NEWS AND INSIGHTS FROM THE WORLD OF ID SECURITY

NOVEMBER 2016 | #13

The VAULT

INTERNATIONAL

Refugees – the solution to an imminent problem

APPLICATIONS

eID use cases beyond border control | eGovernment – boosting a country's development

TECHNOLOGY

Can FIDO accelerate the uptake of eGov Services? | Shape shifting the embedded system business

Mobile – Where next?

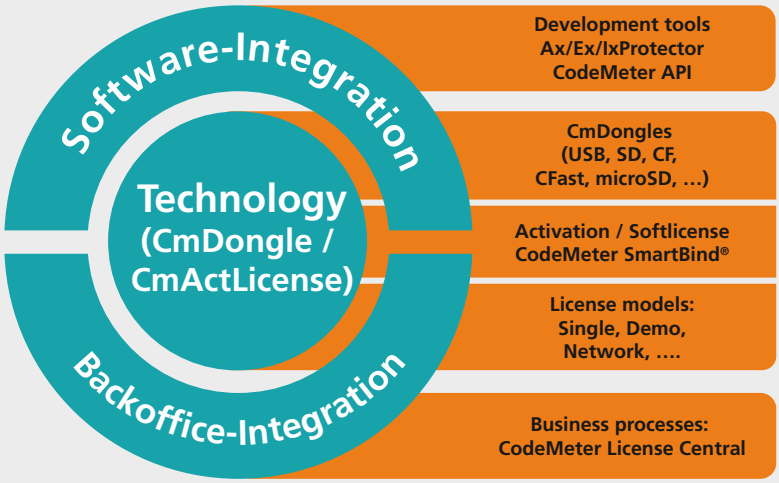
CodeMeter
Securing the Industrial Internet

WIBU SYSTEMS

- Industrie 4.0
- Smart Factories
- Embedded World

CodeMeter Security – Watch the full Video – www.wibu.com/cms

New business models for software publishers and device manufacturers



In its mission to deliver the most secure, unique, and versatile technology, Wibu-Systems has developed CodeMeter®, a comprehensive, award-winning suite of hardware and software solutions for **computers, embedded systems, mobile devices, PLCs, and microcontrollers** that incorporates internationally patented processes dedicated to protecting the **integrity of digital assets**.

With its motto "**Perfection in Protection, Licensing, and Security**", Wibu-Systems supports ISVs and OEMs in their fight to **safeguard the intellectual property** of their applications against illicit and fraudulent use, reverse engineering, tampering, sabotage, espionage, and cyber-attacks, while generating new **software-feature based business models** fully integrated with ERP, CRM, and e-commerce platforms.

The unparalleled lineup of **hardware secure elements** (USB dongles, SD cards, microSD cards, CF cards, CFast cards, ASICs) designed to withstand high fluctuations in temperature, humidity, and vibration, coupled with the support of all mainstream operating systems and M2M communication standards makes CodeMeter the ideal candidate for both **brown and green field** applications.

5. Deutscher IT-Sicherheitspreis 2014

SECURITY
LICENSING
PERFECTION IN PROTECTION

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

Shape SHIFTING the *embedded* system *BUSINESS*

By Daniela Previtali, Wibu-Systems

The Industrial Internet business has ignited a technological revolution and an economic renaissance that are proceeding at an unprecedented ppace. As the McKinsey Global Institute mapped out the value beyond the hype, they estimated that the IoT (Internet of Things) has a total potential economic impact of USD 3.9 to 11.1 trillion a year. From a less visionary and more analytical approach, Ernst & Young has come to an additional observation: a combination of digital disruption and slow organic growth has propelled the global Tech M&A to a record Q2 2016, with deals worth more than USD 1 bn. Academia, governments, and industrial organizations are supporting the shift, but how can manufacturing stakeholders really get ready and restructure their entire production and sales organizations to take full advantage of this transformation?

☐ The Hype Cycle of IoT starts with Security

An uncontrolled explosion of data in between cyber-physical systems expose systems, workforces, and vendors to new inadvertent risks and malicious attacks. The underlying factor that should be designed from ground up in the entire infrastructure is trustworthiness, which the Industrial Internet Consortium categorizes in five core elements in their Security Framework:

- **Security**, as the condition of a system that is protected against unintended or unauthorized access, change, or destruction
- **Safety**, as the condition of a system that is safeguarded against tampering to avoid direct or indirect injury or damage to people, property, or the environment
- **Reliability**, as the ability of a system to perform its required functions for a predefined time expectancy
- **Resilience**, as the ability of a system to avoid, absorb, or manage adversarial conditions, and reconstitute full operation after the incident
- **Privacy**, as the right of individuals to control what and how personal information is being collected, stored, and disclosed

“Our Approtect is a game changer in the ECT business: Coupling out-of-the-box security with hardware manufacturing components will increase user and operational confidence in the new IoT designs.

Jens Wiegand, Kontron CTO

“Technological versatility and business model scalability are the key to a granular implementation of new security paradigms across all industry sectors, that will monetize software-powered processes.

