SPRING/SUMMER 2025

KEYnote 49

THE WIBU-MAGAZINE

Licensing on Microcontrollers with Just a Few Kilobytes of Memory: Here's How!

Highlights

- CodeMeter License Reporting – A Data-Driven Solution
- AxProtector: Next-Gen Protection for Objective-C, Swift & JavaScript
- Project management in CodeMeter License Portal

WIBU SYSTEMS

Content

Dear Clients and Partners,

Cyberattacks occur every second. The lines between cybercrime and hybrid warfare and between private and state actors are becoming increasingly blurred. Innovations in cybersecurity and their integration into products are essential.

Enhancing cyber resilience and thereby improving the robustness of products is a key priority. Legally mandated requirements for devices, such as software updateability, help ensure that products can be marketed as secure over the long term. A tamper-proof Digital Product Passport (DPP) further supports this approach.

As automated and networked as possible, procedures for identifying and remediating incidents (vulnerabilities) in components and systems are becoming increasingly important. Examples include a Single Reporting Platform (SRP), the Common Security Advisory Framework (CSAF), SBOMs, RFC9116, and others.

With Wibu-Systems, you can rely on a partner who continuously keeps its products up to date and supports you in meeting the above requirements. For over 35 years, we have been providing compatible solutions. With CodeMeter, we offer you a "total solution" that combines protection, licensing, and security while also assisting you in implementing new business models and integrating them into your business processes.

In this issue of our KEYnote magazine, you will find interesting articles about the upcoming CodeMeter License Reporting capability, the use of CodeMeter in small embedded systems, and the enhancements of CodeMeter Protection Suite for Swift, Objective-C, and high security requirements. Additionally, you will learn

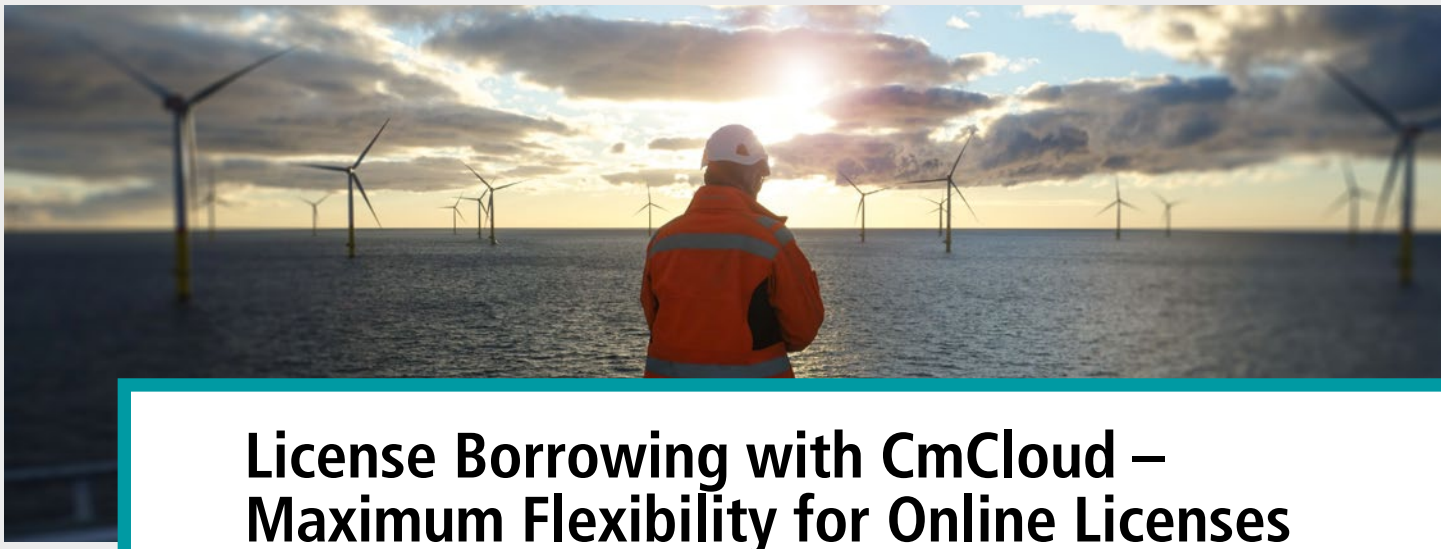
how CodeMeter supports you in implementing the EU Cyber Resilience Act. You will also discover insights into CmCloud Borrowing, the ability to lease CmCloud licenses to local systems, project licensing with CodeMeter License Portal, and how to deliver licenses to SAP via CodeMeter License Portal.

Despite the many challenges ahead, I wish you a successful year and hope that our innovations will bring value to you and your users. I hope you can plan to visit us at one of the spring trade fairs or at our headquarters, for example, during INNO DAYS in early July. I look forward to our personal exchange.

Yours,

Oliver Winzenried

CEO and Founder



License Borrowing with CmCloud – Maximum Flexibility for Online Licenses

Digital transformation demands flexible licensing models that enable software vendors and end users to efficiently utilize their software. With License Borrowing for CmCloud, Wibu-Systems significantly expands the possibilities of cloud-based license management. This feature allows licenses to be temporarily transferred from the cloud to local devices as needed, enabling offline use.

Whether for mobile deployments, maintenance work in remote areas, or flexible work models, License Borrowing with CmCloud ensures that users can access the licenses they need at any time, without relying on a permanent Internet connection.

Once the borrowing period expires, the license is automatically returned to CmCloud, preventing misuse, and ensuring seamless license management.

This extension not only reduces the administrative burden of license management but also enhances the efficiency of license usage. The automatic return of borrowed licenses ensures smooth license operations. Businesses benefit from improved software availability while maintaining full security and control over their licenses at all times.

Functionality and Technical Implementation

Software vendors can activate License Borrowing in CodeMeter License Central. Licenses are temporarily transferred from a CmCloudContainer to a local device, such as a CmDongle or a CmActLicense. During the borrowing period, the license remains visible in the CmCloud dashboard, including its remaining offline duration, ensuring transparent management. This means you always have a complete overview of how long a license is still borrowed and when it will be available for use or further borrowing again.

Once the predefined borrowing period expires, the license automatically returns to CmCloud without requiring any manual intervention. Additionally, software vendors can set security policies, such as restrictions on usage in virtual machines or the definition of permissible end devices.

Application Scenarios

License Borrowing with CmCloud is particularly useful for companies operating in environments with limited or no Internet connectivity. Service technicians performing maintenance work in remote industrial facilities, offshore wind farms, or mines can pre-load their licenses from the cloud onto their devices. This ensures that they can fully access the required software even without an Internet connection.

In mobile work models, where employees frequently switch between different locations or work on temporary project sites, License Borrowing enables flexible and uninterrupted license use. The automatic return after the defined period minimizes administrative overhead and ensures optimal utilization of licenses.

Software vendors can tailor License Borrowing to fit their licensing strategy. The maximum borrowing duration can be individually configured to meet the varying needs of end users. Additionally, License Borrowing is fully compatible with existing licensing models and can be seamlessly integrated into current software solutions.

Summary

With License Borrowing for CmCloud, Wibu-Systems offers a future-proof solution for flexible and efficient license management. The ability to temporarily transfer licenses to local devices as needed makes it easier for businesses and end users to utilize licensed software in various scenarios.

