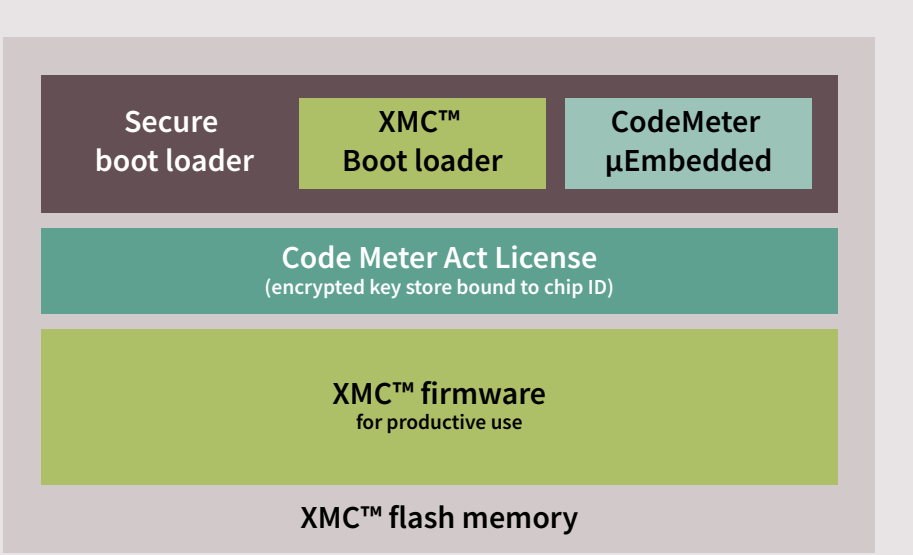
Security Partner

Partner Use Case

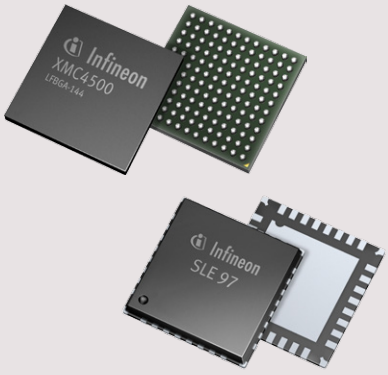
Secure License Management for XMC4500 Microcontrollers

A new flavour of Wibu-Systems' CodeMeter Technology provides IP Protection and License Lifecycle Management for IoT-Ready Products.



Product

XMC4500 and SLE97



Security Partner

Use case

Application context and security requirement

An increasing number of systems in the professional and consumer markets are managed by microcontrollers. These units make use of sophisticated algorithms and likely need firmware updates during their lifetime. Vendors thus face a double threat: product know-how stolen by competitors and tampering attacks during updates and upgrades of the firmware. Either of which can occur in any insecure and unpredictable environment regulated by end users.

Challenge

The firmware of today's microcontrollers is generally loaded onto controllers as a compiled hex image using a serial connection, such JTAG or RS232, without any protection against reverse engineering or fraudulent manipulation. This leaves the file vulnerable in its transfer from the build system to the controller. The end-to-end production's overall trustworthiness should therefore be analyzed. Even if the manufacturer trusts his own build process the microcontroller is no longer in a controlled environment after it has left the production site.

Implementation

Wibu-Systems has ported its established technology from desktop, embedded systems and Programmable Logic Controllers (PLC) to XMC4500 microcontrollers and also created CodeMeter µEmbedded. Original Equipment Manufacturers (OEM) can utilise CodeMeter's ubiquitous reach over a diverse array of hardware platforms. Given the smaller storage capacity and reduced computational power of microcontrollers, CodeMeter's footprint and the secure file (CmActLicense) where the software license is stored had to be shrunk down while preserving their essential functionality. This adaptation to the specific requirements of the XMC™ environment was successful; the CmActLicense was bound to the individual attributes of Infineon's microcontroller and the Infineon DAVE™ toolchain was automated with a plugin to facilitate the creation of secure software in just a few clicks.

User benefits

- State-of-the-art security features ready for use by microcontroller developers
- Intellectual property protection for intelligent-device manufacturers
- Confidence for end users that firmware updates or upgrades are genuine and will cause no unexpected behavior of the target device

Security Partner

Solution

To achieve a comprehensive solution that meets the goals of know-how protection, integrity protection, and monetization by license, the firmware has been encrypted with symmetric and asymmetric (AES and ECC) algorithms, digitally signed as part of the build process in DAVE™ and uniquely bound to the microcontroller. The counterpart of the encryptor in DAVE™ is a special secure firmware loader inside the microcontroller, combined with secure binding to the specific chip. The most critical element of the mission was stripping the code of the mainstream CodeMeter down to 60 KB without compromising its essential security features. The whole set of functions resulting in CodeMeter µEmbedded was eventually packed in a new secure firmware loader.

