WIBU SYSTEMS

SECURITY
LICENSING
PERFECTION IN PROTECTION

Authenticate and authorize your IIoT devices

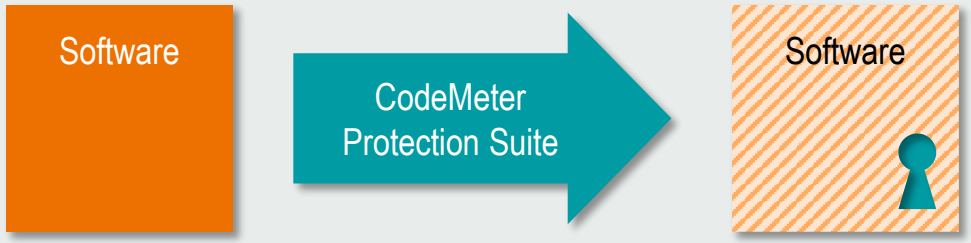
Günther Fischer
WIBU-SYSTEMS AG
guenther.fischer@wibu.com

The CodeMeter® Technology

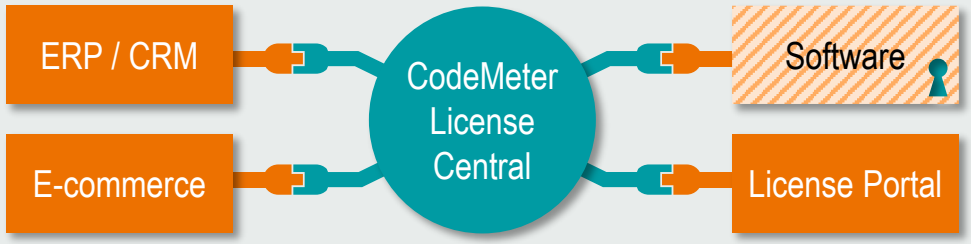
CodeMeter Technology

Integrate Once

Integration into software



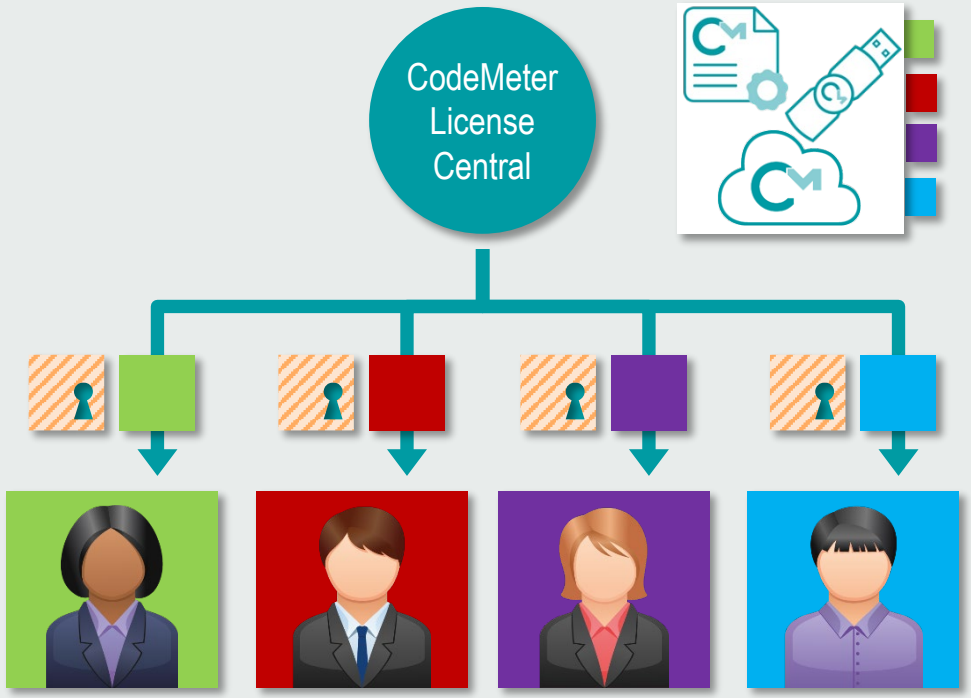
Integration into processes



®

Deliver Many

Delivery to the user

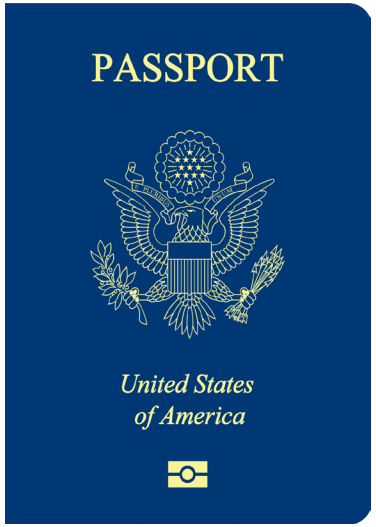


Secure Key Store – Highest Security archived with Secure Module

Infineon SLE/SLM 97

X.509v3 Certificate Added – CodeMeter Certificate Vault

=



Content of an X.509v3 certificate

A X.509v3 certificate includes:

- Version and serial number
- Name of the issuer
- Name of the subject
- Period of validity
- Information on the holder's public key
- Information on the intended use of the certificate ("extensions")
- Digital signature
- Encryption algorithms used

What does a digital Certificate contain?

- Confirms the owner of a public key
- Identity:
  - Person/Device
  - Organisation
- Signed by an authority
- Can contain additional attributes

Certificate

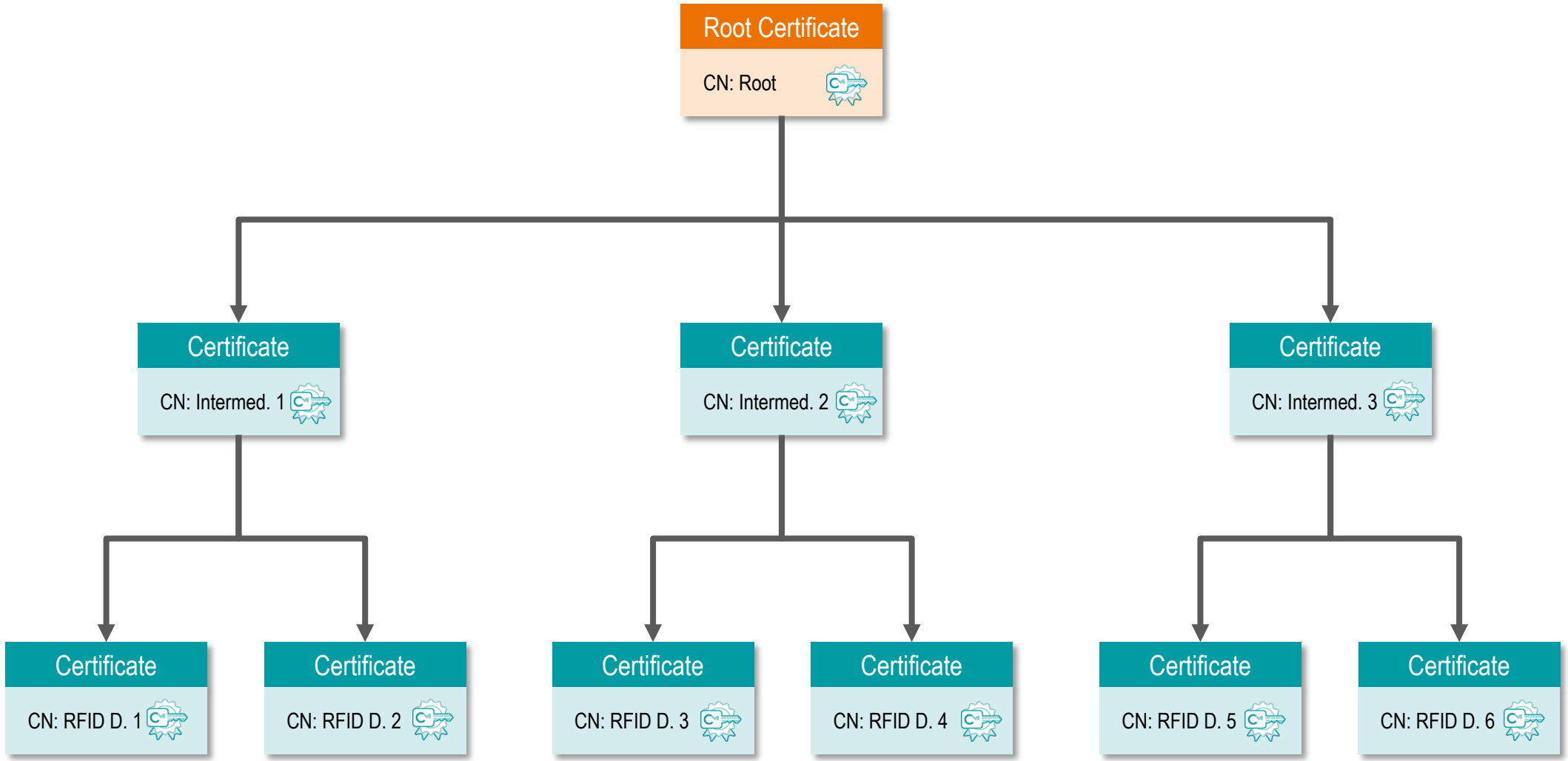
Issued for:

Common name (CN):	Günther Fischer/RFID Reader
Company (O):	WIBU-SYSTEMS AG
Business unit (OU):	PS
Serial number:	1be10001000220613…
Public key:	0x15, 0x3c, 0xd0, 0x26, 0xd6, 0x71, 0xfa, 0xae, 0x20, 0xa6, 0x15, 0x58, 0xea, 0x3d, 0xdd, 0x36, 0x89, …

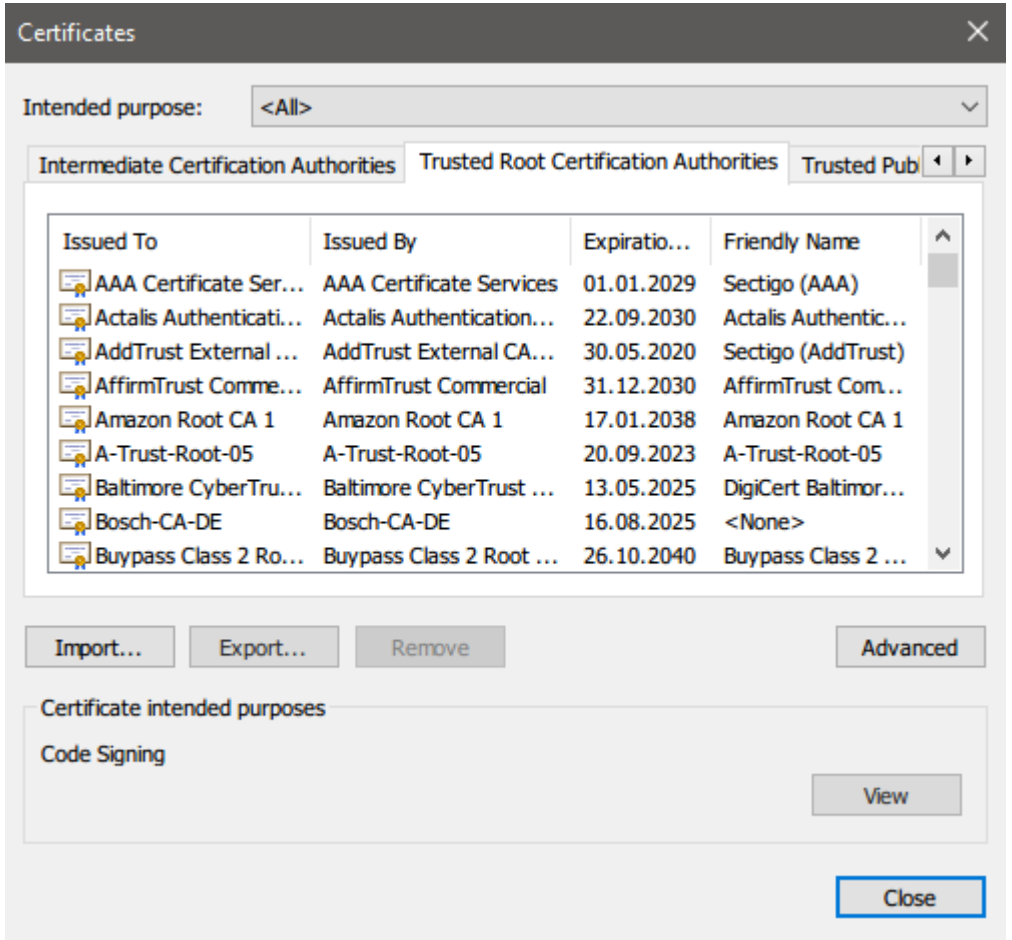
Issued by:

Common name (CN):	WIBU Root
Company (O):	WIBU-SYSTEMS AG
..	
Valid until:	31.12.2022

Certificate Hierarchy / Certificate Chain (Trusted Root Chain)