Your benefits at a glance:

- Maximum flexibility through offline usage of borrowed licenses
- Easy integration into existing licensing models
- Reduced administrative effort through automated return

Would you like to experience License Borrowing with CmCloud firsthand? Request a demo and discover how this solution can optimize your license management.

CodeMeter License Reporting – A Data-Driven Solution

Understanding how end customers use software is a crucial source of information for better addressing their needs. Systematic analysis of this data enables targeted product development, optimization of licensing models, and identification of new business opportunities. However, in the past, such analyses were often complex and employed manual processes associated with high costs and delays.

With CodeMeter License Reporting (CmLR) from Wibu-Systems, a cloud-based platform is now available that provides detailed insights into end customers' license usage. Real-time data, interactive dashboards, and comprehensive analysis tools allow for precise monitoring and optimization of your software's usage. This empowers you to make informed, data-driven business decisions that enhance your competitive edge. Additionally, precise usage data facilitates the implementation of true pay-per-use models based on actual usage duration.

This article provides an overview of the features and benefits of CmLR and explains how data-driven decisions can strengthen your market position. It also highlights how CmLR significantly improves transparency and control over software licenses in the market.

Product Overview

CodeMeter License Reporting is a powerful reporting solution that delivers comprehensive usage analytics for your software products. Operating in a secure, centralized cloud environment, CmLR enables precise monitoring of license usage, providing valuable insights into end-customer behavior.

Key Benefits:

- Detailed insights into license usage and trends over time
- Enablement of new licensing models
- Understanding of feature adoption to improve product development
- Optimization of licensing models through data-driven decision-making
- Intuitive dashboards for visualizing usage data with interactive analytics
- Reduced administrative effort through automated data processing and export functions

True Pay-Per-Use with Precise Usage Data

The precise tracking of usage data enables the implementation of flexible pay-per-use models, allowing for usage-based billing that adapts to customer needs. Software vendors can offer tailored billing models for target groups, ensuring that customers only pay for the software services they actually use. This dynamic approach enhances cost efficiency and promotes better license utilization. All relevant billing data is provided directly in the reporting dashboard, allowing businesses to maintain full transparency and accurate tracking of their cost structure at any time.

Data Privacy and Transparency

CodeMeter License Reporting is designed to collect data only after explicit opt-in consent from end customers. Without this explicit approval, no additional license usage data is transmitted, stored, or analyzed. This opt-in policy ensures maximum transparency and data protection, allowing you and your customers to benefit from CmLR without any privacy concerns.

Easy Implementation

Using CmLR requires no complex software installation. Access is provided via a web browser and only requires authentication through the existing Wibu-Systems login. Automatic daily data updates ensure an always up-to-date data-

base, allowing businesses to access the latest license information at any time.

In the past, ISVs often had to perform these analyses manually, which was not only resource-intensive but also prone to errors. CmLR now enables the automated provisioning of relevant data on demand, significantly reducing operational effort. This leads to more efficient use of internal resources and allows businesses to focus on strategic decisions supported by clear, data-driven insights.

Core Features and Dashboards

CmLR provides a wide range of dashboards that offer detailed analysis of license usage.

Central Dashboards

The main dashboard provides an overview of critical metrics, including usage duration, number of accesses, most-used products, and top customers within a selected timeframe.

Additionally, specific dashboards are available that provide deeper insights into various aspects of license usage.

Usage Analysis Dashboards

- **Failed Access Dashboard** – Identifies failed access attempts for early error detection and resolution. Businesses can take targeted actions to address recurring issues or identify under-licensed customers who are reaching their license limits.
- **Geo-Location Dashboard:** Visualizes global license activities using heat maps to optimize regional strategies. This feature helps identify geographical usage trends, allowing businesses to adjust marketing and sales strategies accordingly.
- **Maximum Parallel Licenses Used Dashboard:** Analyzes the maximum number of concurrently used licenses to identify upselling opportunities. Businesses can detect bottlenecks in license allocation and proactively offer solutions.
- **Maximum Seats Used Dashboard:** Tracks the number of seats used per container, ensuring full cost control over purchased seats.
- **Seats Data Insights Dashboard:** Provides a detailed analysis of the timing and usage patterns of individual seats by end customers, enabling early identification of trends and optimization opportunities.

These dashboards enable ISVs to identify usage patterns early, optimize software and licensing models, and align marketing strategies based on data. Additionally, precise usage analyses allow for targeted customer engagement and the development of personalized licensing packages.

Another key feature of CmLR is its easy implementation: The system can be seamlessly integrated into existing business processes without requiring extensive IT knowledge. This significantly reduces implementation effort and enables quick access to analytics functions.

Sales and Licensing Model

The sales and licensing model of CmLR provides flexible access to the required license usage data. Various models allow businesses to choose the solution that best fits their needs.

Free Dashboard

All CmCloud users have access to a free dashboard that provides basic statistics on seat usage and billing. This feature ensures transparent and traceable license management.

Advanced Analytics Capabilities

If detailed user behavior analyses are required, advanced dashboards can be unlocked through a subscription license. These dashboards provide in-depth license usage evaluations and support data-driven business decisions. Additionally, with an extended license, users can customize the analytics interface to meet their specific needs.

API Access and Data Export

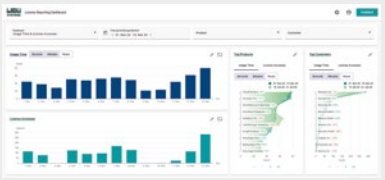
For companies that want to conduct their own analyses, CmLR offers a data export function for all collected data. Alternatively, a REST API can be booked as an additional feature, enabling direct integration into existing analytics environments. This ensures that ISVs always have access to the relevant information they need.

Added Value for Software Vendors

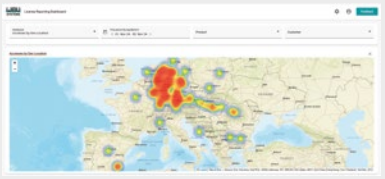
By using CodeMeter License Reporting, you gain valuable insights into your customers' usage behavior. This transparency enables more targeted product development and optimization of existing software solutions based on real usage data. As a result, product strategies can be adjusted more precisely, and investments in feature enhancements can be better evaluated and strategically managed.

CmLR also strengthens customer retention by enabling proactive support for failed access attempts and offering personalized deals based on actual usage patterns. Additionally, it unlocks new revenue opportunities by identifying high-usage customers and highlighting potential for license upgrades or premium feature expansions.

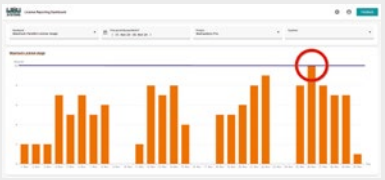
With data-driven insights into software usage, CodeMeter License Reporting enables you to optimize existing licensing models, introduce new licensing approaches, and align business strategies with customer and market demands more effectively.



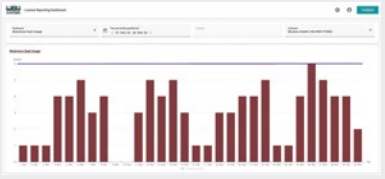
Identify usage trends and detect power users based on individual features of your software.



Uncover marketing potential for international markets.



Identify upselling opportunities with customers who fully utilize their maximum license capacity.



