NEWS & INSIGHTS FROM THE WORLD OF ID SECURITY

NOVEMBER 2020 | SPECIAL EDITION

The VAULT

A SILICON TRUST APPLICATION BRIEFING

THE NEXT BIG QUESTION

What could the new 'normal' be for travel, border crossings and payment, post-andemic?

Digital *Certificates* – A *MATTER* of TRUST

By Guenther Fischer, Senior Consultant, Licensing and Protection at Wibu-Systems AG

The network specialist Cisco predicted a 26 percent increase in IP traffic year on year for the foreseeable future in its white paper "Cisco Visual Networking Index: Forecast and Trends 2017-2022".[1] By 2020, machine communication (M2M) has accounted for more than 14.6 billion connections or the majority of all digital communication, a steep rise from its share of 34 percent in 2017. With the rapid proliferation of Industry 4.0-ready machines, secure, unique, and tamperproof identities are becoming indispensable for all devices engaged in this unceasing and universal digital conversation.

> *Whether a certificate is valid and genuine can be ascertained quite easily by checking its expiry date and the public key of the relevant certificate chain.*

☐ Certificates as Digital Proofs of Identity

All Internet users encounter them every day, at work or in private – but very few people are aware of what they are and why they are so important. We are talking about digital certificates. They are the backbone of all secure transactions over the web. Digital certificates contain the electronic ID of people, organizations, devices, or any other object, and they are protected against tampering and manipulation by cryptographic means. One particularly common type is the public key certificate: These include not only an ID, but also a related public key. Its counterpart, the private key, is stored in some secure place away from the certificate. With the public key contained in them, these certificates are used to prove digital identities beyond all doubt or to encrypt and sign data.

Certification Authorities: Neutral Arbiters

Official certificates are given out by known and recognized certificate authorities (CAs) or trust centers, acting as independent and trustworthy arbiters like public notaries in the physical world. For a person, organization, or object / device to get an official certificate, they need to bring proof of their identity to the CA, which can be a valid identity card, a copy of the company register, or a device's serial number. Their identity is checked, and if it is genuine, the CA creates a key pair and a certificate that contains all of the essential ID information – the public key, the expiry date, and the CA's name and digital signature. CAs act as essential roots of trust, which is why many CAs are household names in the field, like Symantec, Comodo, and GlobalSign. There are also alternative providers, set up to create certificates for free, such as Let's Encrypt (https://letsencrypt.org). Some companies have begun to host their own CAs to create and manage so-called self-signed certificates. Their trustworthiness is, in that case, limited to the specific organization they hail from.

Validity of Certificates

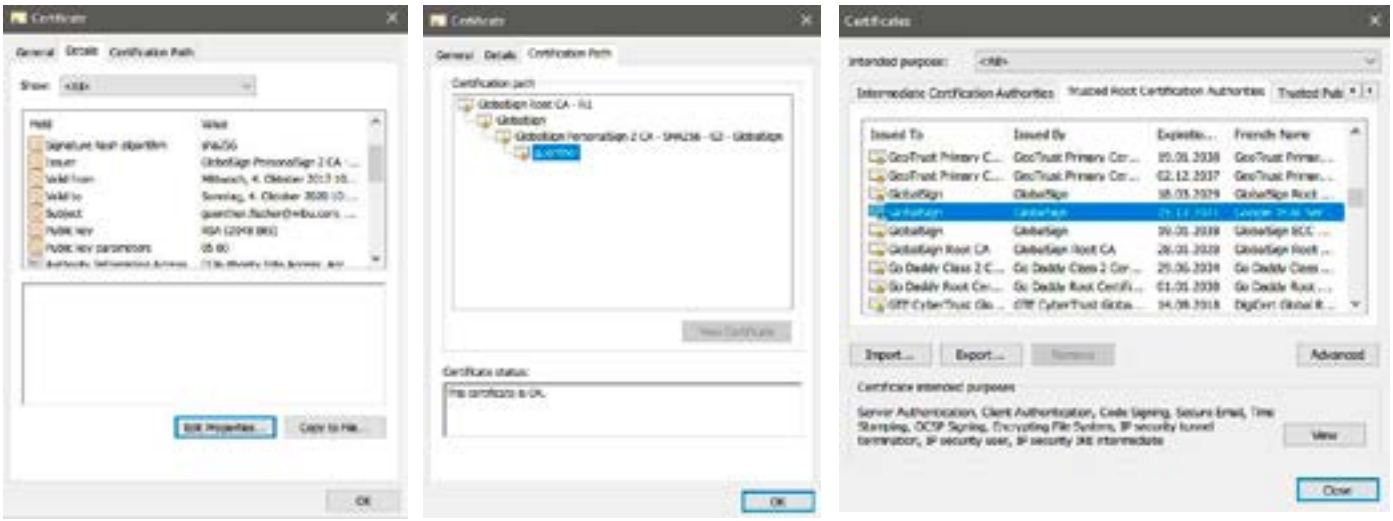
Whether a certificate is valid and genuine can be ascertained quite easily by checking its expiry date and the public key of the relevant certificate chain. Every certificate should come with such an expiry date and only stay valid for that defined period – which depends on systems actually checking the expiry dates. The validity of a certificate can be checked by looking at the at the public key of its certificate chain: Every certificate is signed with the private key of its CA, which can be verified with the certificate assigned by the CA. The process checks the entire chain of certificates back to their root to establish their authenticity, since the genuineness of the root certificate cannot, by definition, be doubted.

