office Paris, Gares du Nord & de l'Est (FR)	5 June 2015	11.00-15.00
London Tech Week, London (UK)	16 June 2015	11.00-15.00

Contact your local sales representative for details		
United Kingdom / Ireland	+44 (0)2031474727	sales@wibu.co.uk
Netherlands	+31 (0)747501495	sales@wibu-systems.nl
Spain / Portugal	+34 (0)914148768	sales@wibu.es
Belgium / Luxembourg	+32 (0)34000314	sales@wibu.be
France	+33 (0)173030491	sales@wibu.fr

Embedded World
24.02 – 26.02.2015
Hall 4, Booth 369
Germany

CeBit 2015
16.03 – 20.03.2015
Hall 6, Booth L18
Hanover Fairground, Germany

rts Embedded Systems + M2M
01.04. – 02.04.2015
CNIT
Paris La Défense, France

Hannover Messe
13.04 – 17.04.2015
Halle 8, Stand D05
Hanover Fairground, Germany

dotnet Cologne
08.05.2015
KOMED im MediaPark
Colongne, Germany

Industrial Automation Bejing
13.05 – 15.05.2015
German pavillion
Beijing Exhibition Center

Internet of Things Event
02.06.2015
High-Tech Campus,
Eindhoven, The Netherlands

Industries Days
03.06. – 04.06.2015
Paris-Orly Airport
Paris, France

London Technology Week
16.06.2015
London
Londonv, United Kingdom

Imprint
KEYnote
29. Edition, Spring 2015
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:
Marco Blume
Rüdiger Kügler
Wolfgang Völker
Oliver Winzenried
Design:
Markus Quintus
Print:
E&B engelhardt und bauer,
Karlsruhe, Germany, EMAS III &
ISO 14001 certified

Letters are always welcome. We will protect the confidentiality of sources. Third party articles do not necessarily reflect the opinion of the editorial office. Write us at global-marketing@wibu.com

SECURITY
LICENSING
PERFECTION IN PROTECTION

WIBU SYSTEMS