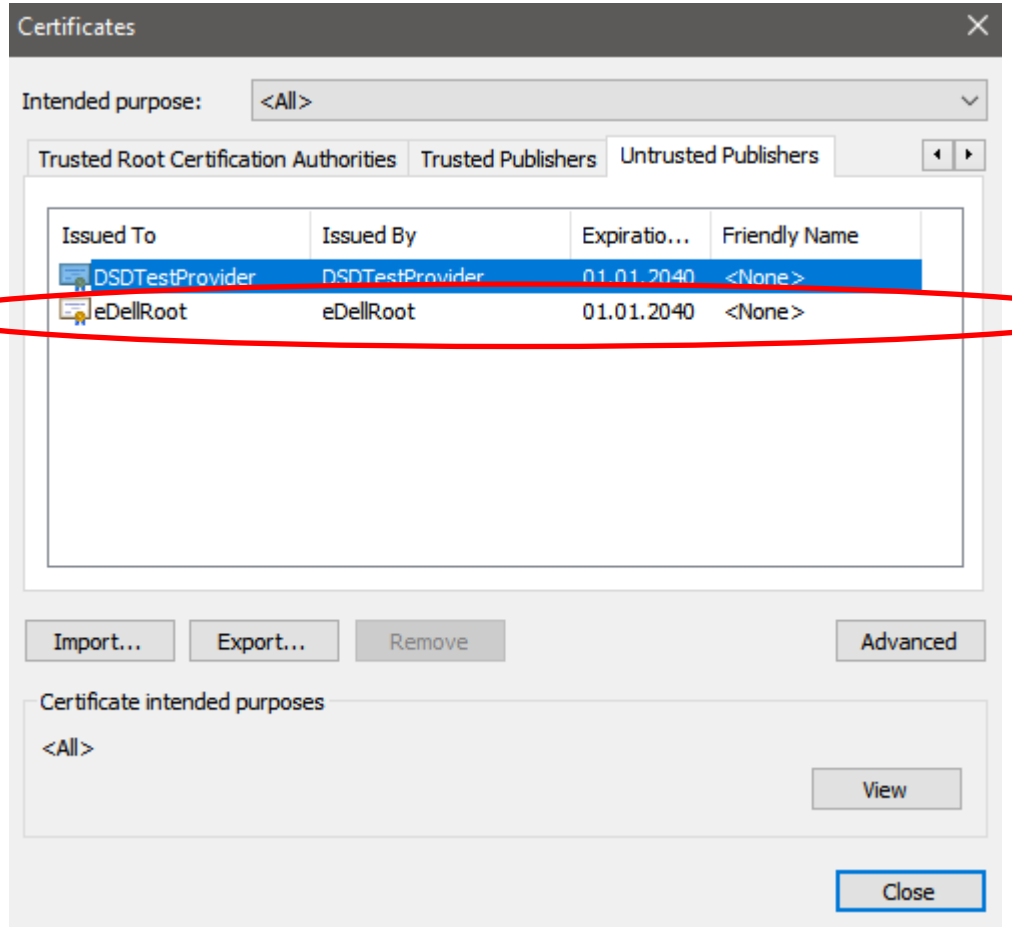
Special Role of Trusted Root Certificates



What are Certificates?

- Digital certificates are used to **uniquely identify** individuals or **devices**.
- The person or **device** has a **key pair** consisting of a **public** and a **secret private** key.
- An Authority (Certificate Authority or CA) confirms that the corresponding **public key** is assigned to this person or device.
- This **confirmation** is available in the form of a certificate signed with a CA **private key**.
- The high security of certificates is particularly evident in comparison to passwords.
- Passwords can be given away or shared intentionally or accidentally.
- Hackers can spy on passwords through phishing attacks.

Major Disaster – Private Key Compromised



Revocation Lists

- CRL (Certificate Revocation List)
- Includes invalid (withdrawn) certificates
- Online query possible, Online Certificate Status Protocol (OCSP)

Usage Scenarios

Usage Scenarios

- Server Certificates
- Client Certificates
- E-Mail Certificates / VPN Certificates
- OPC UA Device Certificates
- Code and Data Integrity of Software
- …

