WIBU SYSTEMS

SECURITY
LICENSING
PERFECTION IN PROTECTION

Real Licenses
in Virtual Environments

Stefan Bamberg
Senior Key Account & Partner Manager

Wolfgang Voelker
Director Product Management & Support

Types of Virtual Environments

- **Virtual machines on a local computer**

  - QA and testing purposes

  - Software evaluation

- **Virtual machines on a server**

  - High availability

  - Hardware layer independence

- **Virtual machines in the cloud (Azure, AWS, …)**

  - Cost effective operation

  - Easy scaling on demand

- Virtual containers (e.g. "Docker" containers)

  - "Light Version" of a virtual machine

  - Easy delivery of complex software

  - Defined system environment

  - Container in virtual machines

Threat Scenarios and Risks

In the context of Software Protection
and License Management

- ■ Duplicating a license

  - ■ Copying a dongle, handing over a license file, being subject to theft, …

- ■ Using a license after expiration

  - ■ Resetting the time on the local machine

- ■ Resetting pay-per-use units

  - ■ Resetting a license to a former state

- ■ Overusing (network) licenses

  - ■ (Simultaneous) use of more licenses than purchased

  - ■ Manipulation using borrowed licenses (resetting borrowed licenses after return)

- Removing copy protection

  - Removing the shell and/or API calls

- Activating non-purchased functionalities

  - Patching API calls

- Extracting IP by means of reverse engineering

  - De-compiling and analyzing the results of the de-compilation

- Losing a license on the user's side

  - Exchanging the hardware container licenses were bound to

  - Losing a dongle

- **Properties simulation**

  - Properties for binding to a machine can be simulated more easily
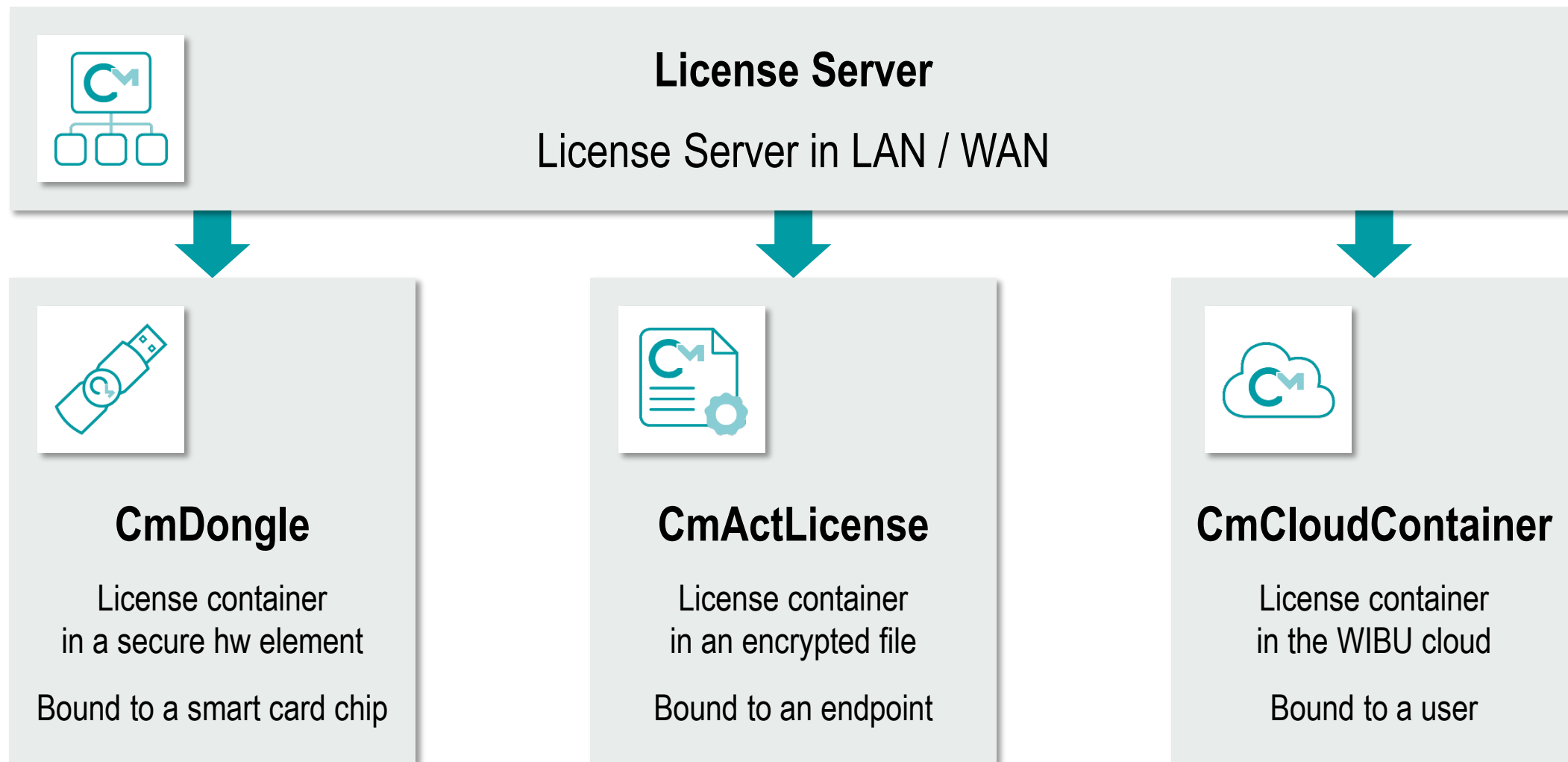
- **Snapshots**

  - Resetting the virtual machine to an old state is easier (snapshot)

- **High availability**

  - In high availability (HA) environments, the hardware of the system used can potentially change

CodeMeter Technology

Overview

CodeMeter Licensing Systems

License Server

License Server in LAN / WAN

CmDongle

License container
in a secure hw element

Bound to a smart card chip

CmActLicense

License container
in an encrypted file

Bound to an endpoint

CmCloudContainer

License container
in the WIBU cloud

Bound to a user

- **CmDongle**
  - Smart card chip
  - Complete license information (keys) is securely stored in the smart card chip

- **CmCloudContainer**
  - Operated by Wibu Operating Services
  - Complete license information (keys) is stored in the cloud