Oliver Winzenried, Wibu-Systems, CEO and co-Founder

A Solid Security Design Focuses on the Endpoints

While a pervasive security approach is recommended to cover all points of data input, output, transmission, and storage, in software engineering the architectural modules that are mostly at risk are the endpoints; namely sensors, devices, and machines where software is being executed and sensitive data produced, analyzed, or archived. Two design perspectives can be intermingled:

- **Security by Design**, where devices are equipped with configuration options that enable security
- **Security by Default**, where a certain level of security is already entrenched in the device

In both cases, you can combine Security by Obscurity, where the secrecy of the design or the implementation is the main security component, or the Kerckoffs’ doctrine, which predicates a public design in which the encryption key is the only element surrounded by absolute secrecy.

Smart Manufacturing with Secure IoT-Ready Components

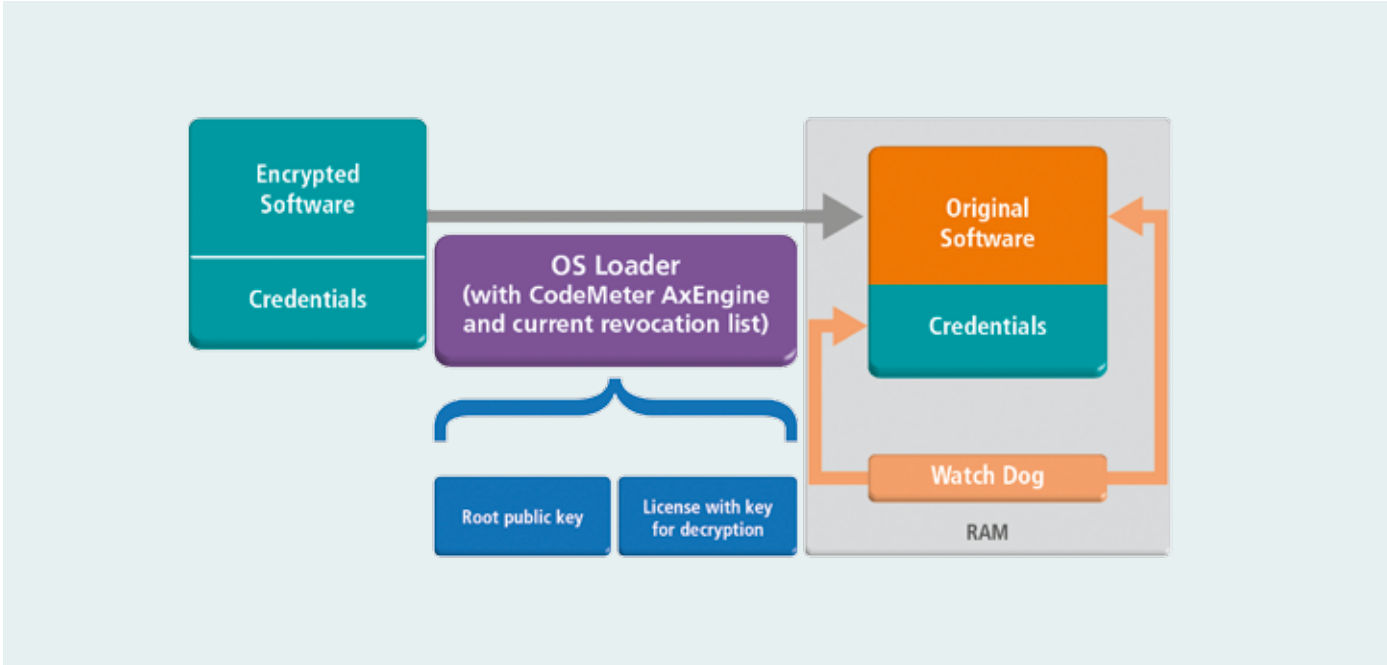
The case of Kontron, a global leading provider of Embedded Computing Technology (ECT) is exemplary. Their Approtect is a turnkey solution powered by Wibu-Systems' CodeMeter that performs software encryption and license management in the brown and green field. Intelligent device manufacturers who select Kontron for the supply of their IoT boards, gateways, modules and systems will inherently receive best in class technology for the protection of their technical know-how against product counterfeiting and software reverse engineering and piracy. Beginning with the 6th generation of Intel® Core™ processors, all Kontron's products will be equipped by default with hardware-based embedded security. A root of trust associated with a hardware secure element that embeds a smart card chip from Infineon's SLM97 security controller family, offers a secure repository for digital keys that preserve software integrity from cyberattacks, sabotage and industrial espionage in the form of tampering.

