

# μCodeMeter

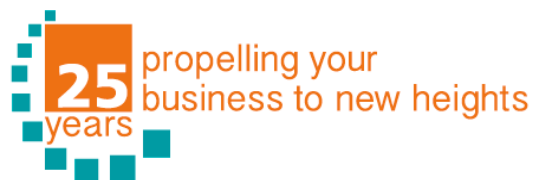
Security für Infineon XMC 4xxx



Marco Blume | Produkt Manager Embedded  
marco.blume@wibu.com

## Wibu-Systems

- Global Player in Software Security
  - UK, NL, FR, USA, CN, ...
- Inhabergeführtes Unternehmen  
aus Karlsruhe
- ~ 100 Mitarbeiter

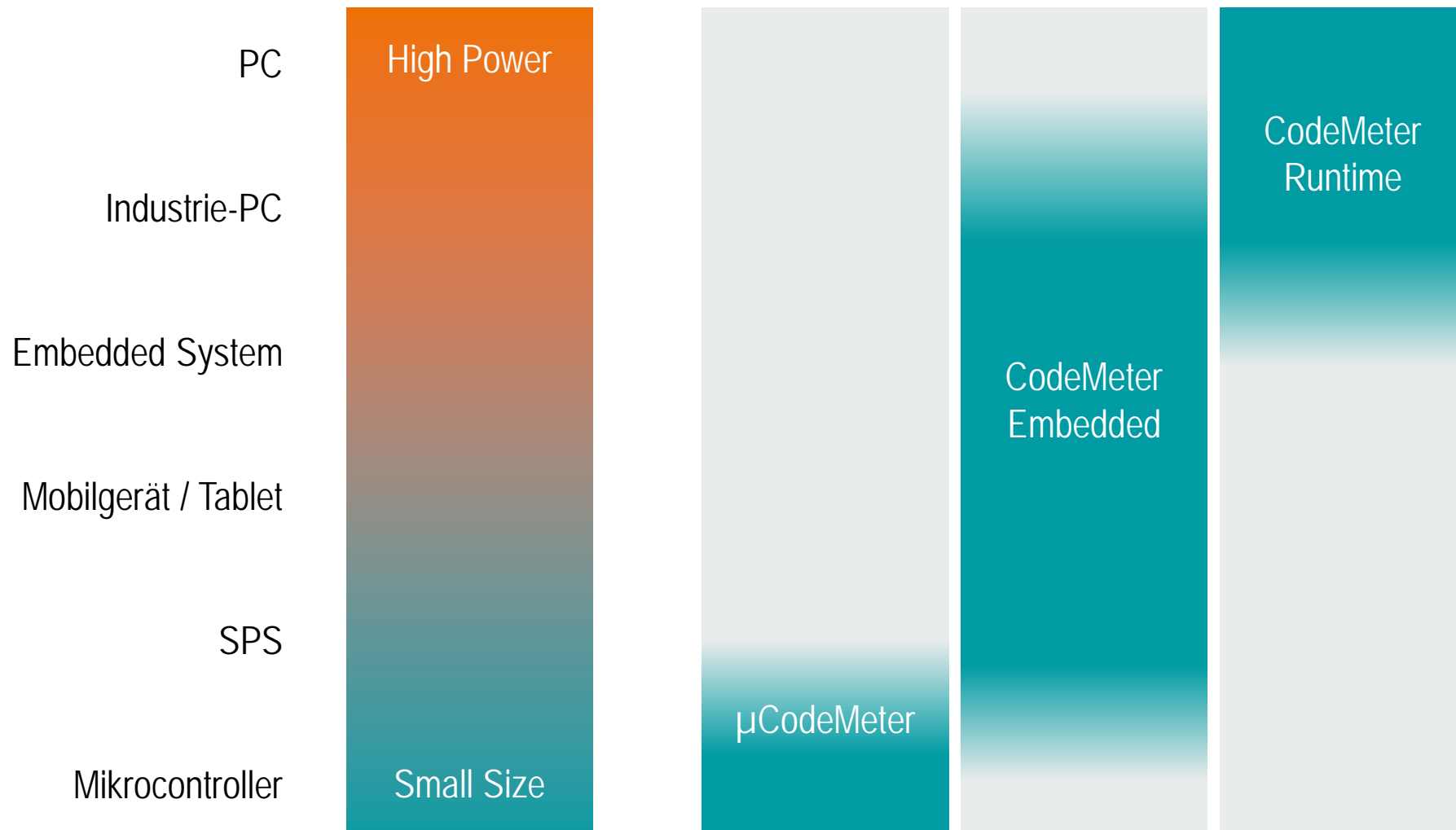


## Schutzziele

- Kopierschutz
- Know How (IP) Schutz
- Manipulationsschutz
- Lizenzierung
- Softwarebasierter CmAct Schutz mit Bindung an individuelle Systemmerkmale
- Hardwarebasierter Schutz mit Infineon SLE97 Chip