Certificate Management and Distribution

Certificates come with one major challenge: Managing and distributing the certificates and private keys. Doing so manually, which is still the norm, can be a recipe for disaster, with catastrophic consequences if the private keys fall into the wrong hands. One prominent example is the eDellRoot certificate preinstalled by DELL – and distributed alongside the private key (https://securesense.ca/sayhello-edellroot).

---

https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html



X.509 certificate with expiry date, certificate chain, and root certificate

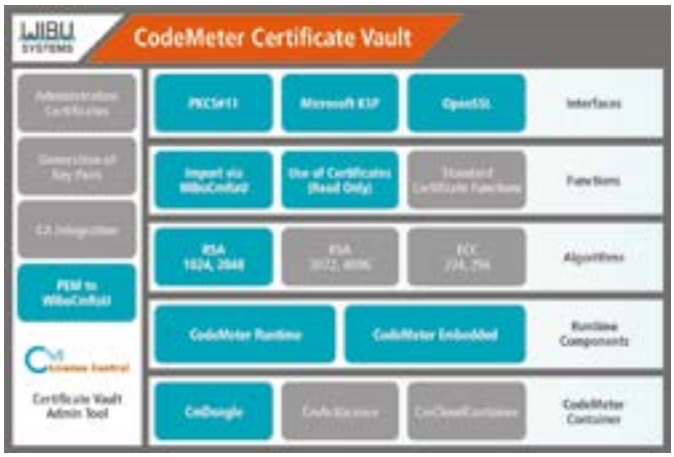
Straightforward and Secure: CodeMeter Certificate Vault and CodeMeter License Central

Wibu-Systems, the innovator of software protection, licensing, and security solutions, takes all of the fuss out of using certificates, without compromising on their security. This is made possible by CodeMeter Certificate Vault, based on the award-winning CodeMeter technology, and Wibu-Systems' CmDongles as special secure elements with integrated smart card chips to serve as protected key storage and cryptographic engines. CmDongles are sold in a choice of form factors ranging from USB, SD, microSD, or CF to directly integrated ASIC options, with industrial grade versions for use even in extreme environments available for each variant. CmDongles can also come fitted with MSD flash memory storage e.g. for signed logs. CodeMeter Certificate Vault stores all certificates in the safe harbor of the smart card chip. On top of CodeMeter's own API, it works with other standard interfaces like PKCS#11, KSP, and OpenSSL to make the solution a perfect fit for any existing application and every client's needs. The PKCS#11-compliant token provider was designed to work with Microsoft's Cryptographic API Next Generation (CNG) and the OpenSSL API to empower users with easier access to secure identities, digital signatures, emails, or VPNs with robust authentication systems.

