NEWS AND INSIGHTS FROM THE WORLD OF ID SECURITY

NOVEMBER 2023

# The VAULT

## HOW DO YOU KNOW IF IT'S REAL OR FAKE?

FEATURED ARTICLE

**CodeMeter Certificate Vault: Certified Genuine**

Wibu-Systems

ALSO IN THIS ISSUE

Silicon Trust
**Unmasking the Threat: AI and the future of Digital ID**

Mühlbauer Group
**Queuing was Yesterday**

Infineon Technologies
**Revolutionizing Security with Integrity Guard 32**

# CODEMETER *Certificate* VAULT: *Certified* Genuine

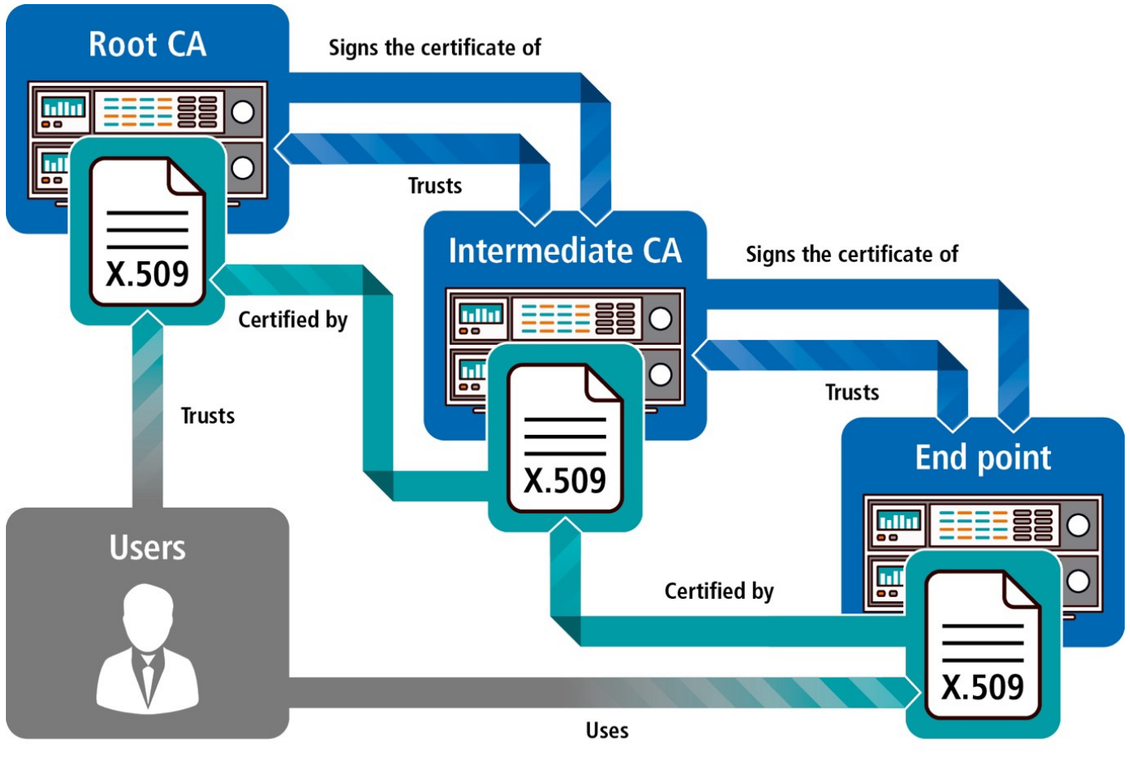
By Marco Blume, Wibu-Systems

When the police came knocking on his door in 1995, John Myatt instantly knew his game was up. One of the art world's most prolific forgers confessed on the spot to creating fake works by some of modern art's greatest masters. Braques, Giacomettis, Chagalls: Myatt faked them all, made to order for the real mastermind behind the criminal enterprise: John Drewe. Where Myatt faked the paintings, Drewe faked much more. He faked their identity.

The style, technique, even the paints themselves? All fake. The reams of papers to prove the works' provenance? Fake. The previous owners listed on them? Fake. Drewe's credentials, his claimed PhDs, his entire backstory? Fake. Not even Drewe's name was genuine. He was born John Cockett in genteel Sussex in the south of England.