# Skalierbare CodeMeter Varianten

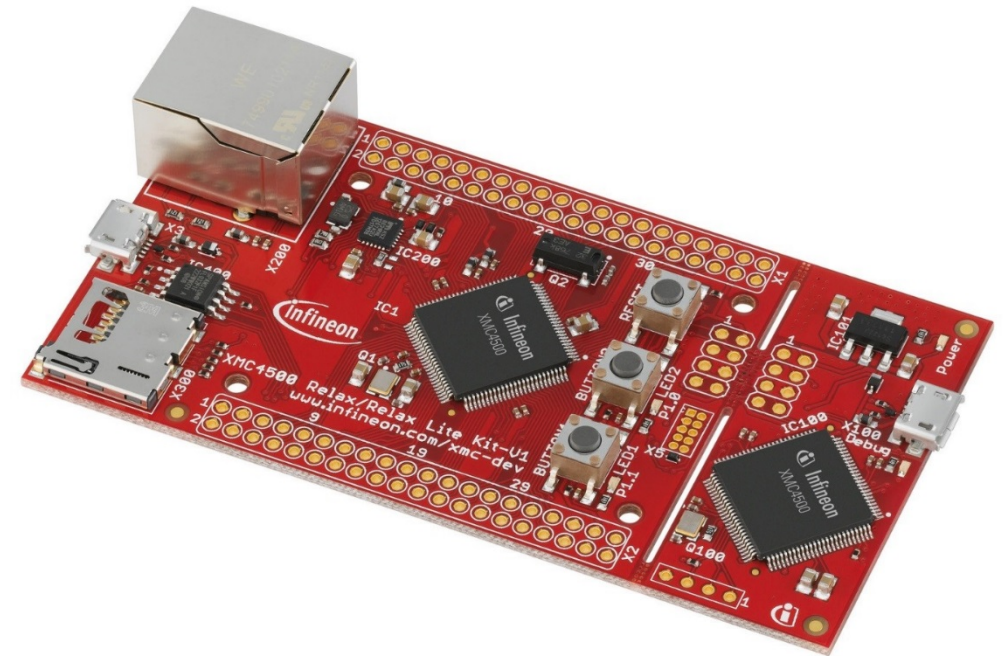


## CodeMeter Security

Integration der  $\mu$ CodeMeter Technik  
in die XMC 4xxx Hardware

➔ Security Plattform in XMC Bootloader  
und Firmware integriert

## XMC Mikrocontroller

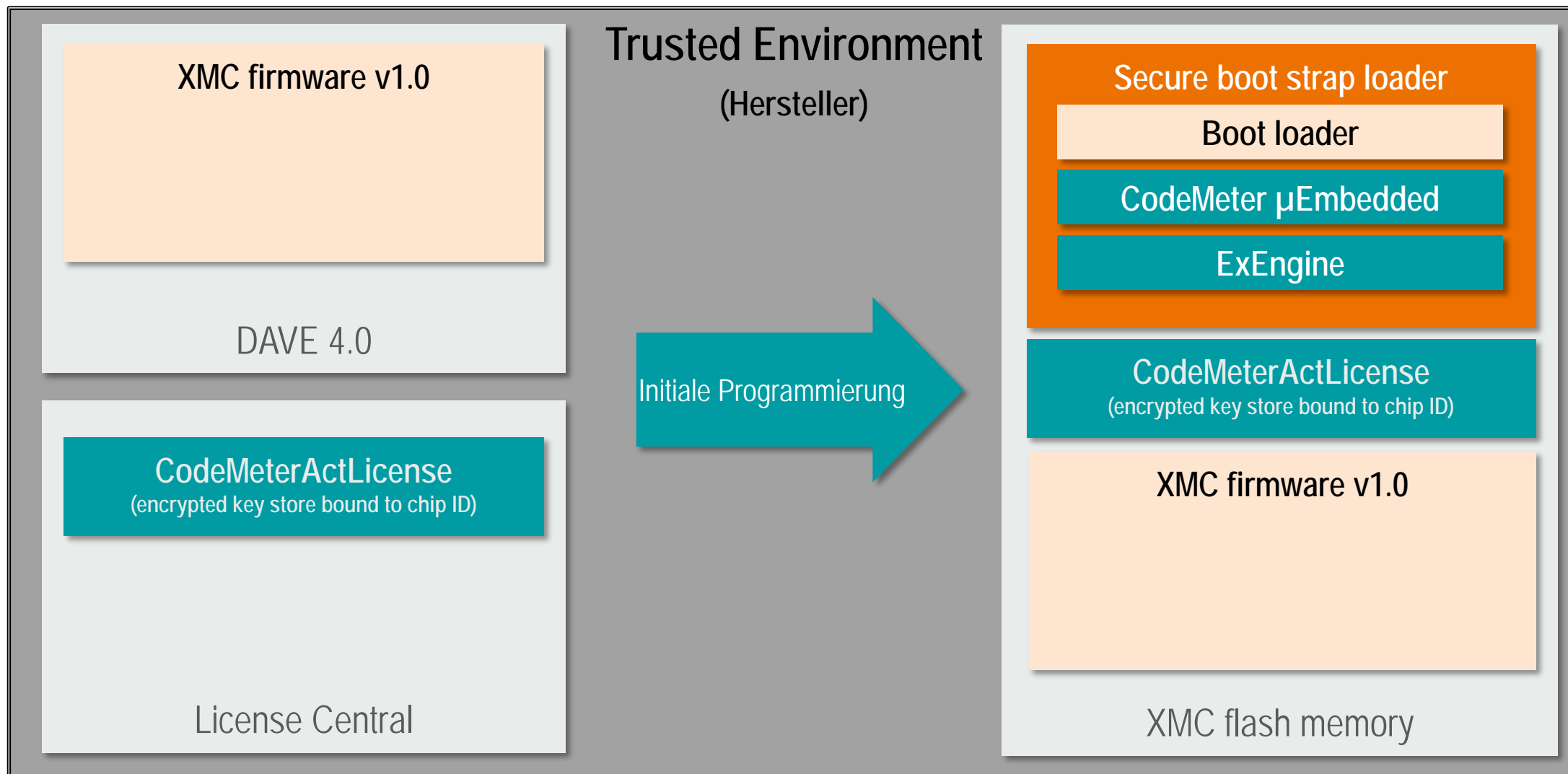


# µCodeMeter @ XMC 4xxx

- Schutzziele
  - Schutz vor Reverse Engineering und Codemanipulation
  - Kopierschutz
- Neue Möglichkeiten im After Sales Geschäft
  - Sichere Firmwareupdates
  - Funktionslizensierung und –erweiterungen
- Anforderungen:
  - Einfache Handhabung
  - „State of the art“ Sicherheit

- Use Case:
  - Ausrollen von Firmwareupdates in unsicheren Umgebungen (System steht bereits beim Kunden)
  - Firmware über unsichere Medien verteilen (Email, Webseiten, ...)





