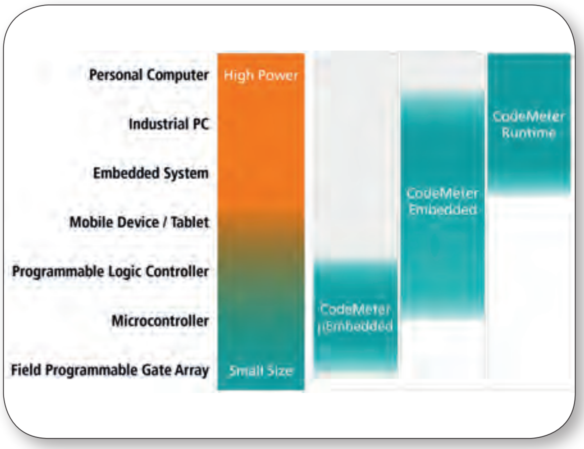
Protection and licensing solution from the sensor to the cloud

This article is contributed by Wibu-Systems

Today's software and devices are increasingly connecting with and speaking to each other. But in a connected world, cybersecurity and protection against tampering are becoming paramount in order to safeguard and actually implement new business models.



CodeMeter - Scalable protection and licensing

■ Software and firmware used to live in separate worlds, existing in isolation as autonomous entities with fixed and clearly delineated jobs and capabilities. Today's software and devices are increasingly connecting with and speaking to each other. New software and hardware platforms allow functions to be retrofitted or activated at a later time, as smartphones have shown to great effect. This can make development more efficient, reduce the time to market, and enable novel business models, such as pay-per-use concepts. In this new world, cybersecurity and protection against tampering are becoming paramount in order to safeguard and actually implement these new business models with the commercial effectiveness they deserve.

As more and more devices get connected, all sectors of industry stand to benefit from unparalleled efficiency effects. At the same time, the risk of manipulation increases, e.g. by illicit tampering with device configurations. Data incidents and hacker attacks have become a common experience in almost all sectors of industry. Businesses need to shield themselves against this threat with consistent and effective protections that cover every link in the chain, down to the last endpoint. Protecting sensitive data against theft and manipulation is of no less importance. Devices can only be meaningfully protected with solutions that offer copy, know-how, and integrity safeguards in combination with flexible licensing capabilities. It does not matter whether diagnostics software on PCs or full-blown embedded applications in medical devices are concerned – at the heart, it is all about software and the data generated and used by it. This data can come in many shapes and sizes, from operating parameters to maintenance instructions and from hardware logs to patients' data.

The purposes of protection can also be very varied. The makers of devices want to know that their products are shielded against reverse engineering, tampering with their operating settings, and other forms of sabotage down to the level of the code itself.

In order to protect the know-how invested in software, the executable application needs to be encrypted before it is released into the wild. This can mean the full encryption of the entire application, or selective encryption of individual functions. All users receive the same protected software, but, depending on the licenses and entitlements they acquire when purchasing the product, they will get only the keys to the functions they have paid for. Product managers can define the right types of user rights and licenses, be it single user, network, or time-limited licenses. The CodeMeter technology made by Wibu-Systems shows how developers can protect and encrypt their work.

The functions of the devices are realized by separately protected functional blocks that are activated by the right licenses and keys – which can be updated at a later point if need be. This simplifies the production process by reducing the number of variants that need to be made, in turn making inventory, ordering, and logistics processes simpler and easier to handle. On top of simply protecting the intellectual property in the device, these new capabilities help bring down the cost of production.

Following Kerckhoffs' principle, the encryption protocols themselves are public knowledge. The only secret piece in the puzzle is the encryption key. These keys need to be kept behind particularly tough safeguards. The optimum protection is offered by hardware key storage with integrated encryption, so-called smart card chips that can withstand even side channel attacks (Differential Power Analysis, DPA).