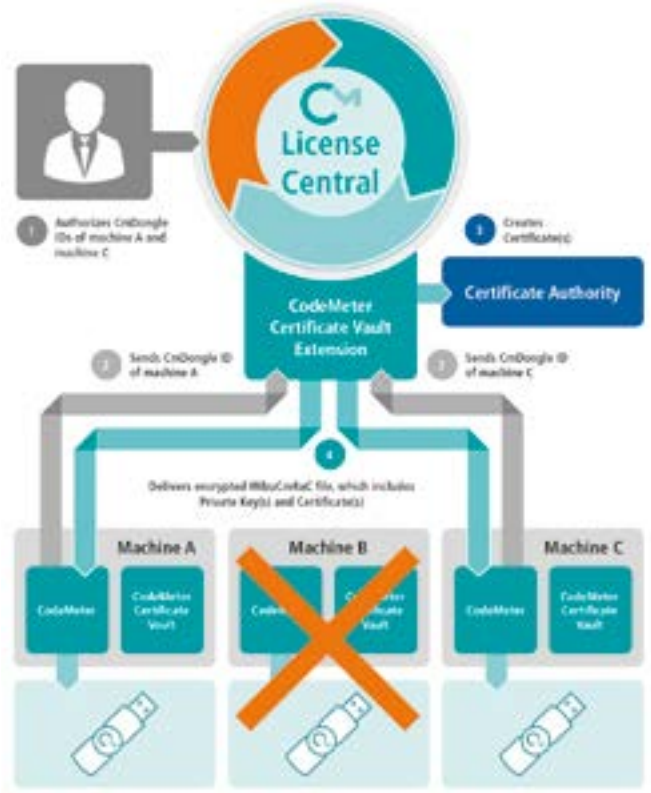
CodeMeter License Central, the popular backend system for creating, managing, and distributing licenses, can now also be used to distribute certificates and keys securely via CmDongles. Certificates can be created and rolled out automatically and with minimum effort, and the private keys and certificates are safe from being read, shared, duplicated, or otherwise compromised. Whenever a certificate is used, a cryptographic operation using the private key is executed.

> *Certificates can be created and rolled out automatically and with minimum effort, and the private keys and certificates are safe from being read, shared, duplicated, or otherwise compromised.*

CodeMeter License Central streamlines the formerly circuitous process of requesting, updating, or installing signed certificates. The entire administration and certificate creation process happens in one central place, with the option of including a higher certificate authority, such as a company's own CA. This CA could act as a trust center to verify that the public key is indeed valid and assigned to the machine or device in question.



Features of CodeMeter Certificate Vault Felder highlighted in turquoise



CodeMeter Certificate Vault

Public key certificates are indispensable for authenticating the identity of individuals, organizations, or other entities, like machines or hardware devices.

Keys and certificates created in a central and secure environment are taken by the CodeMeter Certificate Vault Admin Tool or CodeMeter License Central and repackaged in an encrypted update file (WibuCmRaU) that moves them for exclusive use on a dedicated CmDongle. Updating the dongles happens in a sophisticated sequence of steps using a request (WibuCmRaC) and response file (WibuCmRaU), which makes for a far simpler, but highly secure process. It also allows the additional security features of CodeMeter to be used, like time limits for certificates, since CodeMeter has an internal and tamperproof UTC clock.

Conclusion

Public key certificates are indispensable for authenticating the identity of individuals, organizations, or other entities, like machines or hardware devices. They are proof that data is genuine and has not been tampered with. The combination of public and private keys can be used to establish a secure channel of communication, as long as the private key is safely stored away in a separate and impenetrable secure element, like a CmDongle. This also goes for the storage of certificates if they are to be trusted as standard and their authenticity not checked separately. To enable all of this, Wibu-Systems provides its powerful CodeMeter License Central as the backend system for the central management and distribution of certificates and private keys. It fulfills all the requirements for truly secure machine / device identities, facilitating the type of reliable machine communication that underlies the vision of Industry 4.0.☒

