WIBU SYSTEMS

SECURITY
LICENSING
PERFECTION IN PROTECTION

Who are you?
Authentication by Certificates

- Introduction to certificates
- Application Scenarios
- CodeMeter Certificate Vault

Stefan Bamberg | Senior Key Account Manager
stefan.bamberg@wibu.com

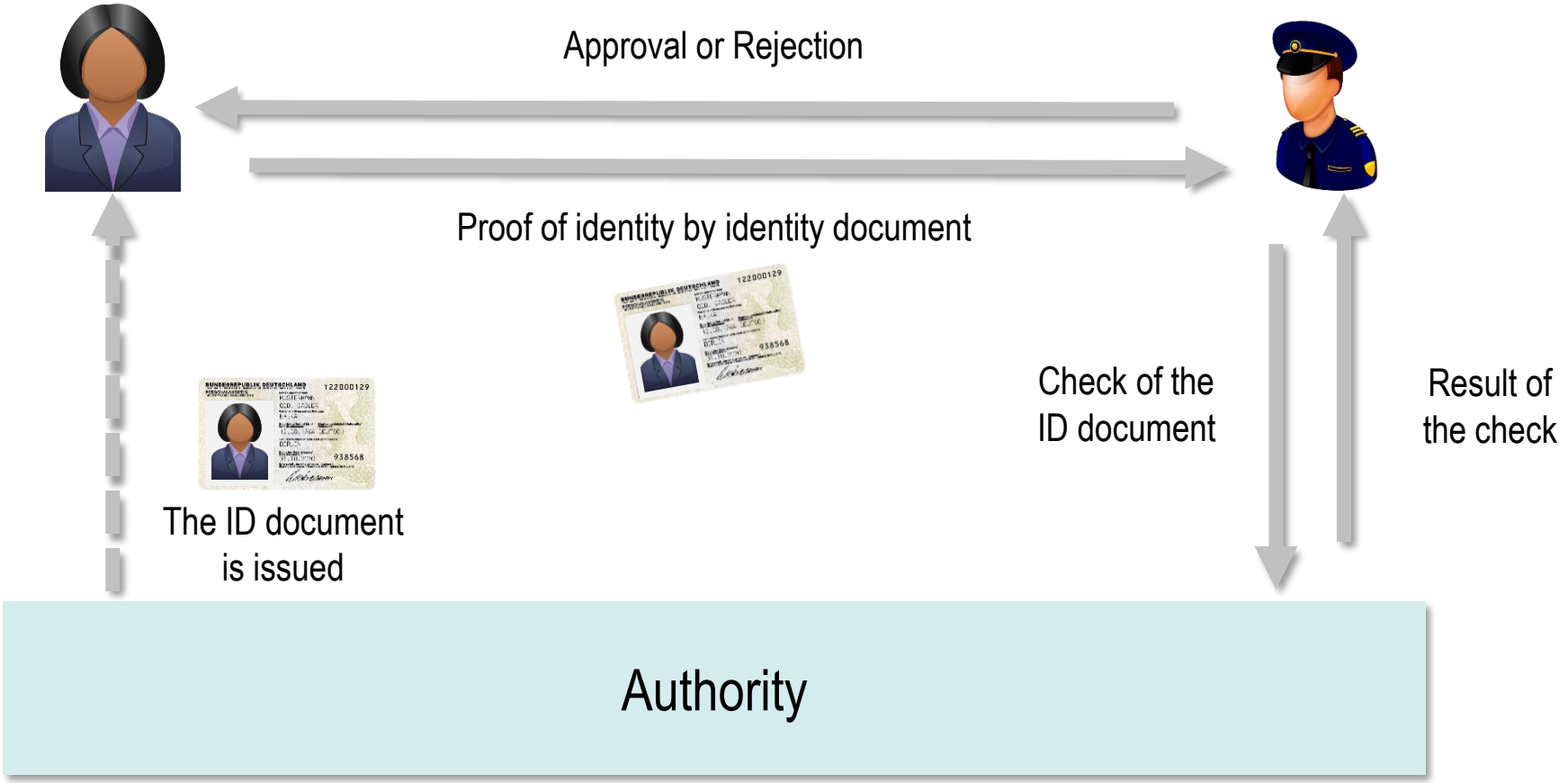
Philipp Luedtke| R&D Software
philipp.luedtke@wibu.com

Who are you?

Proof of identity – Examples

- In certain situations, persons must identify themselves, i.e. you must prove your identity with legal certainty, e.g.:
  - Police checks
  - Opening a bank account
  - Registration of a new vehicle
  - Purchase of alcohol (proof of age)
  - Check-in at airports
  - And many more

Proof of identity – Process



Proof of identity – Digital and automated?

- Authentication is essential for secure digital communication and secure networks
  - Persons must authenticate themselves to machines and applications
  - Machines must authenticate to other machines

How do we make this work ?

(X.509v3) Certificates

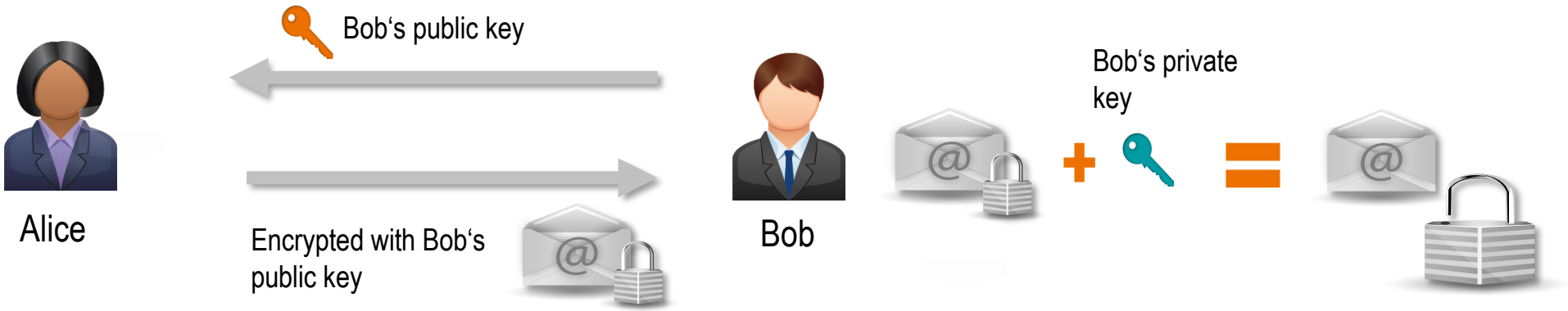
- Asymmetric Encryption
- Digital Certificates
- PKI