Maintain full cost control by keeping track of the seats used in your CmCloudContainers.

CmLR is the next evolution in license management – Request a demo now and take advantage of its comprehensive analytics capabilities!

AxProtector: Next-Gen Protection for Objective-C, Swift & JavaScript

In a world where software products and digital solutions increasingly form the backbone of global businesses, the need for robust protection against unauthorized access, misuse, and reverse engineering is growing. Developers face the challenge of securing their software against theft, data leaks, and manipulation while requiring easy integration and high flexibility. With the latest version 11.60, AxProtector offers a comprehensive solution specifically designed to meet the needs of developers and businesses looking to protect their software from a wide range of threats. The range of supported programming languages has been expanded to include Objective-C and Swift, enabling even more digital products to benefit from powerful and flexible protection.

AxProtector GUI – The Intuitive User Interface

The AxProtector GUI provides a modern and intuitive user interface for **CodeMeter Protection Suite**, enabling efficient integration and management of software protection. The AxProtector GUI runs on the most common desktop operating systems, including Windows, macOS, and Linux, offering a consistent user experience across all platforms.

The advantage of this cross-platform support is clear: software developers can easily configure the protection of their applications, regardless of the programming language used or the target platform.

Special attention has been given to **user-friendliness**. The **multilingual support** and **integrated help function** ensure that developers are optimally guided through the protection process. The GUI leads users step by step through the necessary configurations, making the protection process intuitive and easy even for less experienced users.

Thanks to the new **unified operating concept**, developers no longer need to make complex adjustments to implement protection across different software platforms. Another advantage of the AxProtector GUI is its **full modularity**, allowing users to customize protection parameters to meet their specific needs.

The GUI allows for easy selection of protection modes tailored to the specific application.

The available options include:

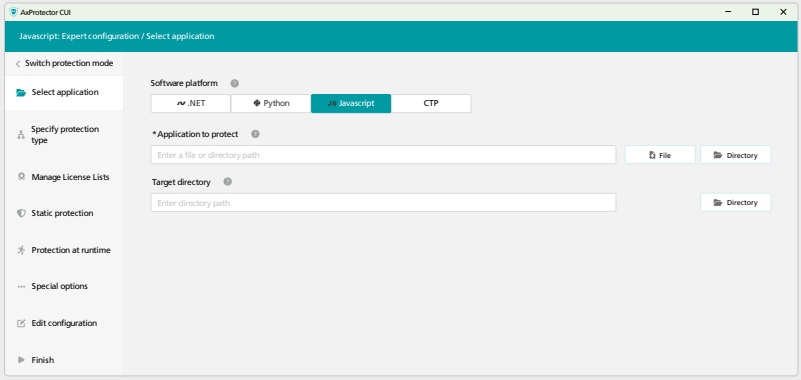
- **Quick-Mode:** A fast protection mode that provides basic security for the application using recommended parameters and enables straightforward licensing.
- **Basic Mode:** Offers extended options for users who want to define more customized protection parameters.
- **Expert Mode:** Provides full control over the protection system, including the implementation of tailored licensing models.
- **License-Free Protection:** Ideal for securing applications without license binding, particularly useful for **IP protection only**.

With **AxProtector 11.60**, the protection portfolio has been significantly expanded. Developers now have the ability to configure **JavaScript** and **Compile Time Protection (CTP)** directly via the AxProtector GUI, greatly simplifying the protection of applications.

AxProtector for JavaScript – Security for Modern Applications

JavaScript is no longer just a language for websites; it has become a key technology for desktop and server-side applications, especially with the rise of Node.js. This evolution increases the need for robust protection of JavaScript applications. With the growing use of **JavaScript in the desktop environment**, the demand for security solutions that safeguard code from reverse engineering and manipulation is becoming more urgent than ever.

With the new version of the AxProtector GUI, software developers now have an easy way to protect **JavaScript applications** for both **desktop systems and servers**. Users can choose to protect either a single JavaScript file or an entire project directory. Protection is applied with just a few clicks; **Quick Mode** ensures fast and straightforward security, while **Expert Mode** is available for more complex applications and customized requirements.



In the enhanced GUI, **JavaScript code protection** cannot only be configured but also encrypted directly. This encryption not only prevents unauthorized access but also enables users to implement **freemium licensing models** or **customized licensing strategies**. This opens up a range of options for scaling software economically and adapting business models with greater flexibility.

AxProtector CTP – Advanced Protection for Native Applications

With AxProtector CTP, software developers gain a powerful solution to protect **native applications** from reverse engineering and manipulation. This protection is achieved through an innovative combination of **obfuscation** and **control flow encryption**, elevating software security to a new level.

While CTP protection is applied directly during the **compile process**, the AxProtector GUI now provides an **intuitive way** to create the necessary configuration files. A key highlight is the **Obfuscation Only** option, which allows developers to implement pure IP protection without licensing requirements or external dependencies (e.g., CodeMeter Protection Suite Runtime – short CPSRT). This is particularly beneficial for applications that do not require licensing but still need protection against reverse engineering.

Another valuable feature of AxProtector CTP is its full integration into the compile process, ensuring that protection is applied directly within the application's **build process**. This guarantees fast and seamless security without requiring any modifications to the source code.

Protection for Objective-C and Swift – Security for Apple Ecosystems

Objective-C

Despite the growing importance of Swift, Objective-C remains a key programming language within the Apple ecosystem. However, its dynamic structure presents certain security risks, as many metadata elements are embedded in the code due to its message-based architecture. This provides attackers with valuable insights into the software. With **AxProtector 11.60**, users can now apply enhanced security measures to **Objective-C applications**. Specialized protection mechanisms prevent **selectors and class names** from being easily extracted through static analysis. By combining **obfuscation** and **control flow encryption**, the machine code is effectively safeguarded against both static and dynamic analysis.

AxProtector CTP for Objective-C applications integrates directly with the bundled **Clang compiler**, which supports the **CTP plugin**. This allows for seamless integration into existing Objective-C projects without requiring any modifications to the source code.

Swift

Swift is one of the most secure and fastest programming languages developed by Apple, offering static method resolution that enhances application security at runtime. However, Swift applications also require protection mechanisms to defend against reverse engineering and manipulation. **AxProtector 11.60** provides powerful security features for **Swift applications**, including encryption of sensitive information (such as **strings and metadata**), advanced **obfuscation**, and **control flow encryption**. These protection measures ensure that even with extensive static and dynamic analysis, intellectual property remains extremely difficult to reconstruct from the machine code.

For Swift projects, a specially adapted **Swift 6 compiler** is provided with the integrated CTP plugin. This enables easy and fast integration of protection without requiring extensive modifications to the build system.

Compatibility with Apple Code-Signing & Hardened Runtime

A key advantage of **AxProtector CTP** is its full **compatibility with Apple's CodeSigning** and **Hardened Runtime**. This ensures that the **executable code** protected by AxProtector remains unchanged at runtime while being presented in a more **obfuscated form** with **encrypted control flow**, making code analysis and manipulation significantly more difficult. This provides maximum security without compromising the **stability** of the application.

