License Management with TPM powered with CodeMeter

Protecting IP in the IoT with Trusted Computing

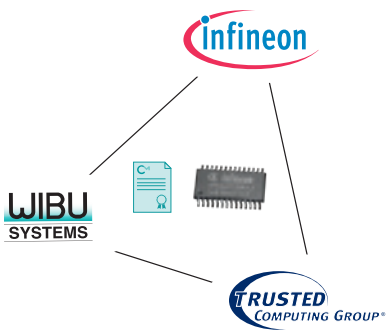
Ever since software has gained a predominant role in our lives, new revenue streams have been created; at the same time, all countries have been affected by commercial losses due to product, know-how, or data piracy, eroding large chunks of their GDP. In the era of connected devices, as value in the supply chain is being transferred from hardware to software, the number of counterfeiting, tampering, and espionage incidents is on the rise. Software protection is therefore becoming the vital backbone of any mature cyber security strategy.

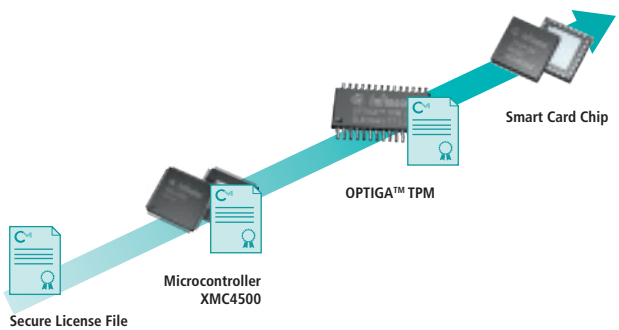
By combining endpoint security with skillfully designed licensing models that mirror the success of app stores, software-powered businesses can meet customers' demands in a granular way and in turn expand their reach globally. In the new economy led by Industrie 4.0, the secure upgradability and updatability of system features and functionalities open the doors for a shorter time to market, adaptive process optimization, and global competitiveness.

The demonstration shows a two-step process: how to protect an application against reverse engineering and counterfeiting, and how to enable new business models with license and entitlement management. The process relies entirely on CodeMeter from Wibu-Systems, the all-in-one technology for the protection of IP and production data designed for intelligent device manufacturers. CodeMeter encrypts software, firmware, and data and creates secure licenses. Hardware secure elements (like industry-grade dongles, memory cards, ASICs, or Trusted Platform Modules) in the target system offer a secure repository where cryptographic keys can be safely stored. All hardware secure elements produced by Wibu-Systems embed a smart card chip from Infineon. The wide range of temperature, humidity, and vibration these security microcontrollers can withstand makes them ideal for ruggedized industrial environments. Their Common Criteria EAL5+ certification provides an additional element of trust for highly sensitive projects.

In this demonstration, the protected license associated with individual functions of the software is bound to an OPTIGA™ TPM from Infineon Technologies. The software would then run only on the IoT device, computer, mobile device, embedded system, or PLC that has been enabled, and provide the functionalities associated with the license, safe from any sort of hacking. The license lifecycle management can also be seamlessly integrated in back office processes, e.g. ERP, CRM, or e-commerce platforms, to further enhance the monetization process and significantly reduce the bottomline costs related to logistic and service aspects.

The Trusted Computing Group (TCG) was formed to develop, define, and promote open, vendor-neutral, global industry standards for interoperable Trusted Computing platforms. TCG conducts regular seminars and demonstrations to assist fellow industry stakeholders in their quest for IoT security.





Licensing and Security for the Internet of Things

Trends in IoT

Connected systems prevail over closed infrastructures

Manufacturing used to be the domain of closed systems and capital equipment with long life expectancy. With the IoT, factories and manufacturing methods are being re-engineered. Remote maintenance, remote operations, remote monitoring, and remote management are already an everyday reality.

Software prevails over hardware

Computing hardware and operating systems are becoming increasingly standardized. What differentiates one piece of equipment from the next is the applications running on it. Security by design guarantees the integrity of these applications and protects against reverse engineering, product piracy, and tampering.

Business models are evolving

Software-based functions can be brought to market as extras or after-sales options by means of license activation. Paid upgrades, pay-to-use features, or time and volume-controlled operations protect the commercial success of equipment manufacturers. The more versatile the licensing options, the more flexible the marketization opportunities. Licenses and entitlement rights guarantee business continuity, but only if the relevant logistics are transparently integrated into the OEM's and the end users' processes.

A diversified architectural landscape

The components of diverse manufacturers and software from diverse sources come together to form heterogeneous systems. Post-hoc expansions or additions keep the system flexible and evolving. New interfaces and communication standards emerge that allows transparency, easy integration, and lower implementation overheads.

New use cases and services

The digital transformation fuelled by cyber-physical systems of any shape and form is entering all market verticals to form giant neural landscapes. New applications that take advantage of this evolving connectivity are created every day and restricted only by the limits of our creativity. Comprehensive protection covering all parts of any system, including miniature components and devices with minimal storage space or computing power, is imperative for all ISVs and IDMs.

CodeMeter – Industrial IoT-Ready Technology

The core technology of CodeMeter stands on six solid pillars:

Uniformity

- One technology for protection, licensing, and security
- One family of license containers where hardware, software, server, and cloud vessels interact seamlessly
- One framework for multiple platforms that supports PC, mobile, embedded, PLC, and microcontroller-based systems
- One infrastructure for license creation, delivery, and management
- One system for license monitoring by software publishers and end users

Comprehensiveness

- One hardware concept for all of our USB sticks, memory cards, and ASICs
- One solution for many platforms, programming languages, and processors
- One comprehensive API for license and encryption operations
- Connectors for all of your CRM, ERP, and e-commerce solutions
- One source for all possible license models

Robustness

- One answer to piracy, reverse engineering, tampering, and cyber-attacks
- One strong encryption technology that relies on established international standards (AES 256, ECC 224, RSA 2048) and digital certificates
- Winner of the German IT Security Prize in 2014
- Winner of the 2017 CODiE Award for the Best Content Rights and Entitlement Solution
- Strongest security that no hacking contest could break

Simplicity

- Easy integration in many applications
- Simple kickstart for Licensing as a Service
- Transparent customization of the license portal for the user

Uniqueness

- One dongle for standalone, network, and time-based scenarios
- One dongle for multiple vendors handled independently
- One secure clock for all license containers (dongles, license files, server)
- Patented technology for the secure and dynamic binding of licenses to PCs

Continuity

Legacy support and security updates from 1989 to today

Protection

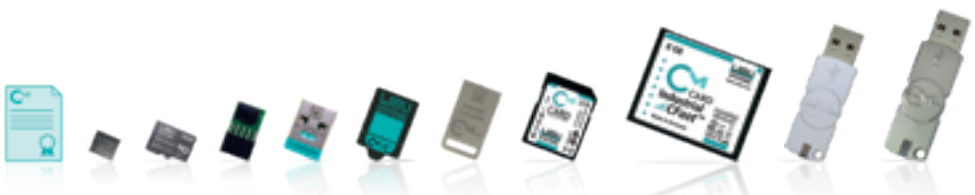
www.wibu.com/cm

Licensing

www.wibu.com/cml

Security

www.wibu.com/cms



WIBU-SYSTEMS AG | Rueppurrer Strasse 52-54 | 76137 Karlsruhe, Germany | Tel.: +49 721 931 72-0 | Fax: +49 721 931 72-22 | sales@wibu.com | www.wibu.com

20171027