

The VAULT

SECURED WITH SECORA™

FEATURED ARTICLE

SECORA™ ID X drives introduction of contactless multi-application ID solutions based on JAVA Card™
Infineon Technologies & cryptovision

ALSO IN THIS ISSUE

Wibu-Systems

Licensing in a highly fluid environment: Maximum flexibility for ISVs and their clients

Infineon Technologies

Brand protection is buyer protection: SECORA™

Infineon Technologies & Tribe


Infineon and Tribe join hands to strengthen Singapore's Blockchain Ecosystem

Fingerprints

Biometrics in a card: workplace security, no matter where you are

Infineon Technologies

SECORA™ Pay solutions enable contactless payments with environmentally friendly card body materials

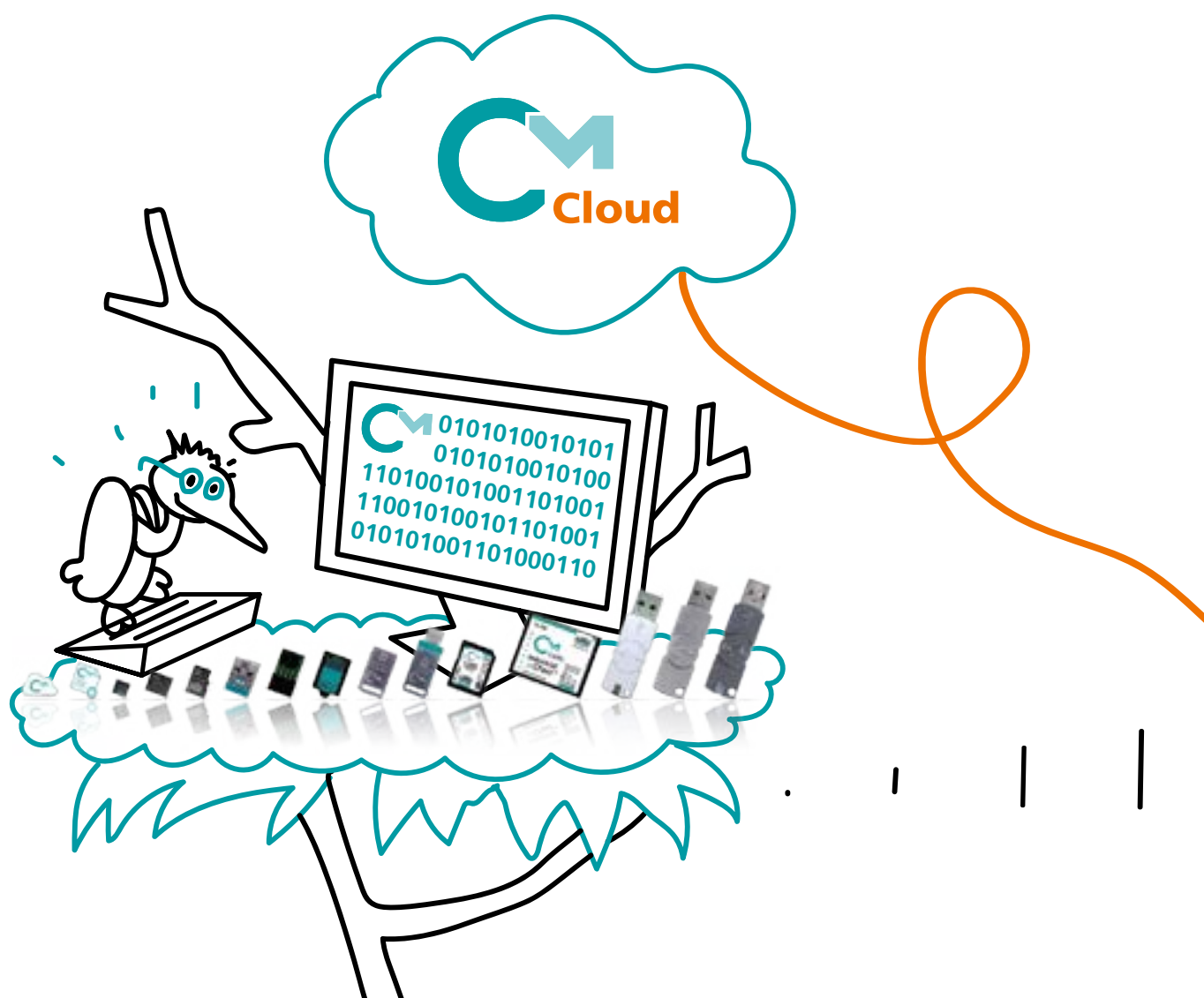


Licensing in a HIGHLY
FLUID environment:
Maximum *FLEXIBILITY*
for ISVs and *their*
CLIENTS