During the third party production of a XMC4500-based device the secure firmware is loaded into the controller. When powering up for the first time the loader communicates with the production system, generates a fingerprint of the device and is injected with a license. From then on, only encrypted, licensed, and signed firmware can be loaded into the XMC™ microcontroller. If needed, the firmware can also use the license information for custom behaviors. The firmware cannot be extracted from the XMC™, and it is read-protected by internal XMC™ mechanisms.

To bolster security further, it is possibe to extend the hardware binding to an external secure element like an OPTIGA™ TPM (Trusted Platform Module) or a SLE security controller communicating via Serial Peripheral Interface (SPI) with the XMC™ controller.

Developer

- Releases the firmware in DAVE™
- Signs and encrypts the the compiled firmware

Production

- Loads the secure boot loader into XMC™
- XMC™ communicates with the license server and receives license and keys
- Initial firmware is safely loaded for delivery > Device is ready to run

End User in Field

- Receives a firmware update e.g. via email
- Transfers the firmware (e.g. via USB or CAN) to XMC™
- The XMC™ loads, decrypts, and checks the integrity of the firmware before executing it

Main benefits of the Infineon product

- Encrypted and signed firmware can be transferred, loaded, and operated even in insecure environments.
- The cryptographic binding of the license to the controller makes it copy-resistant.
- CodeMeter µEmbedded is easy to integrate, and license management can run on a single PC or with an Enterprise Resource Planning (ERP) system.

Security Partner

Partner

Partners from the Infineon Security Partner Network help you secure your devices and applications: understand which threats can undermine your business, propose solutions that will protect your business, build and implement such security solutions and, when relevant manage their operation. They have been selected by Infineon on the basis of their system security competence and ability to design and deliver strong and trustworthy security solutions. Their activities are diverse and include security consulting, security solution provision, electronic design, systems integration and trust services management. For some, offers are off-the-shelf, while for others, offers are custom-built.

Wibu-Systems
Wibu-Systems is an innovative technology leader in the global software license entitlement market.

In its mission to deliver unique, most secure and highly flexible technologies to software publishers and intelligent device manufacturers, Wibu-Systems has developed a suite of hardware- and software-based solutions dedicated to the integrity protection of digital assets and intellectual property. Its product portfolio addresses a wide variety of license delivery models, including personal computers, Programmable Logic Controllers, mobile, embedded systems, cloud computing, software as a service, and virtualized architectures.

Through its motto “Perfection in Protection, Licensing and Security”, Wibu-Systems reinforces its commitment to eradicate software counterfeiting, reverse-engineering, code tampering, as well as device and smart factory sabotage, espionage and cyber-attacks.

Headquartered in Karlsruhe, Germany, Wibu-Systems holds subsidiaries in USA and China; the company also has sales offices in Belgium, France, the Netherlands, Portugal, Spain, the United Kingdom, and a capillary world distribution network.

Wibu-System’s contribution to the Infineon Security Partner Network
More than the sum of its parts: Infineon’s and Wibu-Systems’ complementary technologies have broadened the range of applications for both companies.

Over its history, Wibu-Systems has broadened its focus to embrace not just Independent Software Vendors, but also industrial automation. With a vocation to provide intelligent device manufacturers with industrial-grade units, Wibu-Systems has powered its entire hardware product line with the SLE 97 security controller made by Infineon Technologies, an ARM® SecurCore® SC300TM, 32-bit, USB 2.0 full speed, CC EAL 5+ certified crucial component for the data security and system integrity of computers and embedded systems in smart factories.

Additionally, Wibu-Systems has successfully integrated the embedded variant of CodeMeter® (its flagship solution for software protection, licensing, and security) with Infineon’s 4000 industrial microcontroller family. Software developers of field programmable gate arrays and microcontrollers can now protect application code and intellectual property against reverse engineering and implement a license control system.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 08 / 2016

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices please contact your nearest Infineon Technologies office (www.infineon.com).

Please note!
THIS DOCUMENT IS FOR INFORMATION PURPOSES ONLY AND ANY INFORMATION GIVEN HEREIN SHALL IN NO EVENT BE REGARDED AS A WARRANTY, GUARANTEE OR DESCRIPTION OF ANY FUNCTIONALITY, CONDITIONS AND/OR QUALITY OF OUR PRODUCTS OR ANY SUITABILITY FOR A PARTICULAR PURPOSE. WITH REGARD TO THE TECHNICAL SPECIFICATIONS OF OUR PRODUCTS, WE KINDLY ASK YOU TO REFER TO THE RELEVANT PRODUCT DATA SHEETS PROVIDED BY US. OUR CUSTOMERS AND THEIR TECHNICAL DEPARTMENTS ARE REQUIRED TO EVALUATE THE SUITABILITY OF OUR PRODUCTS FOR THE INTENDED APPLICATION.

WE RESERVE THE RIGHT TO CHANGE THIS DOCUMENT AND/OR THE INFORMATION GIVEN HEREIN AT ANY TIME.

Warnings
Due to technical requirements, our products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life endangering applications, including but not limited to medical, nuclear, military, life critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.