The keys never need to leave their secure home, and all essential cryptographic operations are conducted on the secure hardware. Alternatively, encrypted license files can be used that

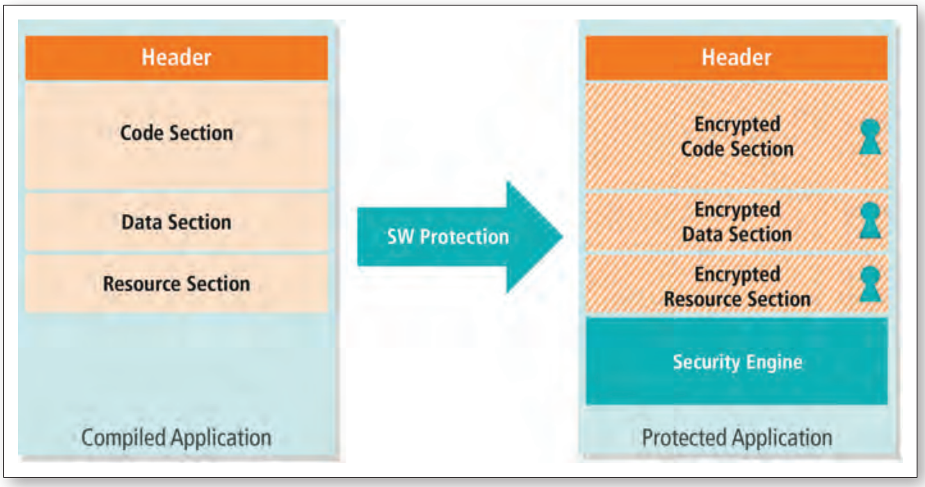


Figure 1.1 Encrypting the entire application

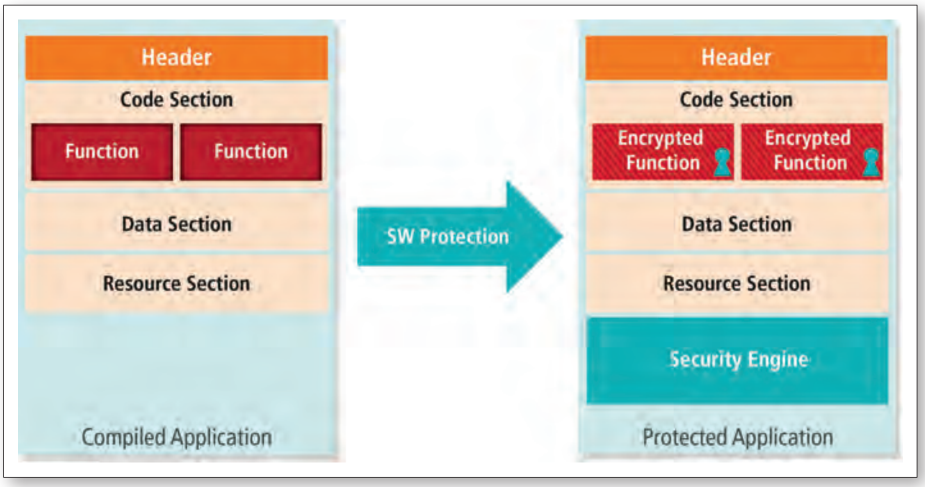


Figure 1.2 Encrypting individual blocks of functions

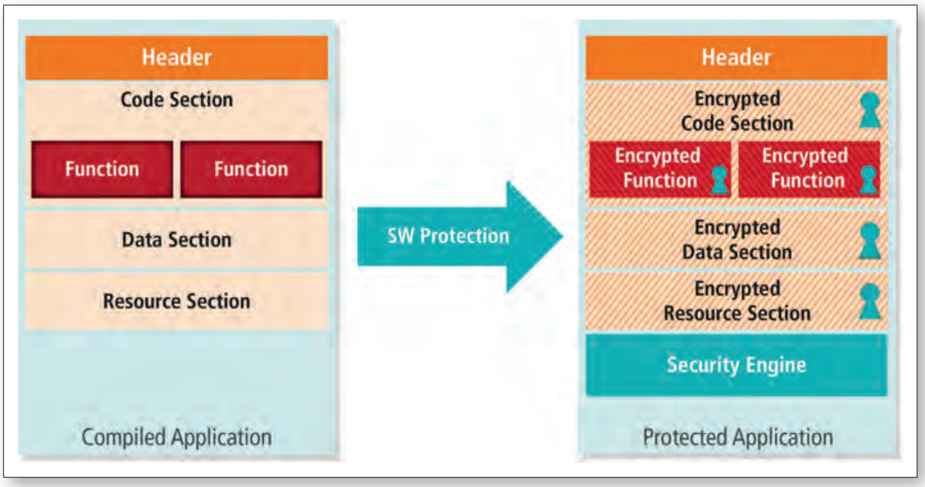


Figure 1.3. Combining 1 and 2

work with a fingerprint of the devices they are used on, such as the serial number, a TPM, or other combinations of uniquely identifiable and non-modifiable hardware properties. An ideal solution is flexible enough to accommodate each platform with a specific custom implementation without compromising on the protection technology, its tools, license models, and formats. Despite all optimization for specific platforms, the entire solution has to remain consistent, using the same API in all cases and only adjusting the active feature set to match the given application. CodeMeter µEmbedded is a CodeMeter variant made in Standard C and designed for portability, with the lower computing power and often very restricted memory footprint of MCUs in mind. CodeMeter µEmbedded is typically packaged with the development platform for each MCU. For instance, developers can find MCUs packaged with the DAVE™ plug-in, the professional development platform for Infineon. This makes it perfectly easy for developers to integrate software protection and licensing capabilities for individual functional blocks. Although CodeMeter µEmbedded has been optimized for the special case of MCUs, it includes the same tools and license distribution processes as e.g. CodeMeter Embedded and CodeMeter Runtime. The advantage is that license definitions can be used across CodeMeter variants. The programming interface represents a subset of CodeMeter Embedded, optimized for MCUs, but coming with the identical API and a specially selected feature set that matches the use case.

