

ホワイトペーパー エグゼクティブサマリー

CodeMeter Certificate Vault

CodeMeter による証明書管理：快適さとセキュリティ

CodeMeter Certificate Vault は、CodeMeter の テクノロジーを使用し、CodeMeter 専用ハードウェア上へ X.509 証明書をセキュアに保存、および標準インターフェイス経由での X.509 証明書の利用を可能にします。

証明書は、個人またはデバイスの真正性を、インターネット、電子メール、マシン間通信などで証明·識別するために使用されます。X.509 形式は、PKI（Public Key Infrastructure、公開鍵基盤）の標準規格です。各証明書は、公開鍵と秘密鍵で構成される非対称鍵のペアで動作します。公開鍵は証明書の一部である一方、秘密鍵は別の場所で保管されます。このように、理論上安全に見えるこのシステムですが、実は欠点があります。それは、セキュアであるべき秘密鍵が、暗号化操作などのために保管場所の外に出た際に攻撃を受けるリスクがあるということです。

一般的な解決策としては、閉じられたエンクレーブとしての HSM (Hardware Security Module) が挙げられます。しかし、秘密鍵の保存とアクセスに TPM（Trusted Platform Module）のようなセキュアな要素を使用する多くのユーザーは、このような洗練されたハードウェアを利用することができません。そこで考案されたのが、CodeMeter Certificate Vault です。既存の環境に統合するためのインターフェイスと、セキュアな CodeMeter 専用ハードウェア（例：ドングル、ASIC）に証明書を保存する機能を備えています。一旦この CodeMeter Certificate Vault に秘密鍵が保管されれば、機密情報が漏れることはなく、 前述した X.509 形式の欠点を補うことができます。

CodeMeter Certificate Vault の統合には、専用ライブラリ、専用ハードウェアの CmDongle、証明書や鍵など様々な手段があります。また、PKCS#11、OpenSSL、および KSP 用の別バージョンでは、CodeMeter Certificate Vault のユニークな機能（ドングルまたは ASIC 内での鍵の保管と暗号化操作）を追加することができます。

PKCS#11 は、鍵や X.509 証明書のような暗号化オブジェクトを扱いながらも、アプリケーションと暗号化操作を分離して管理します。一方 OpenSSL では、暗号化通信や CA（CertificateAuthority、認証局）機能など、追加の暗号化技術が提供されますが、鍵と証明書の管理はできません。繰り返しにはなりますが、CodeMeter CertificateVault の専用ライブラリでは、ドングルのセキュアな環境に鍵と証明書を保管することができるため、そのギャップを埋めることが可能です。同様に Microsoft Key Storage Provider KSP）も、CodeMeter Certificate Vault と共に使用することで、機密性の高い暗号化オブジェクトをドングル上でセキュアに保管することができます。

さらに、CodeMeter Certificate Vault を使用した証明書の展開·管理にもいくつか方法があります。標準的なプロセスでは、CodeMeter ハードウェアのセキュリティチップで作成された公開鍵と秘密鍵のペアと、CA に送信された証明書署名要求（CSR）から始まる一方、秘密鍵は、ハードウェア内でセキュアに保管されます。このプロセスは、CodeMeterCertificate Vault の OpenSSL および PKCS#11 インターフェイスを介して自動化することが可能です。

また、CA にて証明書と鍵のペアを作成し、CodeMeter のセキュアなリモート更新プロセスを介して CodeMeter CertificateVault に供給することもできます。この処理は、暗号化面で安全であるだけでなく、自動化も容易です。

ホワイトペーパーをダウンロード

sales-jp@wibu.com | www.wibu.jp

WIBU SYSTEMS

2026-03-03