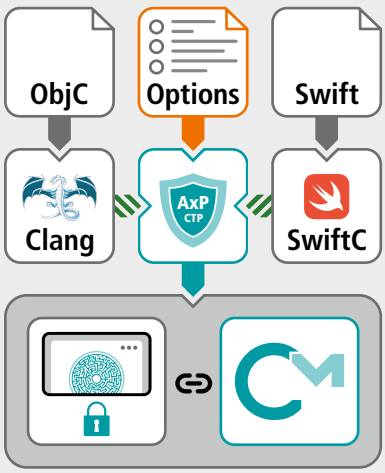
Why CodeMeter Protection Suite?

CodeMeter Protection Suite extends protection across a wide range of software platforms, enabling developers to safeguard their applications against **reverse engineering** and **manipulation**. Whether implementing basic security measures or complex licensing models, AxProtector offers a solution tailored to the specific needs of each software developer.

By combining **robust intellectual property protection** with **flexible licensing options**, CodeMeter Protection Suite delivers an outstanding security solution. Additionally, innovative technologies like **Blurry Box** and **CodeMoving** ensure applications are secured at the highest level. Their integration with AxProtector CTP and AxProtector .NET NC (Native Core) is further simplified with the newly added support for **code annotations**.

Summary

With the new features of **CodeMeter Protection Suite** and the enhanced **AxProtector 11.60**, software developers gain a powerful and user-friendly solution to protect their applications from unauthorized access. The modern **AxProtector GUI** and comprehensive support for **.NET**, **Python**, **JavaScript**, **Objective-C**, and **Swift** provide developers with the flexibility to secure and optimize their applications more efficiently. AxProtector ensures that software products are not only protected against threats but also economically safeguarded, offering flexible licensing models and innovative protection technologies.



Project Management in CodeMeter License Portal

Anyone who has ever built a house knows that a construction site involves many different roles, and the success of the project depends on the seamless interaction between them. The architect designs the project, the workers on-site implement it, and the logistics coordinator ensures that the necessary materials are available.

Software projects delivered to plants and factories have a comparable level of complexity. A project planner creates an overview of which licenses are needed and how they should be distributed within the facility. The purchaser procures the licenses, and the on-site employee activates them. The more precisely the project planner specifies the distribution of the licenses, the more efficiently the activation is carried out on-site.

This is where the project management function in CodeMeter License Portal comes into play. The project planner organizes the project and assigns the licenses to the devices. An on-site employee then simply imports the preconfigured license packages. This saves time, prevents errors in the field, and reduces the need for employee training.

Different Roles

In this use case, we consider three roles: the purchaser who procures the licenses, the project planner who assigns the licenses, and the on-site employee who activates the licenses. In the terminology of CodeMeter License Portal, the purchaser and the project planner are group administrators, while the on-site employee is a group user. Administrators can assign licenses to groups and projects. Users can activate and deactivate licenses. Groups can represent either real or virtual entities in which licenses are organized, such as departments, teams, or virtual license pools like a purchasing pool.

Procurement of Licenses

The workflow typically begins with the procurement of licenses. In most cases, the system integrator purchases a larger quantity of licenses through a volume contract. These licenses are generated by the software manufacturer upon order and delivered to CodeMeter License Portal. The delivery is made to a group, such as the purchasing pool. Typically, purchasers and project planners are administrators of the purchasing pool. They can withdraw licenses from this virtual inventory and distribute them to other groups or projects.

Project Preparation

A project planner from the system integrator selects a group and then creates a project in the next step. Within this project, the project planner defines the individual devices. From CodeMeter's perspective, each device receives exactly one CmContainer, where the licenses will later be activated and securely stored. When a device is defined, a virtual CmContainer is automatically created.

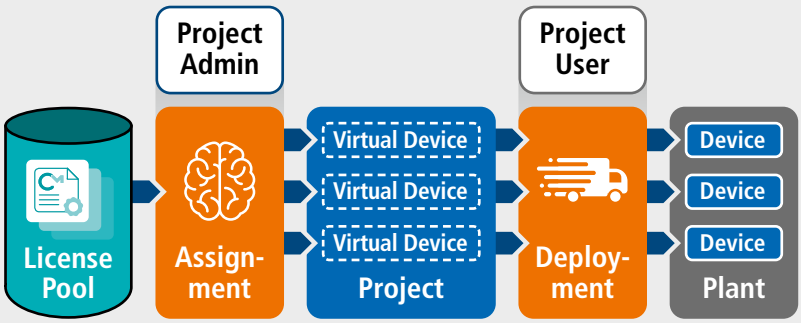
An exception to this single-container approach applies when licenses from different software vendors need to be activated on the same device and involve machine-bound CmActLicenses. This use case is not covered here.

After defining the devices, additional users can be assigned to the project. These users can be given either the role of Project User or Project Administrator. Users who are already administrators of the group in which the project was created automatically inherit the administrator role for the project. However, group users must be explicitly assigned to the project. This allows for granular control over project access.

Once the project is created, it is automatically set to the status "In Progress".

Assignment of Licenses

To assign licenses to a project, the logged-in



user must have the following permissions: They must be an administrator of the project and also an administrator of the group where the licenses are currently stored. This is typically the group where the licenses were initially delivered, such as the purchasing pool or the virtual inventory.

The assignment can only take place while the project is in the "In Progress" state. In this state, project users cannot activate licenses on the device. This restriction prevents the accidental activation of an incomplete or unapproved configuration that might not function correctly. Once the project administrator has completed the configuration, they change the status to "Published".

Activation of Licenses

To activate licenses, the logged-in user must be either a user or an administrator of the project. The activation process consists of two steps:

1. The user selects the device to be activated in the device view of CodeMeter License Portal.
2. The user selects a new (empty) CmContainer on the target device.

In the case of a machine-bound CmActLicense or a CmCloudContainer in the cloud, the CmContainer can be automatically created during this process. If no direct online connection is available, activation can also be performed via file exchange using a CodeMeter Context file.

After activation, the licenses are available on the device and are marked as activated in CodeMeter License Portal.

Before activation, the licenses have the status "Assigned". They can only be activated through this workflow to ensure that the intended configuration is deployed correctly. This prevents accidental activation of a license in an unintended CmContainer.

Changes in the Field

In the unlikely event that the project was configured incorrectly, it can be set back to the "In Progress" state at any time to make adjustments. This action can be performed either by a project administrator in the back office or by a user in the field. To do so, the user temporarily receives administrative rights for the project from a project administrator. Once the changes are complete, the status is set back to "Published", allowing the licenses to be transferred again.

Changes at a Later Stage

Even Heraclitus knew: "Nothing is as constant as change". This is especially true for software projects. If the requirements for a device change at a later stage, a project administrator switches the project to "In Progress" mode. They can then add or remove licenses from the device. Once the modifications are ready to be deployed, the project is set to "Published" again.

A particularly critical aspect is transferring a license between two devices. In the standard process, the license must first be deactivated on the old device. Then, the new state must be confirmed before the license can be activated on the new device. This approach ensures the highest level of protection against license misuse but also makes the process more complex. To simplify this, CodeMeter License Portal offers the option to prepare all actions in advance using a push update, allowing ready-to-use updates to be rolled out across all devices. This creates a theoretical temporary overlap, where the same license could be used on two devices for a short period. However, all such actions are logged to track usage patterns.

Regardless of the selected security option, project users can easily synchronize the connected CmContainer in the device view of CodeMeter License Portal with a single click, ensuring that the latest project configuration is applied. If no direct online connection is available, synchronization can also be performed via file exchange using a CodeMeter Context file.