WIBU SYSTEMS

CodeMeter – the Catalyst of the IoT driven Economy

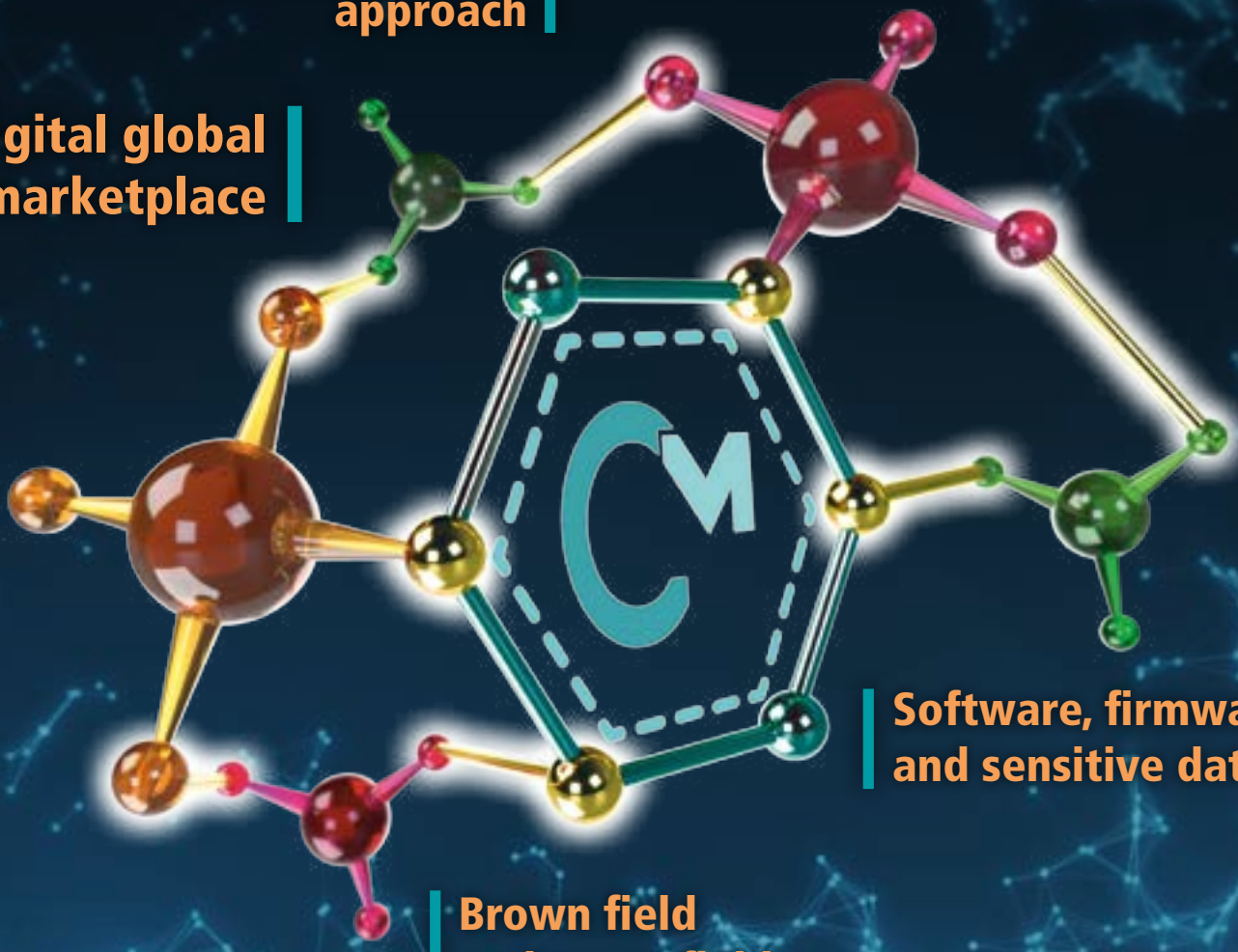
Let CodeMeter inspire you with new license-driven business models

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

From the cloud down to FPGAs

Customer centric approach

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