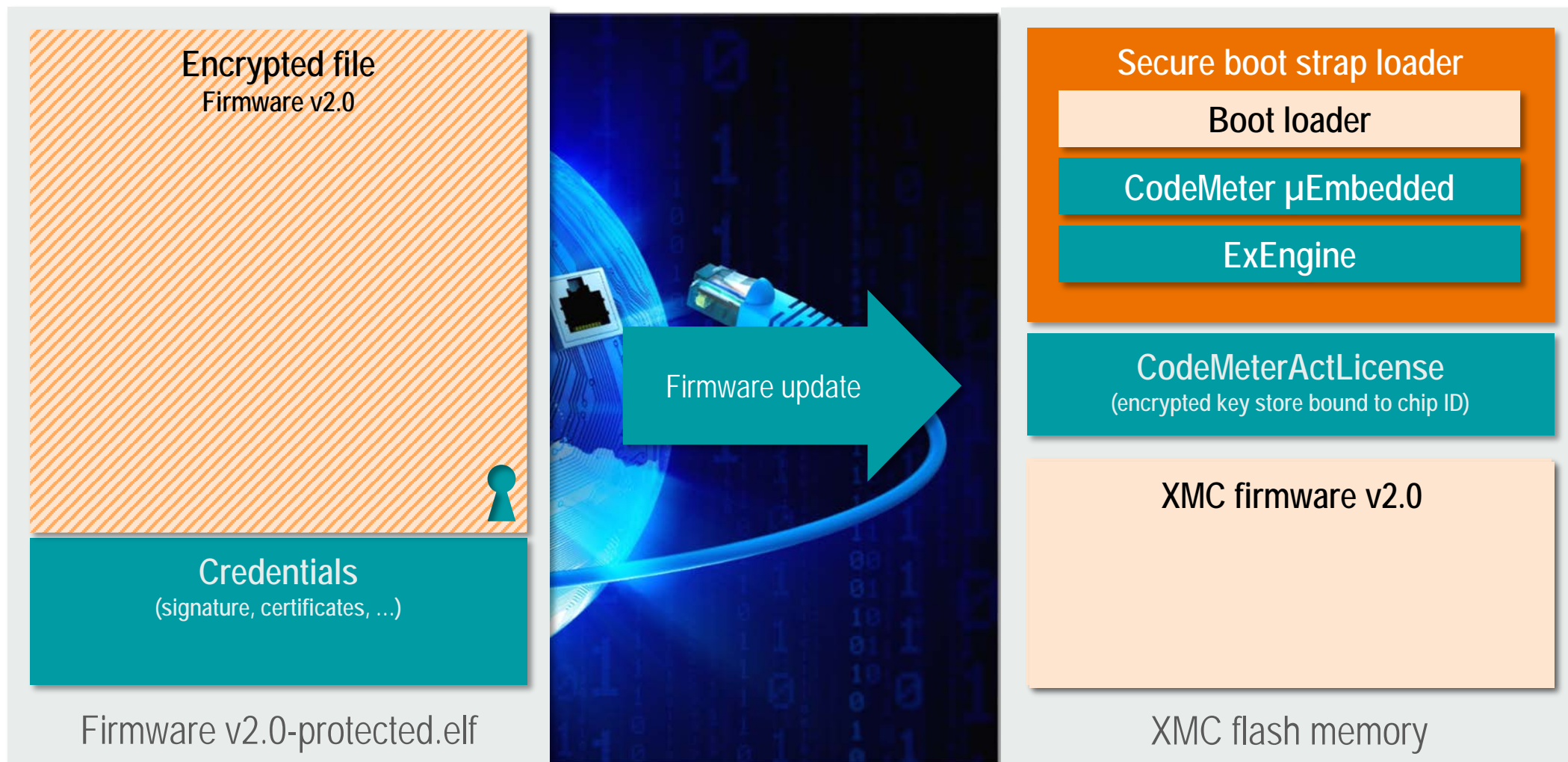


Encrypted file  
Firmware v2.0

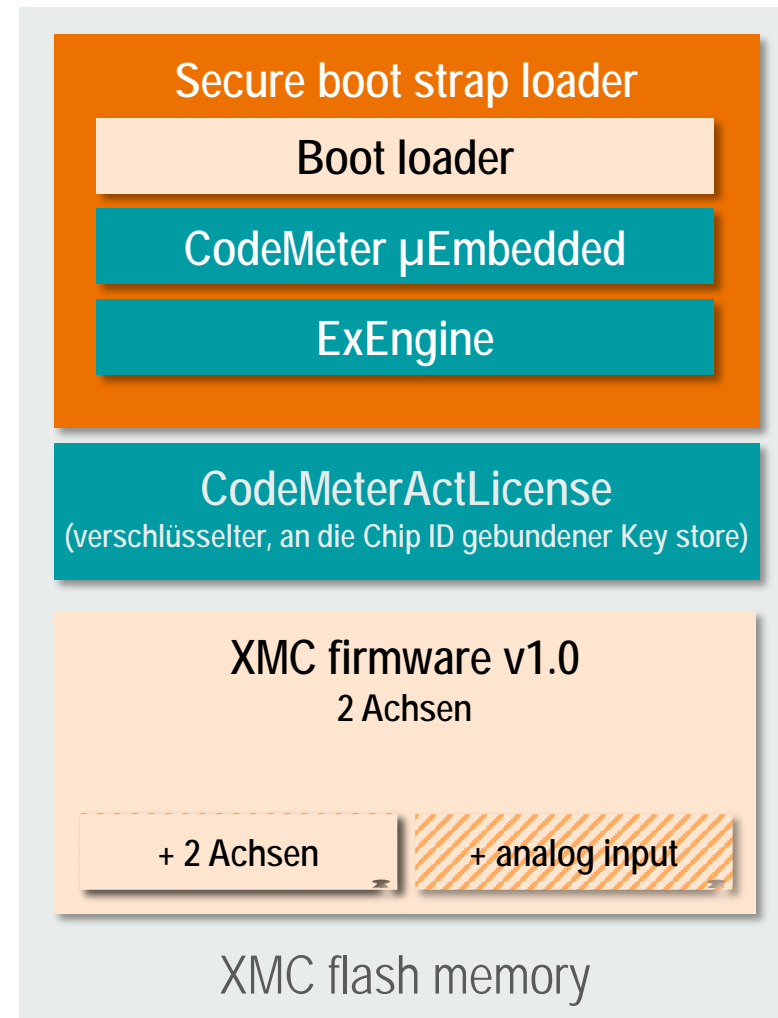