- **Network License Server**
  - Makes licenses available in the local network with the option "LQ,network"
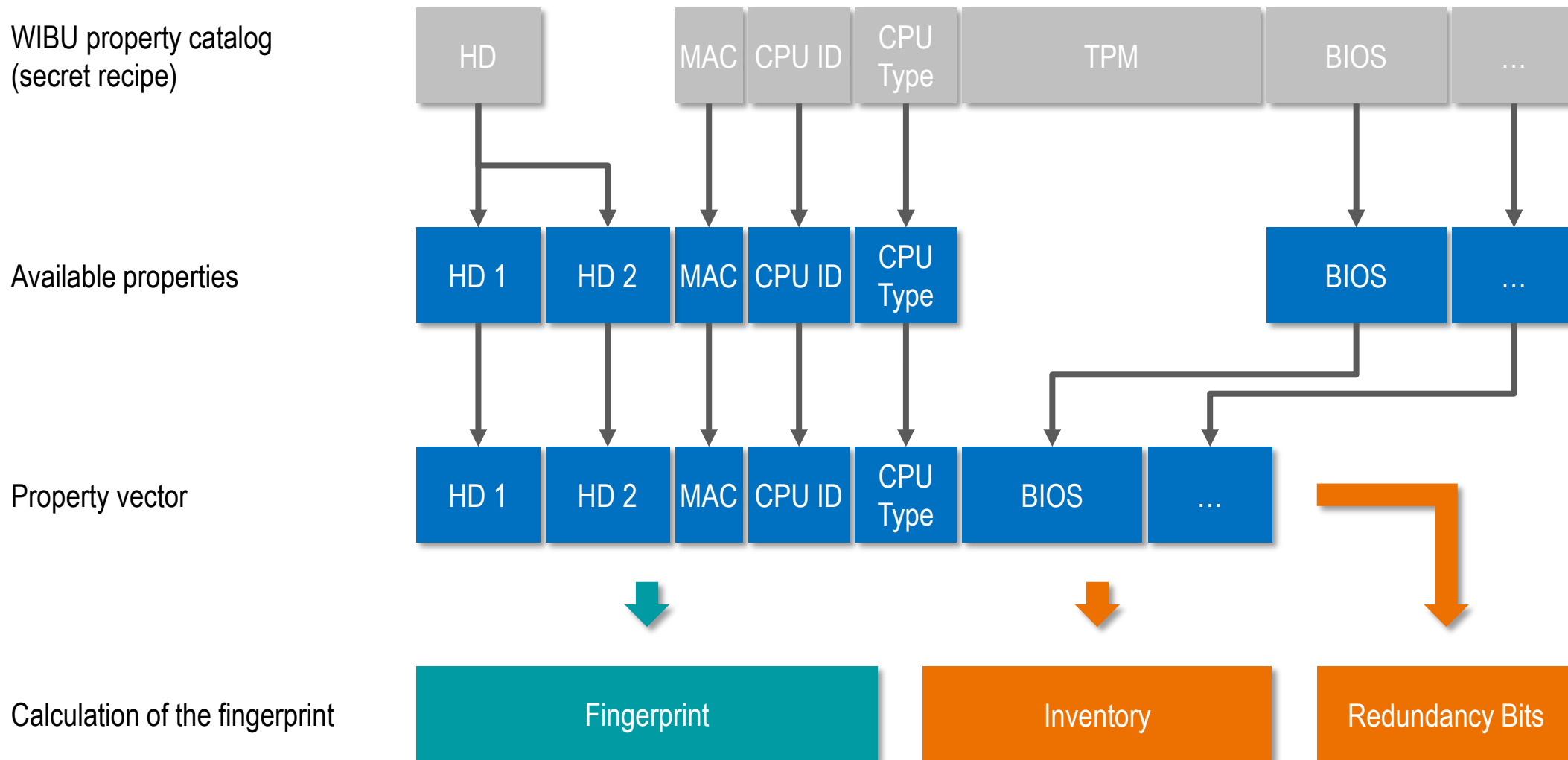 - Requires a CmDongle, a CmActLicense or a CmCloudContainer

CmActLicense

- Encrypted license file

- Bound to and encrypted for the intended computer

- All license information is securely saved in the encrypted license file

- Additionally, dynamic data is stored securely on the computer (last time of usage, pay-per-use units, locking flags …)

- A generation counter ensures the protection against the reset of the license file and the dynamic data
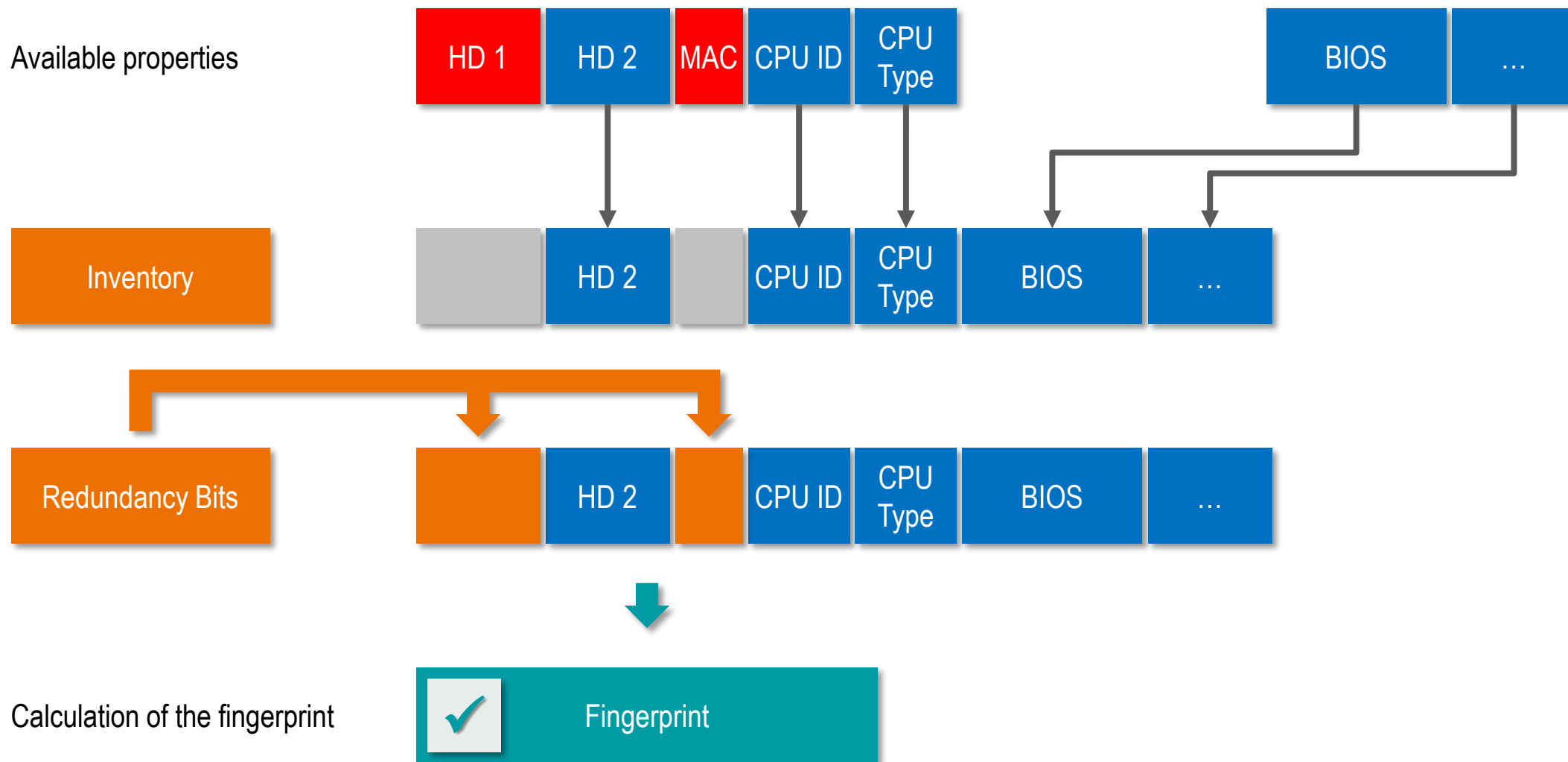
CodeMeter Technologies