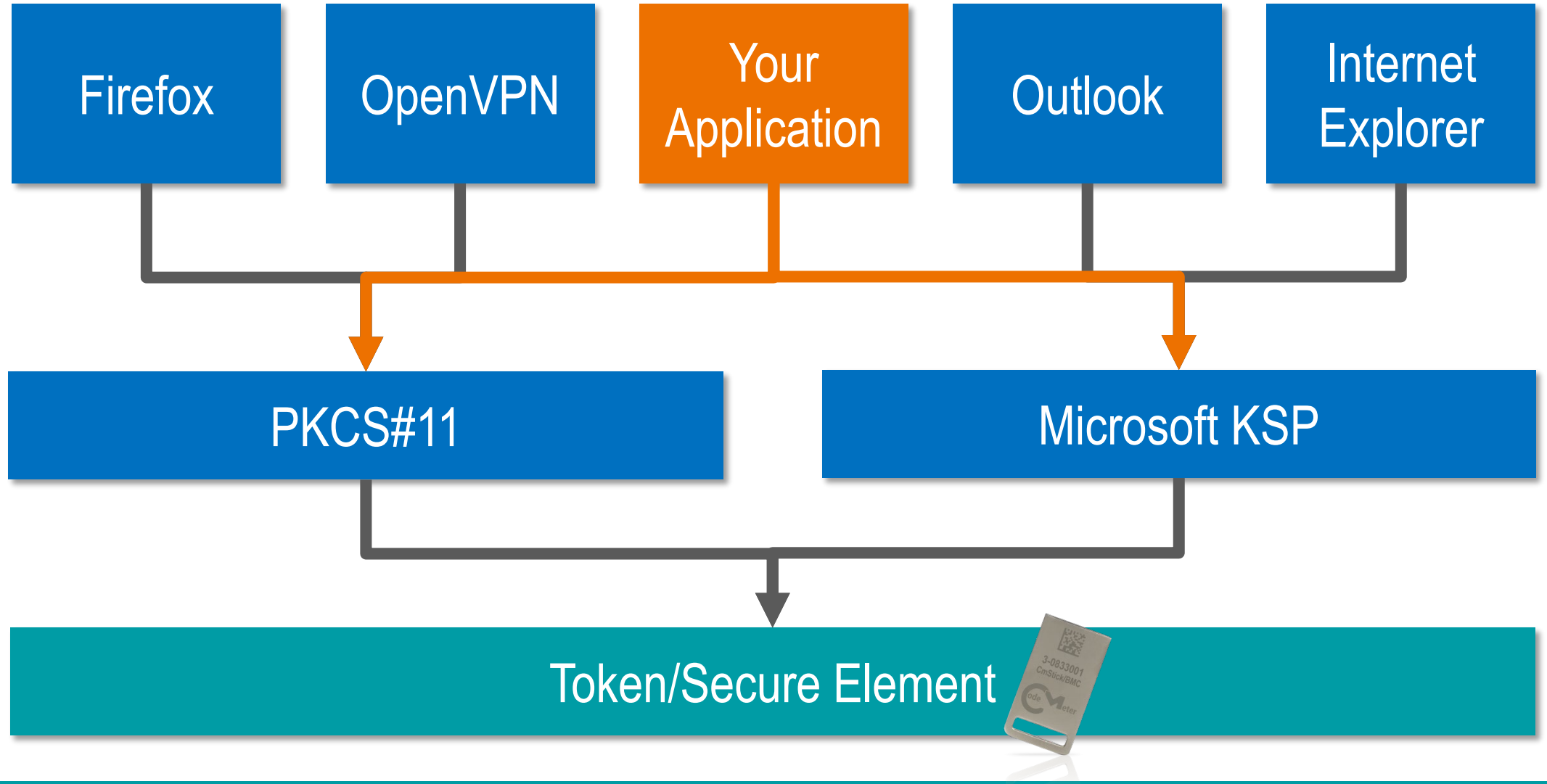
Storing Certificates and Private Keys

Storing Certificates and private keys

- As file in the file system (PEM-File)
