White Paper Executive Summary

CodeMeter Certificate Vault

Certificate Management with CodeMeter Comfort and Security

CodeMeter Certificate Vault uses CodeMeter technology to provide a secure means to store X.509 certificates on CodeMeter hardware and make them available via standard interfaces.

Certificates are used to prove authenticity and identify users or devices on the Internet, in emails, machine-to-machine communication, or elsewhere. The X.509 standard has become quasi-ubiquitous for Public Key Infrastructures (PKI). Each certificate works with an asymmetric key pair: The public key is part of the certificate, while the private key is kept separate. But this theoretically safe system has weak points: Private keys should stay secure, but can be attacked when outside their place of storage e.g. for cryptographic operations.

Common solutions include hardware secure modules (HSM) as closed enclaves. Such sophisticated hardware is not available for many users, who use secure elements like TPM modules to store and access private keys. CodeMeter Certificate Vault was designed for this, with interfaces for integrating in existing environments and the ability to store certificates on secure CodeMeter hardware like dongles or ASICs. Once there, no sensitive information ever leaves its safe haven, removing the essential flaw of the process.

Several routes are available for integrating CodeMeter Certificate Vault, starting with the self-contained CodeMeter Certificate Vault library, a CmDongle, certificates and keys. Alternatively, separate versions for PKCS#11, OpenSSL, and KSP add CodeMeter Certificate Vault's unique ability to handle key storage and cryptographic operations inside a dongle or ASIC to these common standards.

PKCS#11 handles cryptographic objects like keys or X.509 certificates, while keeping applications and crypto operations separate. OpenSSL offers additional cryptographic skills, with encrypted communication and even CA capabilities, but lacks key and certificate management. Again, the CodeMeter Certificate Vault libraries fill that gap with key and certificate storage inside the secure environs of a dongle. Microsoft Key Storage Provider (KSP) can also be used with CodeMeter Certificate Vault to keep sensitive cryptographic objects secure on a dongle.

Several routes can be used to roll out and manage certificates with CodeMeter Certificate Vault. The standard process begins with a key pair created by the CodeMeter hardware's security chip and a certificate signing request sent to a CA, while private keys remain secure inside the hardware. The process can be automated via CodeMeter Certificate Vault's OpenSSL and PKCS#11interfaces.

Alternatively, CAs can create certificates and key pairs and feed them into CodeMeter Certificate Vault via CodeMeter's secure remote update process. The transit is cryptographically secure and can be automated for added ease.

Download the complete white paper

2026-03-03

sales@wibu.com | www.wibu.com

WIBU SYSTEMS