Excursus: Asymmetric cryptography

- **Symmetric Cryptography**
  - **One** key to encrypt and decrypt
  - AES (Advanced Encryption Standard) is a symmetrical procedure
  - Is used for large amounts of data thanks to its fast speed
- **Asymmetric Cryptography** = Public Key Cryptography
  - **Key pair**: private and public keys
  - It's **impossible** to derive the private key from the public key
  - RSA (named after Rivest, Shamir, and Adleman) is an asymmetrical procedure

Example: E-Mail encryption

- Use of asymmetric encryption
  - Alice wants to send Bob an encrypted email



- **Challenge**: Key distribution
- **Solution**: Digital certificate

What is a digital certificate?

- A digital certificate
  - **links identities with cryptographic keys**
  - contains information about an entity (process participant)
  - contains the public key of the entity
  - has a standardized structure (RFC 5280)
  - comes with a signature calculated from the information the certificate holds
  - can be checked for authenticity using cryptographic methods
  - can be checked for integrity using cryptographic methods

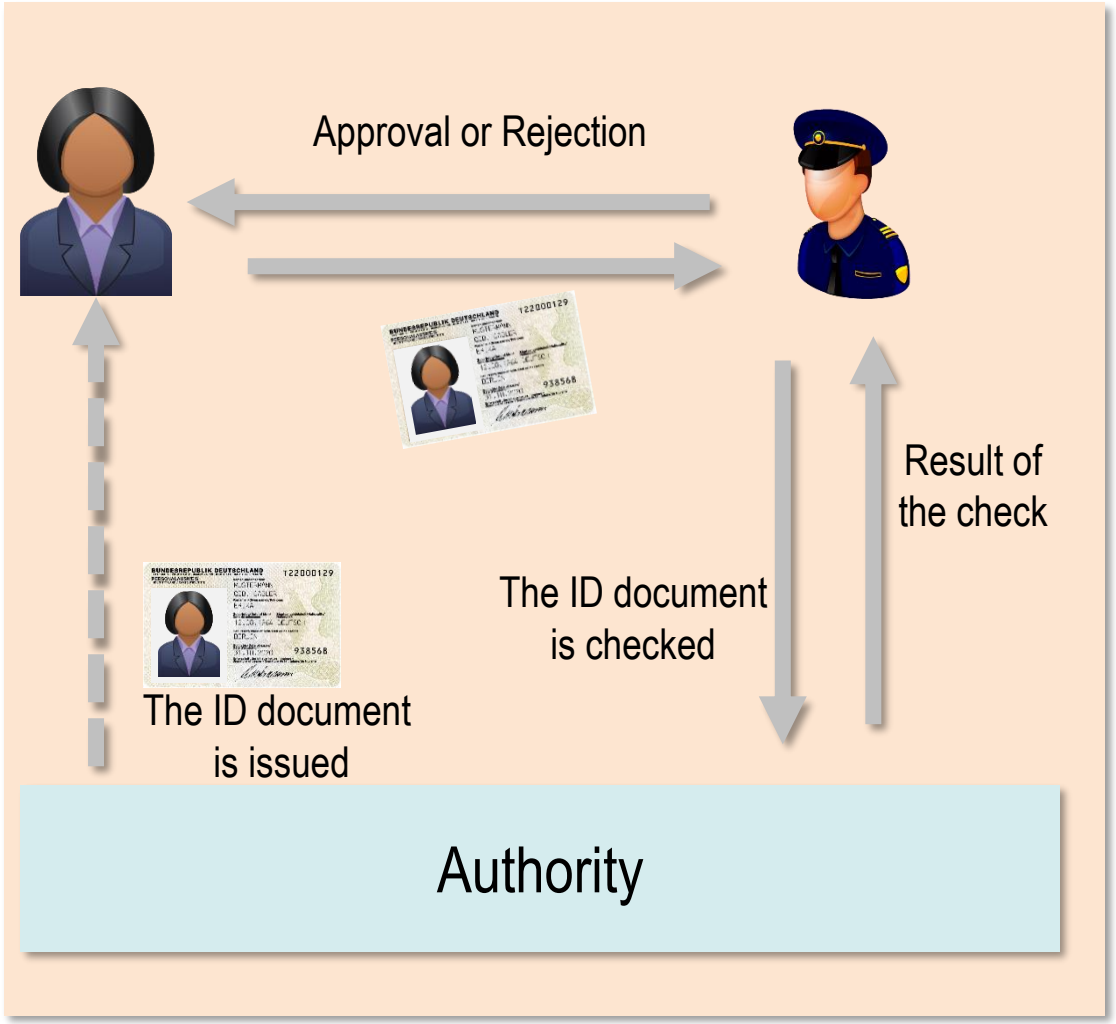
Structure of an X.509v3 certificate

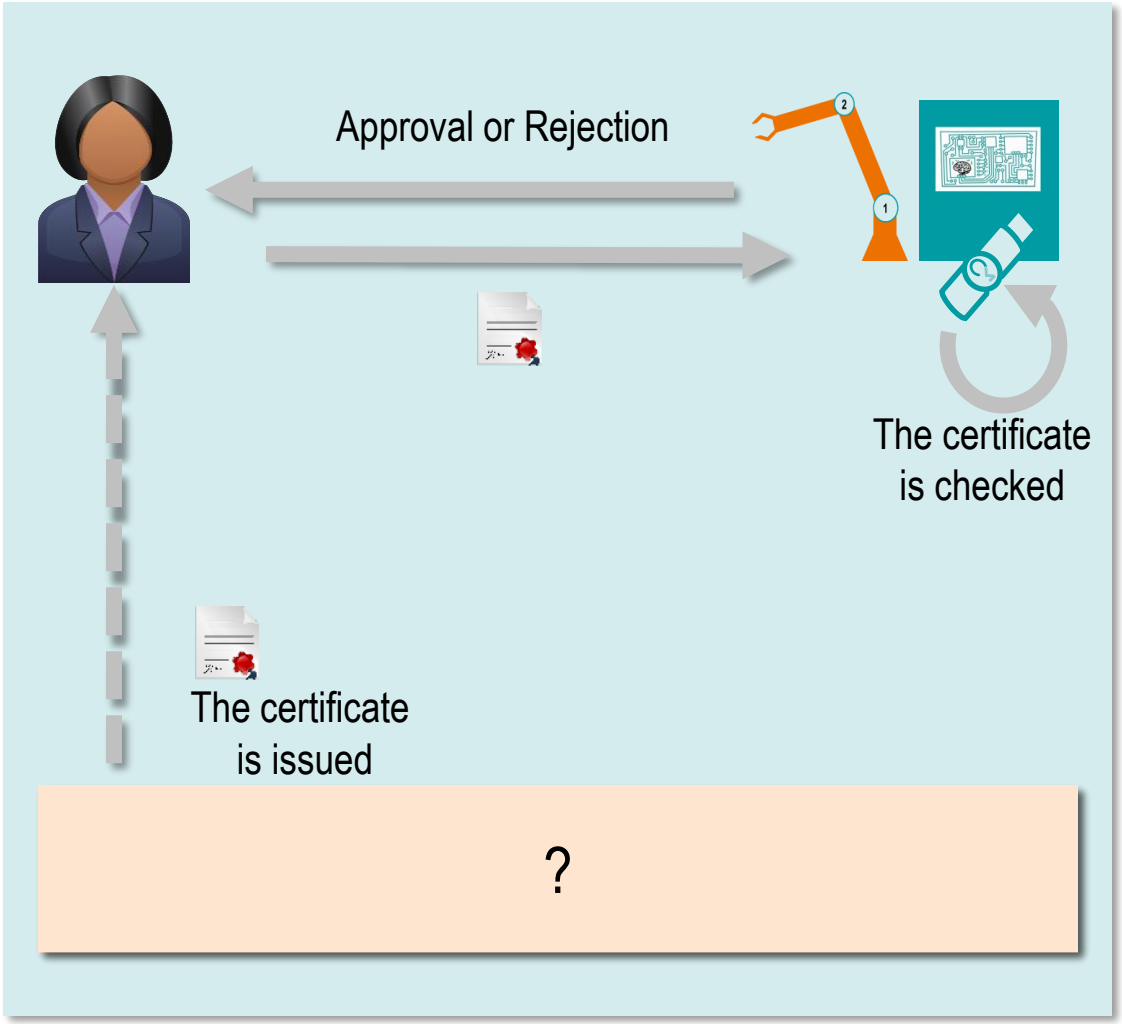
- A X.509v3 certificate includes among others the following elements:
  - Version number and serial number
  - Name of the issuer
  - Name of the subject
  - Period of validity
  - Information on the holder's public key
  - Information on the intended use of the certificate ("extensions")
  - Digital signature
  - Encryption algorithms used

Example: Certificate content (Demo)

