

Security 4.0 by Default – Growth 4.0 by Design

- Protecting digital assets
- Monetizing Industrie 4.0
- Envisioning new business models

WIBU
SYSTEMS

Contents

Serving ISVs and IDMs	3
B&R	4
CODESYS	5
KONTRON	6
PHOENIX CONTACT	7
ROCKWELL AUTOMATION	8
SIEMENS	9
UNIFIED AUTOMATION	10
WIND RIVER	11
White papers	12
Webinars	13
Economy 4.0	14
Protecting and Monetizing IP in Additive Manufacturing	16
Securing the Machine Learning Lifecycle	17
CmReady – License Mobility with Industrial Memory Cards	18
Cryptoagility for Post-Quantum Security	19



Ruediger Kuegler

VP Professional Services
Security Expert



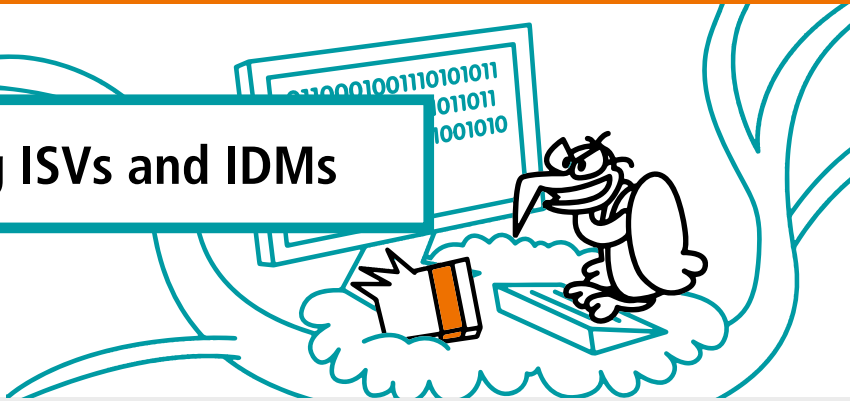
Guenther Fischer

Senior Consultant, Licensing and Protection



Subscribe for our KEYflash and stay up to date with all the news at WIBU, including new innovations and product features, virtual and on-site events, and inspiring success stories and partnerships: <https://www.wibu.com/newsletter.html>.

Serving ISVs and IDMs



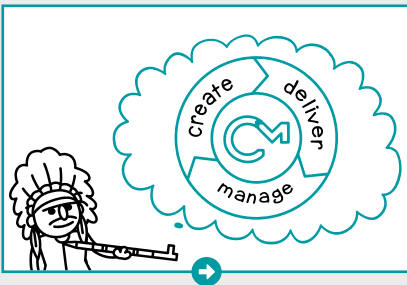
CodeMeter is the all-in-one solution for monetizing software securely and effectively, made possible through the full integration of a vast range of systems, platforms, back-office landscapes, and license containers.



Protecting Software

Make sure that every license in the field is a license you sold.

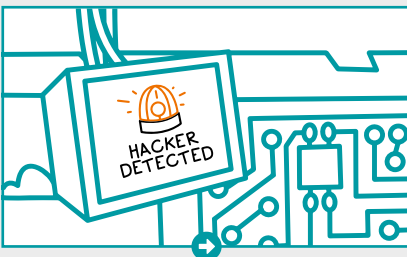
CodeMeter Protection Suite stops software piracy and reverse engineering in its tracks by enabling software authenticity mechanisms, protecting its integrity and the intellectual assets contained within it, and robustly encrypting entire binaries or selected functions.



Managing Software Licenses

Offer structured services with a versatile licensing strategy.

CodeMeter License Central makes easy work of creating, distributing, and managing licenses throughout the entire software lifecycle, supported by a powerful selection of licensing models and efficient integration with existing ERP, CRM, and e-commerce systems.



Safeguarding IoT Devices

Apply familiar PC technology to the industrial realm.

The CodeMeter universe includes specific variants for embedded devices, PLCs, and microcontrollers, designed to support the principal operating systems and architectures in the field and shield software and firmware downloads and upgrades from tampering.