CmActLicenses – SmartBind

CodeMeter License Server

- Runs as a local service

- Hides the generation counter for dynamic data and license files

- Detects the hardware properties and the configuration data of the system

- Detects virtual environments

- Detects cloud environments (e.g. Microsoft Azure, Amazon AWS)
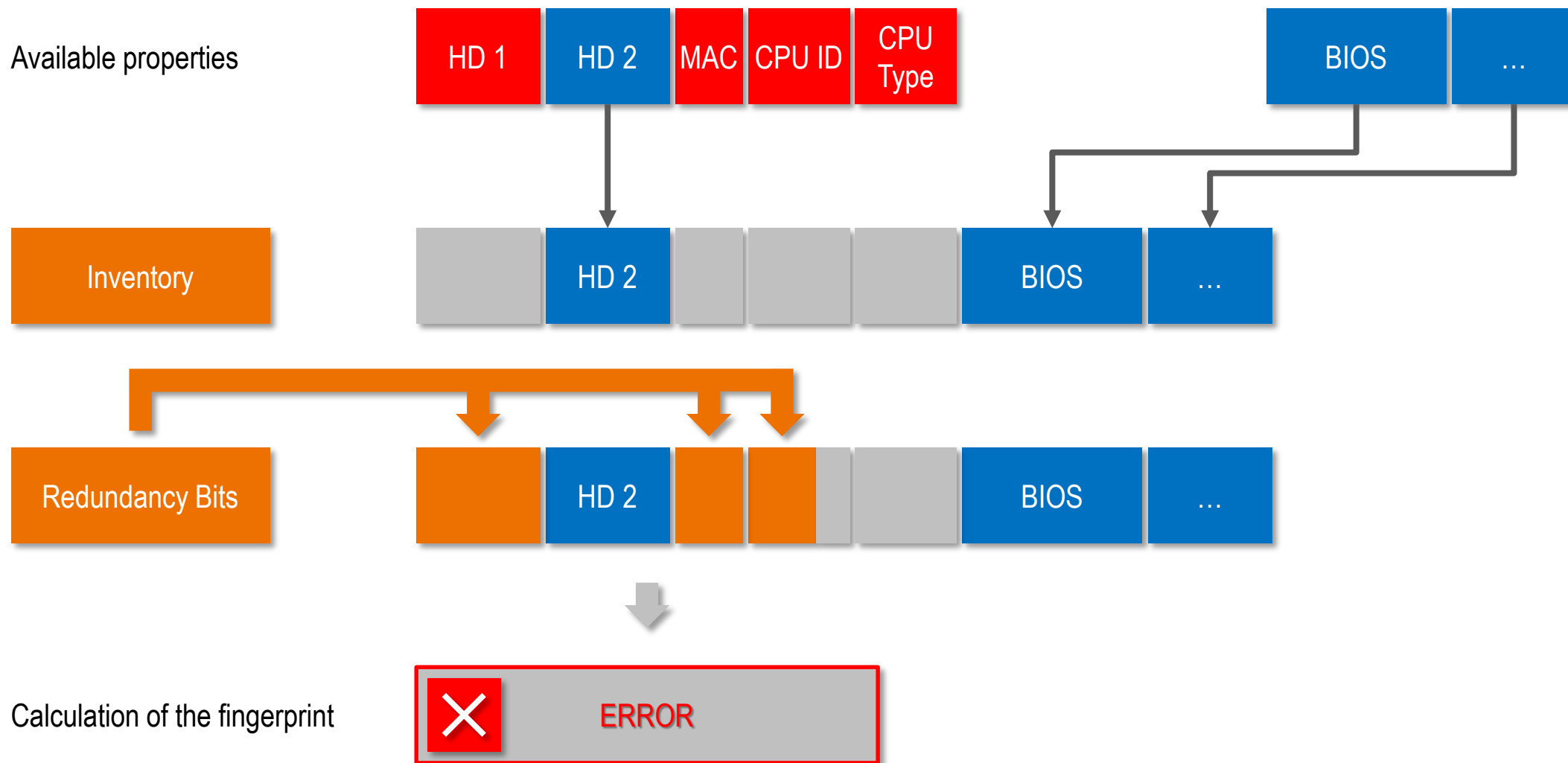
- Detects Docker environments

WIBU property catalog
(secret recipe)

| HD | | MAC | CPU ID | CPU Type | TPM | BIOS | ... |

Available properties

| HD 1 | HD 2 | MAC | CPU ID | CPU Type | | BIOS | ... |

Property vector

| HD 1 | HD 2 | MAC | CPU ID | CPU Type | BIOS | ... |

Calculation of the fingerprint

| Fingerprint | Inventory | Redundancy Bits |

Available properties

| HD 1 | HD 2 | MAC | CPU ID | CPU Type | | BIOS | ... |

Inventory

| | HD 2 | | CPU ID | CPU Type | BIOS | ... |

Redundancy Bits

| | HD 2 | | CPU ID | CPU Type | BIOS | ... |

Calculation of the fingerprint

✓ Fingerprint

Available properties

| HD 1 | HD 2 | MAC | CPU ID | CPU Type | | BIOS | ... |

Inventory

| | HD 2 | | | | BIOS | ... |

Redundancy Bits

| | HD 2 | | | | | BIOS | ... |

Calculation of the fingerprint

✕ ERROR

- Different catalogues for different systems
  - Windows, Linux, Linux ARM, macOS
  - Virtual machines, Microsoft Azure, Amazon AWS
- Weighting is based on many years of Wibu-Systems' experience in the field
- Different tolerance levels: Tight | Medium | Loose
- Special weighting in virtual machines (including Generation-ID)
- Uses an Azure-ID in Microsoft Azure environment automatically
- Uses an AWS Instance-ID in Amazon AWS environment automatically

WIBU property catalog Azure

| Azure-ID | AWS Instance-ID |

Property vector

| Azure-ID | AWS Instance-ID |

Calculation of the fingerprint

| Fingerprint | Fingerprint |
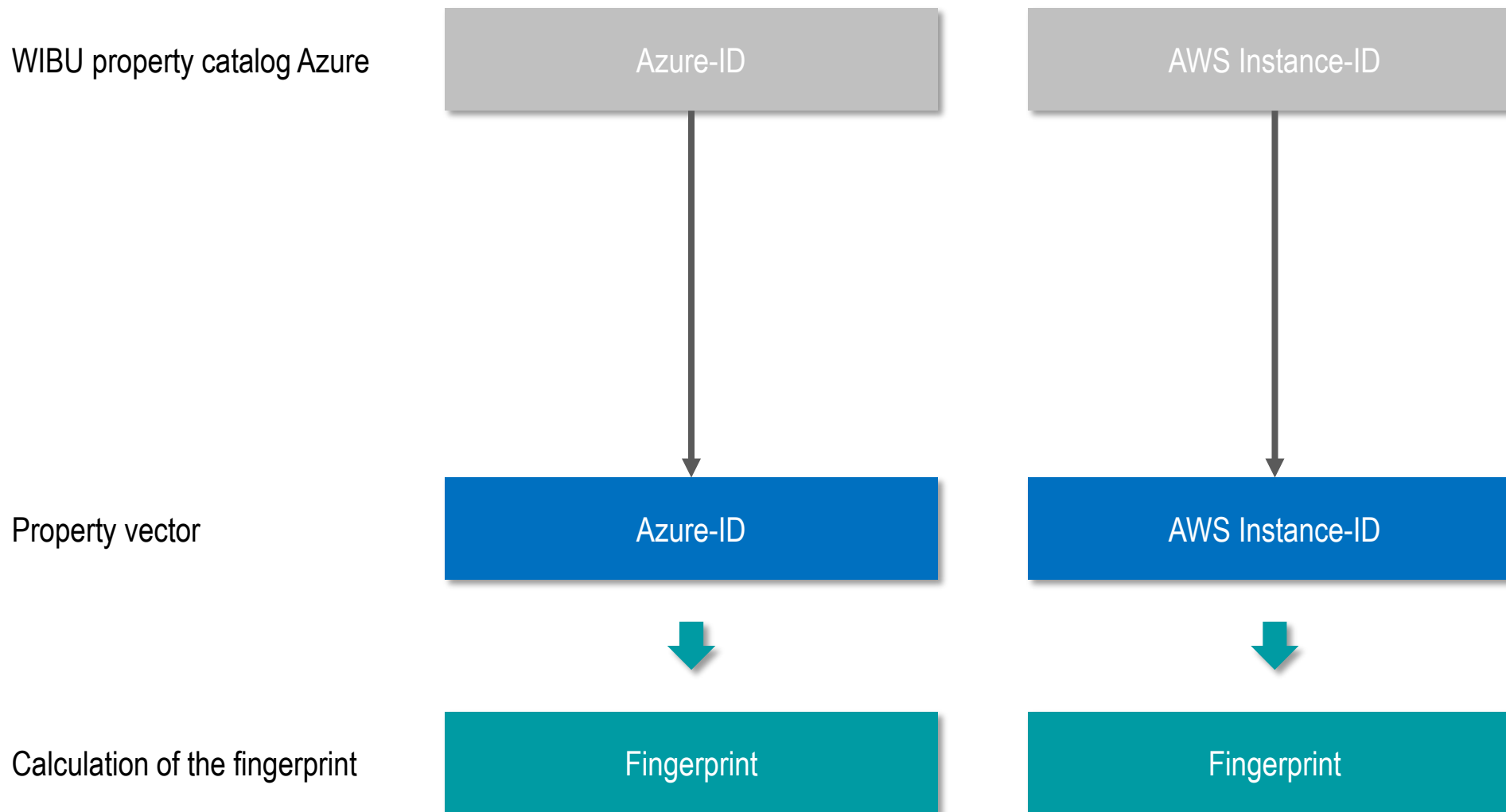
CodeMeter Technologies

More CmActLicenses

NoneBind licenses

- Encrypted license file

- No binding to the hardware (constant fingerprint)