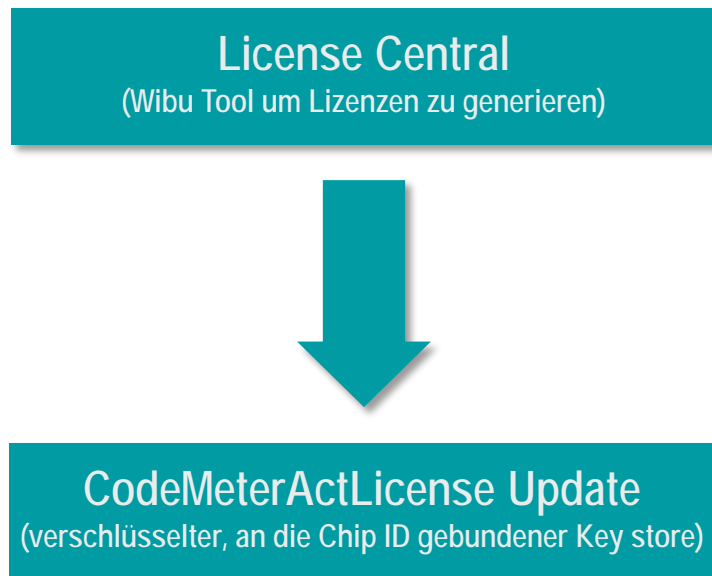


Credentials  
(signature, certificates, ...)