- In a Token/Secure Element

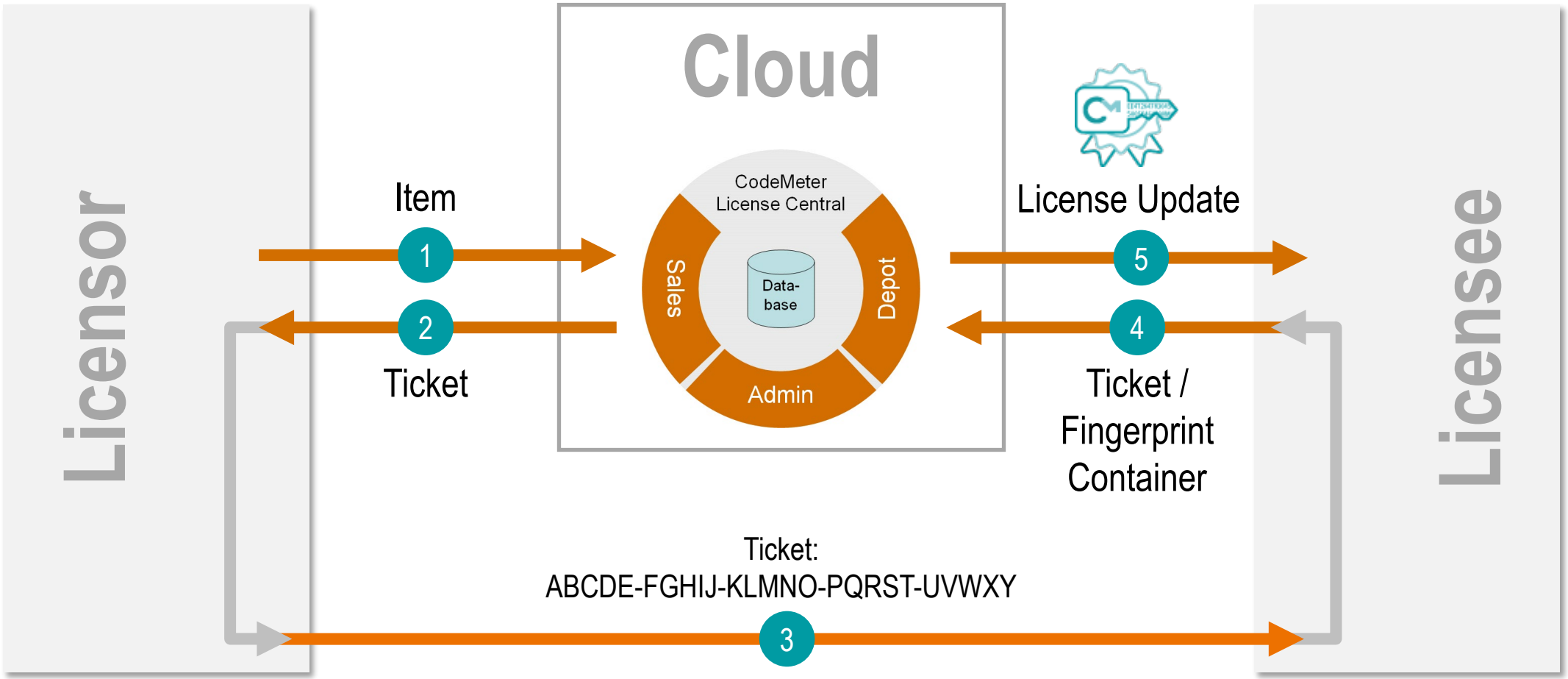
- Certificate Store accessible via
  - OpenSSL
  - PKCS#11
  - Microsoft KSP API (Key Storage Provider)