CodeMeter Embedded is more versatile than CodeMeter µEmbedded as another CodeMeter flavor realized in Standard C and designed specifically for the requirements of embedded systems. CodeMeter Embedded is highly modular and portable; it is integrated in a range of modern development platforms of several makers, including the VxWorks Workbench by Wind River and CODESYS by 3S-Smart Software Solutions.

CodeMeter Embedded is also used in QNX and Linux systems on various microprocessor architectures like ARM, x86, ia64, and PPC. With its modular and portable architecture, there are also several other custom ports of the solution for additional operating systems, ranging from FreeRTOS to bare metal implementations. CodeMeter Embedded again comes with the same tools and license distribution systems as the other variants. The same license definitions can be used with all of them without requiring any adjustments. The programming interface is a super-set of CodeMeter µEmbedded and a subset of the CodeMeter Runtime API, optimized for embedded devices.

CodeMeter Runtime is the premium product for all off-the-shelf operating systems, including macOS, Windows, and Linux and standard x86 hardware. CodeMeter Runtime is a super-set of CodeMeter µEmbedded and CodeMeter Embedded, offers top ease-of-use, and is delivered only in binary format for use with standard hardware and standard operating systems. Embedded devices that can accommodate this with their hardware can use either CodeMeter Embedded or CodeMeter Runtime. Again, the system offers the same tools and license distribution processes, giving device makers a great choice. As a premium product, CodeMeter Runtime comes with the full set of features