- Option 1: Re-Import: Protection Only License (reset dynamic data allowed)
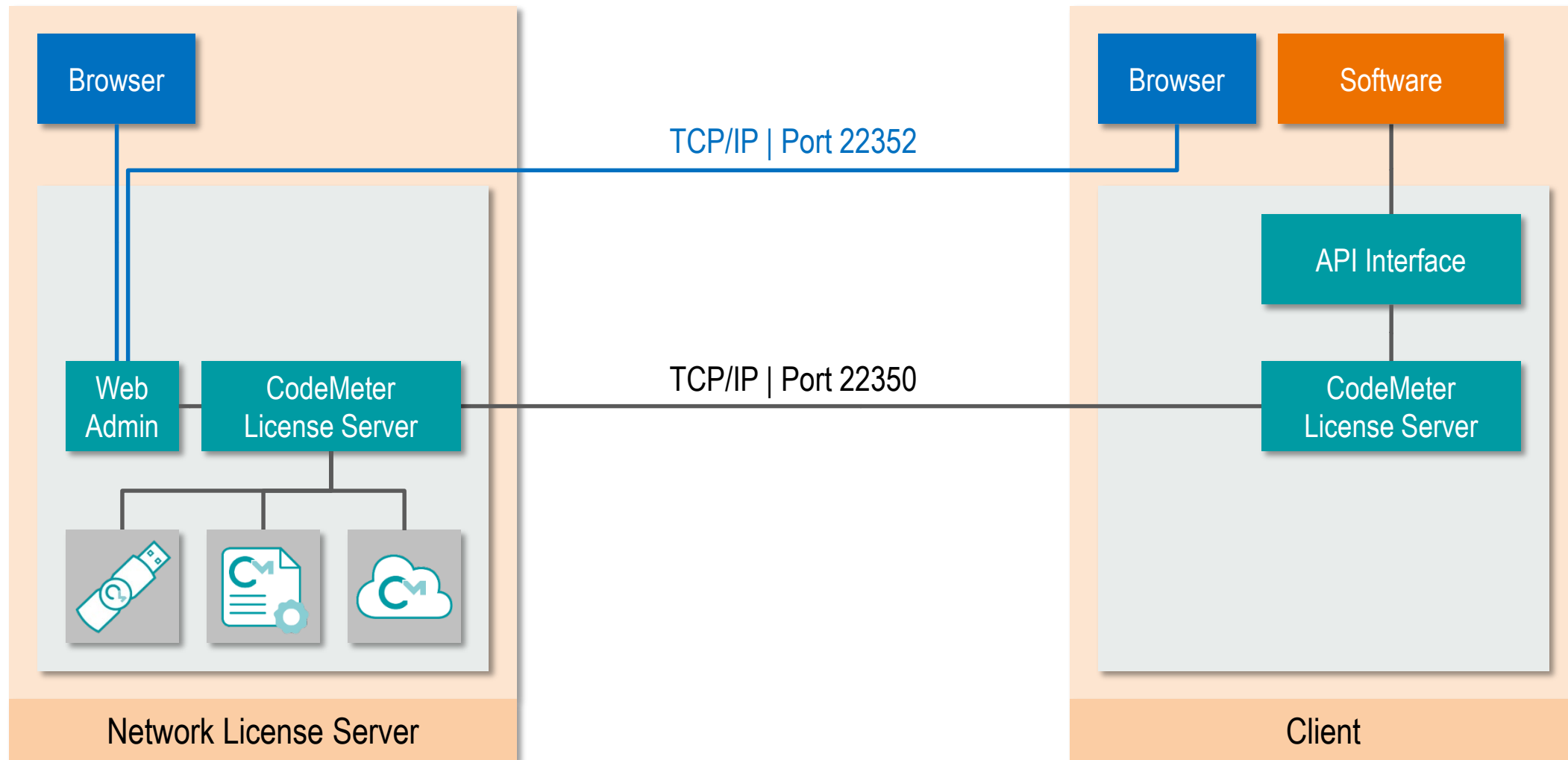
- Option 2: ~~Re-Import~~, Expiration date: Trial Licenses (secure dynamic data)

Binding Extension / Runtime Extension

- Individual extension of the binding mechanism
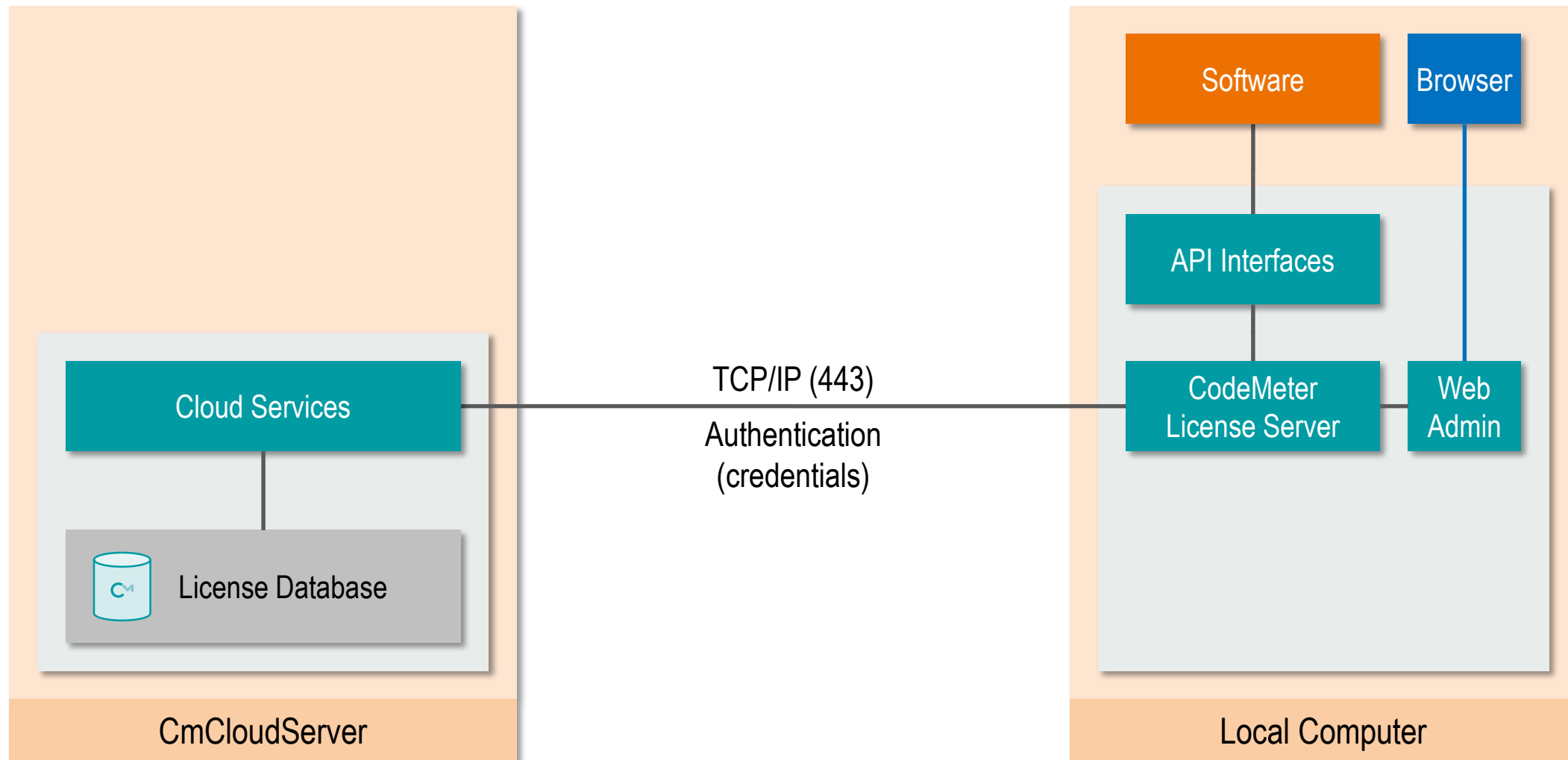
CodeMeter Technologies

Network License Server

CodeMeter Technologies

CmCloudContainer

CodeMeter in
Virtual Environments

- CodeMeter Runtime is able to detect the Azure environment automatically

- SmartBind licenses automatically use a specific "recipe" for the binding operation

  - They use an Azure-ID that is coordinated with Microsoft for the unique identification of the virtual machine

  - The status of the licenses depends on the change of the Azure-ID

- In general: CmActLicenses in virtual environments are not allowed by default.