PKCS#11 / Microsoft KSP

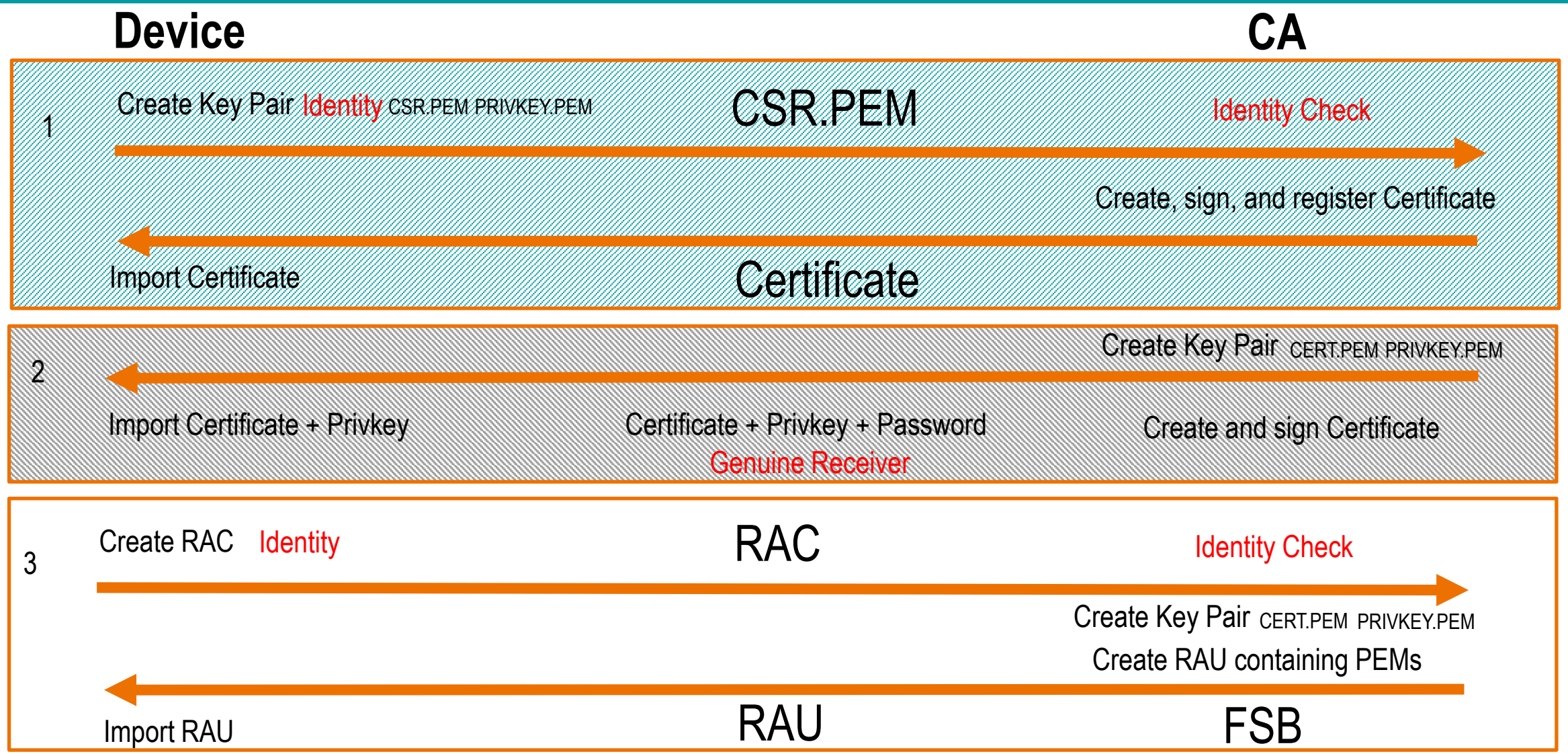


Deployment of Certificates

Secure key management and certificate distribution



Scenarios



Diebold Nixdorf CrypTA (Cryptographic Technician Authentification)

Authorized Service Technician

- Securing the diagnostic software against unauthorized use
- Authorizing advanced service functions
- Encrypting documents for manuals and service information
- Meeting PCI DSS requirements for unique identification
- Support in collecting service-relevant system data (hardware inventory + flight records)
- Interface to the training system and automatic assignment of access rights depending on the achieved learning success
- Securing the component test systems in production

