

The VAULT

Identity management *goes global*



APPLICATIONS

Modern Border Management challenges | LDS2 – Key to mobile travel documents?

INTERNATIONAL

People, Birth and Legal Identity
The Angola National ID program

TECHNOLOGY

The 4 prime elements of an eID project | Industry 4.0: Wibu-Systems and Infineon get serious

Wibu-Systems AND Infineon *get* SERIOUS

By Oliver Winzenried, Wibu-Systems

The numbers that characterize the Industrial Internet of Things are staggering: \$15 trillion added to global GDP over the next 20 years¹, an annual economic impact of \$2.7 to \$6.2 trillion by 2025², an installed base of IoT units reaching 28.1 billion units in 2020³. This revolution is thrilling and alarming at the same time, as jobs, technology, trends, and ways of living are going to be revolutionized. The mission is to make the industrial ecosystem more efficient, sustainable, and responsive to buyers' demands; the risks for security and safety could, however, spread like wildfire, and disrupt not just single businesses, but entire cities.



□ How to prevent these dark repercussions and enjoy the fruits of the transformation? Modern industry is moved by a constellation of systems that include personal computers, industrial PCs, embedded systems, mobile devices, tablets, programmable logic controllers, and microcontrollers. Along the line, the computational power of these devices decreases, which also makes the implementation of

security measures a quite complex task. Additionally, intelligent device manufacturers cannot be expected to offer constant training in security, especially with all the novel threats we are facing every day. The challenge was therefore twofold: Bringing about innovations in a way that would be feasible even under unfavorable conditions and in ruggedized environments, and making them easy to integrate.

¹ Source: General Electric

² Source: McKinsey Global Institute

³ Source: IDC

“ CodeMeter μ Embedded offers users of our XMC4000 Cortex M4 microcontroller a secured solution for updating the firmware of their already installed embedded systems in the field and for releasing new functionality through licensing.

Maurizio Skerlj, Senior Director responsible for the Industry Microcontrollers business unit at Infineon.

“ By working with Infineon, we have mastered the challenge of implementing a DRM system in a microcontroller. CodeMeter μ Embedded gives our shared customers a solution that protects their firmware against tampering, cyberattacks, and reverse engineering. And since CodeMeter μ Embedded is fully compatible with CodeMeter – our security solution for PCs and embedded devices – and with DAVE, they can immediately start protecting and licensing their software.

Ruediger Kuegler, VP Sales and Security Expert at Wibu-Systems

Based on the popular and widely accepted CodeMeter® solution for protection, licensing, and security, the German security specialists at Wibu-Systems have developed CodeMeter μ Embedded, which addresses the specific needs for firmware updates or upgrades to microcontroller-based systems: code integrity, license controls, reverse engineering protection, and code copy protection. As if the technological benefits were not enough, Wibu-Systems has also provided a means to monetize the economy of the future.

To reach such an unprecedented level of sophistication, Wibu-Systems has partnered with Infineon Technologies to enable secure update functionality in Infineon’s range of XMC4000 microcontrollers. In its first release, CodeMeter μ Embedded is set to enhance the standard tool chain and provide secured firmware updates and functional upgrades in embedded systems built around XMC4000 microcontrollers.

As controllers are being used more and more in demanding and control-based tasks such as pump controllers, motor controllers, sensors with fieldbus connections and the like, secure loading solutions become a critical factor. The job of CodeMeter μ Embedded is to facilitate the loading of updates into the Infineon XMC4000 microcontroller series and enable additional features in any insecure environment. In a highly connected smart system, several factors need therefore to be taken into account:

1. Only code from a trusted source must be loaded in the controller. The code has to be encrypted during transport and loading, and decrypted inside the controller, based on a controller-bound, individual keyfile in the boot ROM.
2. There should be measurable and verifiable license controls over the controller loading the code, with the ability to unlock (activate) additional features of the microcontroller.
3. The code must be loaded and decrypted only in an authorized (licensed) controller. Its use on non-licensed controllers or in an emulator should be prevented and discouraged.

CodeMeter μ Embedded aims to protect the firmware of the controller during updating in the field against tampering, reverse engineering, and copying. Furthermore, it becomes possible for OEMs (the developers of the software that runs on the controller) to expand the functionality of the hardware or software, so that their client (the user) can take full advantage of the product solution.

With CodeMeter μ Embedded, the user can now import an encrypted file into the OEM firmware file from an external environment. Encryption is triggered via the development environment – DAVE® 4.0 from Infineon. For this purpose, ExProtector is run via a plug-in installed in DAVE to encrypt the firmware

“ CodeMeter μ Embedded does not just safeguard intelligent device manufacturers against external threats coming from unknown violators. It also protects customers against subcontractors’ malpractice; manufacturing devices equipped with XMC4000 can inherently control production volumes and prevent illegal batches of goods from ending up on the grey market. We see a double advantage in this partnership: Infineon and Wibu-Systems have streamlined a complex security process and help eradicate product counterfeiting.