By combining CodeMeter from the outset with new B&R hardware, their users can benefit from the same degree of protection for their products that B&R has been enjoying.


A Single Technology for Two Purposes

More and more features of industrial machine and manufacturing systems are determined only by the software controlling them, from the production plans to the machine data itself. Such know-how is invaluable for mechanical engineers and deserves strong ring-fencing to prevent tampering, be it by ruthless competitors, criminal out-fits, or simply careless operators.

With Technology Guarding, the clients of B&R receive a USB dongle alongside their equipment (CmStick/C) which offers licensing functionality for their software running on a B&R PLC. CodeMeter licensing methods are already integrated

into Automation Studio, the Integrated Development Environment used to build software for B&R PLCs, to help B&R clients accelerate and facilitate the integration of licensing capabilities.

They can use the same USB dongle to store licenses for B&R software packages created and delivered by B&R as well as licenses of the software generated and rolled out by themselves. With this option, they can implement their own license models and count on a reliable revenue stream for their assets.

Also, CodeMeter License Central is used to create and deliver licenses for B&R software packages. B&R clients can use their own CodeMeter License Central to deliver licenses to their users. 





CODESYS



Software and hardware security add-on for the CODESYS development system, guarding CODESYS-compatible devices and SoftPLCs, now available directly from the CODESYS web store.

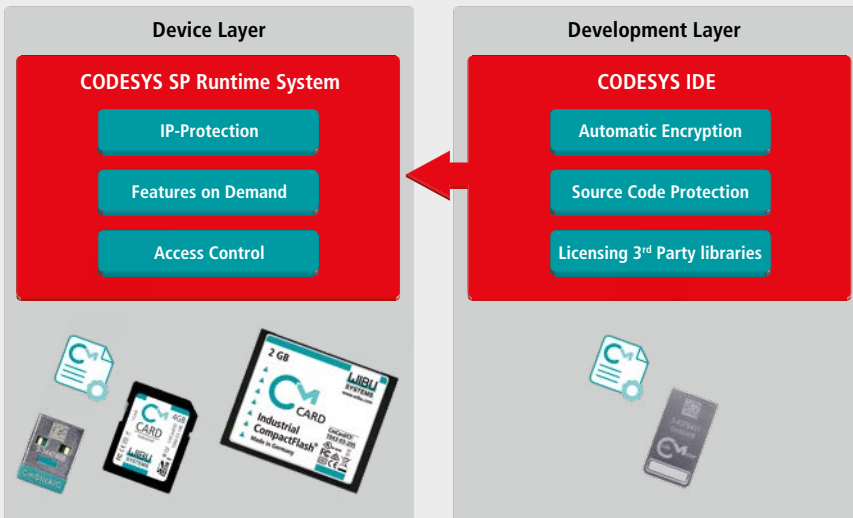
Ad-Hoc Tools for CODESYS

CODESYS is the most popular independent IEC 61131-3 development system there is, with a particularly committed fan base in the automation world. The partnership between CODESYS and Wibu-Systems is a natural response to the need to protect intellectual assets from reverse engineering and counterfeiting.

Bringing together CodeMeter and CODESYS bolsters security on several levels: Protecting the source code

of the IEC 61131-3 application in the development tool, protecting functions and libraries during development and runtime, and creating protected code for the target PLCs to ensure that the application's launch requires a valid license.

CodeMeter licensing and protection methods are already integrated into the CODESYS Integrated Development Environment (IDE). The developer only needs an additional standard CodeMeter SDK to create licenses.



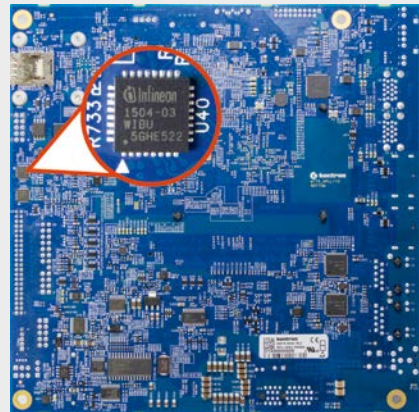


Fitting all new embedded systems and IoT boards with security modules for security-by-default software protections and ready-to-use license management.