Handover to the End User

Typically, once the project is completed, the system integrator hands over the plant and its devices to the operator. There are two possible scenarios: Either the system integrator continues to handle maintenance and support or the operator takes over full control independently in the future.

In the first case, CodeMeter License Portal allows both the operator's employees and the system integrator's employees to access the project with different roles.

In the second case, the project is transferred from the system integrator to the operator, and the system integrator's permissions are removed.

Recovery in Case of Failure

In the event of a license loss, recovery is straightforward. Depending on the software vendor's policy, the licenses of a device within a project can be restored to a new CmContainer. Thanks to project management, all required licenses are clearly organized in one place within the project. The software vendor's policy always applies to the entire device, eliminating the need to define specific permissions and rules for individual licenses.

Automated Processes

As with all processes in CodeMeter License Portal, the workflows described here can also be mapped via the API. This enables full automation, such as creating a new project automatically for each new order received through an ERP or shop system, pre-registering CmContainers, or generating a recommended configuration.

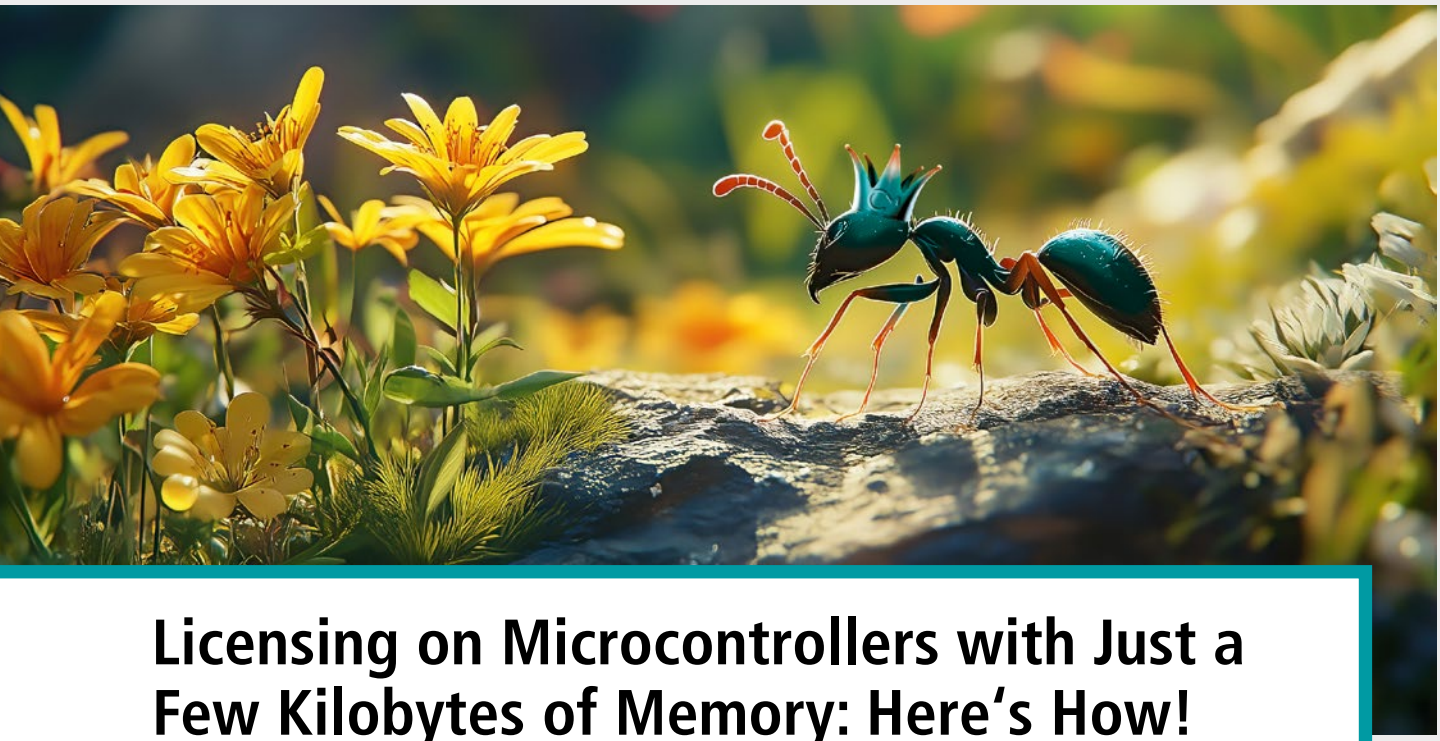
CodeMeter gives software vendors the flexibility to automate processes according to their specific needs. Additionally, if a network connection is available, the software product can periodically check for new updates for the CmContainer and install them automatically. This allows configuration changes to be deployed without user intervention.

Summary

The project management feature in CodeMeter License Portal accounts for the different roles in complex software projects.

- A purchaser procures licenses, either for a specific project or as stock.
- A project planner assigns the licenses to the respective devices in the back office.
- An on-site employee simply activates the pre-assigned licenses.

This approach reduces training requirements, increases efficiency, and minimizes errors. Additionally, future updates can be handled just as easily, ensuring a streamlined and error-free process.



Licensing on Microcontrollers with Just a Few Kilobytes of Memory: Here's How!

More and more manufacturers from the industrial sector are asking us how they can use Wibu-Systems' license management solutions to protect the firmware or functionalities of small microcontrollers in the field. In this context, licensing is the primary focus. The key requirement for the licensing solution is minimal memory consumption – just a few kilobytes. To discuss this topic, the KEYnote editorial team spoke with Wibu-Systems' Embedded Product Manager (PM) and the microcontroller specialist from our Professional Services team (PS).

Editorial Team: Today, we're discussing how to bring the CodeMeter licensing solution to devices with such limited resources that even CodeMeter µEmbedded is too large. My question to the Embedded Product Manager: Where is such a solution needed, and who is using it?

PM: Our industrial customers manufacture sensors and actuators in large quantities, such as frequency converters for motors, sensors for mechanical engineering, or valve controls in hydraulics. These devices require only minimal computing power but often contain high-value control algorithms or complex measurement functions. This software represents valuable intellectual property (IP) that needs protection. However, on these platforms, even the 64 KB of CodeMeter µEmbedded and the required RAM are too large to be implemented.

Editorial Team: Aren't microcontrollers becoming more powerful? Many can now render web interfaces or communicate with the cloud.

PM: That's correct. For more powerful systems, CodeMeter Embedded is a great choice. However, let's take the example of a frequency converter used to control the speed of a servo motor. Here, the focus is on load monitoring, acceleration and braking ramps, and motor characteristics. Such devices operate with only a few kilobytes of RAM. The manufacturer, however, wants to license individual functions and control the number of devices produced at the contract manufacturer. These devices are produced in high volumes, and cost-sensitive component selection is crucial. A multifunctional security solution like CodeMeter simply doesn't fit within the limited memory available.

Editorial Team: How can a manufacturer still use the CodeMeter licensing concept?

PM: With a specially adapted solution that optimally utilizes the available resources while ensuring a secure binding of the license to the hardware. At the same time, compatibility with CodeMeter License Central and remote updates must be maintained. CodeMeter is highly flexible, allowing the necessary solution to be built from existing functions.