  - Use option lopt:vm to allow activation in virtual environments.

Behaviour of Licenses in Azure

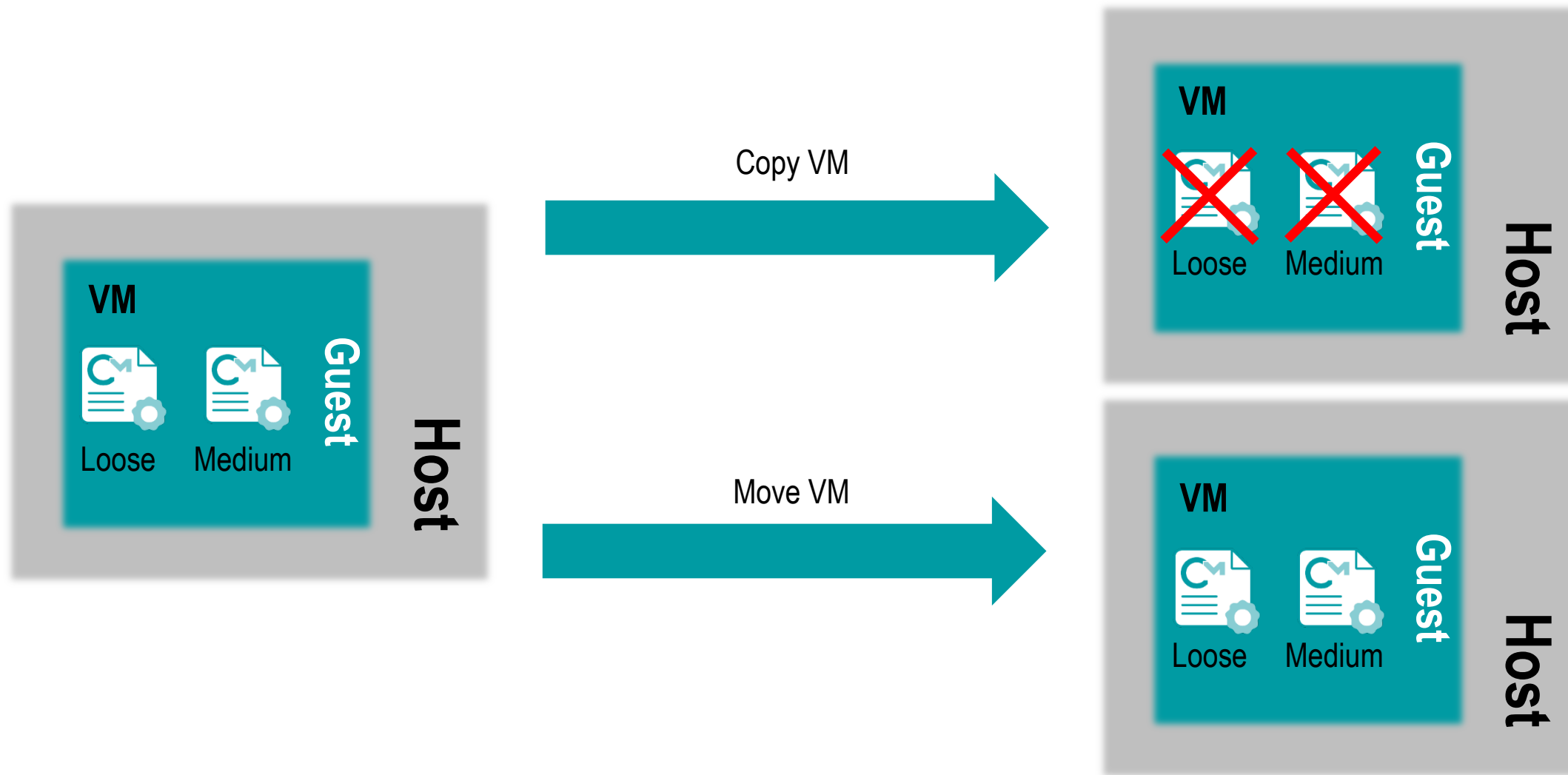| VM Scenario	Impact on Azure-ID	Impact on Licenses
Pause and resume	no impact	no impact
VM reboot	no impact	no impact
Host reboot	no impact	no impact
High availibility restart	no impact	no impact
Fault tolerant failover	no impact	no impact
Import ("Move")	changes	invalild
Import ("Copy")	changes	invalild
Clone	changes	invalild
Cold snapshot revert	N/A	N/A
Hot snapshot revert	N/A	N/A
Replication	changes	invalild

- CodeMeter Runtime is able to detect the Instance-ID of the AWS environment automatically

- SmartBind licenses automatically use a specific "recipe" for the binding operation

  - They use an AWS Instance-ID that is coordinated with Amazon for the unique identification of the virtual machine

  - The status of the licenses depends on the change of the Instance-ID

- In general: CmActLicenses in virtual environments are not allowed by default.

  - Use option lopt:vm to allow activation in virtual environments.
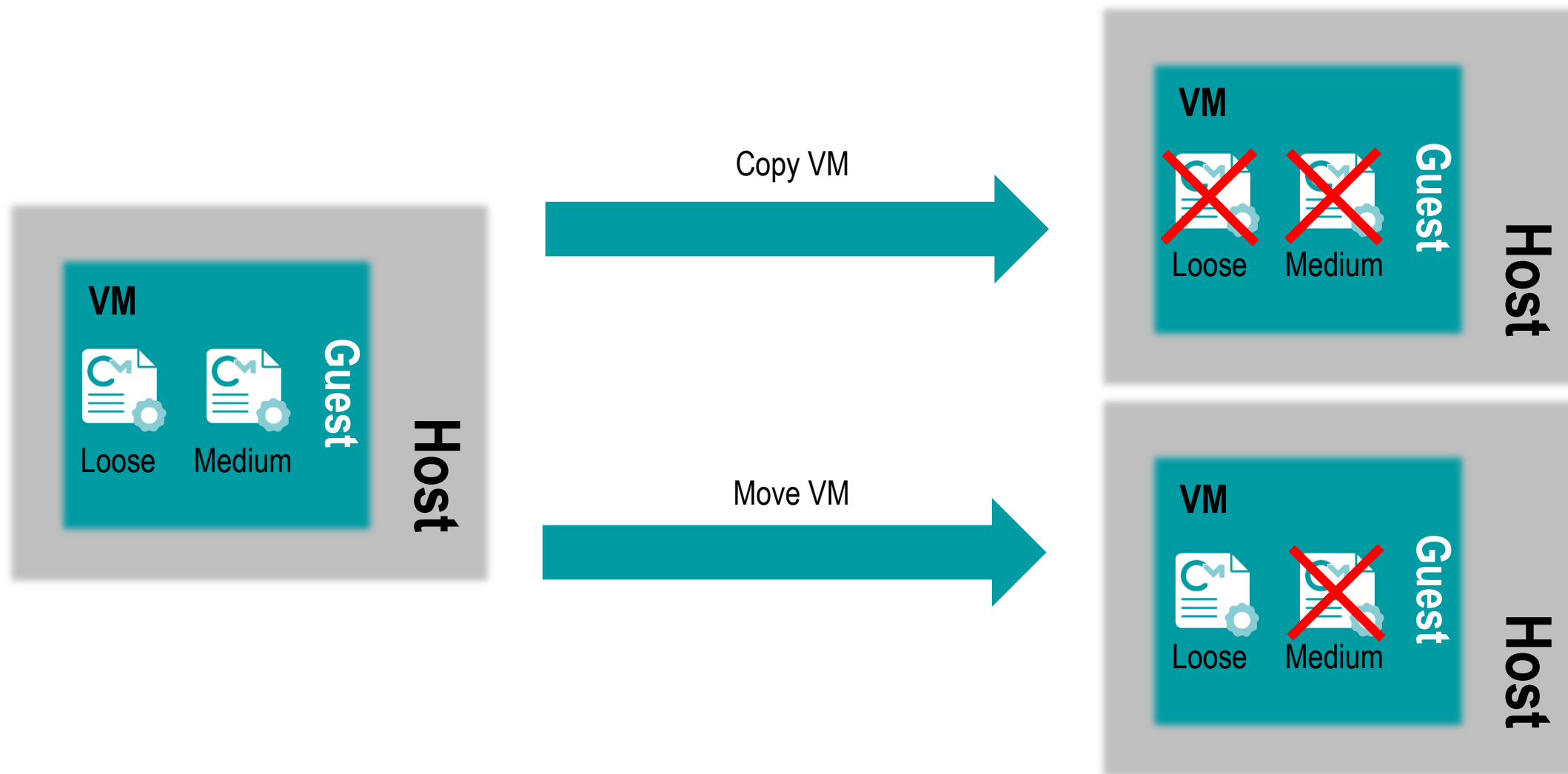
Behaviour of Licenses in AWS