Security by Default

In 2016, Wibu-Systems entered a unique technological and commercial agreement with Kontron to fit all of Kontron's products (modules, motherboards, and systems) coming with sixth-generation Intel® Core™ and Intel® Xeon®, Intel® Atom™, Intel® Celeron®, or the most recent iteration of Intel® Pentium® processors with the APPROTECT technology and furnish upgrade kits for previous Kontron models. APPROTECT combines a software framework with an integrated security chip (CodeMeter ASIC) and TPM 2.0 (Trusted Platform Module) to achieve the optimum in software protection.

At its heart, Kontron's APPROTECT is built around CodeMeter, which encrypts the source code of applications executed on embedded components to prevent any illicit copies or reverse engineering. On top of these fundamental capabilities, CodeMeter also offers product managers



other license management functions to pave the way for more diversified marketing strategies with per-use or time-based licensing and the after-sales activation of new features in the field. 





Straightforward, responsive, secure, and flexible order management for PC WORX Engineer Licenses made possible by integrating SAP and Baan with CodeMeter License Central.

Managing PC WORX Licenses

Phoenix Contact has chosen CodeMeter to market PC WORX Engineer, the comprehensive software development solution for PLCnext controllers, with a modular, scalable, and efficient solution.

The decision was driven by the unique technological competence of Wibu-Systems when it comes

to protecting digital know-how with the synergy obtained by combining automatic encryption of classes and methods with software and hardware licenses, working seamlessly with PCs and PLC devices alike, supporting the ERP systems already in place at Phoenix Contact, and offering new prospects in the cloud.






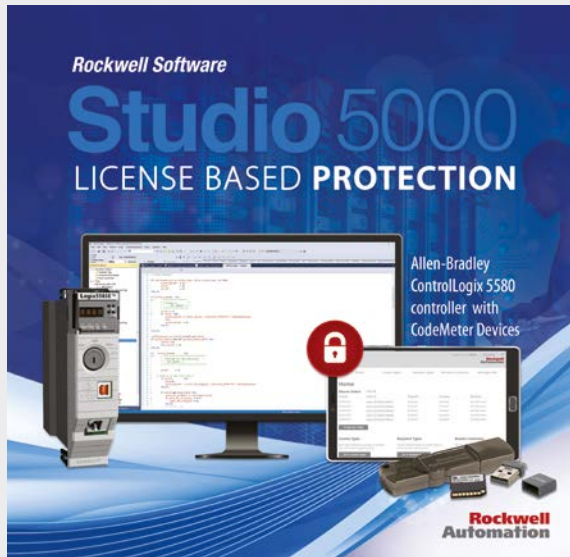
Managing access to invaluable digital assets for smart device makers, commissioning or servicing technicians, and the end user.

Restricted Logical Access

Studio 5000 Logix Designer® by Rockwell Software® includes CodeMeter technology for the comprehensive protection of intellectual property at all links in the product chain, from the initial creation of the source code to the finished and compiled applications running on industrial controllers.

This license-based protection system rests on three pillars:

- **Source Protection** – Protection for sensitive code: Built right into the Studio 5000 environment, software developers now have a choice of which part of their source code should be protected, which licenses used, and which users can utilize CodeMeter hardware secure elements to view and edit protected content.
- **Execution Protection** – Runtime protection in controllers: The applications running on the Allen-Bradley® ControlLogix 5580, CompactLogix 5380, and CompactLogix 5480 PLCs of Rockwell Automation can only be launched if
 - a CodeMeter secure memory card is available in the controller.
- **Web Portal** – Rights and entitlement management: Licenses for source code and executables can be created, assigned, delivered, and managed efficiently via a dedicated web portal. 