## Certificates of Authenticity

Certificates of authenticity are not just a thing in the art world, in the jewelry business, or in the wine trade. In the digital world, certificates are also the crucial means to say: This person, this device, this program, or this line of communication is who they say they are.
Digital certificates operate by a simple principle: They are little pieces of data, issued with a set of cryptographic keys. That key pair is where the magic happens: One key is public, one is private. Both only go with each other and no other key. Having the key pair together shows that one is the real deal. In ages past, traders would make notches on sticks, split them down the middle and give one side to their trading partner in a deal. If, at a later point, the other partner had to authenticate themselves, they could bring their half of the tally stick and check if the notches match: An early form of asymmetric authentication and a (simplistic) explanation of how cryptographic key pairs work. The X.509 standard lays out what goes into the tally stick's modern successor, the digital certificate: Identity information, a serial number, information about the cryptographic algorithm, the public key, and the signature by a certificate authority (CA) that has vouched that the certificate goes with the public key for the person, device, or service it belongs to – its proof of provenance, in a way.




*The rollout process of X.509 certificates*

The standard practice for rolling out X.509 certificates to their destination is deceptively simple: It all begins with a root certificate authority that has the original root certificate on which all subordinate certificates depend. The root CA signs the certificates of intermediate CAs which eventually sign the certificates of end users. It is a long chain of trust, which has to be protected at all costs. As long as it holds, the end user or end point device can be sure that the certificate they are shown is genuine, that the person or machine they are communicating with is who they say they are, and so on. A simple, yet powerful way to ensure trustworthiness across our digital globe.

## No Strings Attached?

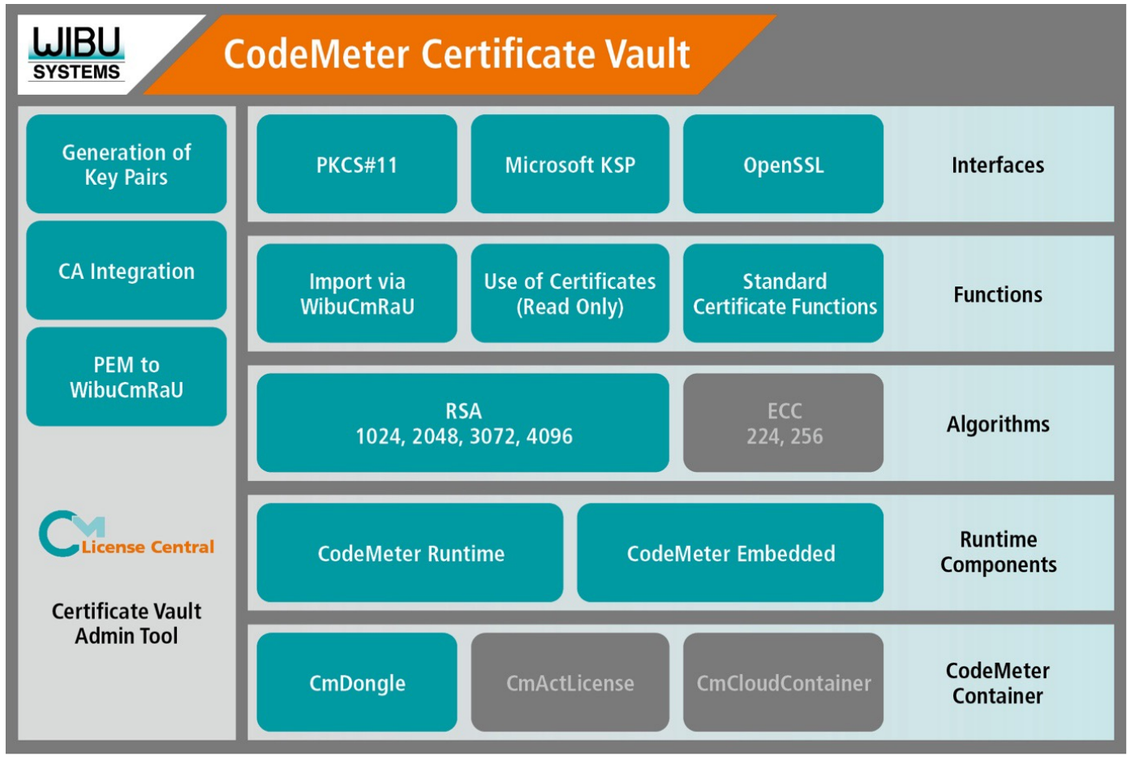
If certificates are such a great and universally accepted currency for authenticity and identity, why is the digital world not a haven of security and trustworthiness? Put simply: Digital certificates are the keys to our digital homes, vehicles, and safes. And as in the real world, even the highest walls, most complicated locks, or sturdiest safes will not guarantee security if we do not take care of our keys.
And like physical keys, keeping track of our digital certificates and keeping them secure can be a frustratingly complicated business. The private cryptographic keys that work the digital certificate wizardry must never be allowed to be lost, stolen, or otherwise tampered with. And it does not suffice to keep the digital certificates they are part of in a secure place. The private keys have to sometimes leave that safe space to be used in the cryptographic operations that make certificates do their jobs. Even if that moment is as brief as can be, a compromised system could allow an attacker to access that critical cryptographic data and get all they need to do their illicit work.
Sensible workflows, good compliance practices, and a bit of care and common sense would seem all that is needed to keep certificates secure, but that is far from true. It is not all due to human error – sophisticated hackers can find other technical means to crack even apparently safe systems – but human users often become the unwitting assistants of hackers by relying on unsafe practices or not doing their IT security homework.
Who has not shrugged off a warning message that a certificate has expired? Who among the vast masses of regular users, not trained IT professionals, understands what certificates do or how they can become problematic? As John Drewe found out when selling one of Myatt's forged Giacomettis to two art dealers: If a deal is attractive, but checking the paperwork (or, indeed, keeping your certificates up to date) is too much of a hassle, people will tell themselves that everything is alright, because it looks alright on the surface. People want to be deceived.