VM Scenario	Impact on Instance-ID	Impact on Licenses
Pause and resume	no impact	no impact
VM reboot	no impact	no impact
Host reboot	no impact	no impact
High availibility restart	no impact	no impact
Fault tolerant failover	N/A	N/A
Import ("Move")	no impact	no impact
Import ("Copy")	changes	invalild
Clone	changes	invalild
Cold snapshot revert	no impact	no impact
Hot snapshot revert	N/A	N/A
Replication	N/A	N/A

- CodeMeter Runtime is able to detect virtual machines

- SmartBind licenses use a specific recipe for binding creation in VM

  - Higher weighting of external properties

  - Higher weighting of properties that change during a "copy" process

- Mechanism to detect a reset of the VM!

- In general: CmActLicenses in virtual environments are not allowed by default.

 - Use option lopt:vm to allow activation in virtual environments.

Behaviour of Licenses based on the Generation ID

VM Scenario	Impact on Generation-ID		Impact on Licenses	
Pause and resume	no impact		no impact	
VM reboot	no impact		no impact	
Host reboot	no impact		no impact	
High availibility restart	no impact		no impact	
Fault tolerant failover	no impact		no impact	
Import ("Move", binding "loose")	Same machine no impact	Other machine no impact	Same machine no impact	Other machine no impact
Import ("Move", binding "medium")	Same machine no impact	Other machine no impact	Same machine no impact	Other machine invalid
Import ("Copy")	changes		invalid	
Clone	changes		invalid	
Cold snapshot revert	changes		invalid	
Hot snapshot revert	changes		invalid	
Replication	changes		invallid	

- Licensed software runs in a virtual machine

- The license is stored on a network license server

  - CmActLicense: CmActLicense is bound to the network server

  - CmDongle: Dongle is connected to the server

  - CmCloudContainer: Credentials are stored on the server

- Licenses are used via the CodeMeter network mechanism

  - Maximum volume of available licenses

- The network license server can run on the same host system where the virtual machine is set up as a guest