Dr. Carmen Kempka, Senior Cryptography Expert, Wibu-Systems


```
elif operation == "MIRROR_X":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

#selection at the end add back the deselected mirror modifier object
mirror_ob.select=1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
mirror_ob.select = 0
```



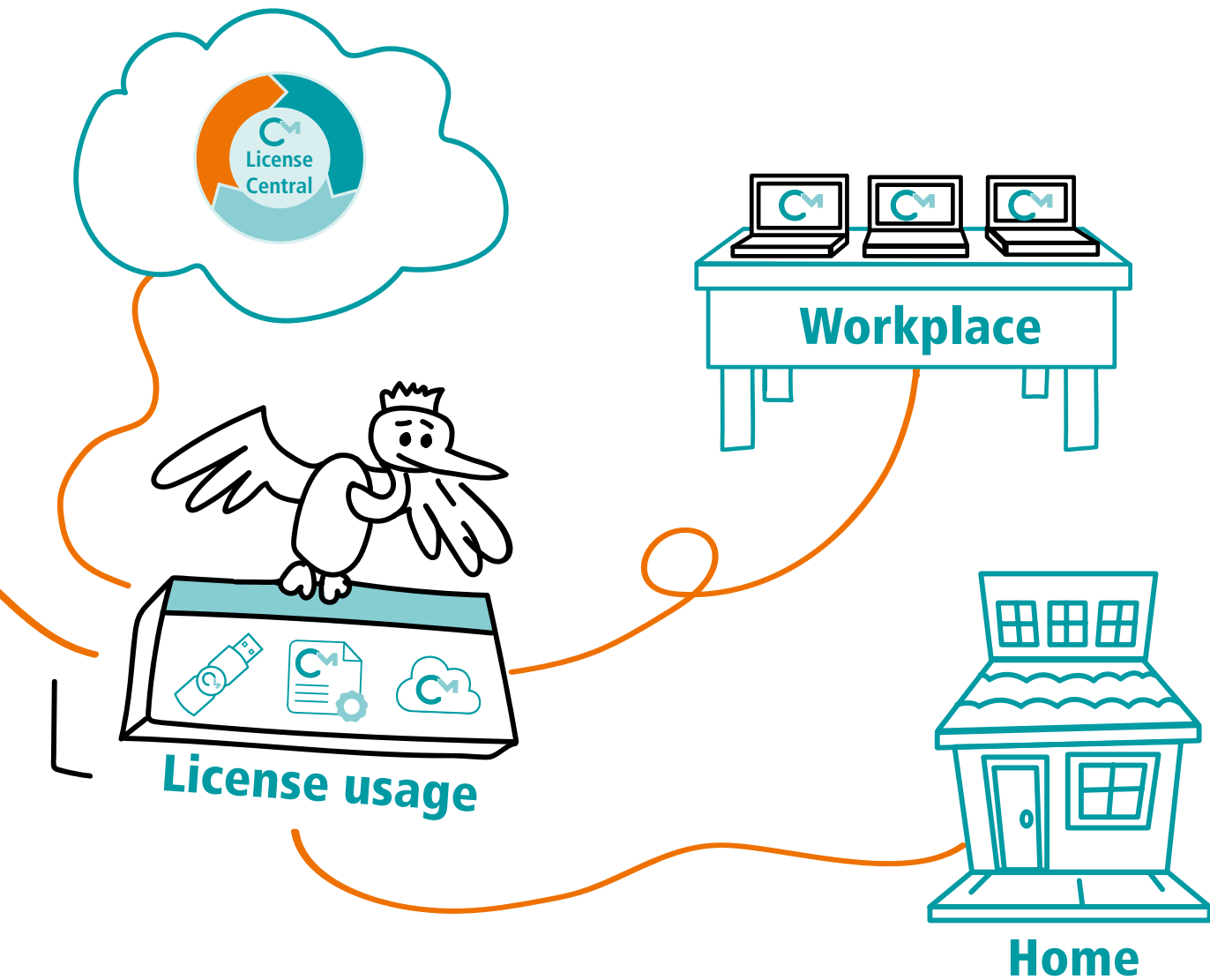
□ The year 2020 has shown us that sometimes, very suddenly, we need to be very adaptive. Wibu-Systems provides independent software vendors (ISVs) with a licensing model unparalleled in versatility, while maintaining high security standards. With a licensing infrastructure relying on standardized cryptographic algorithms, rather than proprietary solutions, the company offers protection against piracy, reverse engineering, tampering and malicious attacks.