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 11259375 (0xabcdef)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = DE, ST = BW, L = KA, O = WIBU, OU = EWS, CN = webinar-demo, emailAddress = webinar@demo.de
        Validity
            Not Before: Jun 16 10:52:00 2020 GMT
            Not After : Aug 21 08:53:00 2020 GMT
        Subject: C = DE, ST = BW, L = KA, O = WIBU, OU = EWS, CN = webinar-demo, emailAddress = webinar@demo.de
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ba:44:5d:93:57:d0:a0:a2:f0:37:74:b0:78:37...
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature, Data Encipherment, Key Agreement
            X509v3 Subject Alternative Name:
                email:webinar@demo.de
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://demo.crl.de
    Signature Algorithm: sha256WithRSAEncryption
         6c:55:db:ff:65:79:2a:c3:2e:b5:5c:94:4b:c2:7d:a9:e0:6b...
```

Proof of identity – Analogue vs. digital

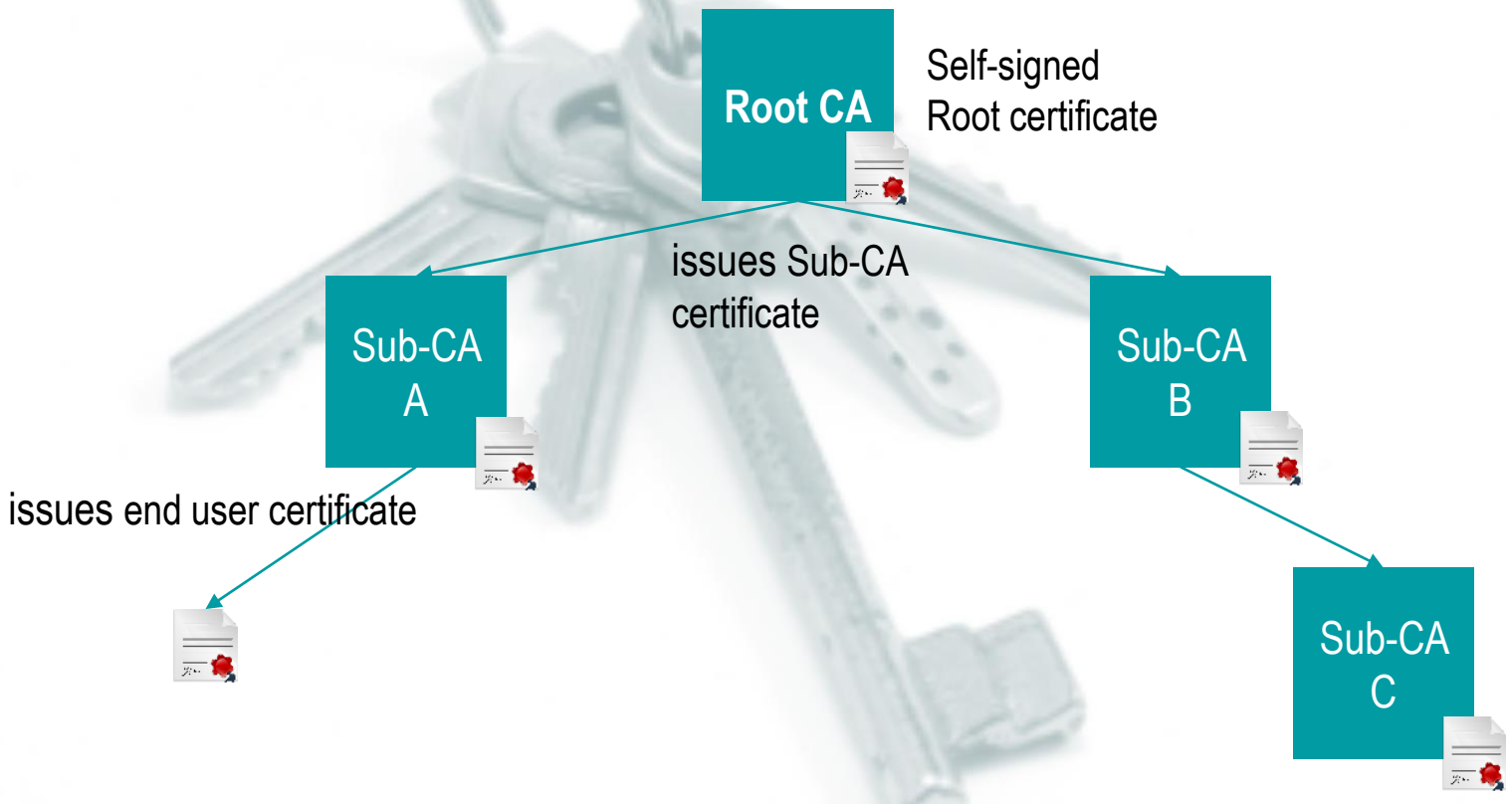