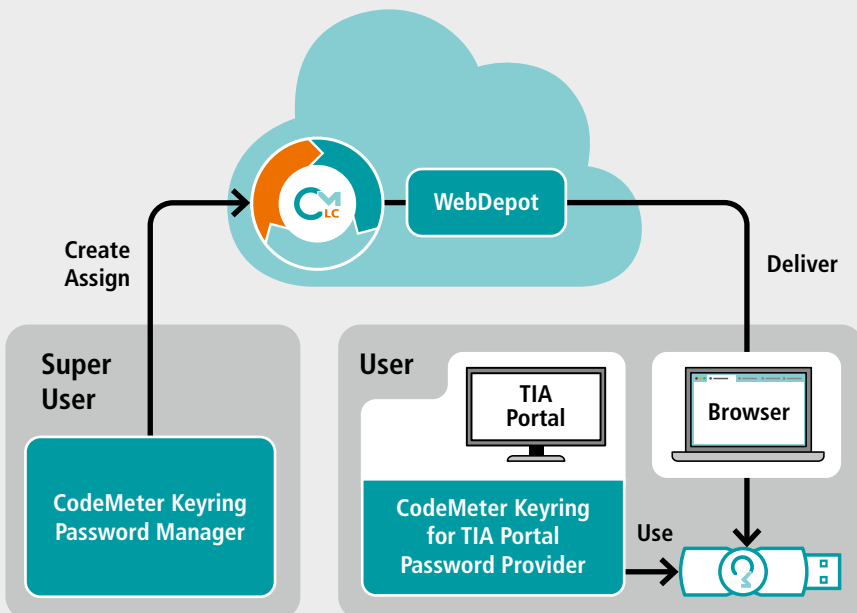


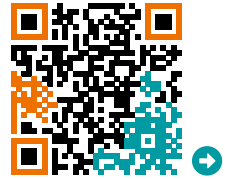
A tailor-made solution for Siemens' Totally Integrated Automation (TIA) Portal® using hardware secure elements for controlled online and offline password allocation.

Secure Password Allocation

The engineering data kept on the TIA portal is typically a highly confidential asset. Only fully authorized users should be able to view or modify projects with the right entitlements; to guarantee this, Siemens' users can rely on a special password manager to protect their digital know-how.

Passwords can be stored on Wibu-Systems' CmDongles, which come in a vast range of form factors, from USB dongles (with optional flash memory) and memory cards (SD, microSD, CF, and CFast) to ASICs. This allows granular and flexible controls over access to engineering data, including by time limits or access counter. 






Bolstering the built-in protections of the OPC UA protocol for secure cryptographic key storage and novel sales concepts in the industrial world.

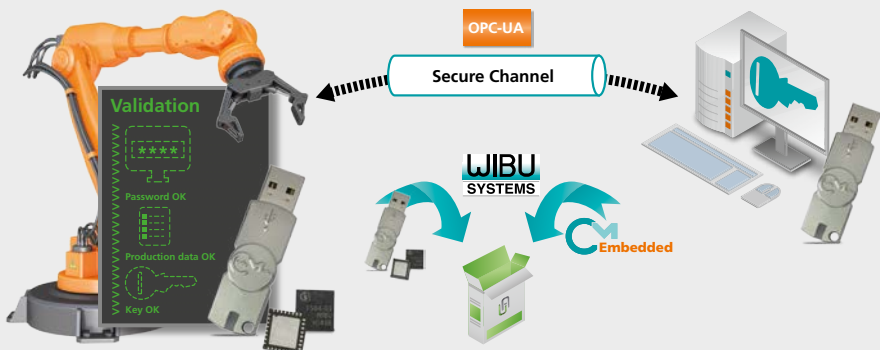
Security Extensions for OPC UA

Keeping cryptographic keys or other sensitive configuration files, such as private RSA keys or trust lists, in the routine file system exposes this data to theft and tampering, especially in the modern, connected cyber-physical world. Among their many insidious ways of compromising their targets, hackers seize on the vulnerabilities of operating systems with Trojans and other ways to sneak into the file systems.

Unified Automation has released its OPC UA SDK based on ANSI C with the complete integration of CodeMeter Embedded, the runtime environment for

embedded systems like Linux Embedded, VxWorks, QNX, and Android. This enables makers of embedded software to use secure CodeMeter hardware elements (USB dongles, memory cards, or ASICs) to store cryptographic keys and trust lists. Cryptographic keys can be used, but not read, and trust lists read, but not changed without the right privileges.

