

Zusammenfassung des White Papers

CodeMeter Certificate Vault

Zertifikate dank CodeMeter komfortabel und sicher verwalten

CodeMeter Certificate Vault basiert auf CodeMeter: In der CodeMeter-Hardware werden X.509-Zertifikate sicher gespeichert und stehen über Standardschnittstellen zur Verfügung.

Zertifikate dienen zur Authentizität und zur Identifizierung von Benutzern oder Geräten, wie im Internet, für E-Mails oder bei der Kommunikation von Maschine zu Maschine. Der X.509-Standard wird für Public-Key-Infrastrukturen (PKI) sehr häufig eingesetzt. Jedes Zertifikat arbeitet mit einem asymmetrischen Schlüsselpaar: Der Public Key ist Teil des Zertifikats, während der Private Key geheim gehalten wird. Die Schwachstelle dieses sicheren Systems ist, dass die Private Keys sicher bleiben sollen, jedoch angegriffen werden können, wenn sie außerhalb ihres Speicherortes, z. B. für kryptografische Operationen, verwendet werden.

Zu den gängigen Lösungen gehören sichere Hardwaremodule (HSM) als geschlossene Enklaven. Diese technisch ausgereifte Hardware ist für viele Anwender nicht verfügbar, die Secure Elements wie TPM-Module verwenden, um Private Keys zu speichern und darauf zuzugreifen. CodeMeter Certificate Vault kann in bestehende Umgebungen integriert werden und speichert Zertifikate in CmDongles oder ASICs. Die dort gespeicherten Zertifikate bleiben als sensiblen Informationen immer in diesem sicheren Ort.

CodeMeter Certificate Vault kann unterschiedlich integriert werden: mit der in sich geschlossenen Library, einem CmDongle, Zertifikaten und Schlüsseln. Alternativ erlauben separate Versionen für PKCS#11, OpenSSL und KSP die Funktionen von CodeMeter Certificate Vault, die Schlüsselspeicherung und kryptografische Operationen innerhalb eines CmDongles oder ASICs zu diesen gängigen Standards, zu verarbeiten.

PKCS#11 arbeitet mit kryptografischen Objekten wie Schlüssel oder X.509-Zertifikate und trennt die Anwendungen und kryptografische Operationen. OpenSSL bietet kryptografische Fähigkeiten, mit verschlüsselter Kommunikation und sogar Zertifizierungsstellen-Fähigkeiten, aber es fehlt die Verwaltung von Schlüsseln und Zertifikaten. Die Lösung hierfür sind die CodeMeter Certificate Vault-Libraries, die Schlüssel und Zertifikate im sicheren CmDongle speichern. Microsoft Key Storage Provider (KSP) kann auch mit dieser Technologie verwendet werden, um sensible kryptographische Objekte in einem CmDongle zu speichern.

Das Ausrollen und Verwalten von Zertifikaten mit CodeMeter Certificate Vault beginnt mit einem Schlüsselpaar, das vom Sicherheitschip der CodeMeter-Hardware erstellt wird, und einer Zertifikatsignierungsanforderung, die an eine Zertifizierungsstelle gesendet wird, während der Private Key sicher in der Hardware bleiben. Der Prozess kann über die OpenSSL- und PKCS#11-Schnittstellen von CodeMeter Certificate Vault automatisiert werden.

Alternativ können Zertifizierungsstellen Zertifikate und Schlüsselpaare erstellen und sie über den sicheren Remote-Update-Prozess von CodeMeter in die CodeMeter-Zertifikatsvewaltung einspeisen. Die Übertragung ist kryptographisch sicher und kann automatisiert werden.

Laden Sie sich das White Paper herunter

sales@wibu.com | www.wibu.com

WIBU SYSTEMS

2026-02-19