Editorial Team: The question goes to the developer: How does this work? A CodeMeter licensing solution without CodeMeter Embedded?

PS: We have developed a compact library for microcontrollers, reduced to the essential functions for license and signature verification, ensuring a minimal footprint. Additionally, we use an optimized license format specifically designed for resource-constrained microcontrollers. The license file is generated on a programming system using a host tool, derived from a regular CodeMeter license. This allows the entire CodeMeter ecosystem to remain fully functional while ensuring that the final license is securely bound to the target system. The host tool can be flexibly integrated into the

production process, making licensing seamless and efficient.

Editorial Team: What functions does the library offer on microcontrollers?

PS: The license content can be individually customized. Typically, a license contains only a few attributes: a device ID, Firm Code, Product Code, validity period, feature map, and the number of license units. Adjustments to specific customer requirements are possible. The library verifies the validity of the license and provides access to its content.

Editorial Team: How large is such a license?

PS: A typical license requires approximately 150 bytes in the parameter storage of the microcontroller. This includes the essential attributes and a cryptographic signature.

Editorial Team: And what about the library? What resources are required for it?

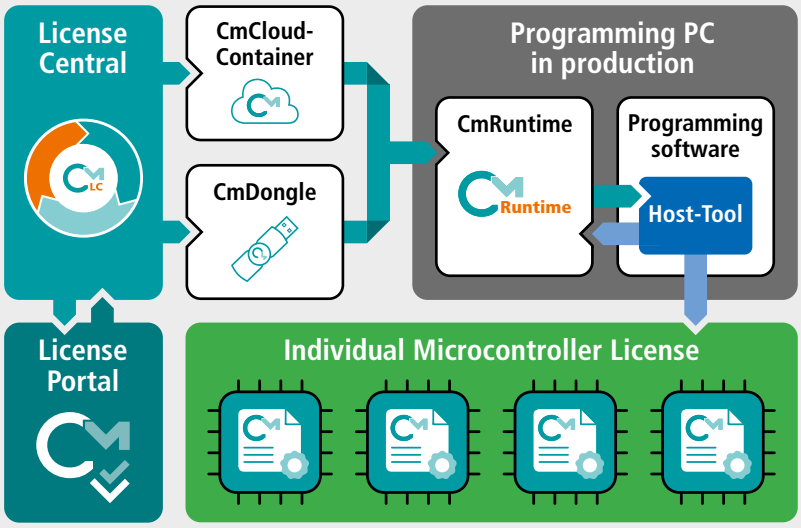
PS: The microcontroller only requires ECDSA signature verification and SHA hash calculation. Depending on the platform, existing hardware can be utilized, or already available cryptographic libraries can be integrated. This ensures flexibility in implementation, and as a result, the required memory size varies.

Editorial Team: How does the licensing process work in practice?

PS: To bind a license to the device, a unique device ID is required, which can either be read from the microcontroller or obtained from an external source. During production, a host tool generates a signed license for the microcontroller using a CmDongle or via CmCloud. A counter in the CodeMeter license container is decremented, ensuring that each license is used only once. The license transfer depends on the application scenario – either automatically on the production line or later by a technician in the field. Future updates are also possible via the host tool.

Editorial Team: And how is the license verified on the device?

PS: At startup or during operation, the license container is read. The signature is verified against a key hidden in the firmware. After verification, the firmware receives the license information – either as a simple Yes/No decision or with additional attributes that control the software functionality.



Editorial Team: How can a customer obtain this solution?

PM: Through our Sales and Professional Services teams. First, we clarify the protection requirements and use case with the customer. Upon request, Professional Services then provides a customized code example for the microcontroller and delivers a secured library for the host tool.

Editorial Team: How secure is the solution against unauthorized license creation by third parties?

PS: A critical aspect is the protection of the host tool, which generates the microcontroller licenses. For this, we use CodeMeter AxProtector. Up to this point, the CodeMeter Remote Update process is fully secured. The host tool then creates a licensed file for the specific target device, ensuring that the entire chain remains protected.

Editorial Team: What about software protection?

PM: Many modern microcontrollers offer integrated security solutions that allow firmware to be signed and encrypted. For example, NXP refers to this as Secure Provisioning. Even the new RP2350 from Raspberry Pi supports Encrypted Boot using an asymmetric cryptographic method.

Editorial Team: Can this also be protected with CodeMeter functions?

PS: This needs to be evaluated on a case-by-case basis and implemented specifically to the microcontroller. A smart combination of the microcontroller's built-in security features and CodeMeter functions for license handling and storage can significantly enhance the level of protection.

Editorial Team: And now, please summarize the entire topic in a single sentence.

PM: Wibu-Systems enables licensing on resource-constrained microcontrollers by combining CodeMeter's license management functions with the built-in security features of modern microcontrollers, ensuring efficient and flexible implementation.

Secure License Management for Small Devices – A Smarter Approach

Traditional license management tools often fall short on small devices due to limited resources. With the Custom Licensing Adapter, CmDongles, and CodeMoving, machine builders and manufacturers can enable secure, centralized licensing via CodeMeter License Central. Watch the webinar replay!

Delivery via CodeMeter License Portal

The integration of ERP, CRM, and e-commerce systems with CodeMeter License Central is done via connectors and has been available for many years. SAP integrations are always the highlight of our projects, where our customers are amazed at how easily and quickly this can be implemented. You can choose between directly addressing our SOAP and REST interfaces or integrating via a special SAP connector from our partner company INFORMATICS. The advantage of the integration with INFORMATICS is that you not only receive an interface but also the expertise on when and how to use it, all the way to a turnkey solution.

How to deliver?

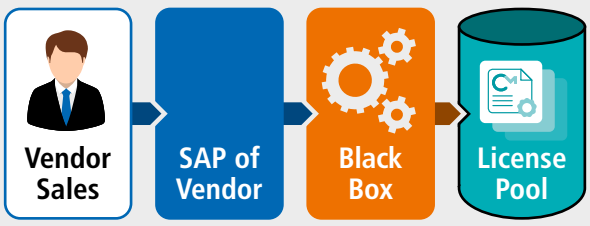
A question that always arises in these projects is: "How do these licenses automatically reach my users?" Some of our customers print the ticket on the delivery note and send it out. Others generate license certificates with the ticket in credit card size, while others create sealed PIN/TAN letters, similar to those used by banks. The trend is moving towards direct digital delivery via email, which has been the norm in current projects. Either the delivery note is sent as a PDF, or the ticket is inserted directly into the email.

Delivery to a Portal

Although delivery via email is currently the state of the art, we asked ourselves whether there are alternatives. Our answer is yes, via direct delivery to CodeMeter License Portal. CodeMeter License Portal is an add-on to CodeMeter License Central that allows you to manage your customers and their users and assign licenses to them. Via an SSO (Single Sign-On) interface, users and hierarchies can be linked to your existing system for managing your customers. You don't have such a system? No problem – CodeMeter License Portal optionally includes its own management system.

Our Pilot Project

In the first pilot project, we implemented a connection between SAP and CodeMeter License Portal together with our partner INFORMATICS. The order containing the licenses is created via the connector. Technically, we integrated this into CodeMeter License Portal to provide a unified interface. After the order is created, SAP queries the internal WIBU ID of the customer. For this purpose, SAP transmits the SAP debtor number and the Ship-To-Mail. CodeMeter License Portal checks whether this customer and user already exist. If they do, the WIBU ID is returned. If not, a customer and/or user is automatically created, and their WIBU ID is returned. In the third and final step, SAP calls the function that links the license to the WIBU ID.