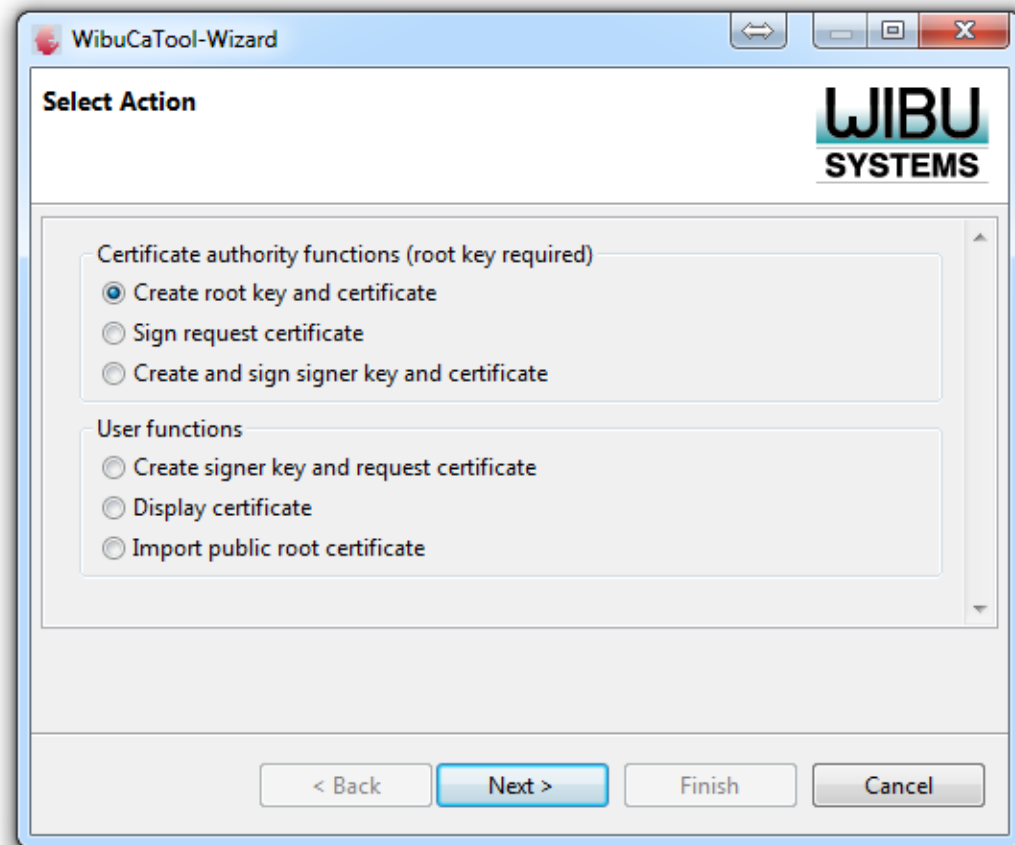
Firmware v2.0-protected.elf



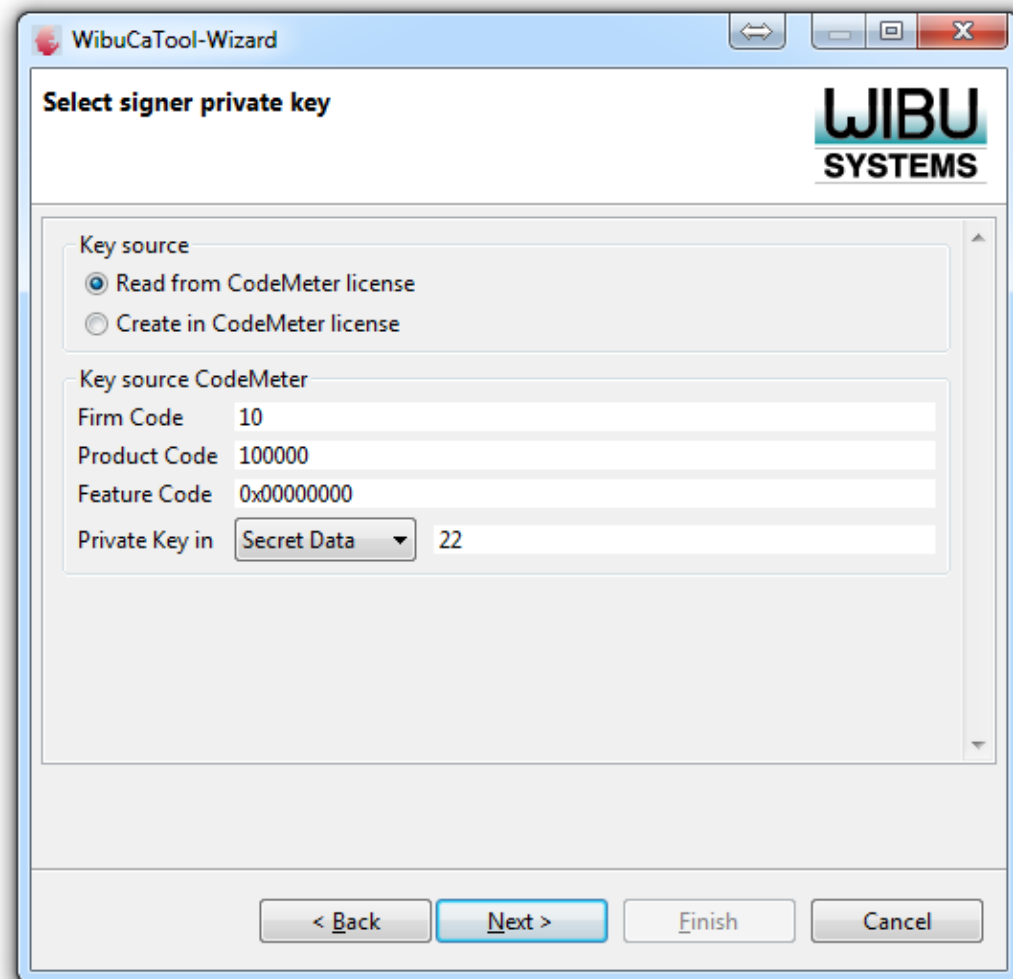
- Use Case:
  - Funktionsupgrade im Feld (z.B. Freischalten weiterer Achsen in einem Motioncontroller)
  - Keine Rezertifizierung der Firmware oder Komponente
  - Funktionsfreischaltung bezogen auf ein individuelles Gerät