Network License Server in Virtual Machines

Virtual Machine

Software

CodeMeter
License Server

CodeMeter
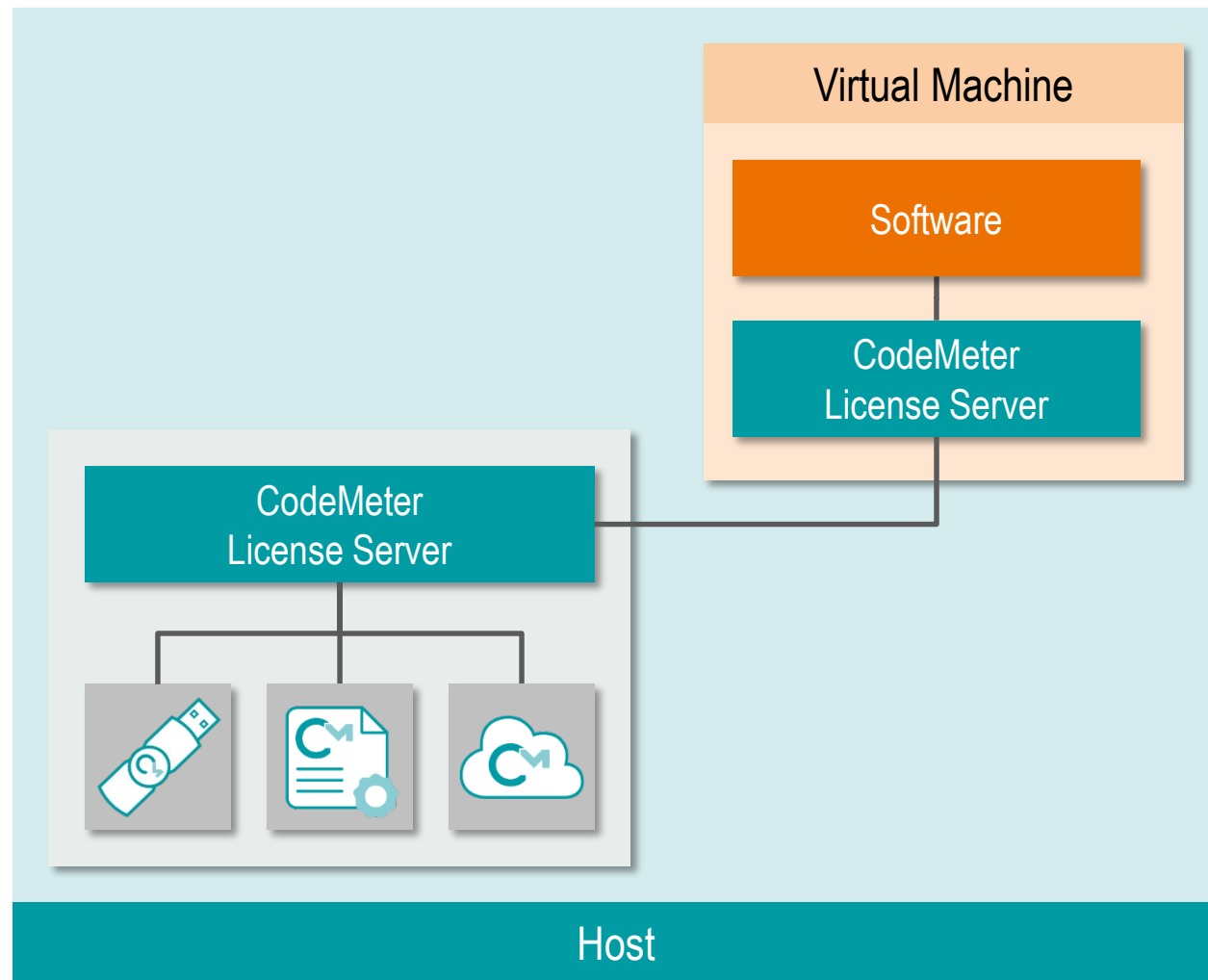License Server

Host
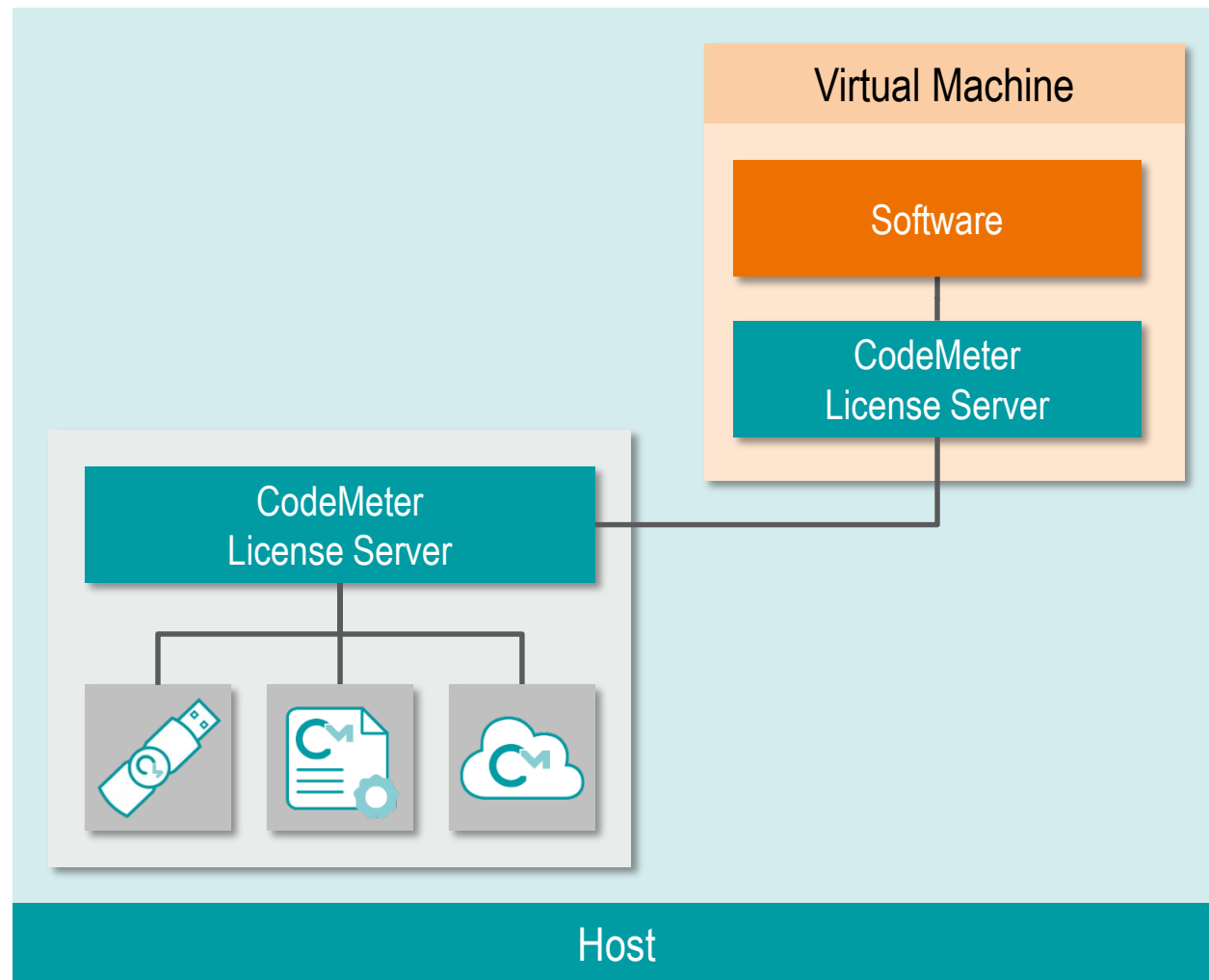
- CodeMeter Runtime is able to detect Docker environments

- By default, CmActLicenses are not allowed in Docker containers

- Exceptions

    - Protection Only licenses with Re-Import flag

    - Licenses for which the "Container" flag is set

- Possibility to operate via network license server on a host system

Docker Container

Software

CodeMeter
License Server

CodeMeter
License Server
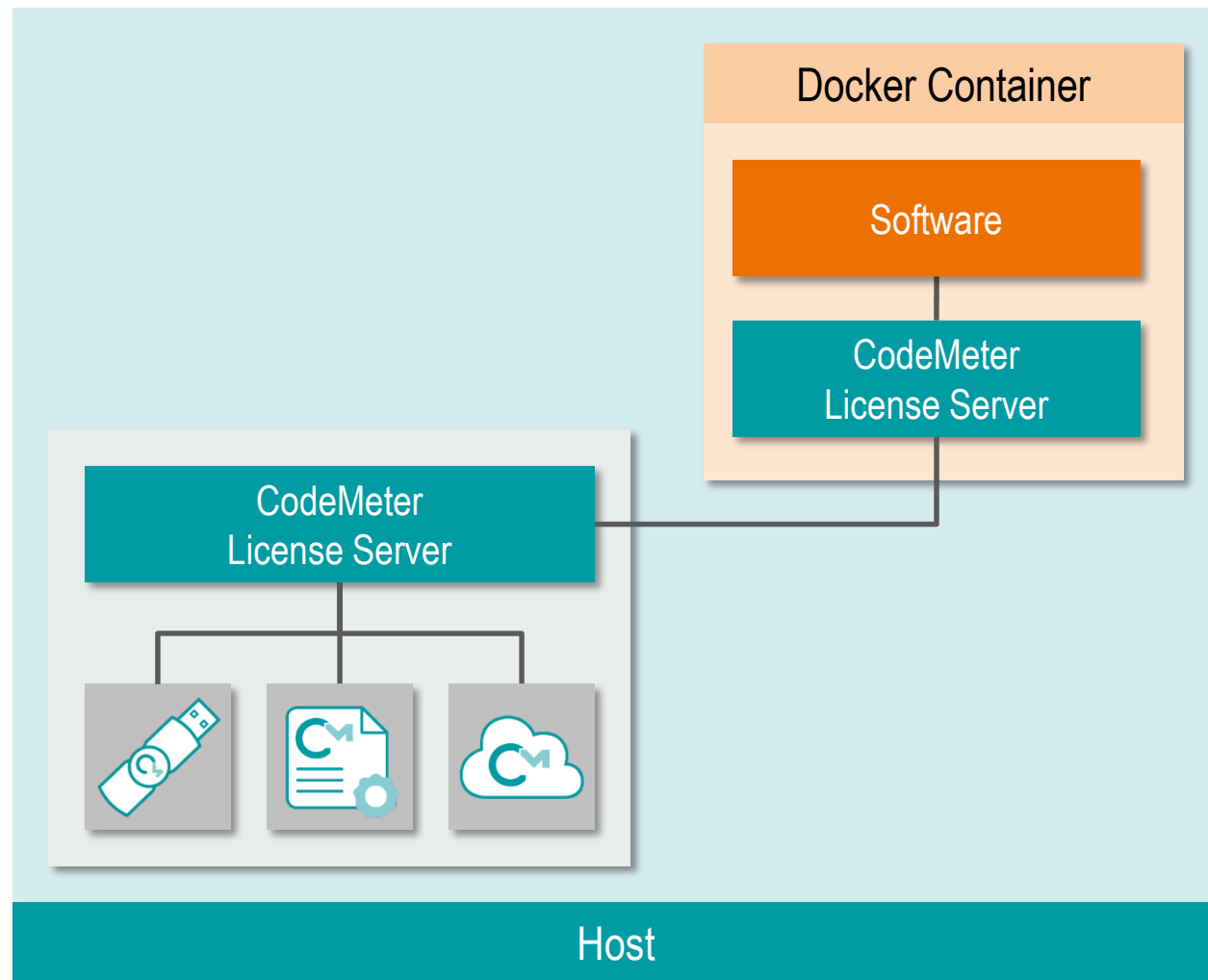
Host

- The functionality is identical in virtual machines
- CodeMeter License Server in a Docker container
- CodeMeter License Server on the host