Customer or User?

When delivering licenses to the Portal, you define who should receive the license. In the Portal, licenses can be assigned to a group (usually the customer) or a user (a specific individual). Licenses in groups can be either "Public" (visible to all members) or "Admin Only" (visible only to administrators).

A typical use case is delivery to the group in "Admin Only" mode. Purchasers and administrators have access to these licenses and can then assign them to employees or distribute them across projects.

Black Box for Automation

You might be wondering why SAP calls CodeMeter License Portal multiple times instead of us simply providing a black box that handles everything at once. This black box is also available, allowing all steps in the Portal to be executed automatically with a single call. In this specific project, however, step-by-step handling was explicitly required for error processing in SAP. The decision on where error handling should take place is entirely up to you. We adapt to your requirements. For the automatic creation of customers and users via CodeMeter License Portal, rules can be defined and implemented. Examples include integration with an SSO system and positioning within the overall group hierarchy.

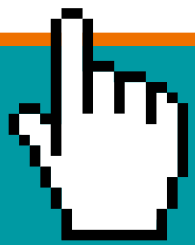
Summary

With delivery to CodeMeter License Portal, Wibu-Systems offers an option that can be used as a complement or alternative to email delivery. Customers and users are automatically created as needed based on predefined rules. Customers receive a notification and can easily retrieve and distribute licenses via the portal. Critical data, such as tickets, is centrally visible to multiple administrators at the customer's end and is not transmitted via email.

WIBU NEWSLETTER

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

Subscribe to our newsletter



Europe's Response to Cybercrime: CRA

In an increasingly digitalized world where cyberattacks are becoming more sophisticated and frequent, the need for a legal framework to ensure cybersecurity is paramount. The EU Cyber Resilience Act (CRA) aims to guarantee the security of digital products and services. This article explores ways to ensure CRA compliance using CodeMeter.

Motivation from Two Directions

Product security is a critical success factor for businesses. On the one hand, companies aim to protect their software know-how from hackers using reverse engineering. On the other hand, software monetization must not be undermined by piracy. External requirements, driven by market demands or legal mandates such as IEC 62443, NIS2, and the EU Artificial Intelligence Act, also play a role.

Since the end of 2024, the EU Cyber Resilience Act has been in effect for all member states. It includes guidelines, processes, security requirements for digital products, detailed information, and reporting obligations. Non-compliance with these regulations can result in fines amounting to millions. Although the CRA allows a transition period until 2027, businesses must act now to prepare. Determining who is affected and in what capacity marks the starting point of the compliance journey.

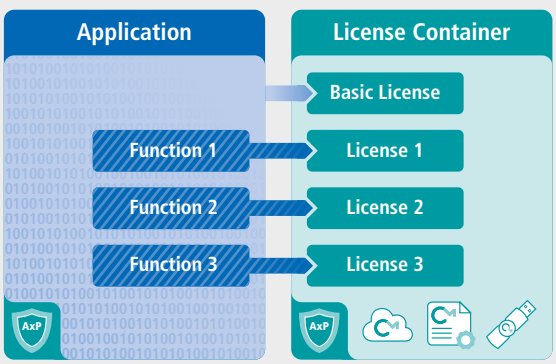
CodeMeter as a Companion for CRA Compliance

The following sections present various examples of how CodeMeter technology can actively support you on this journey. Our experts have identified specific parts of the CRA where Wibu-Systems' products can be leveraged for compliance.

Measures to Restore Compliance CRA Art. 13 (21)

If manufacturers determine that a product with digital elements in the field no longer complies with CRA regulations, they must immediately take measures to restore compliance or, if this is not possible, withdraw the product from the market. Manufacturers must maintain an overview of products and users in the field to inform affected customers.

This can be achieved by leveraging CodeMeter licenses, which provide complete transparency for manufacturers. Programs or functionalities can be disabled or replaced by withdrawing or updating licenses to regain compliance. Using CodeMeter License Central and CodeMeter License Portal, managing licenses in the field becomes seamless and transparent across multiple levels. Roles and rights can be assigned to these levels, and the status of licenses in the field is always accessible.



Access Protection (CRA Annex I, Part I, 2d)

In addition to general authentication and authorization via issued licenses, CodeMeter allows for specific licenses to be assigned–for example, for different software versions, compliance with export controls, regional requirements, or particular user groups or individual users via Named User Licenses. CodeMeter Certificate Vault can securely deploy certificates to the field and integrate them into applications via standard protocols. Access protection based on CodeMeter is also implemented for CODESYS and Siemens' TIA Portal. Rockwell Automation uses the technology for Studio 5000 Logix Designer.

Data Confidentiality and Integrity (CRA Annex I, Part I, 2e, 2f)

Manufacturers must ensure data confidentiality and prevent data manipulation to guarantee data integrity. By utilizing encryption and cryptographic signatures through CodeMeter licenses, CodeMeter API and CodeMeter Protection Suite provide manufacturers with all the tools needed to meet these requirements. CodeMeter License Central ensures secure key distribution.

Compliance and Monetization: An Ideal Combination

By combining product security and licensing, CodeMeter offers an ideal solution that supports CRA compliance while enabling the licensing of products with digital components – An investment with a guaranteed return!

News in Brief

How Hilscher is transforming industrial app deployment

Discover how CodeMeter enables secure deployment of industrial apps, the role of the Flagship Store for the OI4 Community in improving accessibility for industrial apps, CodeMeter's hurdles and solutions for licensing industrial software, overcoming security challenges in Docker environments, the rise of subscription and pay-per-use licensing models in industrial software, and how industry leaders like Siemens and SAP are shaping the future of industrial app marketplaces.

How Tetra Pak reinforced functional and food safety

Gain insights on secure software & IP protection, simplified technician experience, monetizing software & hardware functions, and adapting to evolving cybersecurity regulations. Discover the implementation process, challenges, and the impact of regulations like the Cyber Resilience Act. Learn how secure-by-design solutions and flexible licensing models are shaping the future of industrial automation in the food processing and packaging industry.

How MVTec is driving machine vision innovation

Explore how Wibu-Systems' cutting-edge licensing and security solutions support MVTec's HALCON and MERLIC products across diverse operating systems and industrial environments. Discover how CodeMeter's 4D interoperability enhances software protection, why MVTec chose Wibu-Systems for licensing and security, the role of CodeMeter License Central in streamlining deployments, and how CodeMeter simplifies educational license management with three dedicated portals.

How Desoutter is revolutionizing licensing in Industry 4.0

Discover how the introduction of the Unit Values model delivers unmatched scalability, versatility, and flexibility, empowering customers to only pay for what they need while ensuring robust protection against unauthorized use. Learn about the transition from traditional to dynamic, feature-based licensing, the integration of CodeMeter's secure licensing mechanisms, and the future of cloud-based subscriptions in driving digital transformation.

How INFORMATICS can effortlessly integrate CodeMeter with SAP

Discover the three leading system scenarios between SAP and CodeMeter License Central, how the License Central Connector simplifies integration, reduces costs, and maintains system stability, implementation strategies for subscription models using SAP and CodeMeter License Central, key SAP modules in the License Central Connector for efficient communication and data management, solutions for reseller integration, and tailored consulting services to meet unique licensing requirements.