Public Key Infrastructure (PKI)

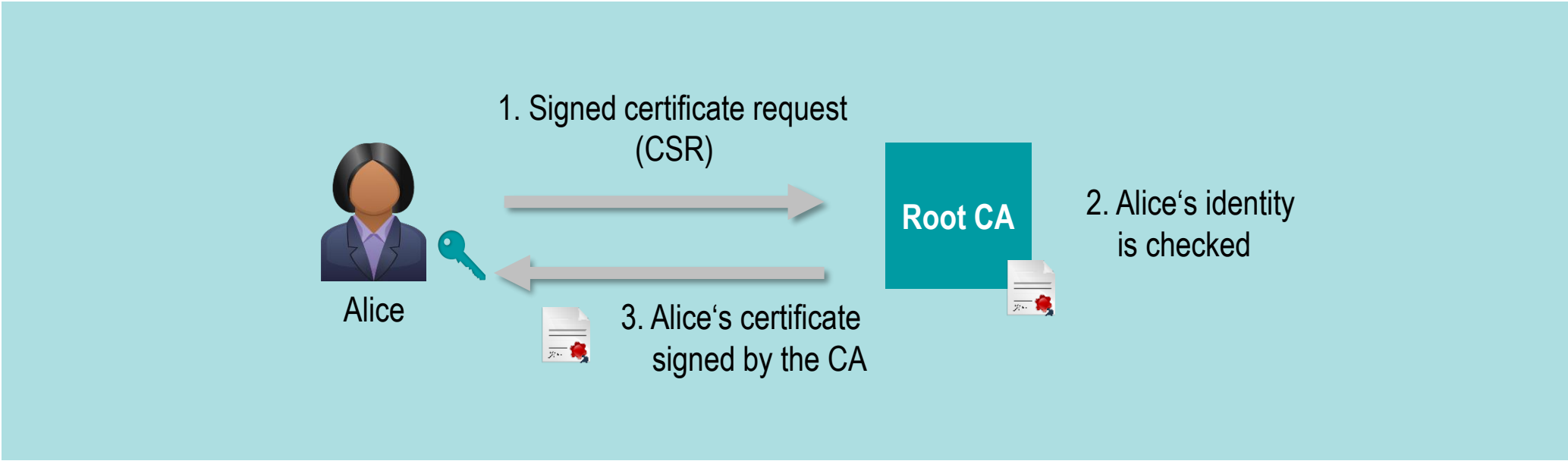
- A PKI
  - **is actually an infrastructure – not just a software program**
  - consists of Certificate Authorities (CAs) (+ processes)
  - is hierarchically structured as follows
    - Root CA
    - Derived subordinate CAs
    - Every Certification Authority holds a key pair and a certificate
  - issues and manages certificates

PKI Structure – Example



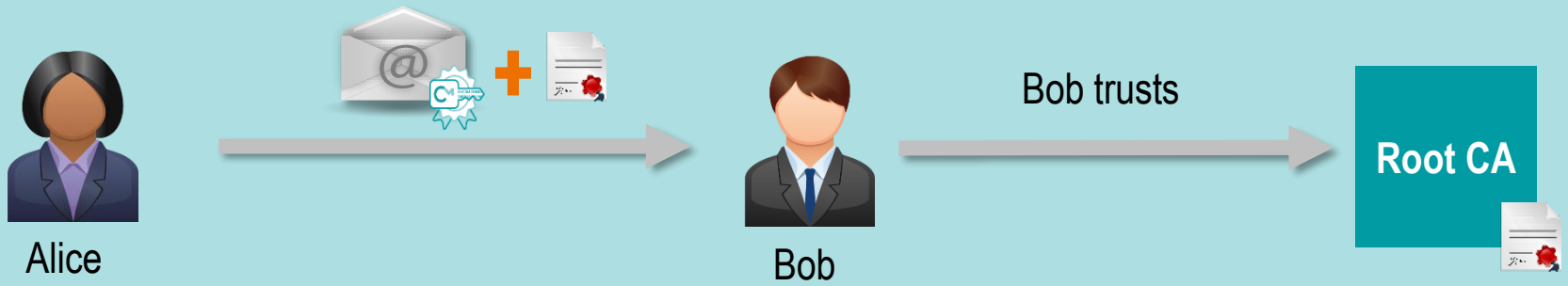
Example: Certificate Enrollment

- Certificate Enrollment



Example: Certificate examination

- Certificate verification



Bob checks:

1. Do I trust the root CA of Alice?
2. Is the Root CA certificate valid?
3. Is Alice's certificate valid?

Application Scenarios

Application scenarios

- E-mail encryption / signature, document signature
  - e.g. Microsoft Outlook, Mozilla Thunderbird, Adobe Acrobat, OpenOffice, …
- Securing communication on the web
  - e.g., HTTPS or TLS, VPN, …