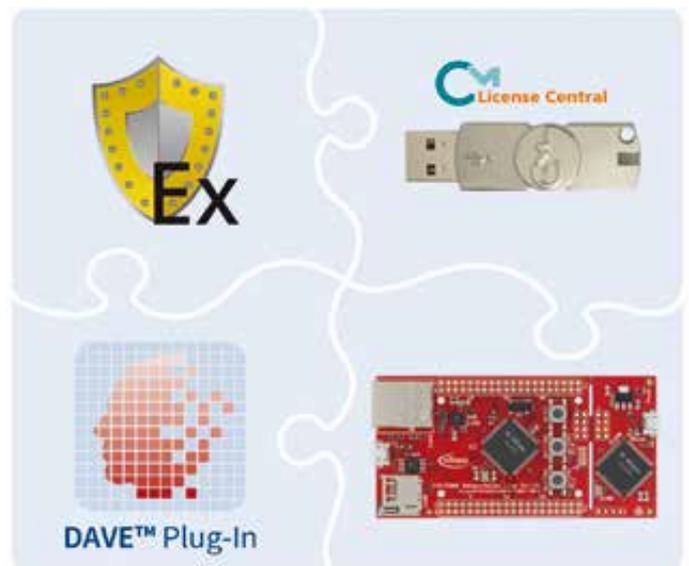
Oliver Winzenried, CEO and Founder of Wibu-Systems

file. After transfer into the XMC4000 controller, the firmware is decrypted and stored in the flash memory, while decoding is handled by the XMC4000 controller.

For optional later upgrades, the microcontroller can generate a request file with the fingerprint of the controller. This encrypted file is transmitted to the manufacturer (by email or online) and a license update is generated and returned. This license update can be transferred to the controller to provide new licenses or make new features available within the microcontroller.

CodeMeter μ Embedded has an extremely small footprint, amounting to less than 60 kBytes. To accomplish this, Wibu-Systems has streamlined its functions to a minimum. The licenses generated are fully compatible with all CodeMeter variants and CodeMeter License Central. They are bound to the unique ID of the microcontroller and can be activated directly during manufacturing. Additionally, Features-On-Demand can be enabled later via remote file updates.

CodeMeter μ Embedded is license-compatible with CodeMeter Runtime. Transferable licenses can be moved onto a device from a CmDongle or a CmActLicense. CodeMeter μ Embedded can also be used to securely store symmetric and asymmetric keys. The keys themselves are located in a protected memory area and can only be used on a device with matching ID.



Utilizing the outlined approach allows multiple use cases with a single technology and tool-chain, while guaranteeing effective firmware protection against copying and reverse engineering. Functional upgrades can take place without any changes to the firmware, and secure firmware updates are now possible even in insecure environments. Fundamentally, this is a user-friendly security solution with state-of-the-art cryptography technology.

CodeMeter μ Embedded has now been successfully integrated into the XMC4000 Infineon microcontroller family. Starting in Q4/2015, developers can fortify their application code against piracy and license it in XMC4000. All tools for protecting the code are now fully integrated in Infineon’s development platform DAVE. ☒

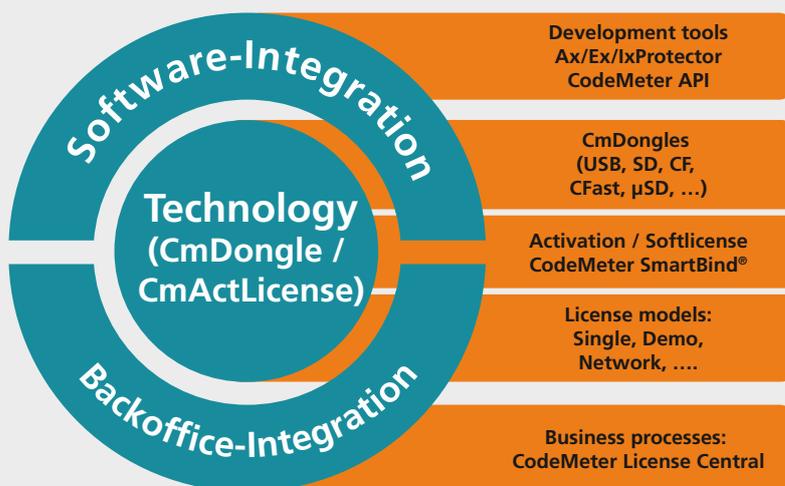
CodeMeter: Security against product piracy and tampering

- Industry 4.0
- Internet of Things
- Embedded Systems



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

Wibu-Systems is the global specialist in protection, licensing and security



CodeMeter® encrypts and signs software. It inhibits software piracy for desktop, server and cloud applications and prevents reverse engineering, counterfeiting and tampering of embedded software in machines and devices. The applications range from CAD and ERP, to ATMs, medical devices, industrial automation, PLCs, as well as energy, logistics, and facility management. In addition, CodeMeter enables new business models by facilitating software configuration of features in production and after sales.

CodeMeter includes protection tools, as well as cloud and intranet based systems for key, certificate and license creation and deployment. At the heart of the technology are secure elements, with built-in smart card chips. They are available for many interfaces, such as USB, µSD, SD and CFast, support extended industrial requirements, including highly reliable flash mass storage, retrofit in existing systems in the brownfield and seamlessly upgrade them. They act like repositories for licenses, keys, certificates, and offer encryption and authentication using AES, ECC and RSA algorithms.