- The dongle is on the host or a network license server
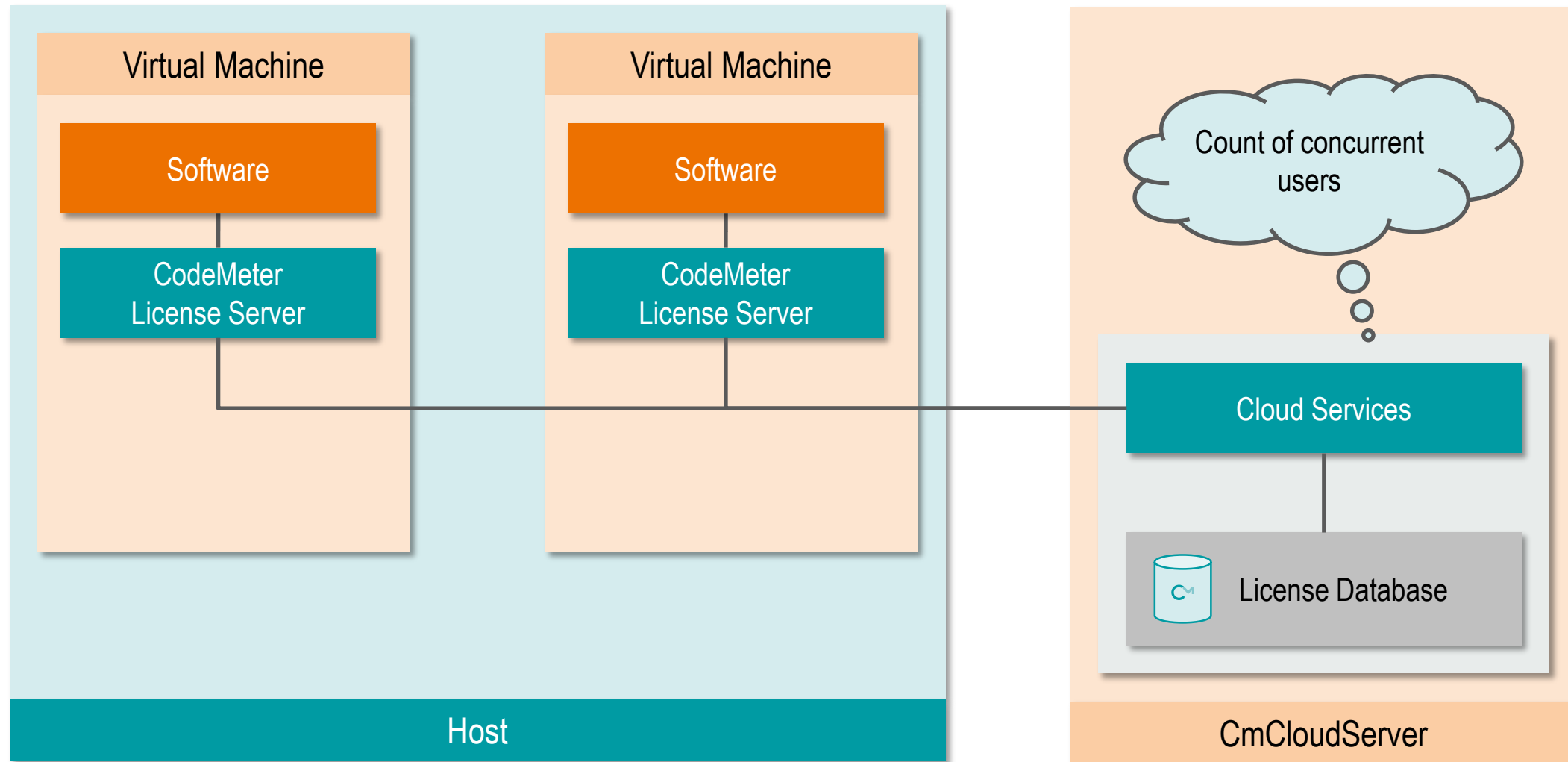
- Licenses are used via network license server
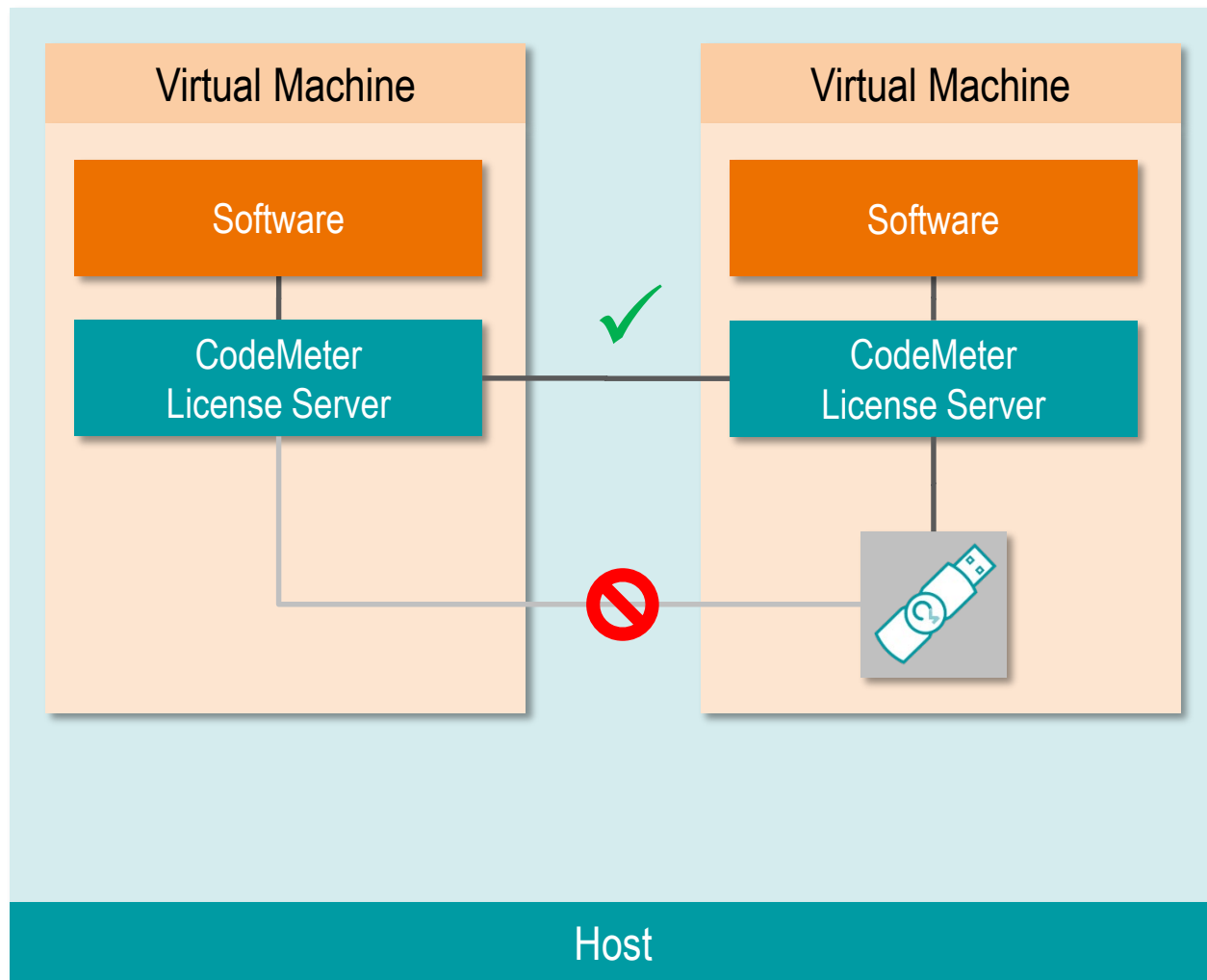
- The dongle is connected to a virtual machine

- Use of local licenses

- Dongles can just be assigned to one VM at a time

- Protection against automatic changes

The CodeMeter Solution

Threats and Risks solved

- Duplicating a license

  - CmDongles / CmCloudContainers: Licenses (keys) are stored in a secure container

  - CmActLicenses: Encrypted license file, strongly bound to a computer

  - CmActLicenses in VM: Encrypted license file, mixture of hardware and virtual properties

- Using a license after its expiration

  - Simulated clock in a CmContainer

  - CmDongles / CmCloudContainers: Clock stored in a secure container

  - CmActLicenses / CmActLicenses in VM: Protected against the reset of CmContainers

- **Resetting pay-per-use units**
  - **CmDongles** / **CmCloudContainers**: Units in secure containers
  - **CmActLicenses** / **CmActLicenses in VM**: Protected against the reset of the container
- **Overusing (network) licenses**
  - Protection of the network server against manipulation
  - **CmDongles**: Borrowed licenses in secure containers
  - **CmActLicenses** / **CmActLicenses in VM**: Protected against the reset of the container

- **Removing** copy protection, **Activating** non-purchased functionalities, and IP extraction by means of **Reverse Engineering**

  - Encryption of software and modules using CodeMeter Protection Suite

- **Losing a license on the user's side**

  - CmDongles: high MTBF

  - CmActLicenses / CmActLicenses in VM: Tolerance level of CodeMeter SmartBind

  - CmCloudContainers: Operated by Wibu Operating Services

  - Emergency licenses with CodeMeter License Central

  - Re-activation of a license with CodeMeter License Central

- **Properties simulation**

  - Using properties especially designed for local virtual machines

  - Using Azure-IDs in Microsoft Azure

- **Snapshots**

  - Detecting the reset of a virtual machine -> CmContainer becomes invalid

- **High availability**

  - Tolerance level of CodeMeter SmartBind

Summary

- **CmDongle** can only be used once at a time, also in virtual environments

- **CmCloudContainers** are automatically counting concurrent users via the server in the cloud

- **CodeMeter SmartBind** handles everything automatically

  - Real machines

  - Virtual machines

  - Docker containers

- **CodeMeter Protection Suite** provides IP protection

Thank you for your attention

Europe: +49-721-931720

USA: +1-425-7756900

China: +86-21-55661790

Japan: +81-3-43608205

https://www.wibu.com

info@wibu.com