- Authentication on machines and applications
  - e.g. Windows smart card logon, SSH, …
- Secure communication and authentication in industrial environments
  - e.g. OPC UA, …

Challenges

- Rollout of certificates
  - How is the authorization check performed?
  - How is the technical rollout of certificates carried out?
  - Where do I keep the keys safely?
- Withdrawal of certificates
  - How is the authorization check performed?
  - How is the certificate revocation made public?
  - When to check the certificate revocation (Time of Revocation vs. Time of Check)?

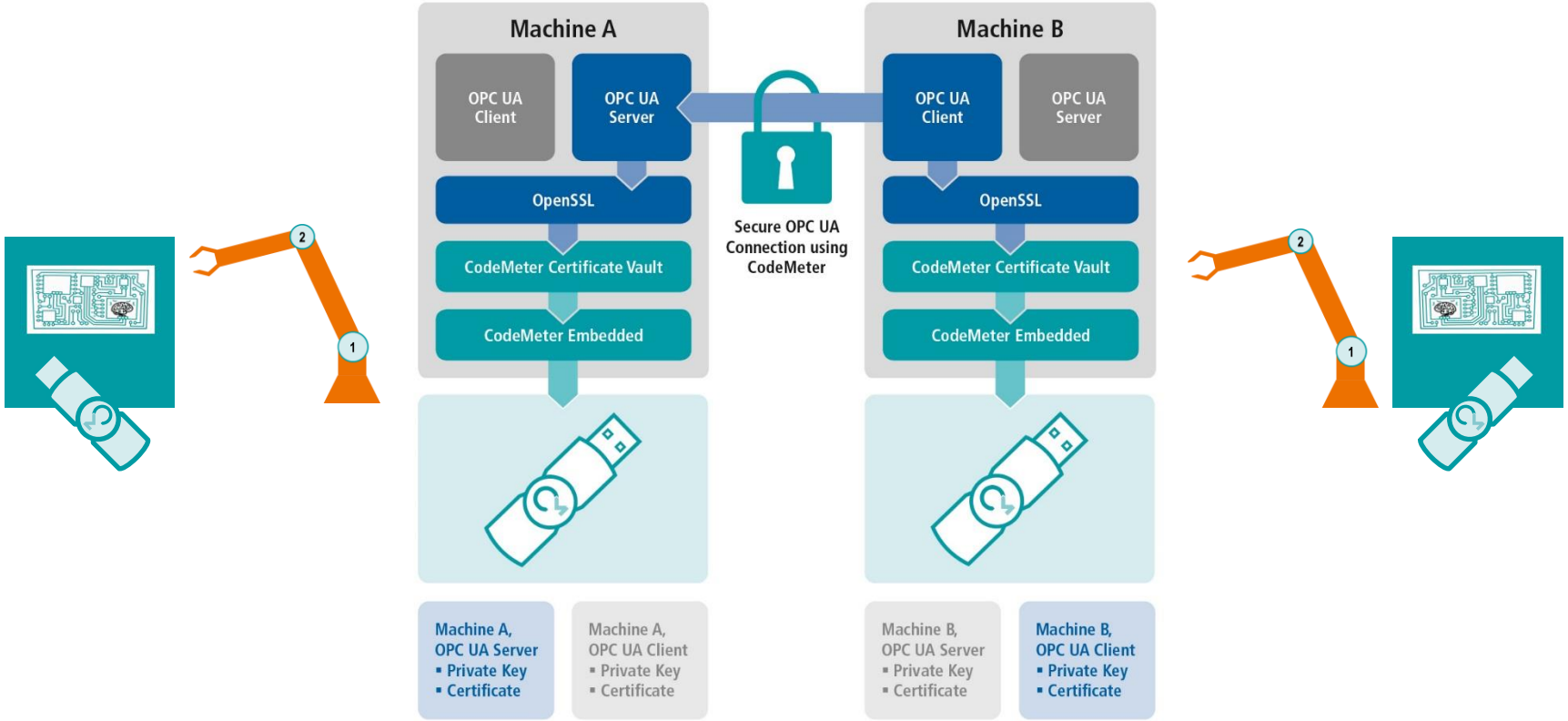
CodeMeter Certificate Vault

Why CodeMeter Certificate Vault

- Simplification of the overall process of certificate usage
  - Support of the standard interfaces PKCS#11, KSP, and OpenSSL
  - Enrollment and update of keys/certificates via CodeMeter License Central online and offline
  - Integration of CodeMeter License Central into existing certificate management systems via web service interfaces