**MARCO BLUME** *has been with WIBU-SYSTEMS AG since 2013, as Product Manager/R&D Manager Embedded. His work covers the range of protection concerns for embedded systems and includes the development of custom concepts for manufacturers and contributions to active research ventures. He has spent his entire career with different embedded systems, including 11 years as product manager for the security of ATMs and checkout systems and previous responsibilities as embedded specialist for video systems and industrial automation..*

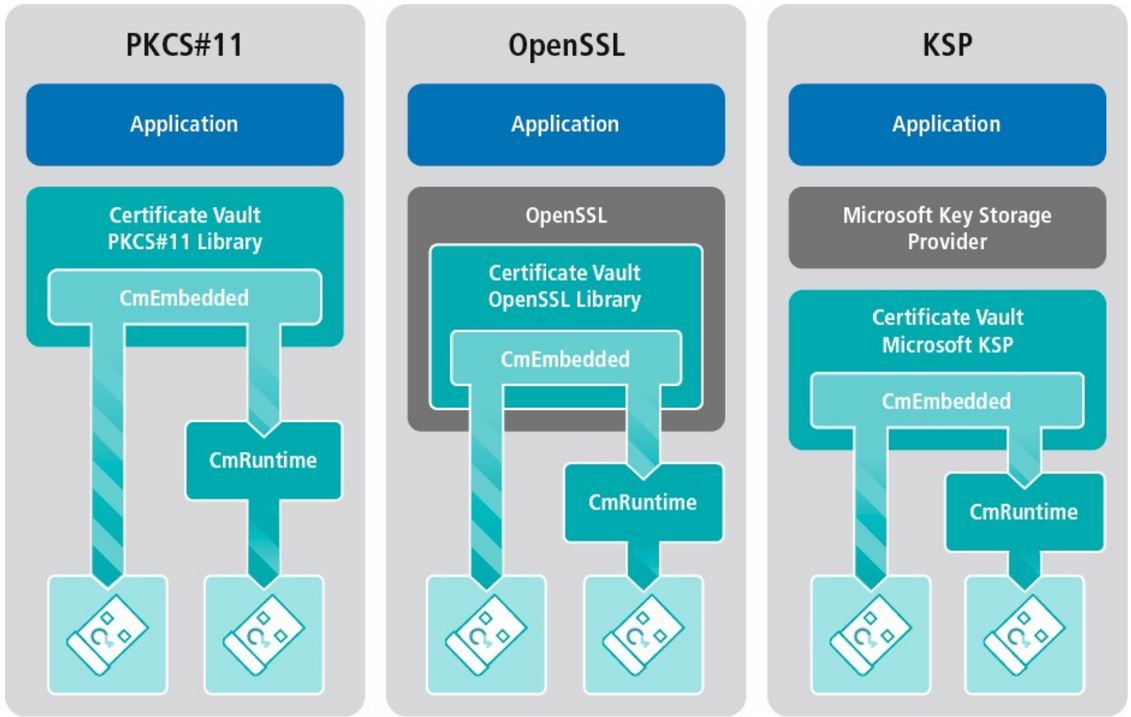
*CodeMeter Certification Vault*

## CodeMeter Certificate Vault: Removing the Weak Spots

Commercial certificate authorities or other sophisticated organizations have the means to protect their certificates with powerful hardware and software. Complex closed systems are used to store the certificates and cryptographic keys, and these normally never leave these secure enclaves as the necessary calculations and cryptographic operations can be run inside those systems, called Hardware Security Modules or HSMs. For less well-equipped organizations, let alone regular end users, this is not an option. They have to rely on less secure options to keep their certificates, or they had to until Wibu-Systems' launched CodeMeter Certificate Vault.






*CodeMeter Certificate Vault can be easily integrated into existing environments*

CodeMeter Certificate Vault essentially lets regular users work with a slimmed-down version of an HSM: Certificates can be stored in secure hardware containers, so-called CmDongles in USB stick, memory card, or ASIC form factors, that come not just with a place to keep them, but even the Common Criteria EAL5+ evaluated smart card chip to run the cryptographic operations. One common standard used for that purpose is PKCS#11, which includes cryptographic algorithms like RSA and is the basis for X.509 certificates. CodeMeter Certificate Vault comes with the necessary PKCS#11 library for key storage purposes, as it does with the OpenSSL library (for securing network protocols) and with Microsoft Key Storage Provider, the Windows-specific means to manage certificates and keys for Windows applications. In all three cases, the critical jobs happen inside the secure dongle: the certificates either never leave the dongle at all or if they do, as is the case with Microsoft KSP, the private key remains hidden, and all cryptographic operations happen on the dongle.