Furthermore, makers of embedded software can use the same hardware to store licenses for their software and employ all license models offered by CodeMeter. This feature enables them to create additional revenue streams for their Intellectual Property. 






Combining cutting-edge protections for devices and data, securing know-how, and enabling a new level of flexibility in license management to seize new commercial opportunities.

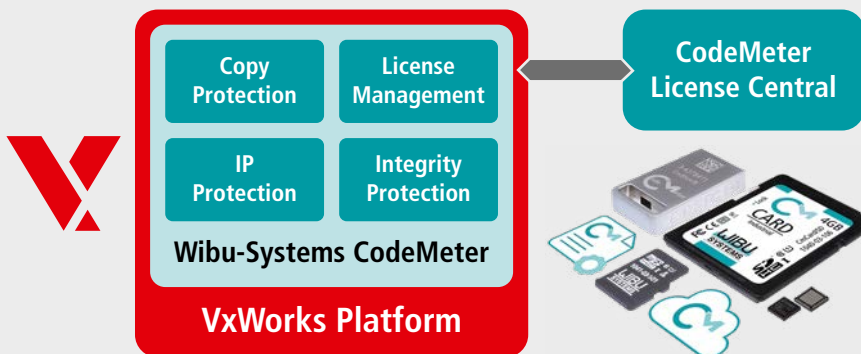
Security Extensions for VxWorks

Wibu-Systems is reinforcing its partnership with Wind River® and offers an integrated installation of CodeMeter® in the VxWorks® workbench, the most popular commercial real-time OS in the world. The module that handles the essential decryption work, ExEngine, is built right into the VxWorks loader to ensure full and unbroken coverage. Together, Wibu-Systems and Wind River have developed a complete turnkey solution with:

- An internal CA (Certification Authority) used to allocate, sign, and manage digital certificates, needed for the secure boot processes that can shield applications from manipulation.

- A secure runtime loader, with a combination of AES cryptography and the real-time authentication of a digital fingerprint of kernels and processes that protects the integrity and intellectual assets invested in software from piracy and reverse engineering.
- License and entitlement management with cryptographic key and license storage on hardware, software, or cloud containers.

CodeMeter is fully compatible with VxWorks 6.9 and VxWorks 7 Core Platform, including the Security and Virtualization Profiles. 



White Papers




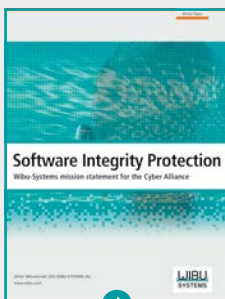
Licensing and Security for the Internet of Things

The Internet of Things has well and truly arrived in our lives, our work, and the future ahead of us. It is up to the makers of smart devices to understand the cyber risks involved, to reimagine their hardware and their processes, to safeguard infrastructures and equipment, and to get active in a completely new dialogue with contractors, technology partners, and clients. Only enterprises that manage to reinvent themselves are ready for success in the new age of digital transformation. 




CodeMeter in the Automation Industry

For the makers of industrial controllers and manufacturing equipment, software has long become indispensable as a means for activating features and delivering after-sales services. Original equipment manufacturers can protect their know-how against illicit copies and shield their production data, software, and firmware from tampering by introducing effective cryptographic capabilities. With these in place, they will win a vital competitive edge that may determine their long-term viability and the application of their engineering potential. 



Software Integrity Protection

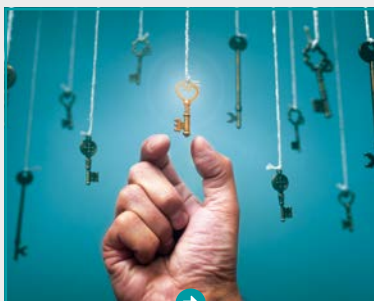
The Industrie 4.0 concept envisions an unprecedented level of connectedness – which creates completely new inroads for would-be cyber criminals setting their sights on OEM manufacturers. With the combined power of cryptographic technology and a battery of real-time checks to verify digital certificates in the boot loader, operating systems, applications, and configurations, the integrity of the embedded system is in safe hands. 