INNO DAYS 2025 – The agenda is live!

Each year, the program grows richer with stunning contributions. In addition to our own talks on innovations in the fields of **software protection**, **license reporting**, and **cloud licensing**, we'll have Dr. Vermeer Consult discussing **business opportunities**, **culture**, **and global impact in India**, **Indonesia**, **and the world**; Bartsch Rechtsanwälte covering the **new regulations applicable to the IT domain that the EU is rolling out between 2025 and 2027**; Rohde & Schwarz addressing **CodeMeter License Central as the keystone for standardization & automation of software license management**; BFK edv-consulting targeting **the future of cyber sabotage and cyber espionage in the context of current geopolitical developments and asymmetric warfare**; Euresys highlighting **the use of CodeMeter in a multi-license**, **cross-platform machine vision library**; and Roche illustrating the usage **of CodeMeter in their product digitization strategy**. Key figures from SAP, Karlsruhe Institute of Technology, and Infineon will conclude the program with a roundtable on **Quantum Computing and Digital Sovereignty**. You cannot miss out – Register Now!

WIBU BLOG

One idea at the right time can change everything.

Subscribe to our blog

Case Study | Tetra Pak

Tetra Pak, a leader in food processing and packaging solutions, operates in over 160 countries, offering complete production lines that extend beyond packaging to include ingredient mixing, blending, and carbonating. As the company expanded its automation strategy, securing its intellectual property and ensuring food and functional safety became critical. In response, Tetra Pak integrated Wibu-Systems' CodeMeter technology, safeguarding its industrial know-how while facilitating maintenance and service.

The Challenge

With a legacy of software protection dating back to 2007, Tetra Pak sought a robust solution that could protect both Rockwell and Siemens PLC environments without relying solely on passwords. Previous measures, including password-based security and source code control, had proven insufficient against evolving cyber threats and intellectual property theft. The company needed a solution that could prevent unauthorized access and modification of critical software controlling production lines. Additionally, Tetra Pak required a system capable of providing role-based, time-limited access to Field Service Engineers (FSEs) while ensuring seamless integration into their existing IT infrastructure.

The Solution

Wibu-Systems provided Tetra Pak with a secure and flexible licensing solution powered by CodeMeter. For Rockwell Automation PLCs, Tetra Pak integrated CodeMeter Source Protection Provider (CSPP) and Content-License Protection (CLP), ensuring program blocks were shielded from unauthorized access. For Siemens PLCs, CodeMeter Keyring for TIA Portal enabled seamless and secure password management. Integration into Tetra Pak's Enterprise Management System allows automated license distribution, ensuring engineers access to only the systems for which they were authorized. The entire system is centrally managed, with licenses stored in CmDongles that require authentication before use, mitigating the risk of credential leaks and unauthorized modifications.

The Result

With Wibu-Systems' CodeMeter technology, Tetra Pak seamlessly integrated advanced security into its automation ecosystem. Functional safety was enhanced by reducing risks that could impact human health, while food safety was fortified through strict tampering protection of food safety parameters. Maintenance and service operations were simplified, granting tamper-proof control over source code, which reduced operational disruptions while enabling compliance with cybersecurity regulations. IP remained safeguarded, securing core knowledge and technological advancements. Financial risks were mitigated by preventing costly machine downtime. Additionally, the solution maintained certification and documentation validity, ensuring compliance with industry best practices.

Pravin Karthick Murugesan
Automation Engineer, Tetra Pak
"The security of our automation software is a non-negotiable factor in maintaining our leadership in the food processing industry. With Wibu-Systems' CodeMeter, we have not only protected our intellectual property but also ensured food safety and enhanced system resilience. The seamless integration of CodeMeter into our existing IT infrastructure allowed us to strengthen security without disrupting our processes."

Join Wibu-Systems at the following events:

HANNOVER MESSE
31 March – 4 April 2025
Hanover, Germany
Hall 16, Booth D10

Automate 2025
12-15 May 2025
Detroit, Michigan, USA
Booth 1739

Infoshare
27-28 May 2025
Gdańsk, Poland

INNO DAYS
2-3 July 2025
Karlsruhe, Germany

SPS
16-18 September 2025
Atlanta, USA
Booth 425

Roadshow
7 October 2025
Berlin, Germany

Roadshow
8 October 2025
Munich, Germany

Formnext
18-21 November 2025
Frankfurt, Germany

SPS
25-27 November 2025
Nuremberg, Germany
Hall 6, Booth 428

Wibu-Systems' INNO DAYS 2025

The premier event for digital strategists aiming to steer their business with a clear, future-focused vision. Attendees will benefit from high-level networking with industry peers, insights from leading experts, and exclusive entertainment. Wibu-Systems' key staff, along with solution partners, clients, and renowned speakers, will lead the discussions. While IP protection and monetization technologies remain central, the event will foster broader engagement on critical industry trends. Register asap! The future begins now.

www.wibu.com/inno-days.html

Wibu-Systems' German Roadshow

We're bringing the full CodeMeter experience directly to you! Join us in Berlin on October 7, 2025, or Munich on October 8, 2025, for a full day of immersive learning. This focused event combines theory and practice, offering the latest trends and best practices in software protection, licensing, and security. You'll have the chance to engage in expert-led, hands-on sessions, participate in live demos, and address your specific questions and needs in tailored discussions. Don't miss this opportunity to expand your network and expertise. Pre-register now to secure your spot!

www.wibu.com/roadshow.html

Wibu-Systems' Masterclasses

Our monthly, fully immersive masterclasses offer exclusive content tailored for all skill levels – whether you're a beginner, intermediate, or advanced user of CodeMeter technology. The 2025 season brings a dynamic miniseries featuring deep dives into CodeMeter License Central, the intersection of Cyber Resilience Act and CodeMeter, the latest advancements in CodeMeter License Portal, and new features like CmCloud Borrowing and CodeMeter License Reporting. Stay tuned for upcoming announcements on our website or via our newsletter, and be ready to register for the sessions that best suit your needs.

https://www.wibu.com/webinars.html

Get in touch with our local representatives

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

WIBU-SYSTEMS (Shanghai) Co., Ltd.
Shanghai: +86 21 5566 1791
Beijing: +86 10 8296 1560
info@wibu.com.cn

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

WIBU-SYSTEMS Korea Ltd.
Republic of Korea
+82 2 6206 9490
sales@wibu.co.kr

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

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

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

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

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

Imprint
KEYnote 49 Issue
Spring/Summer 2025

Publisher
WIBU-SYSTEMS AG
Zimmerstrasse 5
76137 Karlsruhe, Germany
Tel. +49 721 93172-0
info@wibu.com
www.wibu.com

Responsible for the content
Oliver Winzenried

Editors
Stefan Bamberg
Michael Birger
Marco Blume
Axel Engelmann
Lukas Klassen
Ruediger Kuegler
Daniela Previtali
Florian Schneider
Oliver Winzenried

Design
Eugen Olchin

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

SECURITY
LICENSING
PERFECTION IN PROTECTION

WIBU SYSTEMS

5060-002-02/2025-03-05 © 2025 WIBU-SYSTEMS AG