IP Protection for ECT Vendors

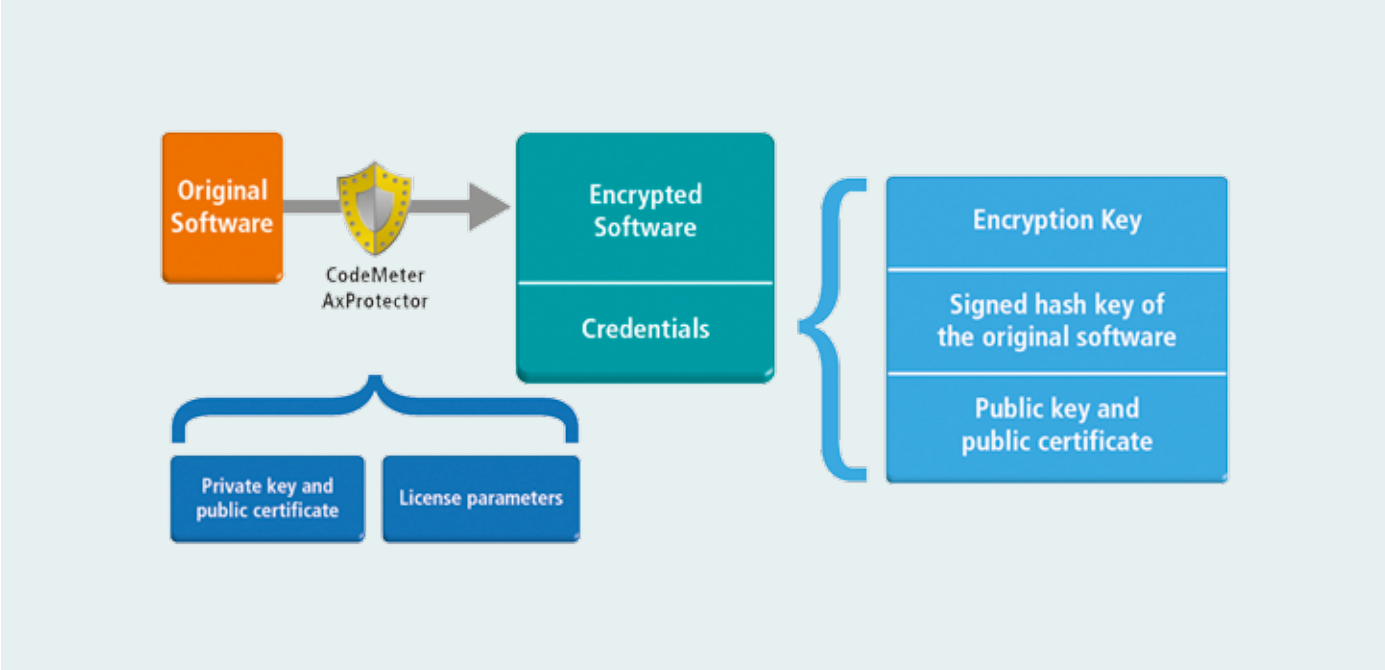
The implementation of security that Kontron has designed covers several business aspects. In the first place, they are fully in control of the distribution of their intellectual property. By protecting their own multi-layer software stack with Wibu-Systems' multi-awarded technology, their revenue collection will exactly match the number of active users.

> *An attack to an Industrial Internet of Things system typically starts with an attack on one or more endpoints. And endpoints are everywhere in the IIoT landscape.*

Only a physical manipulation of the device where the Kontron board is mounted will give access to the security component; still, CodeMeter ASIC won't easily reveal its secrets: symmetric and asymmetric (128-bit AES, SHA-256, 2048-bit RSA, or 224-bit



Integrity Check runtime update



Integrity Check

ECC) encryption keys in secure, non-volatile memory are stored in the CC EAL 5+, FIPS 140-2 prep, EMVCo Infineon chip; a controller that comes in a tiny 5x5mm VQFN-32 package, withstands temperatures from -40°C to +105°C, has a virtual clock and USB and SPI interfaces for easy integration with any CPU module or system, and has enough storage capacity (1MB, including Infineon certified crypto libraries) to accommodate thousands of licenses from multiple vendors.

The software platform supports all mainstream operating systems, including Windows, Linux, and macOS for PCs, Embedded Linux and Windows Embedded for embedded systems, Linux RT, VxWorks, and QNX for RTOS, and CODESYS for PLCs. All Wind River's customers that have adopted VxWorks 7 Security Profile, which already includes CodeMeter basic software protection functionalities, can therefore just purchase a Kontron CodeMeter-enabled board to avail themselves of the complete potential of Wibu-Systems' technology.

Freedom of Choice in Software Licensing

Just like when you purchase a smart phone, you have the possibility to select additional apps that bring customized benefits by triggering certain features of the same hardware components, Kontron's customers will be given full control to decide on the software features they wish to purchase in a second stage. A bootloader on the ASIC will enable the activation of the license-bound features directly in the field; even in insecure environments, firmware updates and upgrades and new functionalities can be safely delivered and installed.

> *"The IoT is creating a new type of software vendor for whom LEM (License Entitlement Management) is vital to protect, differentiate and monetize their offerings" Laurie Wurster, research director at Gartner*

Security as a Service

Kontron is thinking ahead. With the same hardware and software technology, they can protect the intellectual property of their customers at the same time. This holistic vision indeed includes the opportunity to provide Wibu-Systems' secure licensing technology in a variety of product and service offerings designed for the automation, avionics, communication, defense, energy, infotainment, medical, and transportation fields, where Kontron has already established its presence. ☒