Webinars



IP Protection for Siemens TIA Portal

When you invest in Siemens TIA Portal®, you also want to safeguard your applications for Siemens PLC and HMI with a higher gear. CodeMeter License Central is the gateway between CodeMeter Keyring Password Manager (the user, password, and entitlement management tool) and CodeMeter Keyring for TIA Portal Password Provider (the component that links CodeMeter with the TIA Portal). You can then assign clear roles to your team members, protect the IP of your projects, and control user access with a hardware-based solution: CmDongle.



Who are you? Authentication by certificates

Digital certificates have proved their worth as a strong means of authentication for decades. With IIoT taking center stage in industrial automation, machines need to be identified securely as well to stop illicit users or systems from sneaking in and potentially wreaking havoc in networks. X.509 certificates, coupled with communication protocols like OPC UA and hardware-based safe storage solutions like CmDongles, are ideal choices to meet the challenges of today.

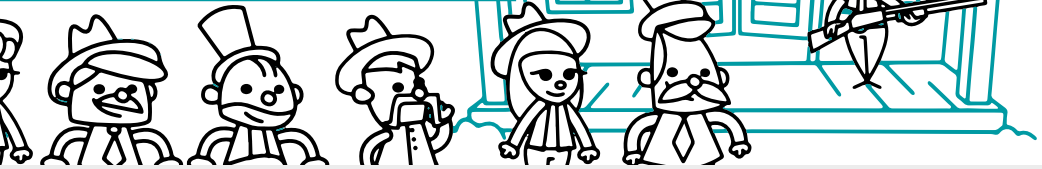


OPC UA Security: Native and Add-Ons Solutions

OPC UA is a machine communication protocol designed with platform independence and plug & play capabilities in mind to serve the smart factories now being developed as the worlds of OT and IT are converging. CodeMeter Embedded supports the full security profile and specifications of the OPC Foundation. With the OPC UA SDK developed with Unified Automation, it offers even stronger protections and more versatile license management for the smart factories of tomorrow.



Economy 4.0



CodeMeter is the key enabler for the new economy: with client-centric solutions and by protecting the invaluable know-how of developers, it opens up new digital markets.

A New Paradigm

As the concept of Industrie 4.0 is becoming reality and cyber-physical systems are getting connected in distributed, flexible industrial networks, plant engineers are shifting their attention from the specialized machines of yesterday to the customization of software. Through software, machine features can be activated or upgraded at the point of need to allow a far more fluent relationship between maker and buyer. The app stores of the mobile phone world have shown the way: Established sales processes can be taken to a new level and modular, scalable business models introduced that

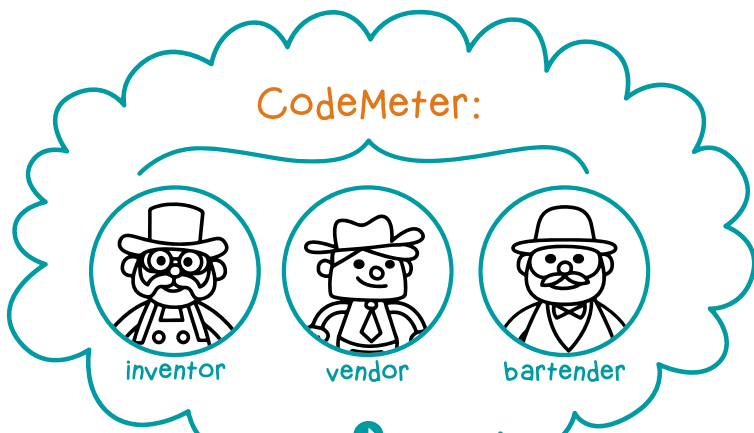
are truly responsive to the needs of the market. This has the very real potential to reduce production, inventory, and logistics costs – and to save the environment almost as a side-effect.