- Storage of keys and certificates in a secure hardware anchor (Dongle)
  - Storage of keys and certificates in a CmDongle embedding a security smart card chip (Infineon SLE97)

Application scenario: Industry

- Additional security in industrial environments
  - OPC UA (Standard for platform-independent data exchange)



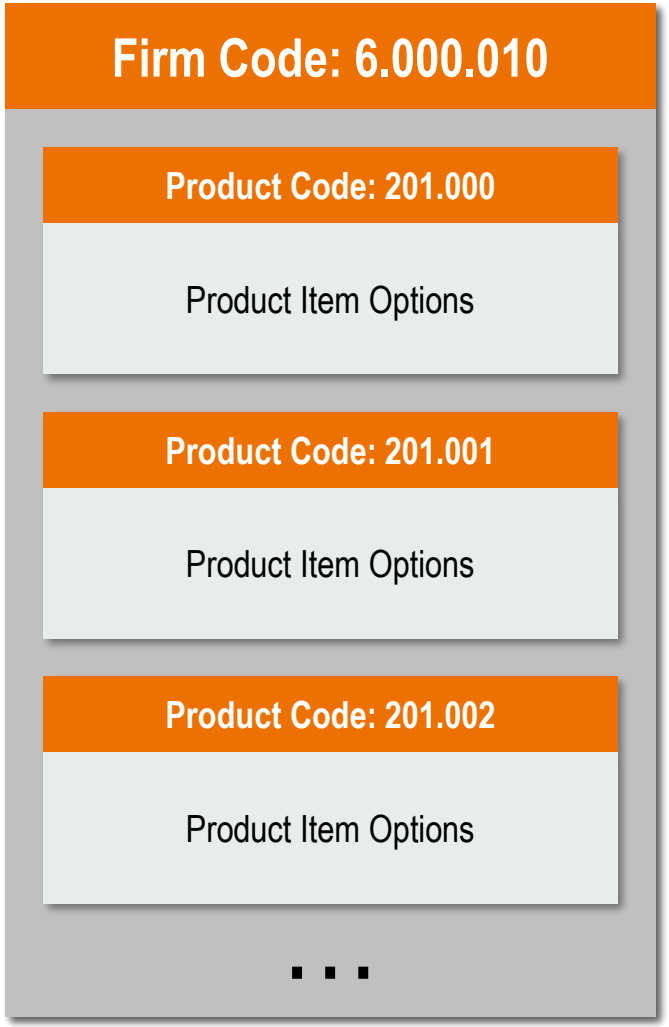
Secure anchor for keys and certificates

Several
Form factors

One
Technology

Use of proven technology

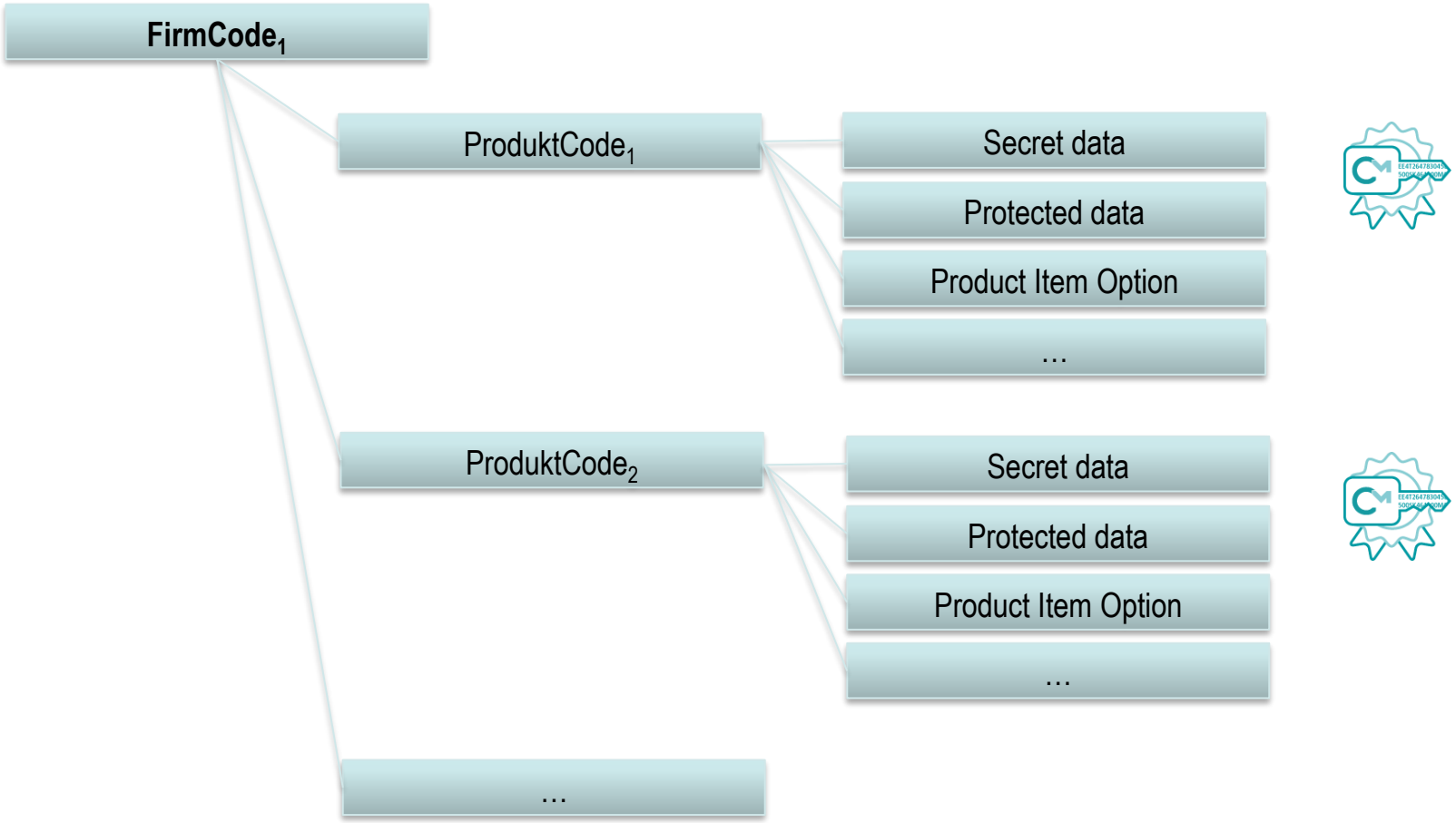
- License entry = Firm Code | Product Code
- Firm Code: assigned by Wibu-Systems
- Product Code:
  - Chosen by the ISV
  - 4 billion Product Codes (UInt32)
- Product Item Options: Each license can have combinable options
  - Among others key and certificate storage



Product Item Options

- Text
- Feature Map
- Minimum Runtime Version
- License Quantity
- Maintenance Period
- User Data
- Activation Time