*Scan the QR Code to access a White Paper Executive Summary on CodeMeter Certificate Vault*

## In Practice

Whether certificates are used to identify a flesh-and-blood person or a machine in a network or to form a public key infrastructure (PKI), e.g. in email communication, CodeMeter Certificate Vault adds a new layer of security in the form of secure key storage and protected lines of communication. For human users, certificates stored on a CmDongle become more portable than ever before, not unlike the passports they resemble, which can be essential for many mobile projects or services and maintenance engineers that have to identify themselves. On the other end of the portability scale, a piece of equipment in a modern smart factory does not have to be moved around much, but it would be useless without a reliable and trustworthy certificate. In that case, a built-in CmASIC is the perfect, physically hidden-away container for that certificate.
In order to get a certificate onto the device where one needs it, the standard process works as it should, only with added CodeMeter security. For a new certificate, a key pair is created, but now by the CodeMeter chip and within the secure container. The key pair is used for the new certificate, which can now contain other identifying data about the container for added authenticity. The certificate is sent to a CA for signing and returned back into the container. During all of this, the private key never has to leave its safe home. (Figure.1)
One of the most critical moments in a certificate's life happens when an update comes around, as many Internet users will know from encountering websites with expired certificates. CodeMeter Certificate Vault again benefits from Wibu-Systems' experience with secure updating mechanisms, and the swapping of CSR and signed certificates again happens in a safe environment with no way for a would-be attacker to intercept anything of value in between: The private key stays inside the secure CodeMeter chip. (Figure. 2)


*Figure. 1*

*Figure. 2*


The secure updating process invented for CodeMeter licensing, swapping a special *.RaC update request and an encrypted *.RaU update file, works as well as an optional way to distribute new or updated certificates securely from the CA to their destination. (Figure. 3)
With CodeMeter Certificate Vault's on-board OpenSSL and PKCS#11 interfaces, all of these processes can be automated and completely taken out of the end user's hands for added reliability and easy supervision.