And New Threats

Industrial espionage, cyberattacks, and outright sabotage are a direct consequence of all these new developments. Industrial availability now increasingly means digital reliability, and the IIoT world needs to remain awake to issues of physical security, privacy, IT security, trustworthiness, and business continuity.



CodeMeter:



- Compose your original code
- Orchestrate your license strategy
- Fine tune your IP protection
- Distribute your work of art

Sounds easy, right?
And it is with CodeMeter



Start now and
request your
CodeMeter SDK
wibu.com/sdk

+49 721 931720
sales@wibu.com
www.wibu.com




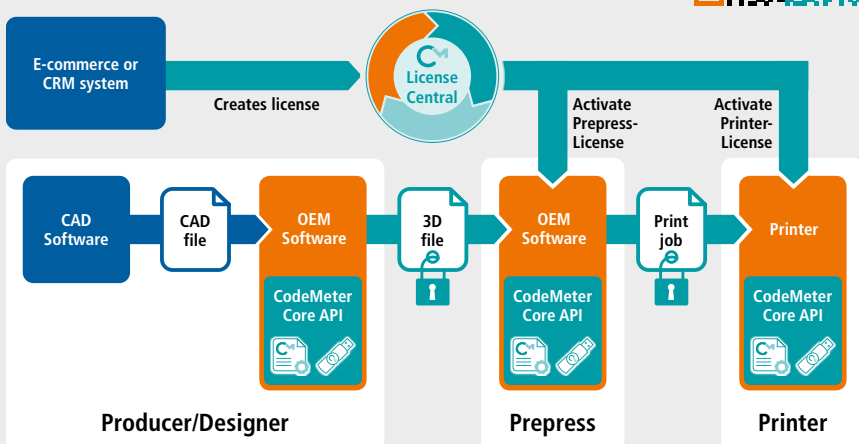
SECURITY
LICENSING
PERFECTION IN PROTECTION

Protecting and Monetizing IP in Additive Manufacturing

People had already begun thinking about 3D printing in the 1970s, but what keeps being overlooked to this date is how to protect 3D printing data from piracy and how to track and bill print jobs correctly and securely for all stakeholders involved.

The 3D printing process starts with the development of a digital object, which contains or represents a crucial piece of intellectual property. This asset needs to be protected, because only protected IP can be marketed in any sensible way. This should not be a problem if the holder of that IP is actually the same person or business doing the processing and printing as well. But the 3D printing market is moving in another direction: In many cases, the digital object will only be one component of a whole array of pieces that an integrator would assemble into a finished product, and the printing happens outside of the direct control of the IP's owner.

With CodeMeter's concept, prepress and printing stages are handled separately, each via a dedicated license. Both licenses include the necessary cryptographic keys; in the case of the printing license, there is also a secure unit counter to keep track of how many copies of an object have actually been printed. 



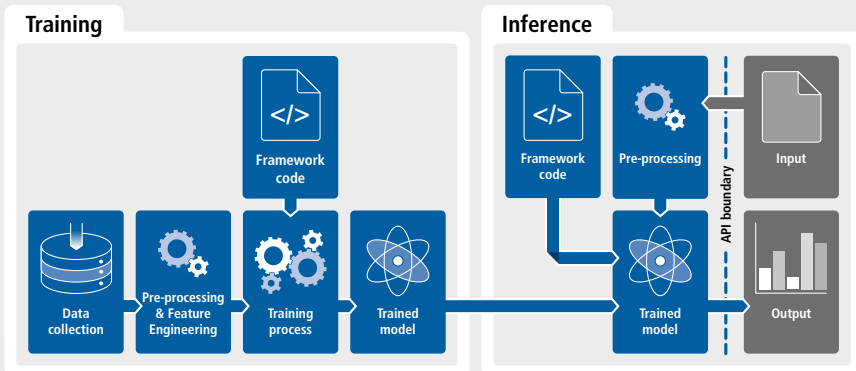
Securing the Machine Learning Lifecycle

Machine Learning can be defined as programming a computer so that it can learn from data. Three core artefacts – training data, training process description, trained model – are key in this context and can be susceptible to inadvertent modifications or even intentional attacks.