- License Transfer
- Protected Data / Extended Protected Data
- Expiration Time
- Module Items
- Customer Own License Information
- Usage Period
- Named User License
- Hidden Data
- Unit Counter
- Linger Time
- Secret Data

License Structure



Storage of keys and certificates

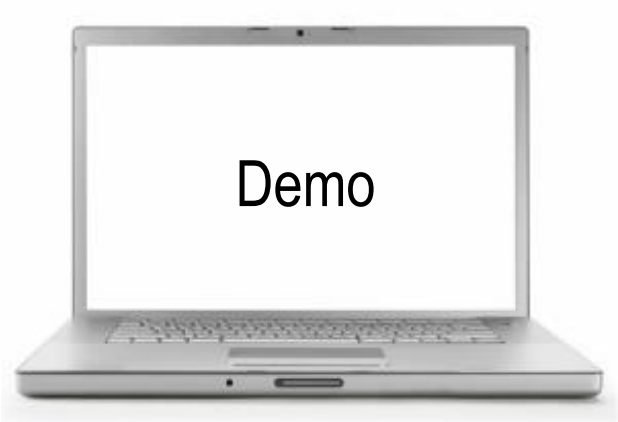
- Using Product Codes you can store many keys and certificates on a single CmDongle:
  - Copying is not possible because storage is happening in the smart card chip!
  - Protected/Extended Protected Data for storing certificates
  - Secret Data for key storage
    - Cannot be read!
    - Works only with the key
  - Each Product Code represents a key/certificate via the parent Product Item Options
  - Update of CmDongles possibile online and offline (for industrial setups)

Support of standard protocols

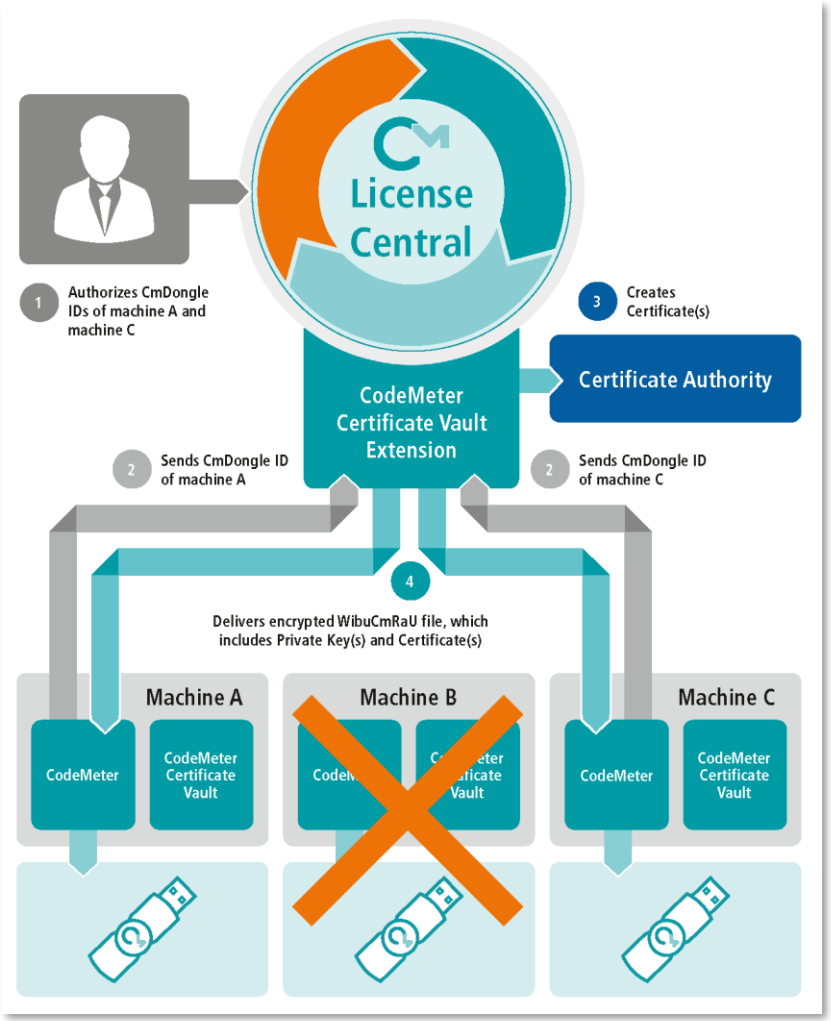
- CodeMeter Certificate Vault
  - operates as a PKCS#11 compliant token provider