Several dimensions of flexibility

Each customer, each situation and each use case have their individual requirements. User A might want to work offline in a pay-per-use setup, while User B shares a network license of an annual subscription with their colleagues, and User C uses a trial subscription to a SaaS application in the cloud.

Customer D wants to protect an IoT device against tampering while customer E wants to protect their desktop application against reverse engineering. Customer F wants to bind their license to a single device, and Customer G requires additional key material within secure hardware. Moreover, circumstances are subject to change: User A might want to switch from pay-per-use to a monthly subscription, User B might have to work remotely as well as in-house and be able to access the license from different devices and locations, and User C might want to upgrade their trial license to the full version.

A good licensing framework needs to provide flexibility in more than one dimension. To keep things simple, the ISV should not have to think about which of the endless possibilities of environments their software is used in when creating their protected application. In an optimal setting, the protected code can stay the same while the license is adapted to the



environment and situation at hand. In fact, requirements might change, as we have seen in the beginning of 2020, where employees had to switch from on-premise work to remote within days. The licensing solution of Wibu-Systems offers several dimensions of flexibility.

Automated or customized: with CodeMeter Protection Suite, applications and libraries can be encrypted either in a completely automated fashion with no manual effort required, or in a more customized way by encrypting individual functions or even weaving cryptographic calls into the code. Cryptographic methods are used by default, and licenses can carry additional key material customizable by the ISV, which can be used by the protected software.

Flexibility in the licensing model: when creating the protected code, the software vendor can, but doesn't have

to, think about the hardware binding or licensing model of a client's license. The same protected piece of software can be used with several license models like pay-per-use, monthly subscriptions, trial or full versions, floating or single user licenses, or permanent licenses. This offers a high level of adaptiveness: changing the licensing model only requires an update of the license itself; the protected application does not need to be modified.

Flexibility in the way and degree licenses are bound to a device: Licenses are stored on a license container. A license container can be a secure hardware element directly connected to a device, or to a license server in the network. Computer-bound software license containers or user-based license containers in the cloud offer mobility for both offline and online usage.

“*Monitoring of the license usage makes it easier for ISVs to adapt their software and licensing model to their customer’s needs, or to detect and prevent malicious usage.*”

Hardware license containers are available for several hardware interfaces, for example **CmDongle** for USB, or **CmASIC** for ASIC. SD, microSD and CF are also among the supported interfaces. They can be used as secure elements to store key material and do cryptographic operations. They can also be used as a certificate vault to store X.509 certificates and to identify devices uniquely.

A **CmActLicense** is a license container in the form of a secure file, which is bound to attributes of the target device. Which and how many attributes are used in the binding, as well as the strictness of the binding, is customizable by the ISV.

The newest license container type and next logical step in Wibu-Systems’ lineup is a license container in the cloud, namely a CmCloudContainer, hosted by Wibu-Systems itself. This licensing solution is called CmCloud and was released in September 2020. A CmCloudContainer offers the maximal level of mobility. It can be accessed from everywhere through an Internet connection and is ideal for software usage because it's not bound to a certain device or location.

CmCloudContainer: A new container type for optimal mobility and security

A CmCloudContainer is tailored to offer the best solution in security, high performance, and high availability; all of this has been incorporated early in the development process. CmCloud

offers many advantages: In a CmCloudContainer, the license always stays accessible and manageable by the ISV. Securely stored in a CmCloudContainer, the license never resides on a client device or any untrusted environment. This way, the client can neither copy nor lose their license.