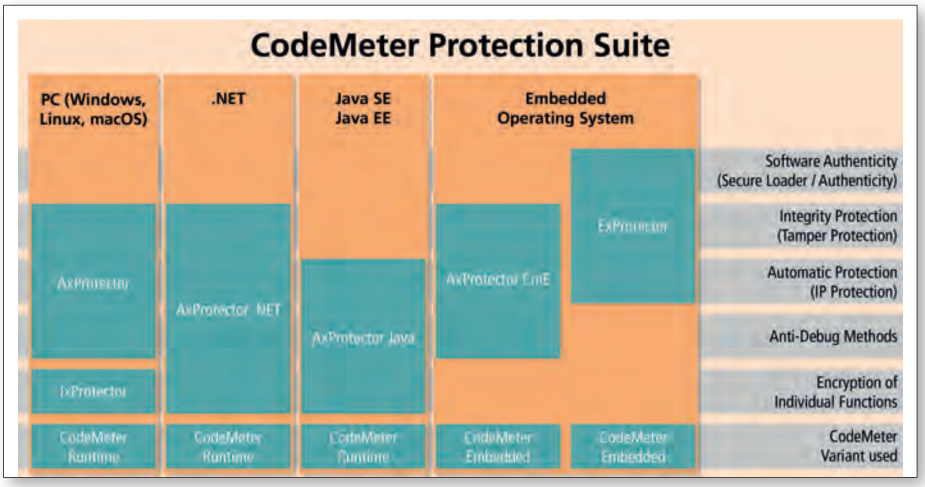

CodeMeter Protection Suite
PC (Windows, Linux, macOS)
.NET
Java SE
Java EE
Embedded Operating System
AxProtector
IxProtector
AxProtector .NET
AxProtector Java
AxProtector CmE
ExProtector
CodeMeter Runtime
CodeMeter Runtime
CodeMeter Runtime
CodeMeter Embedded
CodeMeter Embedded
Software Authenticity (Secure Loader / Authenticity)
Integrity Protection (Tamper Protection)
Automatic Protection (IP Protection)
Anti-Debug Methods
Encryption of Individual Functions
CodeMeter Variant used

Figure 2. One consistent toolset for all platforms

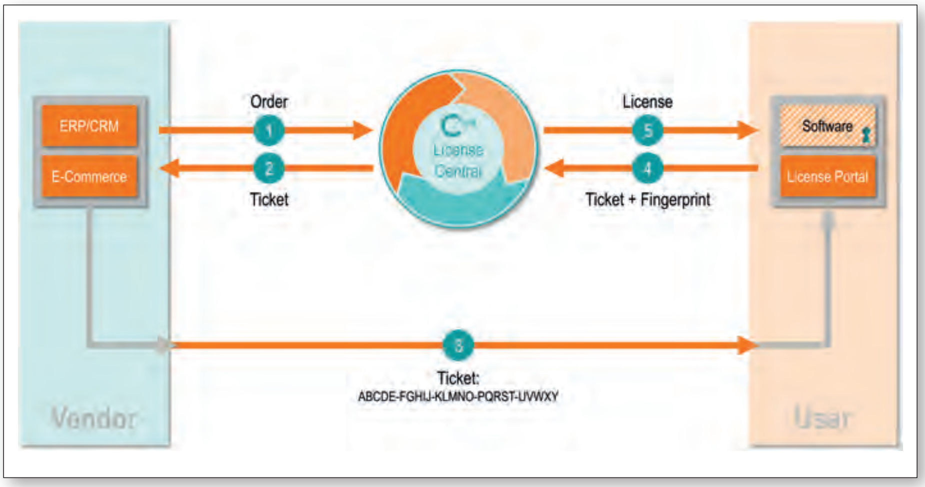


Figure 3. Centralized license management with CodeMeter License Central in the cloud

of all APIs. The license management system CodeMeter License Central makes easy work of the creation, management, and distribution of entitlements and licenses. It supports product management with the definition of products and licenses. Product managers can use the established ERP or CRM systems to create orders; an automated interface then initiates the creation of the right licenses in the license management system. Users can, for instance, activate add-on features in online appstore-like portals; this creates a completely new revenue stream for the device makers. Pay-per-use and subscription models are similarly easy to introduce.

As part of the German national reference project for IT security in Industrie 4.0 (IUNO prototype technology data that employs all of the elements outlined here has been developed. To give this dry-sounding topic a more appealing presence, designed a special cocktail mixer: the cocktail recipes with their exact ingredient lists represent the technology data protected from end-to-end. The system can be transferred to other use cases and is available free of charge at https://github.com/IUNO-TDM.

Whenever the security of devices is concerned, there are two sides and two special sets of requirements to be considered. The makers of the devices want to protect their work from reverse engineering and manipulation, keep their know-how secret, and put new business models or logistical advantages to use. The operators or users, on the other hand, care most about the integrity of the devices and the data stored on them or used with them. In order to reconcile these two sides, the most promising choice is a protection concept that can fulfill both types of requirements.

Ideally, the chosen concept comes with a fully scalable and seamless technology and toolkit included. Since the licenses or containers are the same whether they be used with CodeMeter Runtime, CodeMeter Embedded, or CodeMeter µEmbedded, CodeMeter is a neatly uniform solution perfectly designed for integration into existing business processes. In a departure from the frustrating patchwork often required for tailoring other solutions to the given circumstances, CodeMeter is simply ready to go to work. ■