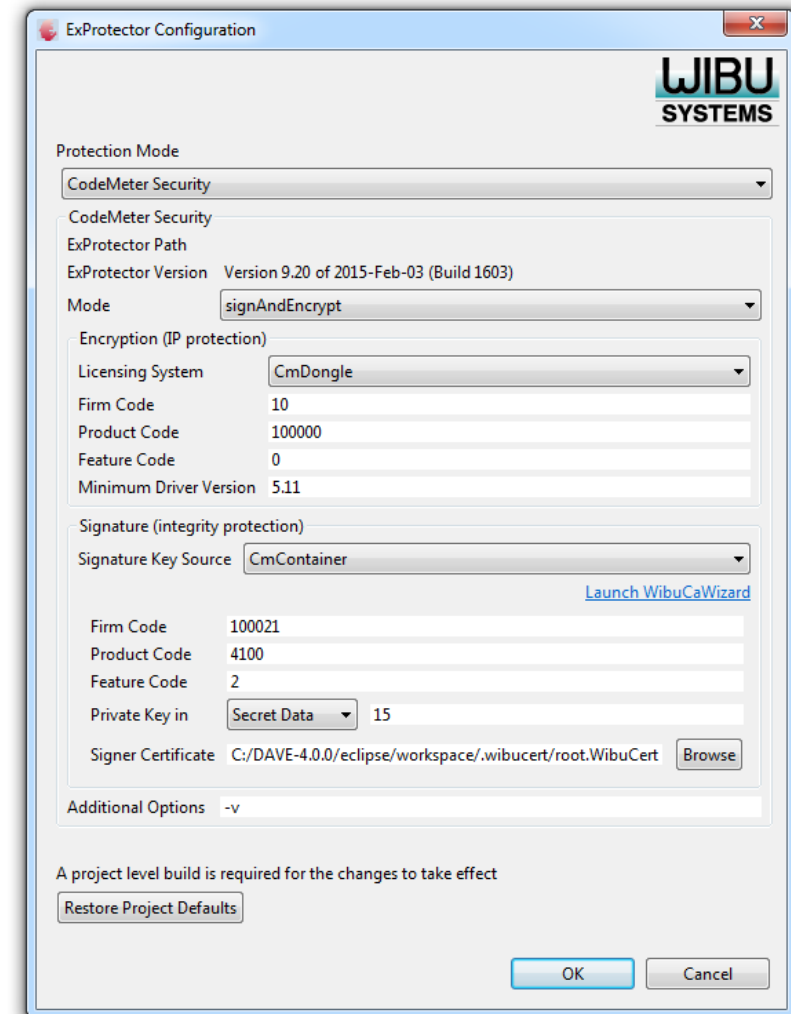
- Tools integriert in DAVE 4
- CA Tool für das Zertifikatsmanagement



- Kryptographie Funktionen im CodeMeter Dongle ausführen.
- Masterkey wird sicher im Dongle des Geräteherstellers gespeichert.