Since ISVs always have access to CmCloud and their license containers, they can easily modify and adapt licenses for their customers, without the need for any interaction with them. This way, licenses can, for example, be updated from trial to the full version, or from pay-per-use to a monthly subscription, without re-activation or software updates on the client side. In the same way, licenses can easily be withdrawn or locked in the case of contract cancellation, or illegal license usage and fraud. No blacklisting of license containers is necessary.

Real-time monitoring of the license usage makes it easier for ISVs to adapt their software and licensing model to their customer’s needs, or to detect and prevent malicious usage.

Since the license container is kept in the cloud, no additional infrastructure like VPN or additional hardware is needed to access a license when working remotely out of office, or on different devices. A CmCloud license does not bind the license to a certain device. However, the number of devices which can use a CmCloud license at the same time can be restricted, and access to the CmCloud license requires a credential on the client device.



Supporting our customers in quarantine time

At the beginning of 2020, the home office became omnipresent in our work life very suddenly, without the time to prepare for any notable changes in infrastructure. To make license access possible from arbitrary places, a pre-release version of CmCloud was set up in May 2020. During this pre-release phase, Wibusystems provided a free of charge CmCloudContainer to their customers, allowing license access when working remotely. The only required prerequisites for this setup were an Internet connection and cryptographic credentials for license access. The pre-release proved to be stable, and we could confidently release CmCloud in September.

Cloud based automatable license deployment

Regardless of the used container type, with CodeMeter License Central, licenses can be managed in the cloud, and activated on the client side when needed, either on a hardware dongle, a CmActLicense soft container, or on a CmCloudContainer. Licenses can, but do not have to, be restricted to a certain license container type or hardware binding scheme.

The complete lifecycle of a license from creation to deployment and activation can be automated: CodeMeter License Central can easily be integrated in existing ERP, CRM, and back office systems to deliver software, create licenses automatically and transfer licenses to the client's license container.

	CmDongle	CmActLicense	CmCloudContainer
Cryptographic operations in secure environment	×		×
Secure key storage	Highest	High	Highest
Unique device authentication	×	×	
Certificate vault	×		
Hardware binding		×	
Access from everywhere			×
Offline usage	×	×	
Monitoring	×	×	×
Real-time monitoring			×
License management in the Cloud (CodeMeter License Central)	×	×	×

Comparing the different license container types

Which container type or licensing model is most suitable needs to be decided individually for each use case. Hardware license containers add to security by acting as secure elements for key and certificate storage, and enable device authentication. They are optimal for a setting where cryptographic operations need to be done within secure hardware.

Hardware license containers can, for example, give IoT devices an all-around protection ranging from anti reverse engineering techniques and copy protection, to integrity protection. Cryptographic methods shield the devices from piracy and manipulation attacks. Unique device authentication is realized using cryptographic techniques and key material protected within the secure hardware.

CmActLicense containers are cryptographically protected software licenses that are stored directly on a device and therefore do not require additional hardware. They can be bound to a device's hardware attributes and are optimal for offline usage.

While hardware dongles offer security by protecting licenses within secure elements, CmCloudContainers offer security through the fact that the license and its key material never leaves the CmCloud hosted by Wibu-Systems. Cryptographic operations are performed within the cloud. Cloud licenses can be accessed from everywhere given the correct credentials, and do not restrict usage to a certain device or location. Since the licenses remain in the cloud, license usage in CmCloud can be monitored real-time by the ISV.

Freedom of choice

Flexibility and adaptiveness are essential not only in days like these. This adaptiveness is achieved with a licensing framework offering suitable degrees of freedom, while being tailored for compatibility and interchangeability between licensing models. You have the freedom of choice. ☒

Let CodeMeter inspire you with new license-driven business models

- Protect your digital assets from piracy and reverse engineering
- Secure the integrity of your endpoints from tampering
- Implement license-based readily adaptable business models

Customer centric approach

From the cloud down to FPGAs

Digital global marketplace

Software, firmware, and sensitive data

Brown field and green field



Don't wait any longer
Start protecting your IP now!
s.wibu.com/sdk-cm

+49 721 931720
sales@wibu.com
www.wibu.com



SECURITY
LICENSING
PERFECTION IN PROTECTION