## Conclusion: No excuses for poor practice

In a nutshell, CodeMeter Certificate Vault is the means to store and manage certificates in secure containers. But it is far more than that: As part of the CodeMeter ecosystem, CodeMeter Certificate Vault feels familiar to users of Wibu-Systems' powerful protection and licensing solution, working with hardware that is as smart as it is tough and offering a similar user experience built around comfort and flexibility coupled with powerful customization and integration capabilities.
CodeMeter Certificate Vault supercharges the CodeMeter universe with a solution for digital certificates that completes the IT security and protection line-up from encryption, protection, and licensing to authentication and secure communication. By removing many, if not most of the obstacles and problems caused by technology or human habit, it leaves no excuses for poor-practice certificate usage. The digital world will be more secure for it.

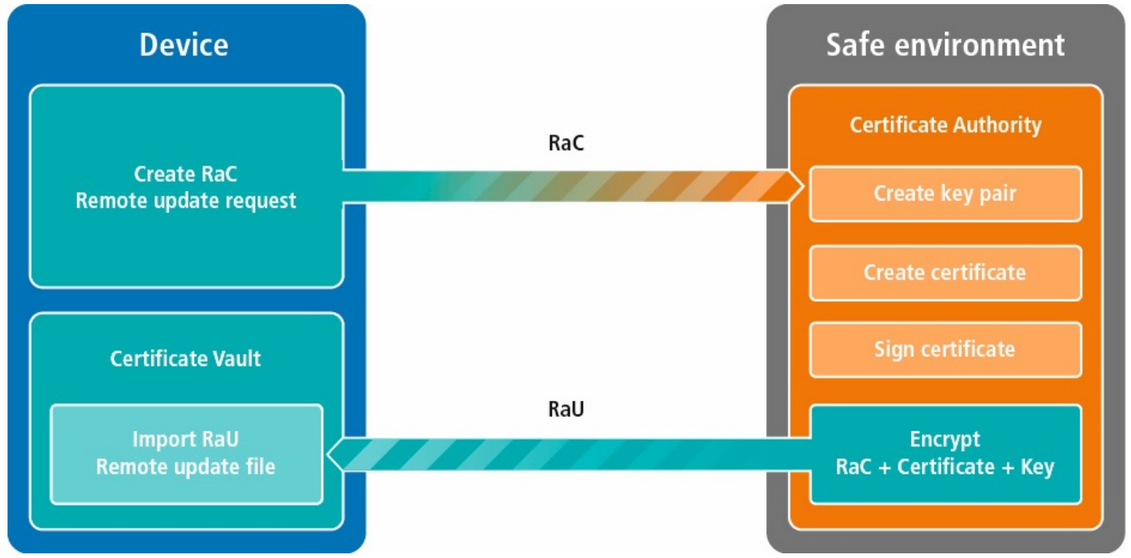



*Figure. 3*

## Postscript

*In 1999, John Myatt, art forger extraordinaire, was released from prison. He never stopped painting in the style of the great modern masters. Today, his works are sought after by collectors worldwide, not as the genuine article, but as – "genuine fakes".*

WIBU SYSTEMS

# CodeMeter – A Symphony of Software Monetization Tools

- Compose your original code
- Orchestrate your license strategy
- Fine tune your IP protection
- Distribute your work of art

Sounds easy, right?
And it is with CodeMeter

CodeMeter Cloud
CodeMeter Certificate Vault
CodeMeter Embedded
CodeMeter Dongle
CodeMeter LC
CodeMeter


Start now and request your CodeMeter SDK
wibu.com/sdk

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

SECURITY
LICENSING
PERFECTION IN PROTECTION