- Konfiguration des ExProtectors
- Verschlüsselung wird direkt aus DAVE 4.0 gestartet





## ■ Symmetrische Verschlüsselung

- 128-bit AES (Advanced Encryption Standard)
- Nutzung für den Softwareschutz
- Individuelle Verschlüsselung über das API

## ■ Asymmetrische Verschlüsselung

- 224-bit ECC (Elliptic Curve Cryptography)
- 2048-bit RSA (Rivest Shamir Adleman)
- Nutzung für Signaturen

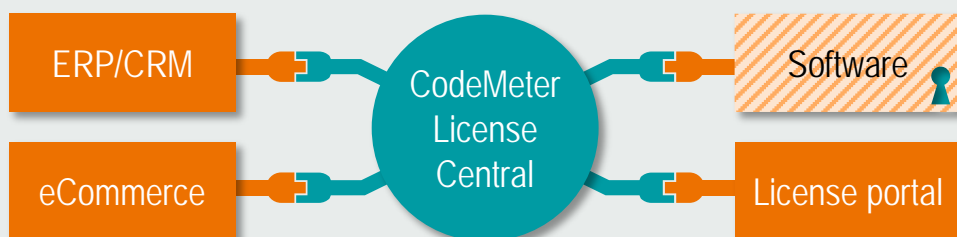
# Summary

## Einmal integrieren

### Integration in DAVE

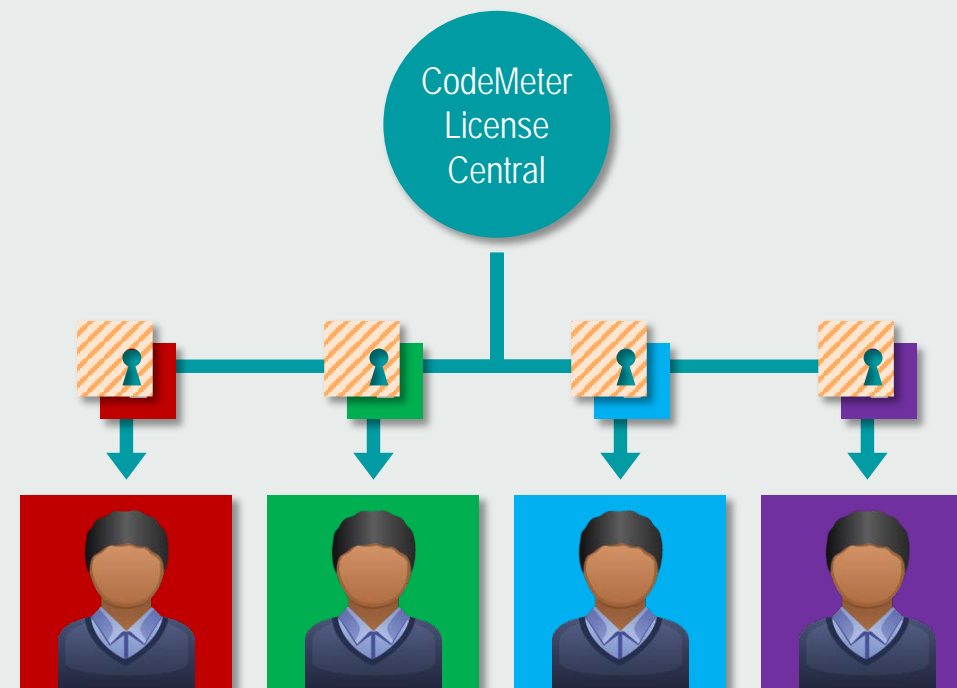


### Integration in die Prozesse



## Vielmals liefern

### Auslieferung an die Nutzer



## Was gibt es sonst noch zu sagen?

- API für die individuelle Nutzung der kryptographischen Funktionen
- Geplanter Use Case für die Integration eines Produktionszählers
- Verfügbar ab IV/2015