  - can be integrated as Key Storage Provider (KSP) in the Microsoft Cryptographic API Next Generation (CNG)
  - can be used with the OpenSSL API to securely store and use the keys of TLS certificates
- Integration in applications such as browsers, VPNs and e-mail clients is therefore already standard

Demo

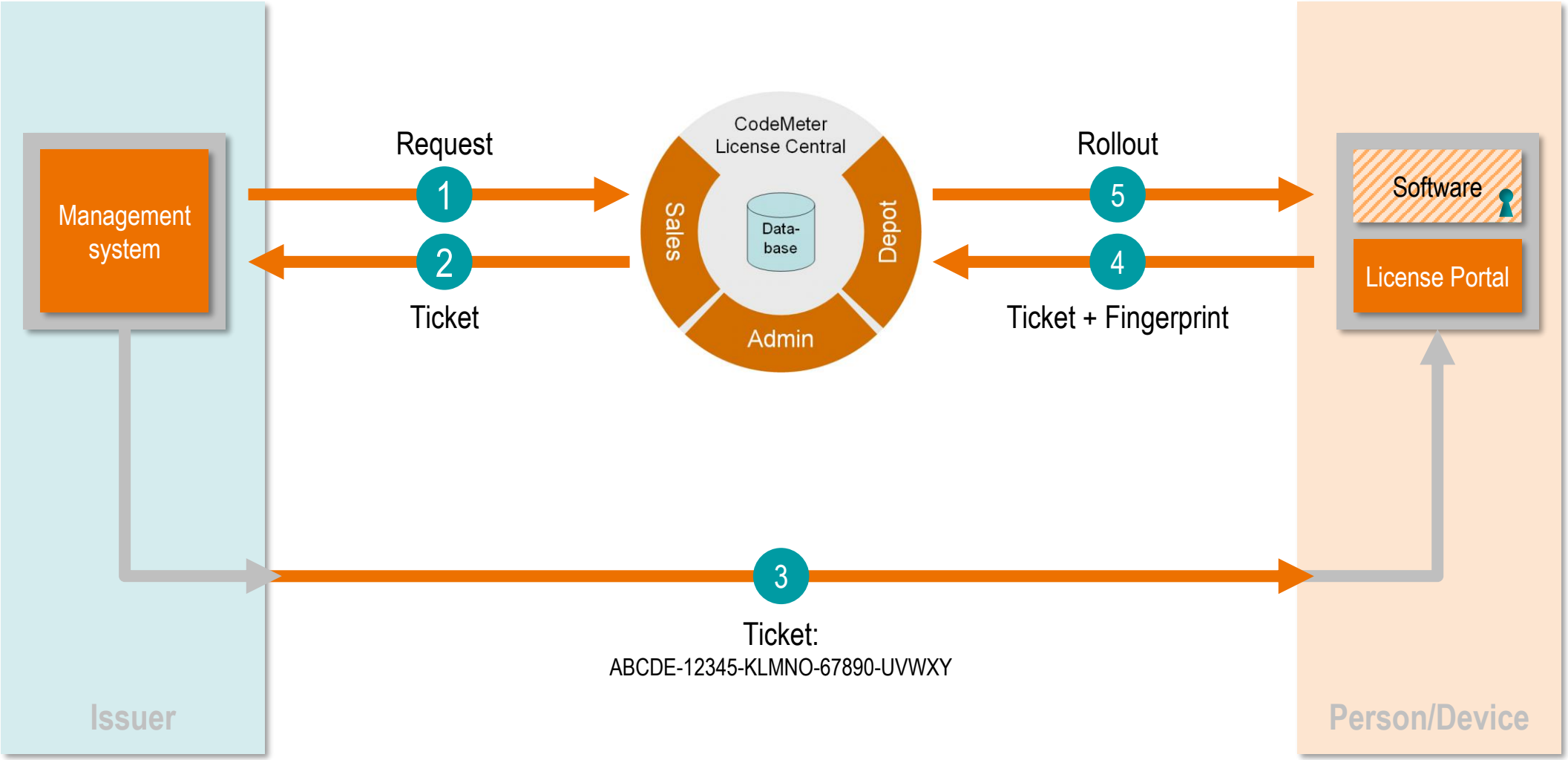
- Authentication using PKCS#11 on a web page
- Creation of a certificate via OpenSSL
- Encryption of a file using OpenSSL



Integration in CA and rollout of certificates

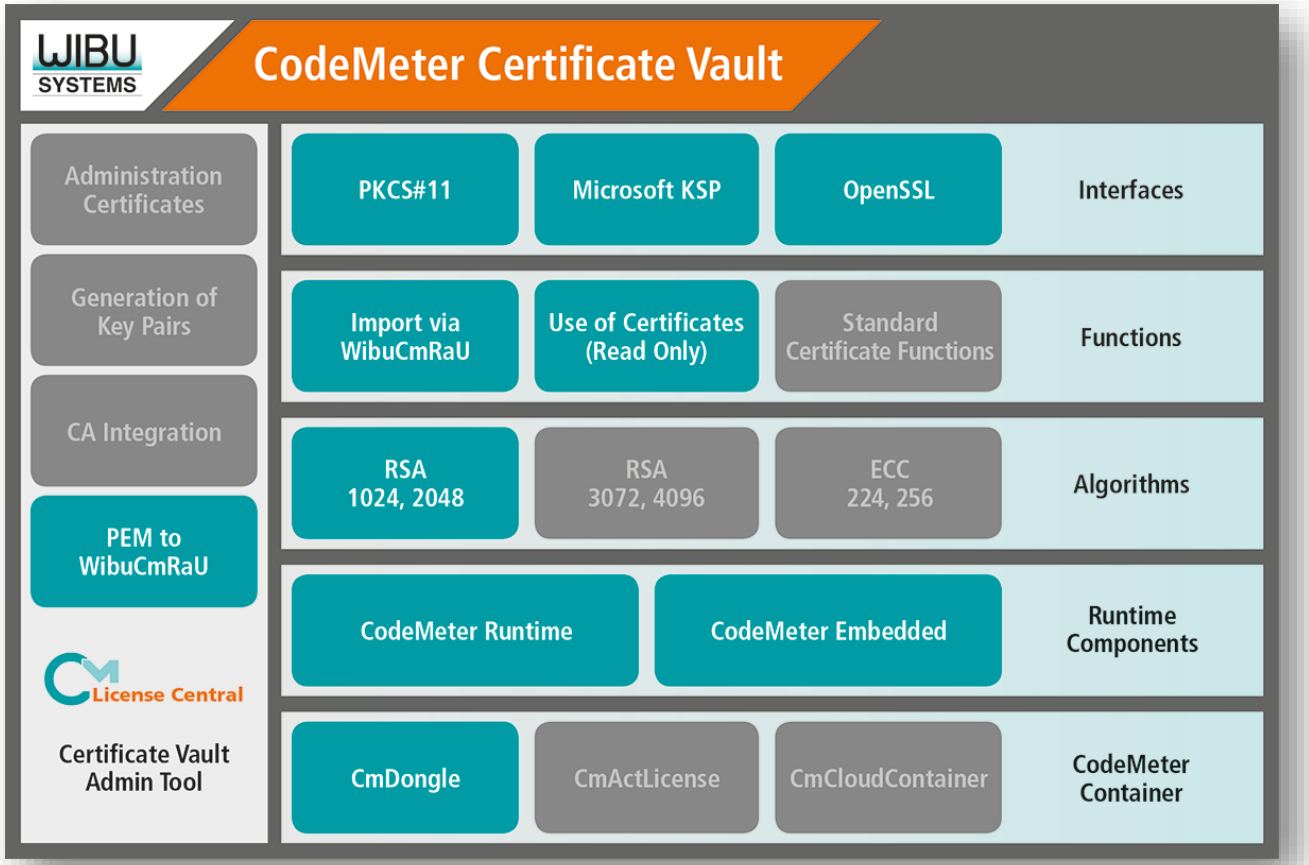


CodeMeter License Central – Ticket system for distribution



Overview of CodeMeter Certificate Vault

- Support of standard interfaces
- Simplification of the complex processes related to distribution and secure storage
- Use of the proven CodeMeter technology



Legend:
Turquoise: available

Thank You – Q&A

Europe: +49-721-931720

USA: +1-425-7756900

China: +86-21-55661790

Japan: +81-3-43608205

https://www.wibu.com

info@wibu.com