The verification and validation mechanisms used in standard software development (e.g., static code analysis or unit testing) do not suffice to guarantee the overall quality of training data, training code, or trained models.

Conventional access controls and integrity protection measures can help mitigate data poisoning attacks. Besides secure communication at the network level, confidentiality and integrity protection at the application layer could be achieved by means of trusted elements, like Wibu-Systems' CodeMeter dongles.

To protect against theft of training models fine-grained software protection services like our CodeMeter Cloud could be the answer. We could even consider shifting parts of the training process to trusted execution environments such as SGX enclaves or secure elements in general.



CmReady – License Mobility with Industrial Memory Cards

Instead of binding a CmActLicense to a device via SmartBind, it can also be bound to a removable device like an SD card or memory stick. This gives the user the ability to move licenses easily between different devices, as can be done with CmDongles. For this purpose, the CmActLicense is not just bound to the removable device, but additionally stored on it.

CmReady by Wibu-Systems and our certified solution partners offers a turnkey solution that is ready for use and saves you the effort of implementing it yourself: CodeMeter comes with standard support for CmReady certified mass storage devices. The CmReady logo is only awarded to devices equipped with secure elements that are guaranteed to work in line with the CmReady standards. The advantages for you: Easier implementation and top security against license tampering on removable and mobile devices.

CmReady lets you use a CmActLicense on a mass storage device similar to a CmDongle and enjoy

all CmActLicense functions on a mobile basis. For highest protection standards, including the ability to execute code away from the user's computer (CodeMoving) or use safely locked-away keys for authentication (CodeMeter Certificate Vault), we recommend our full CmDongles.



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

Cryptoagility for Post-Quantum Security



A sufficiently powerful quantum computer could completely break a large part of the cryptographic methods currently in use and carry out known attacks much more efficiently than conventional computers.

Like most cryptography used so far, post-quantum secure methods are based on complex mathematical problems, for which neither a conventional nor an efficient quantum algorithm has yet been found.

Methods differ strongly with respect to their key size, security, and efficiency. Furthermore, there are strong differences in their suitability for encryption and signatures. PQC algorithms are often less well studied cryptanalytically than conventional cryptography.

Especially for the security of embedded devices, which is dependent on efficient algorithms, this introduces a risk that already implemented methods might have to be replaced. In order to achieve long-term security and to be able to react with sufficient speed to new cryptanalytic results, a high degree of crypto-agility – even across different PQC classes – must be guaranteed.

Wibu-Systems is partnering with leading vendors and academia to:

- Introduce new updating capabilities for hardware secure elements to ensure full compatibility with PQC factory updates.
- Provide an update mechanism for high-end secure elements, including devices already working in the field, to inject new cryptographic capabilities through a secure and backwards-compatible (hybrid) updating scheme without the need for replacing any physical hardware.
- Develop a generic hardware module for low-end, limited-resource cases that ensures crypto-agility by allowing the physical replacement of the module in factory while keeping the established secure element platform in place.

⟨PQC|4|MED⟩



Wibu-Systems is a global leader in cutting-edge cybersecurity and software license lifecycle management. We are committed to delivering unparalleled, award-winning, and internationally patented security solutions that protect the intellectual property embedded in digital assets and amplify the monetization opportunities of technical know-how. Catering to software publishers and intelligent device manufacturers, the interoperable hardware and software modules of our comprehensive CodeMeter suite safeguard against piracy, reverse engineering, tampering, sabotage, and cyberattacks across mainstream platforms and diverse industries.

Wibu-Systems expressly reserves the right to change its programs or this documentation without prior notice.

© 2023 WIBU-SYSTEMS AG – Blurry Box®, CmReady®, CodeMeter®, SmartBind®, SmartShelter®, and Wibu-Systems® are registered trademarks of WIBU-SYSTEMS AG. All other brand names and product names used in this documentation are trade names, service marks, trademarks, or registered trademarks of their respective owners.



WIBU-SYSTEMS AG

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



**SECURITY
LICENSING
PERFECTION IN PROTECTION**