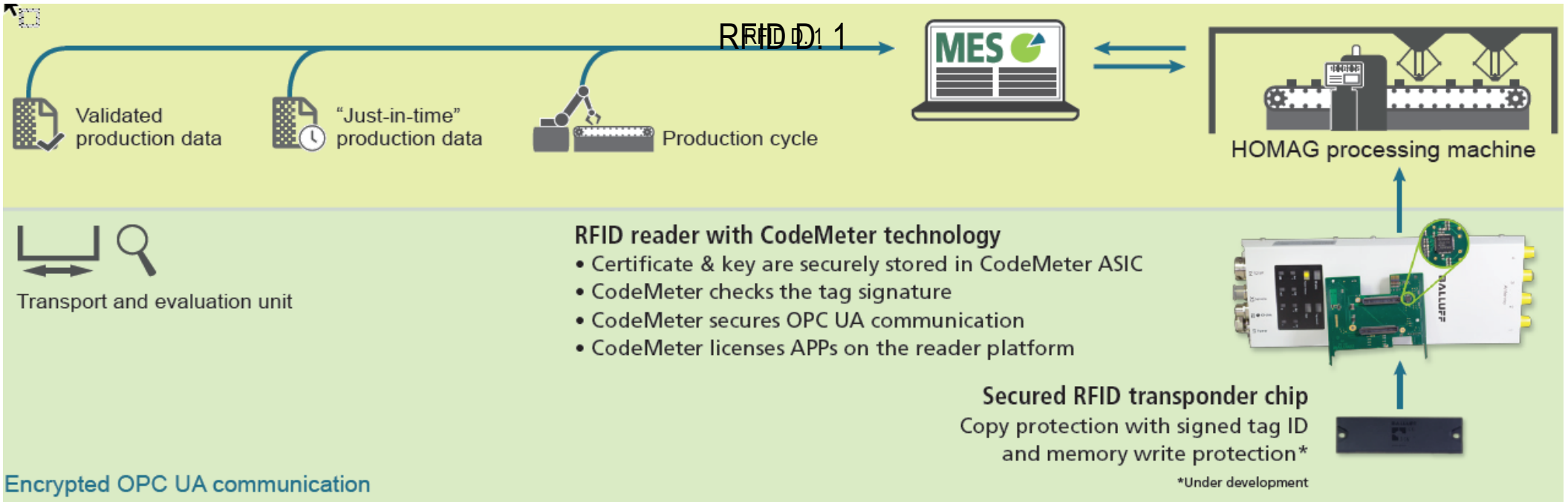
Diebold Nixdorf

Balluff IUNO

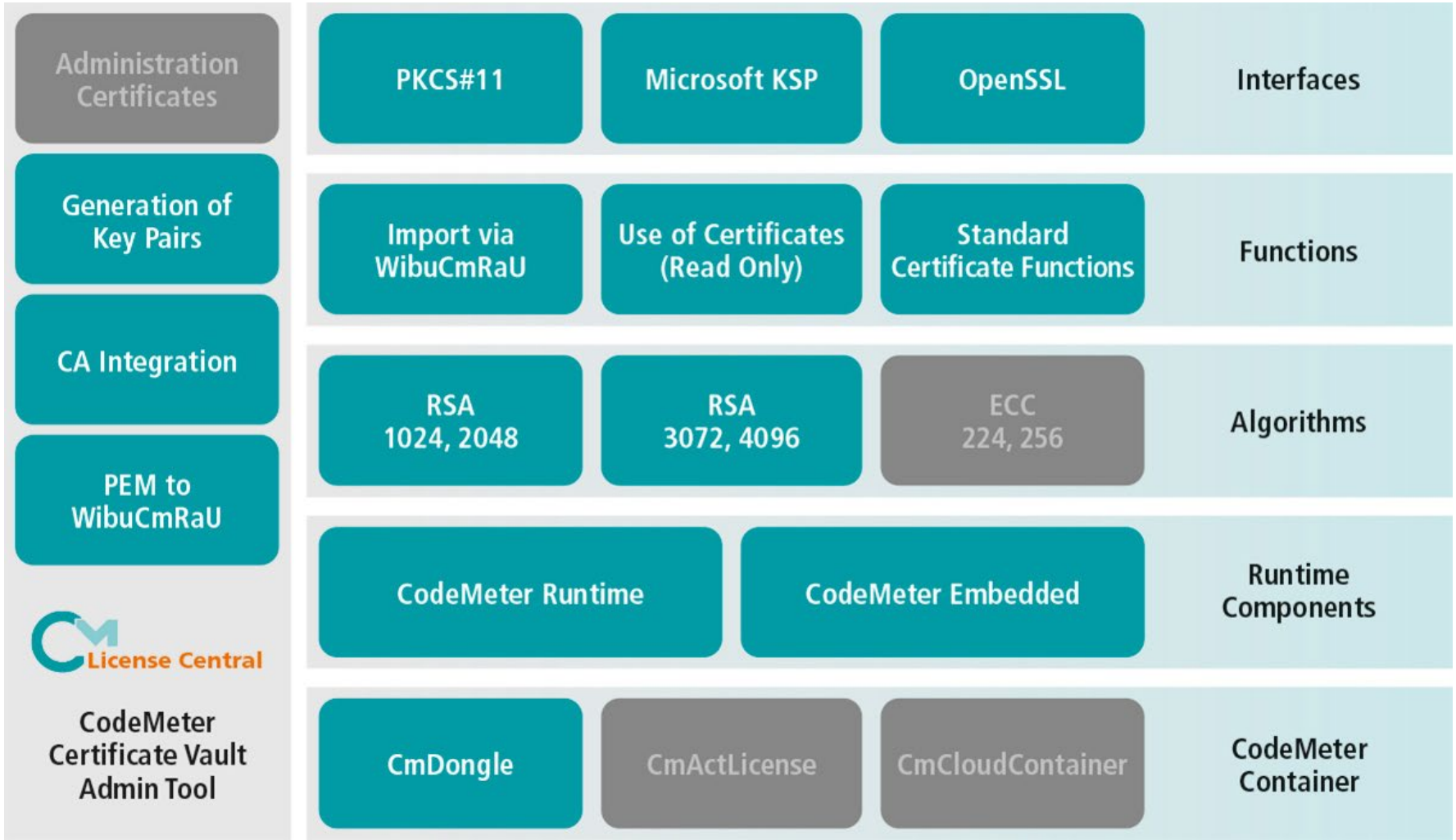
- OPC UA Ascolab/Unified Communication
- RFID Tags

IUNO

Nationales Referenzprojekt
IT-Sicherheit in Industrie 4.0



Token/Secure Element Sample: CodeMeter Cerificate Vault



Thank You very much!

Europe: +49-721-931720

USA: +1-425-7756900

China: +86-21-55661790

Japan: +81-3-43608205

https://www.wibu.com

info@wibu.com